Handbuch zu Arcserve® Unified Data Protection-Lösungen

Version 8.x

arcserve®

Online-Hilfe zu Arcserve® Unified Data Protection-Lösungen

Version 8.x

Liste der Inhalte wird im linken Fensterbereich angezeigt. Wenn Sie alle Themen anzeigen möchten, klicken Sie auf das oben verfügbare TOC -Symbol.

arcserve®

Rechtliche Hinweise

Diese Dokumentation, die eingebettete Hilfssysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von Arcserve jederzeit geändert oder zurückgenommen werden. Diese Dokumentation stellt geistiges Eigentum von Arcserve dar und darf ohne vorherige schriftliche Genehmigung von Arcserve weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden.

Der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt (e) verfügt, ist dazu berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken oder anderweitig verfügbar zu machen, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige rechtliche Hinweise von Arcserve enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber Arcserve schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an Arcserve zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT ARCSERVE DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ARCSERVE GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN ARCSERVE ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Der Gebrauch jedes einzelnen der in der Dokumentation genannten Softwareprodukte unterliegt dem geltenden Lizenzabkommen, und dieses Lizenzabkommen wird durch die Bedingungen dieses Hinweises in keiner Weise geändert.

Der Hersteller dieser Dokumentation ist Arcserve.

Es gelten "Eingeschränkte Rechte". Die Verwendung, Vervielfältigung oder Veröffentlichung durch die Regierung der Vereinigten Staaten unterliegt den jeweils in den FAR-Abschnitten 12.212, 52.227-14 und 52.227-19(c)(1) – (2) sowie dem DFARS-Abschnitt 252.227-7014(b)(3) oder in ihren Nachfolgeabschnitten festgelegten Einschränkungen.

© 2014–2021 Arcserve und seine Schwestergesellschaften und Tochtergesellschaften. Alle Rechte vorbehalten. Drittanbieter-Marken oder Copyrights sind Eigentum der entsprechenden Rechtsinhaber.

Arcserve-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Arcserve-Produkte:

- Arcserve® Unified Data Protection
- Arcserve® Unified Data Protection Agent für Windows
- Arcserve® Unified Data Protection Agent für Linux
- Arcserve® Backup
- Arcserve® Continuous Availability

Kontakt zum Arcserve-Support

Das Arcserve-Support-Team stellt umfangreiche Ressourcen zur Lösung von technischen Problemen zur Verfügung und bietet einfachen Zugriff auf wichtige Produktinformationen.

Support kontaktieren

Der Arcserve-Support ermöglicht Ihnen Folgendes:

- Sie können direkt auf dieselbe Informationsbibliothek zugreifen, die auch intern von Arcserve-Support-Fachleuten verwendet wird. Diese Website bietet Zugriff auf unsere Knowledge Base-Dokumente (KB-Dokumente). Hier können Sie schnell und einfach produktbezogene KB-Artikel suchen und aufrufen, die praxiserprobte Lösungen für viele häufig auftretende Probleme enthalten.
- Sie können unseren Live-Chat-Link verwenden, um sofort ein Echtzeitgespräch mit dem Team für Arcserve-Support zu starten. Über den Live-Chat können Bedenken und Fragen bei noch bestehendem Zugriff auf das Produkt umgehend behandelt werden.
- Sie können sich an der globalen Benutzer-Community von Arcserve beteiligen, um Fragen zu stellen und zu beantworten, Tipps und Tricks weiterzugeben, Best Practices zu diskutieren und sich mit Gleichgesinnten zu unterhalten.
- Sie können ein Support-Ticket öffnen. Wenn Sie ein Online-Support-Ticket öffnen, wird Sie ein Experte aus dem betroffenen Produktbereich zurückrufen.
- Sie können auf weitere hilfreiche Ressourcen für Ihr Arcserve-Produkt zugreifen.

Inhalt

Online-Hilfe zu Arcserve® Unified Data Protection-Lösungen 2

Kapitel 1: Funktionen und Verbesserungen 29

Neue Funktionen 30

Funktionsverbesserungen 32

Linux Agent-Verbesserungen 33

Datenbank- und Plattform-Support 34

Sicherheits- und Drittanbieterverbesserungen 35

Arcserve-Appliance-Verbesserungen 36

Nicht mehr unterstützt 37

Kapitel 2: Informationen zu Arcserve UDP 39

Einführung 40

Funktionsweise von Arcserve UDP 42

Instant Virtual Machine (IVM) im Vergleich zu Virtual Standby (VSB)-Rechner 44

Benutzersicherheit 47

Rollen für Arcserve UDP-Dienste 48

Benutzerrechte für Arcserve UDP-Funktionen 49

Kapitel 3: Installieren von Arcserve UDP 59

Installieren von Arcserve UDP 60

Überprüfen der Voraussetzungen und Hinweise 61

Bestimmen der Installationsart 62

Installieren von Arcserve Unified Data Protection mit dem Setup-Assistenten 63

Installieren von Arcserve Unified Data Protection über die Befehlszeile 68

Arcserve UDP mit dem einheitlichen Installationsprogramm installieren 73

Überprüfen der Installation 75

Von Arcserve UDP verwendete Kommunikationsports 76

Auswirkungen des Installationsprozesses auf das Betriebssystem 97

Installieren von Aktualisierungen für Arcserve UDP 103

Überprüfen der Hinweise für die Installation von Aktualisierungen 104

Festlegen der Voreinstellungen für die Aktualisierungen 105

Überprüfen und Installieren der Aktualisierungen 111

Aktualisieren von Agenten auf Remote-Knoten mit Gateway 113

Aktualisieren des RPS auf Remote-Servern mit Gateway 114

(Optional) Automatisches Installieren von Aktualisierungen für Arcserve UDP 115

Überprüfen, ob die Aktualisierungen erfolgreich installiert wurden 116

So deinstallieren Sie Arcserve UDP 117
Standardmäßige Deinstallation 118
Automatische Deinstallation 119
Entfernen von Komponenten, die nicht durch das Deinstallationsprogramm entfernt wurden 121
Kapitel 4: Aktualisieren auf Arcserve UDP Version 8.0 123
Unterstützte Versionen für Upgrade 124
Upgradesequenz auf der Arcserve Appliance 125
Die Arcserve Appliance aktualisieren, die als Arcserve UDP Console und RPS betrieben wird 126
Die Arcserve Appliance aktualisieren, die nur als Arcserve UDP RPS betrieben wird 127
Upgradeschritte bei Verwendung von mindestens zwei Arcserve Appliances in der Umgebung 128
Den Arcserve Linux Agent auf der Arcserve UDP Appliance aktualisieren 129
Arcserve Backup auf der Arcserve Appliance aktualisieren 130
Unterstützungsrichtlinie zur Abwärtskompatibilität 131
Unterstützungsrichtlinie zur Abwärtskompatibilität für Arcserve UDP Version 8.0 131
Unterstützungsrichtlinie zur Abwärtskompatibilität für Arcserve UDP Version 7.x 134
Support-Richtlinie zur Rückwärtskompatibilität für Arcserve UDP Version 6.5 Update 4 137
Unterstützung der Abwärtskompatibilität für Linux-Sicherungsserver 140
Upgradesequenz für UDP-Konsole, RPS und Agent 141
So aktualisieren Sie auf Arcserve UDP 8.0 von einer früheren Version 142
So aktualisieren Sie auf Arcserve UDP 8.0 mit einem Installationsprogramm 145
So aktualisieren Sie auf Arcserve UDP 8.0 oder Arcserve Backup 18.0, um das Kopieren auf Band zu aktivieren 149
So migrieren Sie die Arcserve UDP-Konsole von einem Server auf einen anderen 152
So aktualisieren Sie das Gateway auf dieselbe Version wie die zugehörige registrierte Konsole 153
So migrieren Sie die Arcserve UDP-Konsole 153
Kapitel 5: Erkennen und Konfigurieren von Arcserve UDP 157
Anmeldung bei der Arcserve UDP-Konsole mit der Multi-Faktor-Authentifizierung 157
Überprüfen der Voraussetzungen 157
So melden Sie sich mit MFA bei der Arcserve UDP-Konsole an 158
Arcserve Unified Data Protection Benutzeroberfläche 163
Navigieren in Arcserve UDP 164
Registerkarten 166
Dialogfeld "Job-Monitor" 182
So konfigurieren Sie Arcserve UDP 183

Konfigurieren des Server-Kommunikationsprotokolls 184
Konfigurieren der Datenbank 186
Konfigurieren der Arcserve Backup-Datensynchronisation 191
SRM konfigurieren 193
Knoten-Discovery-Konfiguration 195
Konfigurieren von E-Mails und Alerts 197
Proxy-Einstellungen konfigurieren 199
Aktualisieren der Konfiguration 201
Konfigurieren des Administratorkontos 203
Einstellungen der Remote-Bereitstellung 204
Zuordnen des Plans zum Benutzerkonto 205
Benutzerverwaltung 207
Konfigurieren der Zeitüberschreitungsdauer der Konsole 208
So migrieren Sie r16.5-Wiederherstellungspunkte zu Arcserve UDP 209
Erstellen eines Datenspeichers zur Replizierung von Daten von einem Arcserve r16.5-Wiederherstellungspunkt 210
Replizieren von Arcserve r16.5-Daten in den UDP-Datenspeicher 211
Einrichten des Konfigurationsassistenten 212
Kapitel 6: Wichtige Funktionen von Arcserve UDP 215
Informationen zur Nutanix Funktion in Arcserve UDP 216
Informationen zur OneDrive Funktion in Arcserve UDP 217
Grundlegendes zur Exchange Online-Funktion in Arcserve UDP 218
Grundlegendes zur Hardware-Snapshot-Funktion in UDP 219
Grundlegendes zur Cloud-Funktion in UDP 220
Grundlegendes zur UNC/NFS-Pfad-Funktion in UDP 222
Grundlegendes zur SharePoint Online-Funktion in UDP 223
Voraussetzungen 223
Kapitel 7: Verwenden der rollenbasierten Arcserve UDP-Verwaltung 225
Zugriff auf die Benutzerverwaltungskonsole 226
Die Arcserve UDP-Benutzerverwaltungskonsole starten 226
Multi-Faktor-Authentifizierung konfigurieren 227
Hinzufügen von Benutzern, Löschen von Benutzern und Ändern des Kennworts 234
Konfigurieren der Benutzerverwaltung 235
Vordefinierte Rollen 236
Zuweisen einer vordefinierten Rolle 240
Anzeigen und Abbrechen einer Rolle 241

Hinzufügen einer neuen Rolle ... 242
Suchen von Benutzern und Rollen ... 244
Integrieren von Arcserve UDP in Active Directory ... 245
So integrieren Sie Arcserve UDP 8.0 in Active Directory unter Verwendung von Windows-Gruppen ... 246
So integrieren Sie Arcserve UDP 8.0 in Active Directory unter Verwendung von Active Directory-Gruppen ... 250
Zugreifen auf Arcserve UDP mithilfe der integrierten Windows-Authentifizierung ... 257
Fehlerbehebung für die integrierte Windows-Authentifizierung (IWA) ... 258
Die Arcserve UDP-Konsole unterstützt IWA nicht, wenn für die Verbindung zur Konsolendatenbank der Windows-Authentifizierungsmodus verwendet wird. ... 260
Fehlerbehebung ... 262
Kapitel 8: Hinzufügen und Verwalten von Quellknoten ... 263
Hinzufügen von Knoten zur Konsole ... 264
Überprüfen der Voraussetzungen ... 265
Hinzufügen von Knoten ... 266
Erkennen von Knoten ... 272
Importieren von Knoten ... 275
So verwalten Sie Knoten ... 283
Überprüfen der Voraussetzungen ... 284
Aktualisieren der Hypervisor-Informationen ... 285
Angeben des Hypervisor ... 286
Aktualisieren der VM-Informationen ... 288
Aktualisieren von Knoten ... 289
Exportieren von Knoten ... 293
Anhalten von Knoten ... 294
Fortsetzen von Knoten ... 295
Synchronisieren von Daten ... 296
Löschen von Knoten aus der Konsole ... 297
Bereitstellen des Agent auf Knoten ... 298
Durchführen von Preflight-Checks für Ihre Sicherungsjobs ... 299
Hinzufügen und Verwalten eines UNC/NFS-Pfades ... 317
Hinzufügen eines UNC/NFS-Pfades ... 318
Aktualisieren eines UNC/NFS-Pfades ... 321
Löschen eines UNC/NFS-Pfades ... 322
Hinzufügen und Verwalten von Knotengruppen ... 323
Überprüfen der Voraussetzungen ... 325
Hinzufügen von Knotengruppen ... 326

Ändern von Knotengruppen ... 327
Löschen von Knotengruppen ... 328
Verwalten von Knoten für die Cloud ... 329
Herunterladen von Wiederherstellungspunkten aus der Cloud ... 330
Hochladen von Wiederherstellungspunkten in die Cloud ... 332
Kopieren von Wiederherstellungspunkten auf einen lokalen Datenträger oder eine Netzwerkfreigabe ... 335
Hinzufügen eines Speicher-Arrays ... 338
Hinzufügen eines NetApp-Speicher-Arrays ... 340
Details von HPE RMC hinzufügen, das ein HPE 3PAR Storeserv Speicher-Array verwaltet ... 346
Hinzufügen eines Nimble-Speicher-Arrays ... 348
So fügen Sie einen Standort hinzu und verwalten ihn ... 350
Angeben des Standortnamens ... 352
Anweisung zur Freigabe der Registrierung ... 353
Überprüfen und Hinzufügen des Standorts ... 354
Ändern der Konsolen-URL ... 355
Ändern des Standorts ... 356
Löschen eines Standorts ... 357
Einrichten eines Proxy-Servers für das Gateway ... 358
So verwalten Sie Exchange Online-Knoten ... 361
Hinzufügen eines Exchange Online-Knotens ... 362
Aktualisieren eines Exchange Online-Knotens ... 364
Löschen eines Exchange Online-Knotens ... 365
Unterstützung für Postfach für öffentliche Ordner für Exchange Online-Schutz ... 366
So verwalten Sie SharePoint Online-Knoten ... 368
Hinzufügen eines SharePoint Online-Knotens ... 369
Aktualisieren eines SharePoint Online-Knotens ... 370
Löschen eines SharePoint Online-Knotens ... 371
So verwalten Sie einen OneDrive-Knoten ... 371
Hinzufügen eines OneDrive-Knotens ... 372
Löschen eines OneDrive Online-Knotens ... 372
So verwalten Sie Oracle-Datenbankgruppen-Knoten ... 372
Aktualisieren des Oracle-Datenbankknotens ... 372
Exportieren von Knoten ... 373
Oracle-Datenbankknoten sichern ... 374
Abbrechen des Sicherungsjobs von Oracle-Datenbankknoten ... 375
Löschen von Oracle-Datenbankknoten ... 376

Kapitel 9: Hinzufügen und Verwalten von Zielen 377

So fügen Sie ein Ziel hinzu 378

So fügen Sie ein Ziel hinzu 379

Hinzufügen von Arcserve Backup-Servern 393

Remote-Konsole hinzufügen 395

Hinzufügen eines Cloud-Kontos 397

Hinzufügen eines Arcserve-Cloud-Kontos 434

Verwalten von Datenspeichern 437

Überprüfen der Voraussetzungen 438

Ändern von Datenspeichern 439

Starten von Datenspeichern 450

Anhalten von Datenspeichern 451

Löschen eines Datenspeichers aus der Konsole 453

Löschen von Knotendaten aus einem Datenspeicher 454

Überwachen der Datenspeicher-Speicherplatzkapazität 456

Durchsuchen von Wiederherstellungspunkten in einem Datenspeicher 464

FQDN-Support für Datenspeicher 466

Ausführen eines manuellen oder On-Demand-Zusammenführungsjobs 467

Ändern von Schwellenwert gleichzeitig aktiver Knoten für manuelle Sicherung 469

Fehlerbehebung: So verwenden Sie einen Datenspeicher, wenn der Sicherungszielordner voll ist 470

Verwalten eines Recovery Point Server 473

Überprüfen der Voraussetzungen 474

Aktualisieren eines Recovery Point Server 475

Löschen eines Recovery Point Server aus der Konsole 476

Importieren von Datenspeichern 477

Installieren/Aktualisieren von Recovery Point-Servern 479

So verwalten Sie Arcserve Backup-Server 480

Aktualisieren von Arcserve Backup-Servern 481

Löschen von Arcserve Backup-Servern 482

So verwalten Sie freigegebene Ordner 483

Freigegebenen Ordner ändern 484

Freigegebenen Ordner löschen 485

Eine Remotekonsole verwalten 486

Ändern einer Remote-Konsole 487

Löschen einer Remote-Konsole 488

Verbindung zur Remote-Konsole testen 489

Kapitel 10: Erstellen von Plänen zum Schützen von Daten 491

Funktionsweise von Plan und Tasks 492

Erstellen eines Sicherungsplans für Windows 496

Überprüfen der Voraussetzungen und Hinweise 497

Erstellen eines Sicherungsplans mit einem Sicherungstask 503

(Optional) Ausführen einer manuellen Sicherung 527

Überprüfen der Sicherung 529

So erstellen Sie einen Nutanix Sicherungsplan 530

So erstellen Sie einen virtuellen Standby für Nutanix AHV 531

Erstellen einer Instant VM auf Nutanix AHV 531

Erstellen eines Assured Recovery-Plans zum Schützen von Nutanix AHV für Linux-Knoten 531

So führen Sie eine Sicherung des Cluster Shared Volume durch 531

Ändern der Agentenrechnereinstellungen für die Sicherung des CSV-Volume 533

So führen Sie die Sicherung von Volumes ohne Laufwerksbuchstaben aus 534

Überprüfen der Voraussetzungen 535

Laden des Volume ohne Laufwerksbuchstaben in NTFS-Ordner 535

Angeben des Volume ohne Laufwerksbuchstaben in der Registrierung 536

So führen Sie eine Sicherung des ausgewählten Volume durch 537

Erstellen eines Sicherungsplans für Linux 539

Überprüfen der Voraussetzungen und Hinweise 540

Erstellen eines Sicherungsplans 541

(Optional) Ausführen einer manuellen Sicherung 564

Überprüfen der Sicherung 566

Fehlerbehebung 567

Erstellen eines Sicherungsplans für hostbasierte virtuelle Rechner 569

Überprüfen der Voraussetzungen und Hinweise 571

Erstellen eines hostbasierten Sicherungsplans 577

(Optional) Ausführen einer manuellen Sicherung 618

Überprüfen des Plans 621

Erstellen eines Plans für ein Virtual Standby in AWS EC2 622

Überprüfen der Voraussetzungen und Hinweise 623

Erstellen eines Plans mit einem Sicherungstask 631

Hinzufügen eines "Virtual Standby auf EC2-Tasks" zum Plan 649

(Optional) Manuelles Ausführen eines "Virtual Standby auf EC2"-Tasks 656

Unterbrechen und Wiederaufnehmen eines Virtual Standby-Jobs 657

Überprüfen des Plans 659

Beenden von EC2-Ressourcen 659
Erstellen eines Virtual Standby in einem Microsoft Azure Plan 661
Überprüfen der Voraussetzungen und Hinweise 662
Erstellen eines Plans mit einem Sicherungstask 663
Hinzufügen eines Virtual Standby-Tasks zum Plan 664
(Optional) Manuelles Ausführen des Virtual Standby-Jobs 672
Aussetzen und Wiederaufnehmen von Heartbeat-Signalen 673
Unterbrechen und Wiederaufnehmen eines Virtual Standby-Jobs 675
Überprüfen des Plans 677
Erstellen eines Virtual Standby-Plans 678
Überprüfen der Voraussetzungen und Hinweise 679
Erstellen eines Plans mit einem Sicherungstask 681
Hinzufügen eines Virtual Standby-Tasks zum Plan 699
(Optional) Manuelles Ausführen des Virtual Standby-Jobs 713
Aussetzen und Wiederaufnehmen von Heartbeat-Signalen 714
Unterbrechen und Wiederaufnehmen eines Virtual Standby-Jobs 716
Überprüfen des Plans 718
Erstellen eines Assured Recovery-Plans 719
Überprüfen der Voraussetzungen und Hinweise 720
Hinzufügen eines Assured Recovery-Tasks zum Plan 722
(Optional) Manuelles Ausführen von Assured Recovery-Testjobs 736
Erstellen eines Sicherungsplans für UNC/NFS-Pfade 739
Überprüfen der Voraussetzungen und Hinweise 740
Erstellen einer Dateifreigabe 740
Erstellen eines Sicherungsplans mit einem UNC/NFS-Pfad-Task 745
(Optional) Ausführen einer manuellen Sicherung 768
Andere Aufgaben im UNC/NFS-Plan 770
Überprüfen der Sicherung 771
Schützen von Virtual Standby-Rechnern 772
Überprüfen der Voraussetzungen und Hinweise 773
Einschalten von Virtual Standby-Rechnern 774
Schützen von Virtual Standby-Rechnern nach dem Einschalten 781
Überprüfen des Schutzes von Virtual Standby-Rechnern 783
Schützen von Instant VMs 784
Überprüfen der Voraussetzungen und Hinweise 785
Einschalten von Instant VMs aus Wiederherstellungspunkten 786

Schützen einer eingeschalteten Instant VM ... 787
Überprüfen des Schutzes von Instant VMs ... 788
Replizieren von Daten zwischen Datenspeichern, die von einer UDP-Konsole verwaltet werden ... 789
Überprüfen der Voraussetzungen und Hinweise ... 790
Erstellen eines Sicherungstasks ... 791
Hinzufügen eines Replikationstasks zum Plan ... 792
(Optional) Ausführen einer manuellen Replikation ... 795
Überprüfen des Plans ... 796
Replizieren von Daten zwischen Datenspeichern, die von unterschiedlichen UDP-Konsolen verwaltet werden ... 797
Überprüfen der Voraussetzungen ... 800
Erstellen eines Benutzerkontos für die Quellenkonsole ... 801
Erstellen eines Plans zur Definition des Zieldatenspeichers ... 802
Zuordnen des Plans zum Benutzerkonto ... 805
Senden des Plans und der Benutzerkonto-Details an den Quellenadministrator ... 807
Erhalt des Plans und der Benutzerkonto-Details vom Zieladministrator ... 808
Erstellen eines Replikationsplans zum Senden von Daten an die Zielkonsole ... 809
Überprüfen der Datenreplikation ... 814
So führen Sie eine Offline-Datenreplikation mithilfe von RPS Jumpstart aus ... 815
Überprüfen der Voraussetzungen ... 818
Erstellen eines temporären Datenspeichers auf einem externen Gerät ... 819
Replizieren der Quelldaten zum temporären Datenspeicher ... 820
Löschen des temporären Datenspeichers aus der Quellkonsole ... 821
Senden des externen Geräts zum Zielspeicherort ... 822
Erhalt des externen Geräts ... 823
Importieren des temporären Datenspeichers vom externen Gerät ... 824
Erstellen eines Zieldatenspeichers ... 825
Replizieren der Daten vom temporären Datenspeicher zum Zieldatenspeicher ... 826
Überprüfen der Datenreplikation ... 827
(Optional) Festlegen der Anzahl gleichzeitiger Knoten für RPS-Jumpstart ... 828
Ausführen einer umgekehrten Replikation ... 828
Überprüfen der Voraussetzungen ... 828
Durchführen einer Ad-hoc-Replikation ... 829
Durchführen einer umgekehrten Replikation von der Remote-Konsole zum RPS-Server vor Ort ... 836
Erstellen eines Ablaufplans für das Kopieren von Wiederherstellungspunkten ... 844
Überprüfen der Voraussetzungen und Hinweise ... 845

Erstellen eines Plans mit einem Sicherungstask 846
Hinzufügen eines Tasks für das Kopieren von Wiederherstellungspunkten zum Plan 863
Überprüfen des Plans 873
Erstellen eines Ablaufplans für Dateikopie 874
Überprüfen der Voraussetzungen und Hinweise 875
Erstellen eines Plans mit einem Sicherungstask 876
Hinzufügen eines Dateikopietasks zum Plan 894
Ausführen einer manuellen Dateikopie (optional) 905
Überprüfen des Plans 906
Erstellen eines Dateiarchivierungsplans 907
Überprüfen der Voraussetzungen und Hinweise 908
Erstellen eines Plans mit einem Sicherungstask 909
Hinzufügen eines Dateiarchivierungstasks zum Plan 927
Ausführen einer manuellen Dateiarchivierung (optional) 939
Überprüfen des Plans 940
Erstellen eines Zeitplans für das Kopieren auf Band 941
Überprüfen der Voraussetzungen und Hinweise 942
Erstellen eines Plans mit einem Sicherungstask 943
Hinzufügen eines Tasks "Auf Band kopieren" zum Plan 944
So erstellen und verwalten Sie eine Instant VM auf Microsoft Azure 953
Überprüfen der erforderlichen Komponenten für eine Instant VM auf Microsoft Azure 954
Instant Virtual Machine auf Microsoft Azure erstellen 955
Verwalten von Instant VMs 964
Erstellen und Verwalten von Instant VMs auf Hyper-V- und VMware ESX-Servern 967
Überprüfen der Voraussetzungen für eine Instant VM 969
Erstellen einer neuen Instant VM 972
Verwalten von Instant VMs 990
Erstellen und Verwalten von Instant VMs auf Amazon EC2 996
Überprüfen der Voraussetzungen für eine Instant VM auf Amazon EC2 997
Erstellen einer Instant VM auf Amazon EC2 998
Verwalten von Instant VMs 1007
So erstellen Sie einen Plan für die Replikation zwischen Standorten 1013
Erstellen eines Plans für die Replikation zwischen Standorten 1015
Schützen von Microsoft Office 365-Daten 1017
Moderne Authentifizierung 1017
Erstellen eines Exchange Online-Sicherungsplans 1024

So erstellen Sie einen SharePoint Online-Sicherungsplan 1055
So erstellen Sie einen Sicherungsplan für Microsoft Office 365 OneDrive 1075
Verwalten der Sicherung und Wiederherstellung von Microsoft Teams-Daten 1094
Überprüfen der Voraussetzungen und Hinweise 1097
Hinzufügen der erforderlichen Rolle und Gruppe zum Exchange Online-Sicherungskonto zur Durchführung von Sicherungen und Wiederherstellungen 1100
Erstellen eines Plans für Exchange Online-Sicherungen 1102
Angeben der Quelle 1104
Angeben des Ziels 1113
Festlegen des Ablaufplans 1114
Funktionsweise der erweiterten Planung und Aufbewahrung 1118
Festlegen von erweiterten Einstellungen 1121
Überprüfen der Voraussetzungen 1145
Erstellen eines SharePoint Online-Sicherungsplans 1146
Angeben der Quelle 1148
Angeben des Ziels 1153
Festlegen des Ablaufplans 1154
Festlegen von erweiterten Einstellungen 1158
Erstellen und Konfigurieren von gleichzeitigen Instant Virtual Machine(s) auf mehreren Hypervisoren 1176
Auswählen eines oder mehrerer Quell-Recovery Point Server 1179
Auswählen des Speicherorts der VM(s) 1180
Auswählen eines oder mehrerer Wiederherstellungsserver 1184
Konfigurieren der Einstellungen von virtuellen Rechnern 1186
Überprüfen der Zusammenfassung 1191
Konfigurieren von gleichzeitigen Virtual Standby-Rechnern 1194
Kapitel 12: Verwenden eines Hardware-Snapshots für die Sicherung 1199
Verwenden von Hardware-Snapshots für Sicherungen 1200
Verwenden von Hardware-Snapshots für die agentenlose VMware-Sicherung 1201
Hinweise für den NetApp iSCSI/FC-Support für VMware 1203
Hinweise für den NFS-Support für VMware 1207
Hinweise zu Nimble-Speicher bei aktivierter CHAP-Authentifizierung 1210
Verwenden von Hardware-Snapshots für die agentenlose Hyper-V-Sicherung 1212
Verwenden von Hardware-Snapshots für die agentenbasierte Sicherung 1214
Überprüfen, ob die Sicherung Hardware-Snapshots verwendet hat 1215
Kapitel 13: Wiederherstellen von geschützten Daten 1217

So führen Sie eine Wiederherstellung von einem Wiederherstellungspunkt aus .. 1218
Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise 1220
Festlegen der Informationen für den wiederherzustellenden Wiederherstellungspunkt 1227
Wiederherstellen des Inhalts des Wiederherstellungspunkts 1241
Überprüfen, ob der Inhalt wiederhergestellt wurde 1242
So führen Sie eine Wiederherstellung von einer Dateikopie aus 1243
Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise 1246
Angeben der Informationen zur Dateikopiewiederherstellung 1249
Wiederherstellen des Dateikopieinhalts 1262
Überprüfen, ob der Inhalt wiederhergestellt wurde 1264
Ausführen einer Wiederherstellung anhand von einer Dateikopie 1265
Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise 1266
Angeben der Informationen zur Dateikopiewiederherstellung 1268
Wiederherstellen des Inhalts des Wiederherstellungspunkts 1281
Überprüfen, ob der Inhalt wiederhergestellt wurde 1283
So stellen Sie Dateien/Ordner wieder her 1284
Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise 1287
Angeben der Informationen zur Wiederherstellung von Dateien/Ordnern 1294
Wiederherstellen der Datei bzw. des Ordners 1314
Überprüfen, ob die Datei bzw. der Ordner wiederhergestellt wurde 1316
Ausführen einer Bare-Metal-Recovery mithilfe einer Virtual Standby-VM oder Instant VM 1317
Überprüfen der Voraussetzungen und Hinweise für BMR 1319
Definieren der BMR-Optionen 1322
Überprüfen des Erfolgs der BMR 1346
BMR-Referenzinformationen 1347
Beheben von BMR-Problemen 1356
So stellen Sie einen virtuellen Rechner wieder her 1363
Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise 1366
Angeben der wiederherzustellenden Informationen zum virtuellen Rechner 1367
Wiederherstellen eines virtuellen Rechners 1387
Überprüfen, dass der virtuelle Rechner wiederhergestellt wurde 1388
So stellen Sie SQL Filestream wieder her 1388
So wenden Sie den Patch "T00002266" an 1389
Wiederherstellen der SQL-Datenbank am ursprünglichen Speicherort 1390
Wiederherstellen der SQL-Datenbank auf einer alternativen Instanz auf demselben Server 1393

Wiederherstellen der SQL-Datenbank auf einer alternativen Instanz auf einem anderen Server ... 1398
Wiederherstellen der SQL-Datenbank an einem alternativen Speicherort auf derselben Instanz ... 1405
Wiederherstellen des Modus über den Registrierungsschlüssel ... 1408
Verwenden des Hilfsprogramms zur spezifischen Wiederherstellung von Exchange-Objekten (GRT) ... 1415
Einführung ... 1416
Überprüfen der Voraussetzungen und Hinweise ... 1417
Wiederherstellen von Microsoft Exchange-Daten mit dem Hilfsprogramm zur spezifischen Wiederherstellung von Exchange-Objekten (GRT) ... 1418
Wiederherstellen von Microsoft Exchange-Anwendungen ... 1424
Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise ... 1426
Angeben der Microsoft Exchange-Informationen, die wiederhergestellt werden sollen 1428
Wiederherstellen der Microsoft Exchange-Anwendung ... 1435
Überprüfen, ob die Microsoft Exchange-Anwendung wiederhergestellt wurde ... 1437
Wiederherstellen von Exchange-Daten auf einem virtuellen VMware-Rechner ... 1438
So laden Sie Dateien/Ordner ohne Wiederherstellung herunter ... 1439
So laden Sie Dateien/Ordner ohne Wiederherstellung herunter/Ordner ohne Wiederherstellung für Linux-Knoten herunter ... 1441
So stellen Sie Microsoft SQL Server-Anwendungen wieder her ... 1443
Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise ... 1445
Angeben von Microsoft SQL Server-Informationen, die wiederhergestellt werden sollen ... 1448
Wiederherstellen der Microsoft SQL Server-Anwendung ... 1454
Überprüfen, ob die Microsoft SQL Server-Anwendung wiederhergestellt wurde ... 1456
Wiederherstellen von einem UNC/NFS-Pfad aus ... 1457
Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise ... 1458
Angeben der UNC/NFS-Pfad-Informationen, die wiederhergestellt werden sollen ... 1459
Wiederherstellen der unter dem UNC/NFS-Pfad gespeicherten Dateien/Ordner und Inhalte ... 1470
Überprüfen, ob der Inhalt wiederhergestellt wurde ... 1472
Wiederherstellen von Oracle-Datenbanken ... 1473
Überprüfen der Voraussetzungen und Hinweise ... 1475
Wiederherstellen der Server-Parameterdatei ... 1476
Wiederherstellen der Parameterdatei ... 1477
Wiederherstellen der archivierten Redo-Protokolle ... 1478
Wiederherstellen der Tablespaces oder Datendateien ... 1479
Wiederherstellen des Systems oder Rückgängigmachen der Tablespaces oder Datendateien ... 1481

Wiederherstellen aller Tablespaces und Datendateien 1483
Wiederherstellung von Kontrolldateien 1485
Wiederherstellen der gesamten Datenbank (Tablespaces und Kontrolldateien) 1487
Wiederherstellen der Oracle-Datenbank mithilfe von Bare Metal Recovery 1489
So führen Sie eine Wiederherstellung der Dateiebene unter Linux-Knoten aus 1491
Überprüfen der Voraussetzungen 1494
(Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers 1495
Angeben des Wiederherstellungspunkts für agentenbasierte Sicherung 1497
Angeben der Details des Zielcomputers 1504
Festlegen von erweiterten Einstellungen 1508
Erstellen und Ausführen des Wiederherstellungsjobs 1513
Überprüfen, dass Dateien wiederhergestellt wurden 1515
Ausführen von Wiederherstellungen auf Dateiebene über eine hostbasierte, agentenlose Sicherung für Linux-Knoten 1516
Überprüfen der Voraussetzungen 1517
Angeben des Wiederherstellungspunkts 1518
Angeben der Details des Zielcomputers 1523
Festlegen von erweiterten Einstellungen 1527
Erstellen und Ausführen des Wiederherstellungsjobs 1532
Überprüfen, dass Dateien wiederhergestellt wurden 1533
So führen Sie eine IVM-Migration (vom Linux-Wiederherstellungspunkt) aus der Cloud auf einen lokalen Rechner durch 1534
Überprüfen der Voraussetzungen und besonderen Aspekte für die IVM-Migration 1535
Durchführen der IVM-Migration aus der Cloud auf einen lokalen Rechner 1536
So führen Sie eine Bare-Metal-Recovery (BMR) für Linux-Rechner aus 1537
Überprüfen der Voraussetzungen 1540
Abrufen der IP-Adresse des Zielcomputers mithilfe der Live-CD 1541
(Optional) Wiederherstellen von Daten auf dem iSCSI-Volume des Zielcomputers 1543
(Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers 1545
Überprüfen des Backup-Servers 1547
Angeben der Wiederherstellungspunkte 1549
Angeben der Details des Zielcomputers 1552
Festlegen von erweiterten Einstellungen 1554
Erstellen und Ausführen des Wiederherstellungsjobs 1560
Überprüfen, dass der Zielknoten wiederhergestellt wurde 1568
Durchführen einer Migrations-BMR für Linux-Rechner 1569
Überprüfen der Voraussetzungen für die Migrations-BMR 1570

Ausführen einer BMR auf dem temporären Rechner ... 1571
Ausführen der Migrations-BMR ... 1573
Überprüfen, dass der Zielknoten wiederhergestellt wurde ... 1575
So führen Sie eine BMR mithilfe einer Sicherung aus ... 1576
Überprüfen der Voraussetzungen und Hinweise für BMR ... 1578
Definieren der BMR-Optionen ... 1580
Überprüfen des Erfolgs der BMR ... 1601
BMR-Referenzinformationen ... 1602
Beheben von BMR-Problemen ... 1611
So stellen Sie geclusterte Microsoft-Knoten und freigegebene Datenträger wieder her ... 1619
Überprüfen der Voraussetzungen ... 1621
Wiederherstellen von Dateien auf einem freigegebenen Cluster-Datenträger ... 1622
Wiederherstellen eines spezifischen Knotens in einem Cluster ... 1623
Wiederherstellen eines beschädigten freigegebenen Cluster-Datenträgers ... 1624
Wiederherstellen des vollständigen geclusterten Knotens und des freigegebenen Datenträgers ... 1625
Wiederherstellen eines Active Directory ... 1627
Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise ... 1629
Wiederherstellen eines Active Directory ... 1630
Überprüfen, ob das Active Directory wiederhergestellt wurde ... 1634
Wiederherstellen von Active Directory-Daten mithilfe des Dienstprogramms "Arcserve UDP Active Directory Objekt Level Restore" ... 1634
Wiederherstellen von Microsoft Office 365-Daten ... 1642
Wiederherstellen von Exchange Online-Postfachdaten ... 1643
So stellen Sie SharePoint Online-Websitesammlungsdaten wieder her ... 1661
So stellen Sie OneDrive Daten wieder her ... 1673
Durchsuchen Sie "Auf Band-Wiederherstellungspunkt kopieren" zur Wiederherstellung ... 1687
So führen Sie eine Wiederherstellung zu einem bestimmten Zeitpunkt durch ... 1688
Voraussetzungen ... 1688
Hinweise ... 1688
Durchführen einer Wiederherstellung zu einem bestimmten Zeitpunkt ... 1689
So stellen Sie ein Cluster Shared Volume wieder her ... 1693
Überprüfen der Voraussetzungen und Hinweise ... 1694
Festlegen der wiederherzustellenden CSV-Informationen ... 1700
Wiederherstellen des CSV-Inhalts ... 1710
Kapitel 2: Verwalten von Bandsicherung und -wiederherstellung ... 1713

So sichern Sie Deduplizierungsdatenspeicher auf einem Band ... 1714
So stellen Sie einen Deduplizierungsdatenspeicher von einem Band wieder her ... 1715
Überprüfen der Voraussetzungen ... 1717
Wiederherstellen von einem Band an einem alternativen Speicherort ... 1718
Wiederhergestellten Datenspeicher an den RPS importieren ... 1719
Kapitel 3: Verwenden der PowerShell-Schnittstelle ... 1721
So verwenden Sie die PowerShell-Schnittstelle ... 1722
Überprüfen der Voraussetzungen ... 1723
Verwenden der PowerShell-Schnittstelle für Arcserve UDP ... 1724
PowerShell-Syntax und -Parameter ... 1725
PowerShell-Beispiele ... 1738
Konfigurationsdatei und Eigenschaften von PowerCLI ... 1742
Kapitel 4: Schützen von Oracle-Systemen mit Recovery Manager (RMAN) ... 1745
Überprüfen der Voraussetzungen für Oracle-Datenbank mit RMAN (Windows und Linux) ... 1746
Erstellen eines Sicherungsplans für Oracle-Datenbank (Windows und Linux) ... 1755
Erstellen eines Sicherungsplans mit einem Sicherungstask ... 1756
Hinzufügen eines Assured Recovery-Tasks zum Plan ... 1780
(Optional) Ausführen einer manuellen Sicherung ... 1789
Wiederherstellen einer Oracle-Datenbank mit RMAN ... 1791
Auswählen der wiederherzustellenden Oracle-Datenbankelemente ... 1792
Definieren der Wiederherstellungsoptionen ... 1800
Einschränkungen ... 1816
Kapitel 5: Schützen von Microsoft SharePoint-Umgebungen ... 1819
Installationshinweise für Microsoft SharePoint-Umgebungen ... 1820
Schützen von Microsoft SharePoint-Servern ... 1821
Beachten der Hinweise ... 1822
Durchführen einer Sicherung des SharePoint-Servers ... 1823
Wiederherstellen einer SharePoint-Umgebung ... 1826
Wiederherstellen mit der Instant VM ... 1827
Wiederherstellen über die Benutzeroberfläche von Arcserve UDP Agent ... 1837
Wiederherstellen durch Laden einer Datenbank mithilfe eines Wiederherstellungspunkts ... 1843
Erstellen eines isolierten Netzwerks für die SharePoint-Wiederherstellung ... 1868
Erstellen eines isolierten Netzwerks für die SharePoint-Wiederherstellung bei VMware-VMs ... 1869

Erstellen eines isolierten Netzwerks für die SharePoint-Wiederherstellung bei Hyper-V-VMs ... 1875

Kapitel 6: Generieren von Arcserve UDP-Berichten ... 1879

Kennenlernen von Arcserve UDP-Berichten ... 1880

Arcserve UDP-Berichte ... 1881

Verwenden von Filtern und Aktionen ... 1897

Arbeiten mit Arcserve UDP-Berichten ... 1899

Erstellen von SLA-Profilen ... 1900

Planen von E-Mails ... 1903

Senden von Berichten per E-Mail ... 1908

Erstellen von Berichten ... 1910

Anpassen der Aufbewahrungszeit (Tage) für einen Jobstatus-Bericht ... 1911

Rohdatengröße im Bericht zur verwalteten Kapazität für hostbasierte agentenlose Sicherungen von VMs ... 1912

Anzeigen tatsächlicher Werte an Quelle und Ziel für Jobtypen ... 1916

Kapitel 7: Verwalten von High Availability ... 1919

Funktionsweise von High Availability ... 1920

Verwalten von Steuerungsdiensten für High Availability ... 1921

Verwalten von High Availability-Lizenzen ... 1922

Verwalten von Szenarien ... 1923

Remote-Installation ... 1937

High Availability-Berichte ... 1940

Kapitel 8: Verwenden des VSphereConfig-Hilfsprogramms ... 1941

Aktivieren oder Deaktivieren des VSPhereBackupNFC-Tags mithilfe der Eingabeaufforderung ... 1941

Kapitel 9: Verwenden des Diagnosehilfsprogramms ... 1949

Erfassen der Diagnoseinformationen ... 1950

Erfassen von Diagnoseinformationen von einem eigenständigen Agenten ... 1952

Hochladen von Diagnoseinformationen auf die Arcserve-Website über FTP ... 1953

Extrahieren der Agentenprotokolle ... 1955

Extrahieren der Konsolenprotokolle ... 1956

Überspringen der Inhalte des Protokollverlaufsordners über die Registrierung ... 1957

Erfassen des Protokolls vom Gateway-Rechner über die Befehlszeile ... 1957

Sammeln von Protokollen aus dem RPS über die Befehlszeile ... 1958

Erfassen von Stub-Protokollen von Hyper-V mit installiertem Agenten ... 1959

Erfassen von Meldungen aus der Hyper-V-Ereignisanzeige ... 1960

Erfassen des Ordners "Ca_lic" und der OLF-Dateien ... 1960

Erfassen der Verzeichnisliste für Verzeichnisse im Sicherungsziel/Datenspeicher ... 1961

Kapitel 10: Manuelles Installieren von Sophos Intercept X Advanced for Server auf Arcserve UDP 1963
Kapitel 11: Best Practices 1969
Best Practices für den Schutz des Arcserve UDP-Servers 1970
Ausschließen von Dateien vom Antivirusscanning 1971
Konfigurieren von Multistreaming-Parametern 1972
Infos zu Exchange Online 1973
Konfiguration für optimale Leistung 1974
Best Practices für Sicherungen 1975
Best Practices zur Wiederherstellung 1977
Häufig gestellte Fragen zu Exchange Online 1978
Infos zu Microsoft Azure 1979
Best Practices für eine Instant-VM auf Microsoft Azure 1979
Bereitstellen von Arcserve UDP für Microsoft Azure 1979
Kapitel 12: Fehlerbehebung 1981
Bei Arcserve UDP-Kommunikationsfehlern 1982
Arcserve UDP kann nicht mit Windows-Knoten kommunizieren 1983
Es können keine E-Mail-Alerts vom Gmail-Konto empfangen werden 1985
Arcserve UDP kann nicht mit dem Arcserve UDP Linux-Sicherungsserver auf Remote-Knoten kommunizieren 1986
Arcserve UDP kann nicht mit dem Arcserve UDP Recovery Point Server auf Remote-Knoten kommunizieren. 1987
Arcserve UDP kann nicht mit dem Arcserve Backup-Server auf Remote-Knoten kommunizieren 1989
Arcserve UDP kann nicht mit dem Remote-Standort kommunizieren 1990
Bei Plänen, Jobs und Einstellungen 1991
Fehlgeschlagener Sicherungsjob nach Änderung von Hostname/IP-Adresse der Konsole 1992
So fügen Sie ein Verschlüsselungskennwort für ein vorhandenes verschlüsseltes Ziel hinzu 1993
Anwendung von Sicherungseinstellungen für Knoten nicht möglich 1994
Fehlgeschlagene Planbereitstellung nach Änderung des Kennworts des agentenlosen Sicherungs-Proxy-Rechners 1995
Einstellungen beim Öffnen der Agent-Benutzeroberfläche deaktiviert 1996
Unterbrechen und Wiederaufnehmen schlägt fehl, wenn Agent nicht mit dem Netzwerk verbunden ist 1997
Der Arcserve UDP Agent-Dienst wird nur langsam ausgeführt. 1998
Konfigurieren der Registrierung, um einen Kopie auf Band-Job erneut auszuführen 2000
Konfigurieren der Registrierung, um mehrere Wiederherstellungspunkte desselben Typs im gleichen Job auf Band zu kopieren 2001

Datei/Ordner fehlte in der Sicherung des freigegebenen NFS-Ordners oder Datei-/Ordnername wurde in einen unbrauchbaren Namen umgewandelt 2002

Die Sicherung des freigegebenen NFS-Ordners schlägt fehl 2002

Zurücksetzen der MFA-aktivierten UDP-Konsole, wenn TOTP nicht verfügbar ist 2002

Hinweise zu Instant VMs 2010

Fehler bei der Erstellung einer Instant VM in VMware aufgrund eines doppelten NFS-Datenspeichernamens 2011

Fehlgeschlagene Erstellung einer Instant VM mit Windows 2008 R2 als Wiederherstellungsserver für VMware oder Windows 2008 R2 Hyper-V Server 2012

Eine Instant VM kann nicht gestartet werden, wenn es sich bei dem Quellrechner um einen Windows 2008/2012/2016 AD-Server handelt 2013

Einschalten der VM nach der Wiederherstellung von Hyper-V ist fehlgeschlagen 2015

Instant VM-Job schlägt aufgrund eines Windows NFS-Dienstfehlers fehl 2016

Zugreifen auf oder Löschen von Instant VM-Dateiordner ist auch mit Administratorrechten nicht möglich. 2017

Instant VM kann nach dem Neustart des Wiederherstellungsservers nicht in Hyper-V gestartet werden. 2018

Fehlgeschlagene Erstellung eines VMware-NFS-Datenspeichers und Anzeige des Fehlers "Auflösen des Hostnamens nicht möglich" 2019

Fehler beim Bereitstellen des Integrationsdiensts auf der Gast-VM in Hyper-V 2021

Linux-Instant VM-Fehler auf einem nicht englischen Hyper-V-Server 2022

Zusätzlicher Lizenzverbrauch für UNC-Pfade, die sich auf einer VM unter einem lizenzierten Hyper-V befinden 2023

Lizenzfehler wird angezeigt, wenn Sie die Lizenzedition/den Lizenztyp ändern und eine Instant-VM erstellen 2023

Bei Linux-Agenten 2025

Deaktivierte Sicherungsziel-Einstellungen bei Verwendung der Benutzeroberfläche des Linux-Agent 2026

Jobstatus, Jobübersicht und Aktivitätsprotokoll nicht sichtbar 2027

System-Volume des SUSE15 mit XFS-Dateisystem konnte nicht wiederherstellen 2028

Infos zu Wiederherstellungen 2029

Wiederherstellung von Dateien nicht möglich 2030

Hinzufügen der wiederhergestellten Inhaltsdatenbank zur ursprünglichen Webanwendung 2031

Datenbank kann nicht geladen werden, während die Microsoft Exchange-Datenbank wiederhergestellt wird 2034

Feld "Von" wird für E-Mails nicht richtig angezeigt, die von Benutzern mit Vertretungsrechten für ein freigegebenes Postfach gesendet wurden 2036

Wiederherstellungsaufträge schlagen nach Light-Integration-Backups fehl 2037

Bei Wiederherstellung auf einem freigegebenem NFS Ordner wird der Dateiname in einen unbrauchbaren Namen geändert 2037

Bei Gateway, RPS, Datenspeicher, Konsole und Datenbank 2039

Datenspeichername wird bereits verwendet 2040

Verbindung mit dem Datenspeicher aufgrund eines DNS-Fehlers nicht möglich 2041

Datenspeicher wechselt in den Modus für "Nur Wiederherstellen" 2042

Fehler, wenn RPS-Version niedriger ist als Konsolenversion 2044

Hinzufügen derselben Ressource an verschiedenen Standorten wird nicht unterstützt . 2046

Aktivieren von Protokollkürzungen, wenn die SQL-Datenbank sich im vollständigen Wiederherstellungsmodus befindet 2047

Beim Durchsuchen von Wiederherstellungspunkten werden keine verfügbaren Wiederherstellungspunkte angezeigt, wenn RPS mit FQDN konfiguriert sind 2049

Zugriffsverweigerung beim Hinzufügen von RPS 2050

Zuweisen von Administratorrechten und -rollen zu einem Domänenbenutzer 2052

Umschalten in die UDP-Ansicht für Wiederherstellungspunkt nicht möglich 2055

Zugriffsverweigerung beim Hinzufügen oder Aktualisieren von Knoten 2056

UDP-Konsole wird bei Änderung des SQL-Administratorkennworts nicht geöffnet 2058

Fehler beim Laden von Wiederherstellungspunkten aufgrund eines Zeitlimits 2059

Aktualisieren der Anmeldeinformationen des Gateway-Servers 2060

Aktualisieren des Gateways, wenn die Gateway-Proxy-Anmeldeinformationen geändert werden 2062

Konsole zeigt Meldung "Identitätsdienst wird gestartet" 2064

Bei Sicherung und Wiederherstellung des virtuellen Rechners 2065

Hinzufügen von Berechtigungen für VDDK auf Ebene des vCenter-Servers 2068

Jobs für die Sicherung von VM-Vorlagen werden immer in eine vollständige Sicherung konvertiert, und das Volumen der Sicherungsdaten entspricht der Bereitstellungsgröße des virtuellen Datenträgers 2075

Unabhängige Datenträger werden bei der Sicherung von VM-Vorlagen übersprungen . 2077

Die Sicherung von in SMB 3.0-Freigaben abgelegten VMs schlägt mit einer Fehlermeldung fehl 2079

VM-Wiederherstellungsjobs schlagen fehl bei der Wiederherstellung von VMs in eine Windows-Standarddateifreigabe 2080

Volume-Informationen für den Wiederherstellungspunkt nicht verfügbar 2081

Konvertieren von Zuwachssicherungen in Überprüfungssicherungen, weil Snapshots virtueller Rechner seit dem letzten Sicherungsjob geändert wurden oder konsolidiert werden müssen 2082

Agentenlose Sicherungen von VMware-VMs schlagen fehl, wenn das CD/DVD-Gerät der VM mit einem ISO-Image auf einem nicht verbundenen NFS-Datenspeicher verbunden ist 2083

Agent-lose hostbasierte Sicherung für Hyper-V-VM schlägt nach dem Aktualisieren von Arcserve UDP fehl 2084

Hostbasierte agentenlose Sicherung schlägt in VMware ESXi 6.0 fehl 2085

Die agentenlose hostbasierte Sicherung stürzt ab, wenn Windows 2003 R2 64-Bit-als Sicherungs-Proxy verwendet wird. 2087

Hostbasierte agentenlose Sicherung verwendet keinen HotAdd-Transportmodus 2088

Hostbasierter agentenloser Sicherungs- oder Wiederherstellungsjob verwendet den NBD- oder den NBDSSL-Transportmodus auch dann, wenn der SAN-Modus möglich ist 2089

Fehler beim Erstellen eines Snapshot für virtuelle Hyper-V-Rechner bei mehreren ausgeführten Jobs 2091

Hyper-V konnte keinen VSS-Snapshot erstellen 2093

Fehlschlag der Sicherung von virtuellem Datenträger wegen Systemfehler=[The device is not ready(21)] 2094

Fehlgeschlagene Sicherungsjobs 2095

Fehler beim Importieren von VMware-VMs aus vCenter 2097

Sicherungen schlagen wegen ESXi-Lizenz fehl 2098

Der HotAdd-Transportmodus funktioniert nicht, wenn Sie versuchen, eine VMware-VM zu sichern. 2099

Genauere Steuerung für VSS Windows Gast-BS Quiescings 2101

Die virtuelle Maschine kann nicht konfiguriert werden, um den Parameter "Disk.EnableUUUID" zu aktivieren. 2103

Wiederherstellungsvorgänge schlagen fehl, wenn Daten im HOTADD- oder SAN-Transportmodus wiederhergestellt werden 2105

VM-Wiederherstellung schlägt fehl, wenn ein nicht standardmäßiger Port angegeben ist 2107

Geplante Zuwachssicherungsjobs oder vollständige Sicherungsjobs für Hyper-V-VMs schlagen fehl 2108

Hyper-V VSS NTDS-Writer schlägt bei der Erstellung des Snapshot in der VM fehl 2109

Änderungen der MAC-Adresse werden nach der VM-Wiederherstellung nicht beibehalten 2110

VM-Wiederherstellung schlägt fehl mit folgender Fehlermeldung – Öffnen der VMDK-Dateien nicht möglich 2111

Probleme durch doppelte VM-UUID 2113

Dateisystem-Katalogjob schlägt fehl oder die Überprüfung des Wiederherstellungspunktes für die hostbasierte Agent-lose Sicherung schlägt fehl 2115

Inkrementelle Sicherung wird zu Überprüfungssicherung konvertiert oder die Sicherungsgröße in Hyper-V wird erhöht. 2117

Hostbasierte Sicherung schlägt für Hyper-V-VM mit spezieller Konfiguration differenzierender Datenträger fehl 2119

Sicherungsjob für eine VMware-VM schlägt fehl 2120

Deaktivieren der erneuten Überprüfung des HBA während inkrementeller Sicherungen 2122

Deaktivieren der aufeinander folgenden Erstellung von Snapshots in VMware-VM für eine Sicherung 2123

Nach Wiederherstellung von einem Host mit höherer ESXi-Version auf einen Host mit niedrigerer ESXi-Version hängt sich die VM beim Booten auf 2124

RAM-Auslastung erreicht 99 %, wenn Sicherungsjobs an die VM übergeben werden 2125

Hyper-V-Auftrag schlägt fehl, es kann keine Verbindung zum Dienstprogramm auf dem Host hergestellt werden 2126

Automatischer Schutz erkennt und schützt virtuellen Computer nicht 2128

Festlegen der Leseblockgröße beim Sichern einer VMDK-Datei 2131

Beim Klonen von LUNs wird die Reservierung von LUN Speicherplatz vererbt 2131

Infos zu Virtual Standby ... 2133
Operating System Not Found (Betriebssystem nicht gefunden) ... 2134
Virtual Standby-Jobs schlagen aufgrund interner Fehler fehl ... 2135
Virtual Standby-Jobs im HotAdd-Transportmodus schlagen fehl ... 2139
Virtual Standby-Jobs an Hyper-V-Systeme schlagen fehl ... 2141
Problem durch doppelte Agent-UUID ... 2142
Änderungen an der Virtual Private Cloud im Virtual Standby-Task werden in Amazon EC2 wiedergegeben ... 2142
Option "Terminal-EC2-Ressourcen" wird nicht angezeigt ... 2143
Infos zum Kopieren von Wiederherstellungspunkten ... 2144
Konfigurieren der Registrierung für das Kopieren von Wiederherstellungspunkten ... 2145
Bandbreitenüberlastung bei Jobs zum Kopieren von Wiederherstellungspunkten in die Cloud ... 2146
Zusammenführungsjob übersprungen ... 2148
Im Zusammenhang mit Arcserve UDP-Berichten ... 2150
So zeigen Sie Diagramme zur Darstellung von Arcserve UDP-Berichten an ... 2151
Infos zu Microsoft Office 365 Exchange Online ... 2155
Die Liste der Postfächer wird im Dialogfeld Ziel auswählen nicht angezeigt ... 2155
Zugriff oder Berechtigung für Exchange Online-Gruppe verweigert ... 2156
Kapitel 13: Anhang ... 2159
Befehlszeilentool für Deduplizierungsdatenspeicher ... 2160
So zeigen Sie die Option "Überprüfung der Wiederherstellungspunkte" an ... 2164
So wenden Sie eine andere VDDK-Version als die in Arcserve UDP integrierte Version an ... 2167
Manuelles Ändern des VDDK für eine Virtual Standby-Sicherung (VSB) ... 2167
Manuelles Ändern des VDDK für eine hostbasierte Sicherung (HBBU) ... 2168
So migrieren Sie Arcserve D2D r16.5-Sicherungsdaten von zwei Servern mit identischem Hostnamen zu RPS-Datenspeicher ... 2170
So stellen Sie Arcserve UDP in Microsoft Azure bereit ... 2171
Grundlegendes zum Prozessablauf ... 2171
Hinweise ... 2172
Planen der Arcserve UDP-Bereitstellung in Microsoft Azure ... 2173
Bereitstellen von Arcserve UDP in Microsoft Azure ... 2185
Arcserve UDP – Begriffe und Definitionen ... 2198
Agentenbasierte Sicherung ... 2198
Komprimierung ... 2198
Konfiguration ... 2199
Dashboard ... 2199

Datenspeicher ... 2199
Ziel ... 2199
Erkannte Knoten ... 2199
Verschlüsselung ... 2200
Globale Deduplizierung ... 2202
Hostbasierte agentenlose Sicherung ... 2202
HOTADD-Transportmodus ... 2202
Job ... 2202
Jobs ... 2202
NBD-Transportmodus ... 2203
NBDSSL-Transportmodus ... 2203
Knoten ... 2203
Plan ... 2203
Geschützte Knoten ... 2203
Aktuelle Ereignisse ... 2203
Wiederherstellungspunkt ... 2203
Recovery Point Server ... 2204
Replizieren ... 2204
Ressourcen ... 2204
SAN-Transportmodus ... 2204
Systeme ... 2204
Tasks ... 2204
Ungeschützte Knoten ... 2205
Datendeduplizierung ... 2207
Arten der Datendeduplizierung ... 2208
Funktionsweise der Datendeduplizierung ... 2209
Wann sollten Sie Deduplizierung verwenden? ... 2211
Konfigurieren von Datenspeichern mit Deduplizierung in Arcserve UDP ... 2212
Deduplizierung, Verschlüsselung und Komprimierung ... 2214
Einschränkungen bei der Deduplizierung ... 2215

Kapitel 1: Funktionen und Verbesserungen

In diesem Abschnitt werden die Funktionen oder Verbesserungen in jeder Arcserve UDP-Version vorgestellt. Die Arcserve UDP-Lösung ist eine umfassende Lösung für Speicherprobleme der nächsten Generation in Organisationen, die ihre Daten in einer sich schnell verändernden Welt aus virtualisierten Infrastrukturen, Clouds und Diensten effektiv sichern möchten. Die Lösung ermöglicht dies durch die Bereitstellung einer vereinheitlichten Benutzeroberfläche für eine große Bandbreite von Funktionen, mit denen Kunden standortübergreifende Business Continuity erreichen und sich auf Katastrophen und Ausfälle vorbereiten können.

Dieser Abschnitt enthält Informationen über neue Funktionen, Verbesserungen und Support.

Dieser Abschnitt enthält folgende Themen:

Neue Funktionen

Wichtig! Informationen zu den neuesten Funktionen finden Sie unter UDP 8.1.

Im Folgenden finden Sie eine Liste der in Arcserve UDP 8.0 verfügbaren neuen Funktionen.

- **Sicherung auf und Wiederherstellung von versteckten Volumes:** Daten können auf versteckten Volumes gesichert bzw. von diesen wiederhergestellt werden. Versteckte Volumes sind Volumes, die ohne Laufwerksbuchstaben oder Ordnerpfad im Betriebssystem geladen werden. Auf versteckte Volumes kann über die entsprechende Volume-GUID zugegriffen werden.
- **Export und Import von Einstellungen:** Einstellungen können unter Verwendung der JSON-Datei im Windows-Agent exportiert und importiert werden.
- **OneDrive-Unterstützung:** Optionen zum Wiederherstellen am ursprünglichen oder an einem alternativen Speicherort sind verfügbar.
- **SharePoint Online-Unterstützung:** Die folgenden Funktionen sind für SharePoint Online-Unterstützung verfügbar:
  - Listen und Bibliotheken von persönlichen Sites können gesichert werden.
  - Es können mehrere Websitesammlungen gleichzeitig hinzugefügt werden.
  - Die neu hinzugefügten Websitesammlungen können automatisch innerhalb des Plans hinzugefügt werden.
- **Oracle RMAN-Unterstützung:** Arcserve UDP bietet jetzt eine Möglichkeit, Oracle-Systeme mithilfe von Recovery Manager (RMAN) zu schützen. RMAN ist ein Oracle-Hilfsprogramm, das Sicherungs- und Wiederherstellungstasks für Datenbanken ausführt und die Verwaltung von Sicherungsstrategien automatisiert. Weitere Informationen finden Sie unter Schützen von Oracle-Systemen mit Recovery Manager (RMAN).
- **Unterstützung von Office 365-Gruppen:** Für Office 365-Benutzer werden jetzt Gruppen unterstützt.
- **Umgekehrte Replikation:** Daten (Wiederherstellungspunkt) können jetzt aus der Cloud, von MSP oder einem remote verwalteten RPS zum lokalen UDP-Rechner oder RPS-Server vor Ort repliziert werden. Weitere Informationen finden Sie unter Ausführen einer umgekehrten Replikation.

- **Nutanix Files:** Arcserve UDP bietet jetzt eine Möglichkeit, Nutanix Files mithilfe der UNC/NFS-Option in Arcserve UDP zu schützen. Nutanix Files ist eine softwaredefinierte, horizontal skalierbare Dateispeicherlösung, die ein Repository für unstrukturierte Daten wie Stammverzeichnisse, Benutzerprofile, Freigaben auf Abteilungsebene, Anwendungsprotokolle, Sicherungen und Archive bietet. Weitere Informationen finden Sie unter Schützen des UNC/NFS-Pfads.
- **Unterstützung von Teams:** Datensicherung und -wiederherstellung wird jetzt auch für MS Teams unterstützt, eine chatbasierte Plattform für Unternehmenskommunikation. Weitere Informationen finden Sie unter Verwalten der Sicherung und Wiederherstellung von Microsoft Teams-Daten.
- **Unterstützung von unveränderlichem Speicher für "Wiederherstellungspunkt kopieren":** In Amazon S3 kann jetzt mithilfe der Funktion "Objektsperre" unveränderlicher Speicher erstellt werden.
- **Ersatz von Adobe Flash:** Adobe Flash wird nicht mehr benötigt, und die Installation von .NET Framework ermöglicht Ihnen das Anzeigen von Diagrammen.

Funktionsverbesserungen

Wichtig! Informationen zu den neuesten Funktionserweiterungen finden Sie unter UDP 8.1.

- **PowerCLI-Änderungen:** Die folgenden Optionen sind für die UDPPowerCLI.log-Protokolldatei(en) aktiviert:
  - Der Speicherort der UDP-PowerCLI-Protokolldateien darf geändert werden.
  - Die maximale Größe der Protokolldateien kann mithilfe von Protokollzirkulation gesteuert werden.
  - Der Zeitstempel in den Protokolldateien wird in das 24-Stunden-Format geändert.
  - Eine Aufbewahrungsrichtlinie auf Basis des Aufbewahrungszeitraums für UDP-PowerCLI-Protokolldateien ist zulässig.
  - Eine Aufbewahrungsrichtlinie auf Basis der Anzahl der beizubehaltenden Dateien für UDP PowerCLI-Protokolldateien ist zulässig.
- **Snapshot-Verbesserung:** Der Sicherungsplan von Arcserve UDP Agent (Windows/Linux) und der hostbasierte agentenlose Sicherungsplan (Nutanix/ESXI/Hyper-V) können das Skript nach dem Snapshot jetzt auch dann ausführen, wenn der Snapshot fehlschlägt.
- **Moderne Authentifizierung:** Die moderne Authentifizierung für Sicherung und Wiederherstellung in Office 365 wurde aktiviert.
- **Angabe des Netzwerks für Wiederherstellung und Replikation:** Für Wiederherstellung und Replikation kann die Kommunikation zwischen Windows-Agent und Recovery Point Server jetzt über ein Netzwerk hergestellt werden.
- **Angabe des Netzwerks für Linux:** Für Wiederherstellung und Replikation kann die Kommunikation zwischen Linux-Agent und Recovery Point Server jetzt über ein Netzwerk hergestellt werden.
- **Gleichzeitige IVM:** Mithilfe der Arcserve UDP-Konsole können jetzt gleichzeitige Instant Virtual Machine(s) auf mehreren Hypervisoren erstellt und konfiguriert werden.
- **Gleichzeitige VSB:** Mithilfe der Arcserve UDP-Konsole können jetzt gleichzeitige Virtual Standby-Rechner konfiguriert werden.

Linux Agent-Verbesserungen

Wichtig! Informationen zu den neuesten Verbesserungen des Linux-Agenten finden Sie unter UDP 8.1.

- Neue unterstützte Plattformen:
  - Red Hat Enterprise Linux 8.3
  - CentOS 7.9, 8.3
  - Oracle Linux 8.3
  - Debian Linux 9.12, 9.13, 10.6, 10.7
- **Angabe des Netzwerks für Linux:** Für Wiederherstellung und Replikation kann die Kommunikation zwischen Linux-Agent und Recovery Point Server jetzt über ein Netzwerk hergestellt werden.
- **Gleichzeitige IVM:** Mithilfe der Arcserve UDP-Konsole können jetzt gleichzeitige Instant Virtual Machine(s) auf mehreren Hypervisoren erstellt und konfiguriert werden.
- **Snapshot-Verbesserung:** Der Sicherungsplan von Arcserve UDP Agent (Linux) kann das Skript nach dem Snapshot jetzt auch dann ausführen, wenn der Snapshot fehlschlägt.
- **Ersatz von Adobe Flash:** Adobe Flash wird nicht mehr benötigt, um Diagramme auf dem Linux-Agenten anzuzeigen.

Datenbank- und Plattform-Support

Wichtig! Informationen zur aktuellen Datenbank- und Plattformunterstützung finden Sie unter UDP 8.1.

- Nutanix AOS 5.19
- Red Hat Enterprise Linux 8.3
- CentOS 7.9, 8.3
- Oracle Linux 8.3
- Debian Linux 9.12, 9.13, 10.6, 10.7
- VMware vSphere 7.0 Update 1
- Oracle-Datenbank 19c
- Nutanix Files 3.8.z, 3.7.z, 3.6.z

Sicherheits- und Drittanbieterverbesserungen

Wichtig! Informationen zu den neuesten Sicherheits- und Drittanbieterverbesserungen finden Sie unter UDP 8.1.

- **Unterstützung für Open JDK:** Die Open JDK-Version wurde auf 1.8.0.265.b01 aktualisiert.
- **VMware Virtual Disk Development Kit Unterstützung:** VDDK-Version wird auf 7.0 aktualisiert. 1.40833
- **VMware vSphere Web Services SDK-Unterstützung:** Die SDK-Version wird auf 6.7.1 aktualisiert
- **WSO2-Unterstützung:** Die WSO2-Version wurde auf v5.7.0 aktualisiert.
- **Apache-Unterstützung:** Die Apache-Version wurde auf 2.4.46 aktualisiert.
- **OpenSSL-Unterstützung:** Die OpenSSL-Version wurde auf 1.1.1i aktualisiert.
- **Tomcat-Unterstützung:** Die Tomcat-Version wurde auf 9.0.37 aktualisiert.
- **SQLite-Unterstützung:** Die SQLite-Version wurde auf 3.26 aktualisiert.
- **AWS SDK für Java:** Die Version von AWS SDK für Java wurde auf 1.11.852 aktualisiert.
- **AWS SDK für C++:** Die Version von AWS SDK für C++ wurde auf 1.6.53 aktualisiert.

Arcserve-Appliance-Verbesserungen

Wichtig! Informationen zu den neuesten Appliance-Verbesserungen finden Sie unter UDP 8.1.

Bestehende Appliance-Kunden können ein Upgrade auf Arcserve UDP 8.0 durchführen. Weitere Informationen finden Sie unter Installation.

Nicht mehr unterstützt

Wichtig! Weitere Informationen zu den verworfenen Support-Elementen finden Sie unter UDP 8.1.

- vSphere 5.5. Es wird dringend empfohlen, die Umgebung (vCenter/ESXi) auf die neueste von VMware unterstützte Version zu aktualisieren. Weitere Informationen zum Ende der allgemeinen Unterstützung für vSphere 5.5 finden Sie im KB-Artikel.
- Nutanix AHV 5.5.3.1.

Kapitel 2: Informationen zu Arcserve UDP

In diesem Abschnitt werden die folgenden Themen behandelt:

Einführung

Arcserve Unified Data Protection ist eine umfassende Lösung für den Schutz komplexer IT-Umgebungen. Die Lösung schützt Ihre Daten, die sich in verschiedenen Arten von Knoten wie Windows, Linux und virtuellen Maschinen auf VMware ESX-Servern, Microsoft Hyper-V-Servern oder Nutanix AHV-Servern befinden. Sie können Daten entweder auf einem lokalen Rechner oder auf einem Recovery Point Server sichern. Ein Recovery Point Server ist ein zentraler Server, auf dem Sicherungen von verschiedenen Quellen gespeichert werden.

Arcserve UDP bietet folgende Funktionen:

- Schützt verschiedene Arten von Quellknoten, einschließlich Agent Based, Agentless Based, CIFS, Exchange Online, SharePoint Online, OneDrive und so weiter.
- Sichert Daten auf Recovery Point Servers
- Repliziert Sicherungsdaten auf lokalen und Remote-Recovery Point Servers
- Überwacht Arcserve High Availability
- Archiviert Daten
- Kopiert:
  - ausgewählte Quelldateien auf einen sekundären Sicherungsspeicherort
  - Wiederherstellungspunkte auf lokale Speicherorte und Cloud-Speicherorte wie z. B. Freigabeordner und AWS EC2
  - Wiederherstellungspunkte auf Band
- Erstellt:
  - Virtuelle Standby-Maschinen von Sicherungsdaten zum lokalen Hypervisor (Hyper-V, ESX, Nutanix), AWS EC2 oder Microsoft Azure
  - Sofortige virtuelle Maschine auf lokalen Hypervisor (Hyper-V, ESX, Nutanix) für Windows
  - Sofortige virtuelle Maschine für lokalen Hypervisor (Hyper-V, ESX, Nutanix), AWS EC2 oder Microsoft Azure für Linux
- Stellt wieder her:
  - Sicherungsdaten und führt Bare-Metal-Recovery (BMR) durch
  - Microsoft Exchange-E-Mail und E-Mail-Objekte anhand der Arcserve UDP spezifischen Wiederherstellung von Exchange-Objekten.

Hinweis: Weitere Informationen zu unterstützten Spezifikationen, Funktionen und anderen Features finden Sie im Benutzerhandbuch zur spezifischen Wiederherstellung von Exchange-Objekten (esr.pdf).

- Unterstützt:
  - Rollenbasierte Verwaltung
  - Hardware-Snapshots
  - Assured Recovery-Test für Wiederherstellungspunkte
  - SLA -Bericht für RTO und RPO

Arcserve UDPMit können Sie Sicherungsdaten, die auf einem Server als Wiederherstellungspunkte gespeichert wurden, auf einem anderen Recovery Point Server replizieren. Sie können aus den Sicherungsdaten auch virtuelle Rechner erstellen, die bei Fehlern des Quellknotens als Standby-Rechner agieren können. Die Standby-Virtual Machine wird erstellt, indem Wiederherstellungspunkte in VMware ESX, Microsoft Hyper-V Virtual Machine oder Nutanix AHV-Format umgewandelt werden.

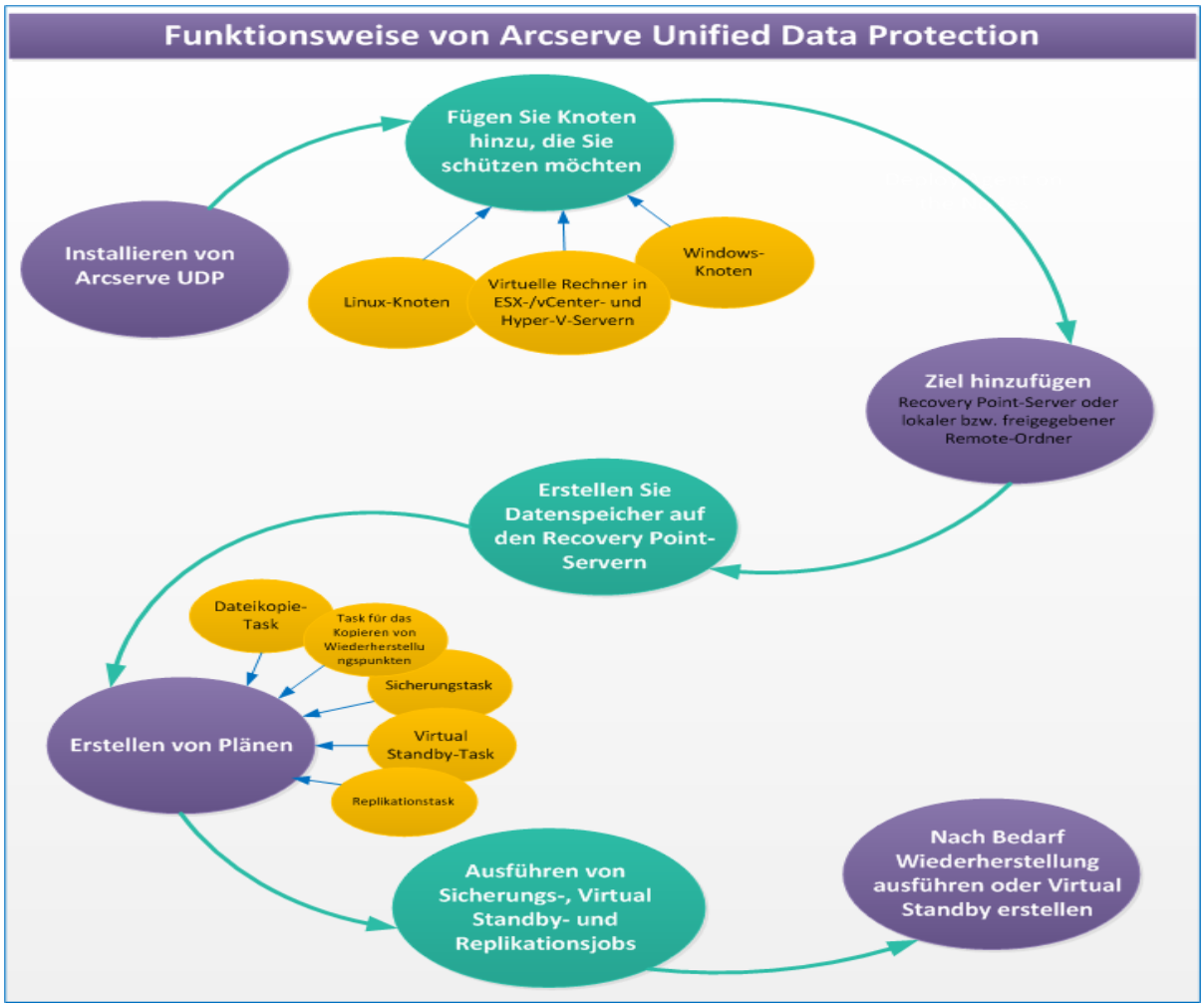
Die Arcserve UDP Lösung bietet Integration mit Arcserve High Availability. Nachdem Sie Szenarien in Arcserve High Availability erstellt haben, können Sie Ihre Szenarien überwachen und Vorgänge wie das Hinzufügen oder Löschen von Zielrechnern verwalten und ausführen.

Funktionsweise von Arcserve UDP

Arcserve UDP ist eine vereinheitlichte Datenschutzlösung für den Schutz Ihrer Computersysteme. Verwenden Sie die folgenden allgemeinen Schritte, um Ihre Systeme mit Arcserve UDP zu schützen.

1. Installieren von Arcserve Unified Data Protection.
2. Fügen Sie Knoten hinzu, die Sie schützen möchten. Sie können Windows- oder Linux-Knoten und virtuelle Maschinen in ESX/vCenter-, Hyper-V-Servern und Nutanix-AHV-Servern hinzufügen.
3. Fügen Sie ein Ziel hinzu. Bei einem Ziel kann es sich um einen Recovery Point Server, lokalen Ordner oder freigegebenen Remote-Ordner handeln.
4. Erstellen Sie Datenspeicher auf dem Recovery Point Server. Ein Datenspeicher ist ein physischer Bereich auf einem Datenträger. Sie können Datenspeicher mit und ohne Deduplizierung erstellen.
5. Erstellen Sie einen Ablaufplan. Ein Plan ist eine Gruppe von Aufgaben, um Sicherungen, Replikationen, Kopien von Wiederherstellungspunkten, Kopien auf Band, die Erstellung von Standby VMs oder Assured Recovery-Tests zu verwalten. Sie können auch UNC Path, Office 365 Exchange online, SharePoint Online oder OneDrive Node hinzufügen und zugehörige Aufgaben erstellen.
6. Führen Sie Jobs wie Sicherung, Erstellen von Virtual Standby und Replikation aus.
7. Führen Sie eine einfache Wiederherstellung oder eine Bare-Metal-Recovery aus.

Das folgende Diagramm gibt einen Überblick über die Schritte, die Sie ausführen müssen, um Daten zu schützen:


Funktionsweise von Arcserve Unified Data Protection
Fügen Sie Knoten hinzu, die Sie schützen möchten
Installieren von Arcserve UDP
Linux-Knoten
Virtuelle Rechner in ESX-/vCenter- und Hyper-V-Servern
Windows-Knoten
Ziel hinzufügen
Recovery Point-Server oder lokaler bzw. freigegebener Remote-Ordner
Erstellen Sie Datenspeicher auf den Recovery Point-Servern
Dateikopie-Task
Task für das Kopieren von Wiederherstellungspunkten
Sicherungstask
Virtual Standby-Task
Replikationstask
Erstellen von Plänen
Ausführen von Sicherungs-, Virtual Standby- und Replikationsjobs
Nach Bedarf Wiederherstellung ausführen oder Virtual Standby erstellen

Instant Virtual Machine (IVM) im Vergleich zu Virtual Standby (VSB)-Rechner

Beim Wiederherstellen von Daten nach einem Systemausfall oder während einer Disaster-Recovery-Schulung müssen Sie möglicherweise virtualisierte Instanzen von Servern starten, die zuvor von Arcserve UDPgeschützt wurden.

Arcserve UDP bietet die folgenden zwei Funktionen, mit denen Sie den virtuellen Rechner von Wiederherstellungspunkten starten können:

- I**nstant Virtual Machine (IVM)**: Erstellt eine virtuelle Maschine umgehend von einem Wiederherstellungspunkt. Durch die Verwendung einer Instant Virtual Machine erhalten Sie direkten Zugriff auf Daten und Anwendungen in den Arcserve UDP-Sicherungssitzungen. Eine Instant VM kommt ohne die mit einer herkömmlichen Wiederherstellung oder Konvertierung der Sicherungssitzung auf einem physischen oder virtuellen Rechner einhergehenden Ausfallzeit aus.

  Weitere Informationen zu Instant Virtual Machine finden Sie unter So erstellen und verwalten Sie eine Instant VM.

- **Virtual Standby Machine (VSB)**: Konvertiert die Wiederherstellungspunkte in Formate für virtuelle Rechner und bereitet einen Snapshot vor, damit Ihre Daten bei Bedarf auf einfache Weise wiederhergestellt werden können. Diese Funktion deckt auch die Hochverfügbarkeitsfunktion ab und stellt sicher, dass der virtuelle Rechner sofort übernehmen kann, wenn der Quellrechner ausfällt. Die Standby-Virtual Machine wird erstellt, indem die Wiederherstellungspunkte in ein beliebiges VMware-, Hyper-V- oder Nutanix AHV-Virtual-Maschinenformat umgewandelt werden.

  Weitere Informationen zu Virtual Standby finden Sie unter So erstellen Sie einen Virtual Standby-Plan.

Um zu bestimmen, welche Funktion am besten geeignet ist, müssen Sie Ihre RTO (Recovery Time Objective, Wiederherstellungszeit) und das Szenario berücksichtigen. In der folgenden Tabelle werden die Funktionen von IVM und VSB verglichen:

FUNKTIONEN	IVM	VSB
Einschalten von Standby-VMs vom aktuellen Wiederherstellungspunkt	Ja (keine Konvertierung erforderlich)	Ja, aber NUR, wenn dem Sicherungsplan ein VSB-Task hinzugefügt wurde. Beispiel: Vorausplanung erforderlich)
Erfordert Sicherungszeitverarbeitung	Nicht benötigt	Erforderlich; dem Plan muss ein VSB-Task hinzugefügt werden, der zum Sichern des

		Quellrechners verwendet wird.
VM-Startzeit	Langsamer (bis zu 30 %) aufgrund von E/A-Umleitung.	Selbe Zeit wie jede andere VM auf dem selben Hypervisor.
Speicherplatzanforderungen:	Minimaler Speicherplatz zum Hosten von untergeordneten Datenträger- oder Speicheränderungen bei Ausführung einer VM.	Ja, Speicherplatz wird auf dem Ziel-Hypervisor verbraucht, auf dem die VSB-Standby-VM verwaltet wird. Erfordert Speicherplatz gleich oder größer der Größe des Quellrechners.
Option "High Availability (HA)"	N/V	VERFÜGBAR Überwacht den Quellrechner und kann die VSB-VM starten, wenn der Quellrechner nicht verfügbar ist.
VM-Leistung	Ausführung ist möglicherweise langsamer im Vergleich zu regulären VMs (bis zu 30 %) aufgrund von E/A-Umleitung, allerdings hängt die Leistung von der Art der Anwendungsarbeitslast ab.	Leistung entspricht der regulärer VMs.
Verwaltung/Konfiguration	Wird von der UDP-Konsole verwaltet, kann die IVM nach Bedarf starten oder anhalten, wenn der Benutzer Zugriff benötigt.	Wird einem Plan als Task hinzugefügt, damit alle gesicherten Daten automatisch in ein VM-Format konvertiert werden. Der VSB-Task wird auf alle Knoten angewendet, die vom Plan geschützt werden.
Beibehalten von Daten und Migrieren der VM in die Produktion	Der virtuelle Datenträger der IVM bezieht sich auf die Datenblöcke im Wiederherstellungspunkt, von dem die VM gestartet wurde. Aus diesem Grund werden beim Zugriff der IVM auf Datenblöcke im virtuellen IVM-Datenträger die Daten tatsächlich von RPS angefordert (dieser Vorgang ist für den Benutzer transparent). Diese E/A-Umleitung hat Aus-	Die virtuellen Datenträger der VSB-VM enthalten bereits die meisten aktuellen Daten vom entsprechenden Wiederherstellungspunkt. Da keine E/A-Umleitung stattfindet (identisch mit IVM), entspricht die Leistung der VSB-VM der regulärer VMs, bei denen keine Abhängigkeit vom RPS oder Wiederherstellungspunkt besteht (verglichen mit dem IVM-Sze-

	wirkungen auf die Leistung. Wenn Sie planen, die IVM in der Produktion zu verwenden, empfehlen wir,die IVM persistent zu machen und den virtuellen Datenträger des virtuellen Rechners mit der eigentlichen Daten zu hydrieren. Die Hydration der IVM kann durch Kopieren/Replizieren der VM erreicht werden. Abhängig von dem in der Produktionsumgebung verwendeten Hypervisor-Typ können Sie VMware Storage vMotion oder Hyper-V VM-Speichermigration/-Replikation verwenden, um die IVM-Daten persistent zu machen, indem Sie die IVM kopieren, auf der die Daten permanent werden.	nario).

Benutzersicherheit

Dieser Abschnitt enthält folgende Themen:

- Rollen für Arcserve UDP-Dienste
- Benutzerrechte für Arcserve UDP-Funktionen

Rollen für Arcserve UDP-Dienste

Die folgende Tabelle beschreibt die Rollen für Arcserve UDP-Dienste:

Dienst	Beschreibung	Ausgeführt auf Rolle
Arcserve-Ereignisprotokollüberwachung	Bietet Lizenzierungs-SDK-Dienst zum Akzeptieren von Lizenzschlüsseln.	Konsole/RPS/Agent
Arcserve UDP Agent-Explorer-Erweiterungsdienst	Bietet Backend-Dienst für UDP-Ansicht im Windows Explorer.	RPS/Agent
Arcserve UDP Agent-Dienst	Bietet Web-Benutzeroberfläche und Webdienst für Arcserve UDP Agent, einschließlich Übergeben von Sicherungs-/Wiederherstellungsjobs.	RPS/Agent
Arcserve UDP-Identitätsdienst	Bietet Authentifizierungs- und Autorisierungsdienst für Arcserve Unified Data Protection-Konsole.	Konsole
Arcserve UDP-Verwaltungsport-Freigabedienst	Bietet Port-Freigabedienst, der es Konsole, Gateway und Identitätsserver erlaubt, einen Port zu teilen.	Konsole
Arcserve UDP-Verwaltungsdienst	Bietet Webdienst für die zentrale Verwaltungskonsole von Arcserve Unified Data Protection.	Konsole
Arcserve Remote Management Gateway-Dienst	Bietet eine Möglichkeit zur bidirektionalen Verarbeitung von Anforderungen zwischen Gateway und Konsole über Intranet oder Internet.	Gateway
Arcserve UDP-RPS-Datenspeicherdienst	Bietet Webdienst für UDP-Datenspeicherverwaltung, einschließlich Erstellen, Ändern, Löschen, Starten und Stoppen.	RPS
Arcserve UDP-RPS-Port-Freigabedienst	Zeigt nur einen Port für den RPS-Server zur Verarbeitung von Kommunikation mit Agent-Web-Benutzeroberfläche/-Dienst, RPS-Webdienst und Replikationsjob an.	RPS
Arcserve UDP-Aktualisierungsdienst	Erkennt Arcserve UDP-Aktualisierung und lädt sie herunter, wenn sie verfügbar ist.	Konsole/RPS/Agent

Benutzerrechte für Arcserve UDP-Funktionen

Die folgende Tabelle beschreibt die Benutzerrechte für Arcserve UDP-Funktionen:

Funktionen	Benutzer	Recht	Kommentare
Installation	**Lokale Administratorengruppe**	**Lokale Administratorengruppe**	
Konsole und Gateway	**Lokale Administratorengruppe**	**Lokale Administratorengruppe**	
Recovery Point Server	**Lokale Administratorengruppe**	**Lokale Administratorengruppe**	
Windows-Client-Sicherung	**Lokale Administratorengruppe**	**Lokale Administratorengruppe** Sicherheitsrichtlinien: • Als Teil des Betriebssystems handeln • Lokal anmelden • Als Dienst anmelden • Als Batch-Job anmelden	**Für viele sicherungsbezogene Vorgänge wie VSS-Snapshot sind Administratorrechte erforderlich.**
Netzwerkfreigabe für Datenspeicher ohne Deduplizierung	Bei aktivierter RPS UAC Domänenkonto oder integrierter Administrator.		
SQL-Protokollkürzung	Lokale Administratorengruppe	Lokaler Administrator mit SQL Systemadministrator oder feste Datenbankrolle Db_owner.	Die Protokollkürzung erfordert die Abfrage von Backup-Datenbank, Rückstandprotokoll sowie eine Verkleinerungsabfrage (Datenbank).
Exchange-Protokollkürzung	Domänenadministratorengruppe	Domänenadministratorengruppe	Benötigt Zugriff auf Exchange-DB.
Active Directory-Schutz	Domänenadministratorengruppe	Domänenadministratorengruppe	

Windows-Client-Wiederherstellung			
Netzwerkfreigabe für Datenspeicher ohne Deduplizierung	Bei aktivierter RPS UAC Domänenkonto oder integrierter Administrator.		
SQL	Lokale Administratorengruppe	Lokaler Administrator mit SQL Systemadministrator oder feste Datenbankrolle Db_owner.	
Exchange	Domänenadministratorengruppe	Domänenadministratorengruppe	Benötigt Zugriff auf Exchange-DB.
Active Directory	Domänenadministratorengruppe	Domänenadministratorengruppe	
Hilfsprogramm zur spezifischen Wiederherstellung von Exchange-Objekten	Wiederherstellen in Postfach: das Konto, das für die Wiederherstellung verwendet wird, sollte für das Zielpostfach über die Berechtigung zum Identitätswechsel verfügen. Für andere Wiederherstellungsoptionen ist für das Konto keine spezielle Anforderung erforderlich.	Wiederherstellen in Postfach: das Konto, das für die Wiederherstellung verwendet wird, sollte für das Zielpostfach über die Berechtigung zum Identitätswechsel verfügen. Für andere Wiederherstellungsoptionen bestehen keine besondere Anforderungen für das Konto.	
Hostbasierte agentenlose Sicherung			
Hinzufügen eines VM-Knotens aus vCenter/ESXi	• vCenter: integrierter Administrator • ESXi: root		Für vCenter: Wenn nicht-integrierter Administrator verwendet wird, nutzen Sie die Informationen unter diesem Link.
Hinzufügen eines VM-Knoten von Nutanix AHV	Cluster-Administrator oder Benutzer-Administrator	Cluster-Administrator oder Benutzer-Administrator	
Hinzufügen eines VM-Knotens aus Hyper-V	• Eigenständiger Hyper-V: integrierter lokaler		Wenn ein anderes Admin-Konto verwendet wird,

	Administrator, integrierter Domänenadministrator oder Domänenkonto, das Mitglied der lokalen Administratorengruppe ist • Hyper-V-Cluster: integrierter Domänenadministrator oder Domänenkonto, das Mitglied der lokalen Administratorengruppe ist.		muss der Remote-Zugriff auf UAC deaktiviert werden. Weitere Details finden Sie unter diesem link.
Ändern der Stilllegungsmethode für VMware-Snapshots im Plan	Integrierter lokaler Administrator oder integrierter Domänenadministrator **Hinweis:** Hier erforderliche Anmeldeinformationen werden von "Knoten aktualisieren" festgelegt		Wenn ein anderes Admin-Konto verwendet wird, muss UAC deaktiviert werden. Weitere Details finden Sie unter diesem link.
Wiederherstellung der Anwendungs-DB-Ebene für Hyper-V VM/Nutanix VM	Integrierter lokaler Administrator, integrierter Domänenadministrator oder Domänenkonto, das Mitglied der lokalen Administratorengruppe ist **Hinweise:** • Hier erforderliche Anmeldeinformationen werden von "Knoten aktualisieren" festgelegt • Wenn VM-Gast-BS Clientversion-Windows (z. B.		Wenn ein anderes Admin-Konto verwendet wird, muss der Remote-Zugriff auf UAC deaktiviert werden. Weitere Details finden Sie unter diesem link.

	Windows 10) ist, muss Firewall manuell so konfiguriert werden, dass Aktivieren Sie die Windows-Verwaltungsinstrumentation (WMI) zugelassen wird		
PFC	• VMware-VM: integrierter lokaler Administrator oder integrierter Domänenadministrator • Hyper-V-VM: integrierter lokaler Administrator, integrierter Domänenadministrator oder Domänenkonto, das Mitglied der lokalen Administratorengruppe ist • Nutanix VM: eingebauter lokaler Administrator, eingebauter Domänenadministrator oder Domänenkonto, das Mitglied der lokalen Administratorengruppe ist. **Hinweise:** • Hier erforderliche Anmeld-		Wenn ein anderes Admin-Konto verwendet wird: • Bei VMware-VM muss UAC deaktiviert werden. Siehe dazu diesen Link. • Für Hyper-V-VM muss der Remote-Zugriff auf UAC deaktiviert werden. Siehe dazu diesen Link.

	einformationen werden von "Knoten aktualisieren" festgelegt • Für Hyper-V VM/Nutanix VM, wenn VM-Gastbetriebssystem Client-Version Windows (wie Windows 10) ist, müssen Sie die Firewall manuell konfigurieren, um Windows Management Instrumentation (WMI) zu ermöglichen.		
Prä-/Post-Befehl	• VMware-VM: integrierter lokaler Administrator oder integrierter Domänenadministrator • Hyper-V-VM: integrierter lokaler Administrator, integrierter Domänenadministrator oder Domänenkonto, das Mitglied der lokalen Administratorengruppe ist • Nutanix VM: eingebauter lokaler Administrator, eingebauter Domänenadministrator oder Domänenkonto, das Mitglied der lokalen Administratorengruppe		Informationen zur Verwendung der Anmeldeinformationen, die von "Knoten aktualisieren" und auf der Registerkarte "Erweitert" eines Plans festgelegt werden, finden Sie unter diesem Link.

	ist. **Hinweise:** • Hier erforderliche Anmeldeinformationen werden von "Knoten aktualisieren" und auf der Registerkarte "Erweitert" eines Plans festgelegt. • Wenn bei einer Hyper-V-VM das VM-Gast-BS Clientversion-Windows (z. B. Windows 10) ist, muss Firewall manuell so konfiguriert werden, dass Aktivieren Sie die Windows-Verwaltungsinstrumentation (WMI) zugelassen wird • Wenn es sich bei Hyper-V VM/Nutanix VM um ein Client-Version Windows handelt (z.B. Windows 10), konfigurieren Sie die Firewall manuell so, dass sie Windows Management Instrumentation (WMI) erlaubt.		
SQL-Pro-	Gleich wie Prä-/Post-		Gleich wie Prä-

tokollkürzung	Befehl		/Post-Befehl
Exchange-Pro-tokollkürzung	Gleich wie Prä-/Post-Befehl		Gleich wie Prä-/Post-Befehl
Wiederherstellung auf Dateiebene am ursprünglichen Speicherort	Integrierter lokaler Administrator, integrierter Domänenadministrator oder Domänenkonto, das Mitglied der lokalen Administratorengruppe ist **Hinweise:** • Hier erforderliche Anmeldeinformationen werden von "Knoten aktualisieren" festgelegt • Für Hyper-V VM/Nutanix VM, wenn VM-Gastbetriebssystem Client-Version Windows (wie Windows 10) ist, müssen Sie die Firewall manuell konfigurieren, um Windows Management Instrumentation (WMI) zu ermöglichen.		Wenn ein anderes Admin-Konto verwendet wird, muss der Remote-Zugriff auf UAC wie in diesem Link deaktiviert werden.
Virtual Standby			
Für Hyper-V	• Integrierter lokaler Administrator • Integrierter Domänenadministrator • Domänenkonto, das Mitglied der lokalen Administratorengruppe ist • Lokales Konto, das Mitglied der lokalen Admi-	Lokale Administratorengruppe	Wenn ein lokales Admin-Konto verwendet wird, muss der Remote-Zugriff auf UAC deaktiviert werden. Siehe dazu diesen Link.

	nistratorengruppe ist		
Für Nutanix	Cluster-Administrator	Cluster-Administrator	
Für VMware	• vCenter: integrierter Administrator • ESXi: root		Für vCenter: Wenn nicht-integrierter Administrator verwendet wird, nutzen Sie die Informationen unter diesem Link.
Instant VM/Assured Recovery			
Für Hyper-V	• Integrierter lokaler Administrator • Integrierter Domänenadministrator • Domänenkonto, das Mitglied der lokalen Administratorengruppe ist • Lokales Konto, das Mitglied der lokalen Administratorengruppe ist		Wenn ein lokales Admin-Konto verwendet wird, muss der Remote-Zugriff auf UAC deaktiviert werden. Siehe dazu diesen Link.
Für VMware	• vCenter: integrierter Administrator • ESXi: root	Lokale Administratorengruppe	Für vCenter: Wenn nicht-integrierter Administrator verwendet wird, nutzen Sie die Informationen unter diesem Link.
Dateikopie und -archivierung	**Lokale Administratorengruppe**	**Lokale Administratorengruppe**	
Wiederherstellungspunkte in die Cloud kopieren	**Lokale Administratorengruppe**	**Lokale Administratorengruppe**	

UNC/NFS-Pfad-schutz	**Jeder Benutzer könnte sich anmelden und imitiert werden.**	**Leseberechtigung für den UNC/NFS-Pfad**	
Virtual Standby für AWS EC2	**Die Amazon IAM-Benutzer, die über die erforderlichen Berechtigungen für die Interaktion mit der AWS-API verfügen**		Informationen zu AWS EC2 finden Sie unter diesem Link.
Virtual StandBy für Microsoft Azure	**Anwendung**	**Beitragendenrolle des ausgewählten Abonnements**	
Linux			
Installieren von	Root	Lesen, Schreiben, Ausführen	
Konsolenregistrierung	Konsolenadministrator		
agentenbasierte Sicherung			
-Netzwerkfreigabe	Speicheradministrator	Lesen, Schreiben	
--Knotenverbindung	Root/Nicht-Root/Sudo	Lesen, Schreiben, Ausführen	
Wiederherstellung auf Dateiebene			
-Netzwerkfreigabe	Speicheradministrator	Lesen, Schreiben	
--Knotenverbindung	Root/Nicht-Root/Sudo	Lesen, Schreiben, Ausführen	Root-Benutzer können an einen beliebigen Ort wiederherstellen; andere Benutzer können nur auf die eigenen Verzeichnisse wiederherstellen.
BMR		Zugreifen auf Informationen zu Hardware	
Migrations-BMR			
Instant VM für Hyper-V			
Instant VM für VMware			
Instant-VM für Nutanix AHV	Cluster-Administrator	Cluster-Administrator	

Instant VM für Amazon EC2	IAM-Benutzer	Vollzugriff auf EC2	
Instant VM für Microsoft Azure	Anwendung	Beitragendenrolle des ausgewählten Abonnements	
Exchange Online-Schutz	Jedes Exchange Online-Konto	Verfügt über die Berechtigung "Application Impersonation" (Anwendungs-Identitätswechsel) auf den geschützten Konten	
SharePoint Online-Schutz	SharePoint Online-Website-sammlungsadministrator	SharePoint Online-Website-sammlungsadministrator	
OneDrive	Azure Active Directory-Administratoren	Azure Active Directory-Administratoren	

Kapitel 3: Installieren von Arcserve UDP

Dieser Abschnitt enthält folgende Themen:

Installieren von Arcserve UDP

Arcserve UDP - Vollversion: Nach der Installation melden Sie sich bei der Arcserve UDP-Konsole (Konsole) an und führen die Funktionen für die Datenverwaltung aus. Mit der Konsole können Sie Überwachungsserverknoten, Recovery Point Server, Sicherungen, Wiederherstellungen und Replikationen überwachen und verwalten.

Arcserve UDP - Agent: Installiert nur den Arcserve UDPAgenten. Installieren Sie den Agenten auf den Knoten, die Sie schützen möchten. Führen Sie diesen Schritt nur aus, wenn Sie den Agenten manuell auf einem Knoten installieren möchten. Normalerweise wird der Agent bei der Erstellung von Plänen über die Konsole automatisch für Knoten bereitgestellt.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Bestimmen der Installationsart
3. Installieren von Arcserve Unified Data Protection mit dem Setup-Assistenten
4. Installieren von Arcserve Unified Data Protection über die Befehlszeile
5. Installieren von Arcserve Unified Data Protection mit dem einheitlichen Installationsprogramm
6. Überprüfen der Installation
7. (Optional) Verwendete Kommunikationsports
8. (Optional) Auswirkungen des Installationsprozesses auf das Betriebssystem

Überprüfen der Voraussetzungen und Hinweise

Überprüfen Sie die folgenden Voraussetzungen und Hinweise, bevor Sie Arcserve UDP installieren:

Voraussetzungen

- Lesen Sie die Arcserve UDP Release Hinweise 8.0. Die Versionshinweise enthalten eine Beschreibung der Systemanforderungen, unterstützte Betriebssysteme und eine Liste der Probleme, die in dieser Version bekannt sind.
- Stellen Sie sicher, dass Ihr System die Software- und Hardwarevoraussetzungen, die für die Installation der Komponenten von Arcserve Unified Data Protection erforderlich sind, erfüllt.
- Stellen Sie sicher, dass Sie über Administratorrechte oder eine gleichwertige Berechtigung zum Installieren von Software auf den Systemen, auf denen Sie Komponenten von Arcserve Unified Data Protection installieren möchten, verfügen.
- Stellen Sie sicher, dass Sie die Benutzernamen und Kennwörter der Computer kennen, auf denen Sie Komponenten von Arcserve Unified Data Protection installieren.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Hinweise

Vor der Installation sollten Sie entscheiden, wie Sie Ihre Arcserve Unified Data Protection-Installation einrichten möchten:

- das System, auf dem Sie die Konsole installieren möchten
- die Knoten, die Sie schützen möchten
- die Anzahl der Recovery Point Server, die als Sicherungsziel eingesetzt werden sollen
- die Anzahl von Replikatservern, die Recovery Point Server replizieren sollen

Bestimmen der Installationsart

Sie können Arcserve UDP unter Verwendung einer der folgenden Vorgangsweisen installieren:

- **Standardinstallation mit dem Setup-Assistenten:** Mit dieser Methode können Sie Arcserve Unified Data Protection mit dem Setup-Assistenten installieren. Bei dieser Methode werden Sie bei jedem Schritt aufgefordert, die gewünschten Optionen auszuwählen.
- **Automatische Installation über die Befehlszeile:** Mit dieser Methode können Sie eine unbeaufsichtigte Installation über die Windows-Befehlszeile ausführen.
- **Installation mit dem einheitlichen Installationsprogramm:** Dieser Methode lässt Sie Arcserve UDP, Arcserve Backup, und Arcserve RHA aus einem einzelnen Installationsprogramm installieren. Sie können alle drei Produkte gleichzeitig installieren oder jedes Produkt separat installieren. Sie können das Installationsprogramm von der Arcserve-Website herunterladen.

Installieren von Arcserve Unified Data Protection mit dem Setup-Assistenten

Mit Arcserve Unified Data Protection können Sie Knoten, Recovery Point Server, virtuelle Rechner auf vCenter-, ESX- oder Microsoft Hyper-V-Servern, Replikatserver und Arcserve Unified Data Protection-Berichte zentral verwalten und überwachen.

Installieren Sie Arcserve Unified Data Protection auf einem Server, über den Sie geschützte Knoten und andere Arcserve Unified Data Protection-Komponenten verwalten können.

Gehen Sie wie folgt vor:

1. Greifen Sie über die Arcserve-Website oder die Produkt-CD auf das Installationspaket für Arcserve UDP zu.

   Hinweis: Wenn eines der unterstützten nicht englischen Betriebssysteme erkannt wird, müssen Sie die Sprache für die Produktinstallation auswählen.

2. Doppelklicken Sie auf das Installationspaket.

   Das Dialogfeld **Lizenzvereinbarung** wird geöffnet.

3. Lesen und akzeptieren Sie die Bedingungen der Lizenzvereinbarung, und klicken Sie auf **Weiter**.

   Das Dialogfeld **Installationstyp** wird geöffnet.

4. Wählen Sie einen Installationstyp aus.

   Standardinstallation

   Mit diesem Typ können Sie entweder nur den Agent oder alle Arcserve Unified Data Protection-Komponenten installieren.

   Arcserve Unified Data Protection-Agent

   Installiert nur Arcserve UDP-Agent.

   Weitere Informationen finden Sie unter *Installieren von Arcserve Unified Data Protection Agent für Windows mithilfe des Installationsassistenten* im *Benutzerhandbuch zum Arcserve UDP-Agent für Windows*.

   Arcserve Unified Data Protection- Vollständige Sicherung

   Installiert Arcserve Unified Data Protection-Konsole, -Recovery Point Server und -Agent.

   Erweiterte Installation

   Mit diesem Typ können Sie eine oder mehrere der folgenden Arcserve Unified Data Protection-Komponenten installieren:

- Arcserve UDP Agent
- Arcserve UDP-Recovery Point Server
- Arcserve UDP Console

5. Legen Sie fest, ob Sie den Treiber zur Änderungsnachverfolgung von Arcserve Unified Data Protection Agent für Windows installieren wollen.

   Standardmäßig ist diese Option aktiviert.

   - Wenn dieser Treiber nicht installiert ist, führt Arcserve Unified Data Protection Agent für Windows immer eine vollständige Sicherung durch.
   - Wenn dieser Treiber installiert ist, benötigen Sie eine gültige Lizenz für Arcserve Unified Data Protection Agent für Windows, um eine lokale Sicherung durchzuführen.
   - Dieser Treiber ist nicht erforderlich, wenn dieser Agent als Virtual Standby-Überwachungsserver oder als Proxy-Server für die hostbasierte VM-Sicherung verwendet wird.

     Hinweis: Sie können diesen Treiber jederzeit nach abgeschlossener Installation installieren, indem Sie das Hilfsprogramm "InstallDriver.bat" unter folgendem Speicherort ausführen:

     <Arcserve UDP-Installationsverzeichnis> \Engine\BIN\DRIVER

6. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Zielordner** wird geöffnet.

7. Geben Sie den Ordner an, in dem Sie Arcserve Unified Data Protection installieren möchten, und klicken Sie auf **Weiter**.

   Das Dialogfeld **Konfiguration** wird geöffnet.

8. Geben Sie im Dialogfeld **Konfiguration** folgende Informationen an:

   a. Wählen Sie das Protokoll aus.

      Hinweis: Wählen Sie für sichere Kommunikation das HTTPS-Protokoll aus.

   b. Geben Sie ggf. die Portnummer für den Agenten ein. Die Portnummer lautet standardmäßig 8014.

   c. Geben Sie ggf. die Portnummer für die Konsole ein. Die Portnummer lautet standardmäßig 8015.

   d. Geben Sie den Namen des Windows-Administrators und das Kennwort ein.

   e. Geben Sie an, ob der Überwachungsserver von Arcserve UDP Agent für alle Benutzer oder nur für den aktuellen Benutzer angezeigt werden soll.

9. Klicken Sie auf **Weiter**.

Das Dialogfeld **Datenbankeinstellungen** wird geöffnet.

10. Klicken Sie im Dialogfeld **Datenbankeinstellungen** auf die Drop-down-Liste **Datenbank**, um einen Datenbanktyp auszuwählen. Sie können eine der folgenden Angaben verwenden:

    - Microsoft SQL Server 2014 Express (eingeschlossen)
    - Microsoft SQL Server

      Wichtig! Wenn mehr als 500 Knoten von der Konsole verwaltet werden sollen, stellen Sie sicher, dass Sie Microsoft SQL Server und nicht SQL Express auswählen.

    Nachdem Sie einen Datenbanktyp angegeben haben, werden die erforderlichen Optionen für die angegebene Datenbank im Dialogfeld **Datenbankeinstellungen** angezeigt. Geben Sie Details zu den Datenbankeinstellungen für eine der Datenbanken, die Sie ausgewählt haben, an.

    Microsoft SQL Server 2014 Express (eingeschlossen):

    Führen Sie im Dialogfeld **Datenbankeinstellungen** folgende Schritte aus:

    a. Geben Sie den Speicherort an, an dem Sie Microsoft SQL Server 2014 Express installieren möchten. Sie können den Standardpfad übernehmen oder einen anderen Pfad angeben.

    b. Geben Sie den Speicherort an, an dem Sie die Datendatei von Arcserve Unified Data Protection installieren möchten. Sie können den Standardpfad übernehmen oder einen anderen Pfad angeben.

       Hinweis: Microsoft SQL Server 2014 Express unterstützt keine Remote-Kommunikation. Installieren Sie daher die Standarddatenbank und die Datendatei auf dem Computer, auf dem Sie die Anwendung installieren.

    Microsoft SQL Server-Datenbanken

    Führen Sie im Dialogfeld **Datenbankeinstellungen** folgende Schritte aus:

    a. **SQL Server-Typ**: Geben Sie die Art der Kommunikation an, die von der Anwendung verwendet werden soll, um mit der SQL Server-Datenbank zu kommunizieren.

       Lokal: Geben Sie "Lokal" an, wenn Anwendung und SQL Server auf demselben Computer installiert sind.

       Remote: Geben Sie "Remote" an, wenn Anwendung und SQL Server auf unterschiedlichen Computern installiert sind.

    b. **SQL Server-Name**: Wenn der SQL Server-Typ "Remote" ist, geben Sie den Namen des Remote-SQL-Servers an. Wenn der SQL Server lokal verwendet

wird, wählen Sie den Server aus der Drop-down-Liste aus.

c. **Sicherheit**: Geben Sie die Art der Anmeldeinformationen an, mit denen Sie die SQL Server-Authentifizierung abwickeln möchten.

Windows-Sicherheit verwenden: Die Authentifizierung wird mit Ihren Windows-Anmeldeinformationen durchgeführt. Sie können sich mit Anmeldeinformationen für die Arcserve UDP-Konsole anmelden.

SQL Server-Sicherheit verwenden: Die Authentifizierung wird mit Ihren SQL Server-Anmeldeinformationen durchgeführt. Geben Sie die Anmelde-ID und das Kennwort für das SQL Server-Konto an.

11. Klicken Sie auf **Weiter**. Das Dialogfeld **Firewall-Ausnahmen** wird geöffnet.

Im Dialogfeld **Firewall-Ausnahmen** werden die Dienste und Programme aufgelistet, die für die Windows-Firewall als Ausnahmen für Arcserve UDP registriert werden sollen.

Hinweis: Firewall-Ausnahmen sind erforderlich, wenn Sie Arcserve UDP von Remote-Rechnern aus konfigurieren und verwalten möchten.

12. Klicken Sie auf **Weiter**. Das Dialogfeld **Meldungen** wird geöffnet.

13. Klicken Sie auf **Weiter**. Das Dialogfeld **Zusammenfassung** wird geöffnet.

14. Klicken Sie auf **Installieren**, um den Installationsvorgang zu starten.

Im Dialogfeld **Fortschritt der Installation** wird der Fortschritt der Installation angezeigt. Nach Abschluss der Installation wird das Dialogfeld **Installationsbericht** angezeigt.

(Optional) Wenn Sie die aktuellsten Produktaktualisierungen überprüfen möchten, führen Sie diese Schritte aus:

a. Wählen Sie **Sofort auf Aktualisierung überprüfen** aus, und klicken Sie auf **Fertig stellen**.

Das Dialogfeld **Nach Aktualisierungen suchen** wird geöffnet.

b. Wählen Sie den Server aus, von dem Sie Aktualisierungen herunterladen möchten, und klicken Sie auf **Aktualisierungen herunterladen und installieren**.

Im Dialogfeld **Prozess aktualisieren** wird der Download-Status angezeigt.

Wenn die Aktualisierung abgeschlossen ist, wird eine Warnmeldung angezeigt.

(Optional) Um Arcserve UDP Agent for Linux zu installieren, befolgen Sie die Anweisung im Abschnitt zum **Installieren des Arcserve Unified Data Protection Agent for Linux**.

15. Klicken Sie auf **Fertig stellen**.

    Arcserve UDP ist auf Ihrem Computer installiert.

Installieren von Arcserve Unified Data Protection über die Befehlszeile

Sie können Arcserve Unified Data Protection automatisch installieren. Bei der automatischen Installation ist kein Benutzereingriff erforderlich. Die folgenden Schritte beschreiben, wie Sie die Anwendung über die Windows-Befehlszeile automatisch installieren können:

Gehen Sie wie folgt vor:

1. Öffnen Sie die Windows-Befehlszeile auf dem Computer, auf dem Sie den automatischen Installationsvorgang starten wollen.
2. Laden Sie das selbstextrahierende Installationspaket auf Ihren Computer herunter.

   Starten Sie den automatischen Installationsvorgang mithilfe der folgenden Befehlszeilen-Syntax:

   Arcserve_Unified_Data_Protection.exe -s -a -q -Products:<ProductList> -Path:<INSTALLDIR> -User:<UserName> -Password:<Password> -Https:<HTTPS> -ConsolePort:<Port Number> -AgentPort:<Port Number> -Driver:<DRIVER> -MonitorFlag:<MONITORFLAG> -StopUA:<STOPUA> -SummaryPath:<SUMMARYPATH> -AutoReboot:<AUTOREBOOT>

   Beispiel:

   Arcserve_Unified_Data_Protection.exe -s -a -q -Products:Agent -User:administrator -Password:test
3. Konfigurieren Sie die automatische Installation mithilfe folgender Syntax und Argumente:

   Wichtig: Wenn Parameter folgende Sonderzeichen enthalten, schließen Sie diese in Anführungszeichen ein:

   - <Leerzeichen>
   - &()[]{}^=;!'+,`~

   Beispiel: Die Eingabe für das Kennwort abc^*123 sollte folgendermaßen aussehen: -Password:"abc^*123".

   -s

   Führt das Paket mit der ausführbaren Datei im automatischen Modus aus.

   -a

   Gibt zusätzliche Befehlszeilenoptionen an.

   -q

   Installiert die Anwendung im automatischen Modus.

-Products:<Produktliste>

(Optional) Gibt die Komponenten an, die automatisch installiert werden sollen. Wenn Sie keinen Wert für dieses Argument angeben, installiert der automatische Installationsvorgang alle Komponenten. Sie können die folgenden Komponenten angeben:

Agent: Installiert die Komponente "Data Protection Agent".

RPS: Installiert die Komponente "Recovery Point Server".

Konsole: Installiert die Komponente "Console".

Alle: Installiert alle Komponenten von Arcserve Unified Data Protection.

Beispiel:

Für die Installation von Data Protection Agent:

-Products:Agent

Für die Installation von Recovery Point Server:

-Products:Agent,RPS

Für die Installation von Data Protection Agent, Recovery Point Server und Data Protection Console:

-Products:Agent,RPS,Console

Für die Installation aller Komponenten im Build:

-Products:All

-User:<Benutzername>

Gibt den Benutzernamen an, den Sie verwenden möchten, um die Anwendung zu installieren und auszuführen.

Hinweis: Der Benutzername muss zu einem Administrator oder zu einem Konto mit Administratorrechten gehören.

-Password:<Kennwort>

Gibt das Kennwort für den Benutzernamen an.

-Https:<HTTPS>

(Optional) Gibt das Kommunikationsprotokoll an. Die Optionen sind 0 und 1. Verwenden Sie 0 für HTTP und 1 für HTTPS.
Standard: 0
Beispiel:

-https:1

-Path:<INSTALLATIONSVERZEICHNIS>

(Optional) Gibt den Pfad für das Installationsziel von Data Protection Agent an.
Beispiel:

-Path:C:\Program Files\Arcserve\Unified Data Protection

Hinweis: Wenn der Wert für INSTALLDIR eine Leerstelle enthält, setzen Sie den Pfad in Anführungszeichen. Zudem darf der Pfad nicht mit einem umgekehrten Schrägstrich enden.

-ConsolePort:<Portnummer>

(Optional) Gibt die Nummer des Kommunikationsports für die Konsole an.

Standard: 8015

Beispiel:

-ConsolePort:8015

Hinweis: Verwenden Sie diese Option, wenn Sie die Konsole installieren möchten.

-AgentPort:<Portnummer>

(Optional) Gibt die Nummer des Kommunikationsports für den Zugriff auf Arcserve Unified Data Protection Agent an.

Standard: 8014
Beispiel:

-AgentPort:8014

Hinweis: Verwenden Sie diese Option, wenn Sie Arcserve Unified Data Protection Agent installieren möchten.

-Driver:<TREIBER>

(Optional) Gibt an, ob der Treiber für die Änderungsverfolgung von Arcserve Unified Data Protection Agent installiert werden soll. Die Optionen sind 0 und 1.

0: Der Treiber wird nicht installiert.
1: Der Treiber wird installiert.

Standard: 1
Beispiel:

-driver:1

-MonitorFlag:<ÜBERWACHUNGSSERVER-FLAG>

(Optional) Legt die Anzeige des Arcserve Unified Data Protection Agent-Überwachungsservers für Benutzer fest. Die Optionen sind 0 und 1.

0: Der Agent-Überwachungsserver wird für alle Benutzer angezeigt.
1: Der Agent-Überwachungsserver wird nur für den aktuellen Benutzer angezeigt.

Standard: 0.

Beispiel:

-MonitorFlag:0

-StopUA:< STOPUA >

(Optional) Gibt an, dass der Arcserve Universal Agent-Dienst angehalten werden soll.

0: Der Arcserve Universal Agent-Dienst wird nicht angehalten, wenn er während des Installationsprozesses ausgeführt wird.
1: Der Arcserve Universal Agent-Dienst wird angehalten, wenn er während des Installationsprozesses ausgeführt wird.
Standard: 0

Beispiel:

-StopUA:1

Hinweis: Verwenden Sie diese Option bei Upgrades auf eine neue Version. Stellen Sie sicher, dass Sie den Wert auf 1 setzen oder den Dienst anhalten, bevor Sie den Upgrade-Vorgang starten. Dies trägt dazu bei, den Erfolg der Installation sicherzustellen.

-SummaryPath:<ÜBERSICHTSPFAD>

(Optional) Gibt den Zielpfad an, unter dem die Übersichtsdatei für die Installation generiert werden soll.

Beispiel:

-SummaryPath:C:\Result

Hinweis: Wenn der Wert für INSTALLDIR eine Leerstelle enthält, setzen Sie den Pfad in Anführungszeichen. Zudem darf der Pfad nicht mit einem umgekehrten Schrägstrich enden.

-AutoReboot:<AUTO-NEUSTART>

(Optional) Lässt Setup nach der Installation einen Rechnerneustart durchführen, wenn die Installation einen Neustart erforderlich macht. Die Optionen sind 0 und 1.

0: Es wird kein Rechnerneustart durchgeführt.

1: Wenn die Installation einen Neustart erforderlich macht, wird ein Rechnerneustart durchgeführt.

Standard: 0

Beispiel:

-AutoReboot:1

Hinweis: Wenn die Installation keinen Neustart erfordert, startet Setup den Rechner nicht neu, auch wenn dieser Parameter auf 1 festgelegt ist.

Sie haben die automatische Installation erfolgreich abgeschlossen.

Arcserve UDP mit dem einheitlichen Installationsprogramm installieren

Arcserve UDP ermöglicht es Ihnen, alle Lösungskomponenten über ein einziges, einheitliches Installationsprogramm zu installieren. Je nach Bedarf schlägt das Installationsprogramm die beste Lizenz für Ihre Anforderungen vor, um dann die Komponenten herunterzuladen und zu installieren.

Gehen Sie wie folgt vor:

1. Laden Sie die Datei "ASDownloader" von der Arcserve-Website herunter.

   Hinweis: Wenn eines der unterstützten nicht englischen Betriebssysteme erkannt wird, müssen Sie die Sprache für die Produktinstallation auswählen.

2. Doppelklicken Sie auf das Installationspaket.

   Das Dialogfeld **Lizenzvereinbarung** wird geöffnet.

3. Lesen und akzeptieren Sie die Bedingungen der Lizenzvereinbarung, und klicken Sie auf **Weiter**.

   Das Dialogfeld **Erste Schritte** wird geöffnet.

4. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Komponenten zum Download auswählen** wird geöffnet.

5. Wählen Sie je nach Ihren Anforderungen eine oder mehrere der folgenden Optionen aus, und klicken Sie auf **Weiter**.

   Arcserve Unified Data Protection

   Installiert Arcserve UDP. Mit Arcserve UDP können Sie physische und virtuelle Windows- und Linux-Knoten schützen. Sie können alle Ihre Datensicherungsanforderungen mithilfe einer einzigen Konsole verwalten. Für die Verwaltung Ihrer Daten können Sie die globale quellseitige Deduplizierung, Replikation, Remote-Replikation und andere Funktionen verwenden.

   Arcserve Backup

   Installiert von Arcserve Backup. In Verbindung mit Arcserve UDP können Sie die Bandsicherung über die Arcserve UDP-Konsole verwalten und alle Vorteile von Arcserve UDP nutzen.

   Das Dialogfeld **Produkt-Download** wird geöffnet.

6. Klicken Sie auf **Download**.

   Der Download startet. Das Produkt wird im ZIP-Format heruntergeladen. Sie können den Download-Status in der Statusleiste überprüfen. Sie können den Download

auch unterbrechen und später fortsetzen. Je nach Bandbreite und Anzahl an Komponenten für den Download kann dies eine Weile dauern

Die Schaltfläche "Weiter" ist bis zum Abschluss des Downloads inaktiv.

7. Wenn der Download abgeschlossen ist, klicken Sie auf **Weiter**.

   Das Dialogfeld **Installationsmethode** wird geöffnet.

8. Wählen Sie einen Installationstyp aus.

   Express-Installation

   Installiert die Komponenten anhand der Standardkonfiguration. Klicken Sie auf **Standardkonfiguration und Komponenten anzeigen**, um die installierten Komponenten anzuzeigen.

   Erweiterte Installation

   Ermöglicht die separate Installation der einzelnen Komponenten.

9. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Kontokonfiguration** wird geöffnet.

10. Geben Sie den Benutzernamen und das Kennwort ein, und klicken Sie auf **Installieren**.

    Die Installation wird gestartet. Der Fortschritt wird im Dialogfeld angezeigt. Schließen Sie nach Abschluss der Installation den Assistenten.

    Arcserve UDP ist auf Ihrem Computer installiert.

Überprüfen der Installation

Gehen Sie wie folgt vor:

1. Überprüfen Sie, ob das Arcserve UDP-Symbol in der Taskleiste angezeigt wird.
2. Überprüfen Sie im Windows-Dienst-Manager, ob die Agent- und Serverdienste aktiviert sind und ausgeführt werden.

   Sie haben Arcserve Unified Data Protection erfolgreich installiert und können Ihren Windows-Rechner nun sichern.

Von Arcserve UDP verwendete Kommunikationsports

Dieser Abschnitt enthält Informationen zu Ports, die für die folgenden Komponenten verwendet werden:

- Unter Microsoft Windows installierte Komponenten
- Unter Linux installierte Komponenten
- Auf dem Hypervisor installierte Komponenten

Die aufgelisteten Ports sind für Sicherungs- und andere Jobs in LAN-Umgebungen erforderlich.

* Die gemeinsame Nutzung von Ports wird für Replikationsjobs unterstützt. Alle Daten auf anderen Ports können an Port 8014 weitergeleitet werden (dies ist der Standardport für den UDP-Server; er kann während der Installation geändert werden). Für Replikationsjobs zwischen zwei Recovery Point Servern über WAN muss nur Port 8014 geöffnet sein.

Für Remote-Replikation muss der Remote-Administrator Port 8014 (für die zu replizierenden Daten) und Port 8015 (Standardport für den UDP-Server, kann während der Installation geändert werden) öffnen bzw. Daten an diese Ports weiterleiten, damit der Replikationsplan zu lokalen Recovery Point Servern gelangt.

Unter Microsoft Windows installierte Komponenten

Dieser Abschnitt enthält Informationen zu Ports, die in UDP Console und UDP Recovery Point Server (RPS) verwendet werden:

- UDP-Konsole
- UDP Recovery Point Server (RPS)
- UDP Windows Agent

UDP-Konsole

In der folgenden Tabelle sind die von der Arcserve UDP-Konsole verwendeten Ports aufgelistet:

Portnummer	Porttyp	Initiiert von	Abhörprozess	Interner/externer Port	Beschreibung
1433	TCP	Remote-Java	sqlsvr.exe	Extern	Standardmäßiger Port für die Kommunikation zwischen der UDP-Konsole und Microsoft SQL Server-Datenbanken, wenn sie sich auf unterschiedlichen Computern befinden **Hinweis:** Sie können den standardmäßigen Kommunikationsport während der Installation von SQL Server ändern.
6052	TCP	Arcserve Backup Global Dashboard	Arcserve.CommunicationFoundation.WindowsService.exe	Extern	Kommunikation für die Synchronisierung von Daten zwischen der UDP-Konsole und dem Primärserver von Arcserve

					Backup Global Dashboard **Hinweis:** Dieser Port wird nur benötigt, wenn Sie Arcserve Backup Global Dashboard-Daten mit der UDP-Konsole synchronisieren möchten.
6054	TCP	Arcserve Backup-Primärserver	Arcserve.CommunicationFoundation.WindowsService.exe	Extern	Kommunikation für die Synchronisierung von Daten zwischen der Konsole und dem Primärserver von Arcserve Backup **Hinweis:** Dieser Port wird nur benötigt, wenn Sie Arcserve Backup Global Dashboard-Daten mit der UDP-Konsole synchronisieren möchten.
8012	TCP	UDP-Konsole	java.exe	Intern	Port, der standardmäßig intern vom Identitätsdienst der UDP-Konsole verwendet wird **Hinweis:** Der Port konnte

					nicht angepasst werden und kann für die Firewall-Einstellung ignoriert werden. Wenn 8012 durch andere Programme belegt ist, weist das UDP-Setup-Programm dynamisch einen anderen verfügbaren Port zu.
8015	TCP	UDP-Konsole UDP-Gateway	httpd.exe	Extern	Standardmäßiger Port für HTTP/HTTPS-Kommunikation, um die UDP-Konsole und das UDP-Gateway abzurufen **Hinweis:** Sie können den standardmäßigen Kommunikationsport während der Installation der UDP-Komponenten ändern.
8029	TCP	UDP-Konsole	tomcat9.exe	Intern	Port, der standardmäßig intern vom Ver-

					wal-tungsdienst der UDP-Kon-sole ver-wendet wird **Hinweis:** Der Port konnte nicht ange-passt werden und kann für die Firewall-Einstellung ignoriert wer-den. Wenn 8029 durch andere Pro-gramme belegt ist, weist das UDP-Setup-Programm dynamisch einen anderen verfügbaren Port zu.
8030	TCP	UDP-Konsole	tomcat9.exe	Intern	Port, der stan-dardmäßig intern vom Ver-wal-tungsdienst der UDP-Kon-sole ver-wendet wird **Hinweis:** Der Port konnte nicht ange-passt werden und kann für die Firewall-Einstellung ignoriert wer-den. Wenn 8030 durch

					andere Programme belegt ist, weist das UDP-Setup-Programm dynamisch einen anderen verfügbaren Port zu.
18007	TCP	TOMCAT	tomcat9.exe	Intern	Intern verwendet vom Tomcat-Verwaltungsdienst. **Hinweis:** Dieser Port kann nur durch Ändern von TOMCAT-Konfigurationsdateien geändert werden. Der Port kann bei der Firewall-Einstellung ignoriert werden.

UDP Recovery Point Server (RPS)

In der folgenden Tabelle sind die von Arcserve UDP Recovery Point Server (RPS) verwendeten Ports aufgelistet:

Portnummer	Porttyp	Initiiert von	Abhörprozess	Interner/externer Port	Beschreibung
8014	TCP	UDP	httpd.exe	Extern	Standardmäßiger Port für HTTP/HTTPS-Kommunikation, um den UDP-RPS und UDP-Agenten abzurufen **Hinweise:** ■ Dieser Port ist der standardmäßige gemeinsam genutzte Port und der einzige Port, den Sie öffnen müssen, wenn Sie den UDP-RPS als Replikationsziel verwenden. Öffnen Sie Portnummer 5000–5060 nicht; diese werden von Datenspeichern mit aktivierter globaler Deduplizierung verwendet. ■ Sie können den standardmäßigen Kommunikationsport während der Installation der UDP-Komponenten ändern.
8016	TCP	UDP	tomcat9.exe	Intern	Intern von den UDP RPS-Webdiensten für die Kommunikation mit dem UDP RPS-Portfreigabedienst auf demselben Server verwendet. **Hinweis:** Der Port konnte nicht angepasst werden und kann für die Firewall-Einstellung ignoriert werden.
5000-5060	TCP	UDP	GDDServer.exe	Intern	Dieser Portbereich ist für UDP RPS-Datenspeicherdienst reserviert. Ein UDP RPS-Deduplizierungsdatenspeicher verwendet vier freie Ports, und ein Nicht-Dedu-

					plizierungsdatenspeicher verwendet einen freien Port. Beide beginnen bei 5000. Sie werden benötigt, wenn Daten bei der Sicherung und Wiederherstellung verarbeitet werden. Wenn Sie RPS nur als Replikationsziel verwenden, ist ein Öffnen in der Firewall-Konfiguration nicht erforderlich. **Hinweis:** Ändern Sie Folgendes, um den Portbereich in der Registrierung anzupassen: ■ HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore ■ Schlüsselname: PortRangeForGDD ■ Typ: Reg_SZ ■ Standardwert: 5000-5060 Nur Datenspeicher, die nach der Änderung der Registrierung erstellt wurden, verwenden den geänderten Portbereich.
18005	TCP	TOMCAT	tomcat9.exe	Intern	Zum Herunterfahren des vom UDP-RPS oder -Agent verwendeten Tomcat-Servers **Hinweis:** Dieser Port kann nur durch Ändern von TOMCAT-Konfigurationsdateien geändert werden. Der Port kann bei der Firewall-Einstellung ignoriert werden.
7788	TCP	UDP	Sync_util_d.exe	Intern	HTTP/HTTPS-Standardkommunikationsport, um Replikation in Anfragen zu akzeptieren.
445	TCP			Extern	Wird vom SMB-Dienst des Windows-Betriebssystems verwendet. Der Port wird verwendet, wenn der RPS den Datenspeicher auf

					einem lokalen Datenträger hostet. Der Datenspeicher zeigt den freigegebenen Ordner als Sicherungsziel für die Datensicherung durch den UDP-Agenten an.

UDP Windows-Agent

Die folgende Tabelle führt die Ports auf, die vom Arcserve UDP-Windows-Agent verwendet werden:

Portnummer	Porttyp	Initiiert von	Abhörprozess	Interner/externer Port	Beschreibung
8014	TCP	UDP Windows-Agent	tomcat9.exe	Extern	Standardmäßiger Port für HTTP/HTTPS-Kommunikation, um den UDP-RPS und UDP-Agenten abzurufen. **Hinweis:** Sie können den standardmäßigen Kommunikationsport während der Installation der UDP-Komponenten ändern.
18005	TCP	TOMCAT	tomcat9.exe	Intern	Zum Herunterfahren des vom UDP-RPS oder -Agent verwendeten Tomcat-Servers **Hinweis:** Dieser Port kann nur durch Ändern von TOMCAT-Konfigurationsdateien geändert werden. Der Port kann bei der Firewall-Einstellung ignoriert werden.
4090	TCP	UDP Windows-Agent	HATransServer.exe	Extern	Für die Übertragung von Daten für Virtual Standby-Tasks im Proxy-Modus **Hinweis:** Dieser Port wird nur benötigt, wenn Sie diesen

					UDP Windows Agent als virtuellen Standby-Monitor angeben.
135	TCP			Extern	Kommunikationsport für den RPC-Dienst unter Windows-Betriebssystemen **Hinweis:** Dieser Port wird nur dann benötigt, wenn die UDP-Konsole den UDP Windows-Agenten per Fernzugriff auf diesem Agentenrechner bereitstellt. Wenn der UDP-Windows-Agent durch lokales Ausführen des Setups installiert wird, ist dieser Port nicht erforderlich.
445	TCP			Extern	Kommunikationsport für den SMB-Dienst, der freigegebene Ordner auf Windows-Betriebssystemen ermöglicht **Hinweis:** Dieser Port wird nur dann benötigt, wenn die UDP-Konsole den UDP Windows-Agenten per Fernzugriff auf diesem Agentenrechner bereitstellt. Wenn der UDP-Windows-Agent durch lokales Ausführen des Setups installiert wird, ist dieser Port

					nicht erforderlich.

Unter Linux installierte Komponenten

Dieser Abschnitt enthält Informationen zu Ports, die in Linux-Sicherungsserver und Vom Linux-Sicherungsserver per Remote-Zugriff geschützte Linux-Knoten verwendet werden.

Linux-Sicherungsserver

In der folgenden Tabelle sind die vom Linux-Sicherungsserver verwendeten Ports aufgelistet:

Portnummer	Porttyp	Initiiert von	Abhörprozess	Interner/externer Port	Beschreibung
67	UDP	UDP Linux	bootpd	Extern	Eingehend, verwendet für PXE-Boot-Server. Nur erforderlich, wenn der Benutzer die PXE-Boot-Funktion verwenden möchte. **Hinweis:** Diese Portnummer kann nicht angepasst werden.
69	UDP	UDP Linux	TFTPD	Extern	Eingehend, verwendet für den PXE-Boot-Server. Nur erforderlich, wenn der Benutzer die PXE-Boot-Funktion verwenden möchte. **Hinweis:** Diese Portnummer kann nicht angepasst werden.
8014	TCP	UDP Linux	Java	Extern	Eingehend und ausgehend. Standardmäßiger Port für HTTP/HTTPS-Kommunikation, um UDP Agent for Linux aufzurufen. **Hinweis:** Sie können den standardmäßigen Kommunikationsport während der Installation der UDP-Komponenten ändern.
8021	TCP	UDP Linux	cresvc	Extern	Eingehende, für Backup-Service verwendet.
18005	TCP	UDP Linux	Java	Intern	Verwendet von Tom-

					cat. Ignorieren Sie diesen Port bei der Firewall-Einstellung. **Hinweis:** Dieser Port kann nur durch Ändern von TOMCAT-Konfigurationsdateien geändert werden.
50.000 oder über 50.000	TCP	UDP Linux	SSH	Extern	UDP Linux, abhängig von Drittanbieter. Nur erforderlich, wenn ein Linux-Migrations-BMR-Job aus der Cloud auf einen lokalen Rechner ausgeführt wird. Es wird ein verfügbarer Port von Port 50.000 ausgewählt und verwendet. UDP Linux öffnet standardmäßig den ausgewählten Port im System.
22	TCP	SSH-Dienst	sshd	Extern	UDP Linux, abhängig von Drittanbieter. Standard für SSH-Dienst, Sie können diesen Port allerdings ändern. Dieser Port ist für eingehende und ausgehende Kommunikation erforderlich.
8016	TCP	UDP Linux	d2ddss	Extern	Eingehend, verwendet für Instant VM- oder Instant BMR-Datendienst. Nur erforderlich, wenn der Benutzer die Instant VM- oder Instant BMR-Funktion verwenden möchte.
111	TCP	Portmapper	rpcbind	Extern	UDP Linux, abhängig von Drittanbieter. Standard für den Port-

					mapper. Nur erforderlich, wenn Sie eine Linux-Instant VM mithilfe einer agentenlosen Sicherung von Wiederherstellungspunkten auf dem vSphere ESX-Server ausführen.
2049	TCP	NFS-Server	nfsd	Extern	UDP Linux, abhängig von Drittanbieter. Standard für NFS-Server. Nur erforderlich, wenn Sie eine Linux-Instant VM mithilfe einer agentenlosen Sicherung von Wiederherstellungspunkten auf dem vSphere ESX-Server ausführen.
Dynamischer Port	TCP	NFS-Bereitstellungsdienst	rpc.mountd	Extern	UDP Linux, abhängig von Drittanbieter. Sehen Sie sich die Man-Page zu rpc.mountd an, um sich darüber zu informieren, wie die Konfiguration zur Überwachung eines festen Ports erfolgt. Nur erforderlich, wenn Sie eine Linux-Instant VM mithilfe einer agentenlosen Sicherung von Wiederherstellungspunkten auf dem vSphere ESX-Server ausführen.

Vom Linux-Sicherungsserver per Remote-Zugriff geschützte Linux-Knoten

Die folgende Tabelle führt die Ports auf, die von Linux-Knoten verwendet werden, die vom Linux-Sicherungsserver per Remote-Zugriff geschützt werden.

Portnummer	Porttyp	Initiiert von	Abhörprozess	Interner/externer Port	Beschreibung
22	TCP	SSH-Dienst		Extern	UDP Linux, abhängig von Drittanbieter. Standard für SSH-Dienst, Sie können diesen Port allerdings ändern. Dieser Port ist für eingehende und ausgehende Kommunikation erforderlich.

Auf dem Hypervisor installierte Komponenten

Dieser Abschnitt enthält Informationen zu den Ports, die für den Hyper-V-Host verwendet werden.

Hyper-V-Host

Die folgende Tabelle führt die Ports auf, die vom Hyper-V-Host verwendet werden:

Port-nummer	Port-typ	Ini-tiiert von	Abhör-prozess	Intern/ex-tern	Beschreibung
135	TCP			Extern	Wird vom WMI-Dienst des Windows-Betriebssystems verwendet. UDP verwendet in bestimmten Situationen WMI zur Interaktion mit dem Hyper-V-Host.
445	TCP			Extern	Wird vom SMB-Dienst des Windows-Betriebssystems verwendet. UDP verwendet in bestimmten Situationen SMB zur Interaktion mit dem Hyper-V-Host.
27000	TCP	UDP-CBT-Dienst	cbt_rep.exe	Extern	Wird vom hostbasierten UDP-CBT-Backup-Dienst verwendet. Sie müssen diesen Port nicht als Firewall-Ausnahme registrieren, da UDP diesen Port während der Sicherung automatisch registriert. Sie müssen sicherstellen, dass keine andere Anwendung mit dem gleichen Port konfiguriert ist.
5895 oder 5986	TCP	WinRM-Dienst		Extern	5895 für WinRM per HTTP-Protokoll, 5896 für WinRM per HTTPS-Protokoll. Nur einer der Ports wird benötigt. Nur erforderlich, wenn die Linux-Instant VM auf Hyper-V ausgeführt wird.
1024 ~ 65535	TCP			Extern	▪ Wird beim Importieren von VMs vom Hyper-V-Host und/oder dem Cluster für den Sicherungsplan verwendet.

					▪ Standardmäßig wählt der VM-Wiederherstellungsauftrag zufällig einen verfügbaren Port im Bereich von 1024 und 65535. Sie können den Bereich manuell anhand von festgelegten Registrierungswerten im Hyper-V-Host angeben. Weitere Informationen finden Sie unter link.

Auswirkungen des Installationsprozesses auf das Betriebssystem

Die folgenden Installationsprozesse aktualisieren verschiedene Windows-Betriebssysteme:

- Installation von nicht signierten Binärdateien
- Installation von Binärdateien mit nicht korrekter Dateiversion
- Installation von Binärdateien mit Manifest ohne Betriebssystem

Installation von nicht signierten Binärdateien

Binärname	Quelle	Binärname	Quelle
AxShockwaveFlashObjects.dll	Adobe	freetype.dll	Oracle
ShockwaveFlashObjects.dll	Adobe	hprof.dll	Oracle
httpd.exe	Apache	instrument.dll	Oracle
libapr-1.dll	Apache	j2pcsc.dll	Oracle
libapriconv-1.dll	Apache	j2pkcs11.dll	Oracle
libaprutil-1.dll	Apache	jaas_nt.dll	Oracle
libeay32.dll	Apache	jabswitch.exe	Oracle
libexpat.dll	Apache	java-rmi.exe	Oracle
libhttpd.dll	Apache	java.dll	Oracle
openssl.exe	Apache	java.exe	Oracle
pcre.dll	Apache	JavaAccessBridge-64.dll	Oracle
rotatelogs.exe	Apache	javaw.exe	Oracle
ssleay32.dll	Apache	java_crw_demo.dll	Oracle
tcnative-1.dll	Apache	jawt.dll	Oracle
CAPatch.dll	APM	JAWTAccessBridge-64.dll	Oracle
AsyncClient.net.dll	Axcient	jdwp.dll	Oracle
doclib.dll	Axcient	jjs.exe	Oracle
docxlib.dll	Axcient	jli.dll	Oracle
DspchConnector.dll	Axcient	jpeg.dll	Oracle
ESR.exe	Axcient	jsdt.dll	Oracle
esrdf.dll	Axcient	jsound.dll	Oracle
esrsdll.dll	Axcient	jsoundds.dll	Oracle
eswrapper.dll	Axcient	keytool.exe	Oracle
html2text.dll	Axcient	kinit.exe	Oracle
LicenseManager.dll	Axcient	klist.exe	Oracle
mhdll.dll	Axcient	ktab.exe	Oracle
pdflib.dll	Axcient	lcms.dll	Oracle
pptlib.dll	Axcient	management.dll	Oracle
pptxlib.dll	Axcient	mlib_image.dll	Oracle
Protection.dll	Axcient	net.dll	Oracle
pstgen.dll	Axcient	nio.dll	Oracle
Resources.dll	Axcient	npt.dll	Oracle
rtf2html.dll	Axcient	ojdkbuild_giflib.dll	Oracle
rtflib.dll	Axcient	ojdkbuild_libjpeg-tur-bo.dll	Oracle

SourceLibrary.dll	Axcient	ojdkbuild_libpng.dll	Oracle
uicommon.dll	Axcient	ojdkbuild_nss.dll	Oracle
xlslib.dll	Axcient	orbd.exe	Oracle
xlsxlib.dll	Axcient	pack200.exe	Oracle
libbind9.dll	BIND	policytool.exe	Oracle
libdns.dll	BIND	rmid.exe	Oracle
libisc.dll	BIND	rmiregistry.exe	Oracle
libisccfg.dll	BIND	sawindbg.dll	Oracle
liblwres.dll	BIND	servertool.exe	Oracle
libxml2.dll	BIND	splashscreen.dll	Oracle
msvcm80.dll	BIND	sunec.dll	Oracle
win_nsupdate.exe	BIND	sunmscapi.dll	Oracle
msvcm90.dll	Microsoft	tnameserv.exe	Oracle
RDXCleanerX64.EXE	Microsoft	unpack.dll	Oracle
RDXForceCleanX64.EXE	Microsoft	unpack200.exe	Oracle
MSCHRT20.OCX	Microsoft	verify.dll	Oracle
Microsoft.Exchange.WebServices.dll	Office 365	w2k_lsa_auth.dll	Oracle
SQLite.CodeFirst.dll	Office 365	WindowsAccessBridge-64.dll	Oracle
System.Data.SQLite.dll	Office 365	zip.dll	Oracle
System.Data.SQLite.EF6.dll	Office 365	jvm.dll	Oracle
System.Data.SQLite.Linq.dll	Office 365	JavaAccessBridge-32.dll	Oracle
System.Management.Automation.dll	Office 365	JavaAccessBridge.dll	Oracle
SQLite.Interop.dll	Office 365	JAWTAccessBridge-32.dll	Oracle
libxml.dll	OpenSSL	JAWTAccessBridge.dll	Oracle
Attach.dll	Oracle	WindowsAccessBridge-32.dll	Oracle
awt.dll	Oracle	WindowsAccessBridge.dll	Oracle
dt_shmem.dll	Oracle	plink.exe	Putty
dt_socket.dll	Oracle	sqlite3.exe	SQLite
fontmanager.dll	Oracle	MinHook.x64.dll	Tsuda Kageyu
javacpl.cpl	Oracle	zlib10.dll	zlib

Installation von Binärdateien mit nicht korrekter Dateiversion

Binärname	Quelle	Binärname	Quelle
AxShockwaveFlashObjects.dll	Adobe	libisccfg.dll	bind
ShockwaveFlashObjects.dll	Adobe	liblwres.dll	bind
openssl.exe	Apache	libxml2.dll	bind
UpdateData.exe	Arcserve-Lizenzierung	win_nsupdate.exe	bind
AsyncClient.net.dll	Axcient	libxml.dll	NetApp
doclib.dll	Axcient	decora-sse.dll	Oracle
docxlib.dll	Axcient	fxplugins.dll	Oracle
DspchConnector.dll	Axcient	glass.dll	Oracle
ESR.exe	Axcient	glib-lite.dll	Oracle
esrdf.dll	Axcient	gstreamer-lite.dll	Oracle
esrsdll.dll	Axcient	javafx-font.dll	Oracle
eswrapper.dll	Axcient	javafx-iio.dll	Oracle
html2text.dll	Axcient	jfxmedia.dll	Oracle
LicenseManager.dll	Axcient	jfxwebkit.dll	Oracle
mhdll.dll	Axcient	libxml2.dll	Oracle
pdflib.dll	Axcient	libxslt.dll	Oracle
pptlib.dll	Axcient	prism-d3d.dll	Oracle
pptxlib.dll	Axcient	sqlite3.exe	sqlite
Protection.dll	Axcient	libcurl.dll	VMware
pstgen.dll	Axcient	libexpat.dll	VMware
Resources.dll	Axcient	liblber.dll	VMware
rtf2html.dll	Axcient	libldap.dll	VMware
rtflib.dll	Axcient	libldap_r.dll	VMware
uicommon.dll	Axcient	libxml2.dll	VMware
xlslib.dll	Axcient	SSOClient.dll	VMware
xlsxlib.dll	Axcient	vddkReporter.exe	VMware
libbind9.dll	bind	zlib1.dll	zlib
libdns.dll	bind	zlib10.dll	zlib
libisc.dll	bind		

Installation von Binärdateien mit Manifest ohne Betriebssystem

Binärname	Quelle
openssl.exe	Apache
win_nsupdate.exe	bind
plink.exe	putty
sqlite3.exe	sqlite
vddkReporter.exe	VMware

Antivirus-Konfiguration

Antivirus-Software kann die reibungslose Ausführung von Arcserve UDP Agent (Windows) behindern, indem sie den Zugriff auf Dateien vorübergehend blockiert oder Dateien, die fälschlicherweise als verdächtig oder gefährlich klassifiziert werden, in Quarantäne stellt oder löscht. Sie können eine Antivirensoftware so konfigurieren, dass sie Dateien oder Ordner ausschließt und keine Zeit mit der Überprüfung von Daten verbringt, die nicht geschützt werden müssen.

Die korrekte Konfiguration Ihrer Antivirensoftware ist erforderlich, um das Sicherungsziel auszuschließen. Durch die richtige Konfiguration können Sie Störungen bei Sicherungs- und Wiederherstellungsvorgängen oder anderen Prozessen wie Zusammenführung und Katalogerstellung vermeiden.

Pfade, die für die Antivirenprüfung auszuschließen sind:

Virenscan für	Auszuschließende Pfade
RPS	Datenspeicherordner Datenzielpfad Indexzielpfad Hash-Zielpfad
Agent für Windows nicht von der Konsole verwaltet	Sicherungsziel

Installieren von Aktualisierungen für Arcserve UDP

Das Abrufen und Installieren von Arcserve UDP-Aktualisierungen ist ein zweiteiliger Vorgang: Überprüfen und Herunterladen der Aktualisierung und anschließend die Installation der Aktualisierung.

Hinweis: Die Aktualisierungen, die für Arcserve UDP herausgegeben werden, sind immer kumulativ. Deshalb enthält jede Aktualisierung auch sämtliche zuvor veröffentlichten Aktualisierungen, um sicherzustellen, dass Ihr Rechner immer auf dem neuesten Stand ist. Im Dialogfeld **Hilfe/Info** wird die Ebene der Aktualisierung, die auf einem Rechner installiert ist, angezeigt. Im Bedarfsfall können Sie diese Informationen verwenden, um einen anderen Server mit der gleichen Konfigurations-/Patch-Ebene zu erstellen.

Führen Sie die folgenden Aufgaben aus, um Aktualisierungen für Arcserve UDP zu installieren:

1. Überprüfen der Hinweise für die Installation von Aktualisierungen
2. Festlegen der Voreinstellungen für Aktualisierungen
3. Überprüfen und Installieren der Aktualisierungen
4. (Optional) Automatisches Installieren von Aktualisierungen für Arcserve UDP
5. Überprüfen, ob die Aktualisierungen erfolgreich installiert wurden

Überprüfen der Hinweise für die Installation von Aktualisierungen

Beachten Sie folgende Hinweise, bevor Sie Aktualisierungen für Arcserve UDP installieren:

- Bei Installation einer Arcserve UDP- oder Arcserve Unified Data Protection Agent für Windows-Aktualisierung ist es wichtig, eine optimale Leistung zwischen der Konsole, dem Recovery Point Server (RPS) und den Agenten sicherzustellen. Wenn die Aktualisierung in einer Umgebung installiert wird, die sowohl eine Konsole als auch einen Agenten umfasst, müssen Sie die Aktualisierung immer zuerst auf der Konsole, dann auf dem RPS und schließlich auf dem Agenten installieren. (Für den Agenten, der auf der Konsole oder dem RPS installiert wird, wird die Aktualisierung gleichzeitig automatisch auf diesem Agenten installiert).
- Sie können die verfügbaren Aktualisierungen bei Bedarf von Arcserve herunterladen – entweder direkt auf einen Client-Rechner oder zuerst auf einen Staging-Server und dann auf einen Client-Rechner.
- Im Bedarfsfall können Sie Ihren Workstation-Knoten als einen Staging-Server zum Herunterladen von Aktualisierungen für Arcserve UDP verwenden.
- Überprüfen Sie, dass die Voreinstellungen für die Aktualisierungen richtig konfiguriert wurden.
  - Aktualisierungen können entweder über die Benutzeroberfläche installiert werden, oder sie können mithilfe der Befehlszeile automatisch installiert werden.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

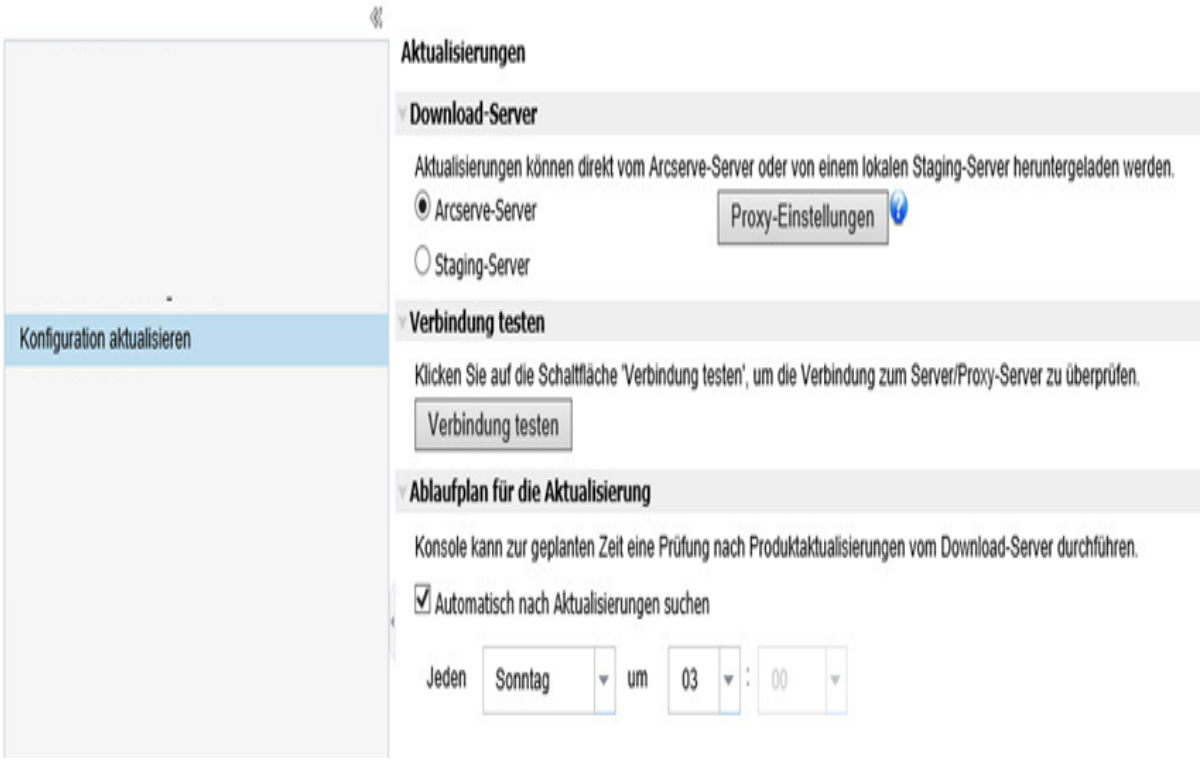
Festlegen der Voreinstellungen für die Aktualisierungen

Mit Arcserve UDP können Sie Ihre Voreinstellungen für die Aktualisierung angeben.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Arcserve UDP-Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Aktualisierungskonfiguration**.

   Die Seite "**Aktualisierungen**" wird im rechten Fensterbereich angezeigt.



3. Geben Sie Ihre Voreinstellungen für **Aktualisierungen** an.

   Download-Server

   Gibt den Quellserver an, von dem aus der Arcserve UDP-Server eine Verbindung herstellt und verfügbare Aktualisierungen herunterlädt.

   - **Arcserve Server**

     Gibt an, dass Aktualisierungen vom Arcserve-Server direkt auf Ihren lokalen Server heruntergeladen werden.

     Dies ist die Standardeinstellung.

   - **Staging-Server**

Gibt an, dass Aktualisierungen vom Staging-Server heruntergeladen werden.

Hinweis: Falls erforderlich, können Sie einen Staging-Server erstellen. Weitere Informationen finden Sie unter So erstellen Sie einen Staging-Server.

Wenn Sie mehr als einen Staging-Server angeben, wird der erste aufgelistete Server als primärer Staging-Server festgelegt. Arcserve UDP versucht zuerst, mit dem primären Staging-Server Verbindung aufzunehmen. Wenn der erste aufgelistete Server nicht verfügbar ist, wird der nächste aufgelistete Server als primärer Staging-Server verwendet. Mit dem gleichen Ablauf wird fortgefahren, bis der letzte aufgelistete Server zum primären Staging-Server wird. (Die Staging-Server-Liste ist auf maximal 5 Server beschränkt).

- Sie können die Reihenfolge der Staging-Server mit den Schaltflächen **Nach unten** und **Nach oben** ändern.
- Sie können die Schaltfläche **Löschen** verwenden, um einen Server aus dieser Auflistung zu entfernen.
- Sie können die Schaltfläche **Server hinzufügen** verwenden, um einen neuen Server zur Auflistung hinzuzufügen. Wenn Sie auf die Schaltfläche **Server hinzufügen** klicken, wird das Dialogfeld **Staging-Server** geöffnet, in dem Sie den Namen des hinzugefügten Staging-Servers angeben können.

Wenn Sie den Staging-Server als Ihren Download-Server auswählen:

- Wenn der angegebene Staging-Server Aktualisierungen hat, dann kann die Arcserve UDP-Konsole die Aktualisierung von diesem Staging-Server abrufen.
- Wenn für den angegebenen Staging-Server keine Aktualisierung vorhanden ist, dann kann die Arcserve UDP-Konsole keine Aktualisierung von diesem Staging-Server herunterladen. Das Protokoll enthält folgende Meldung:

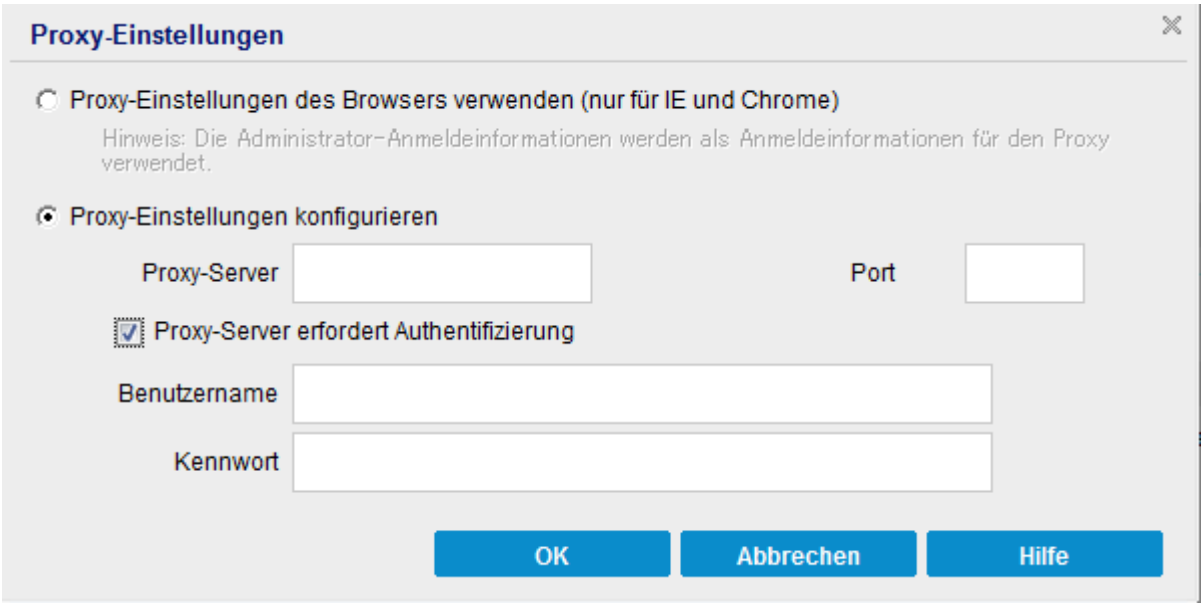
  Keine neuen Aktualisierungen verfügbar.

- **Proxy-Einstellungen**

  Hinweis: Diese **Proxy-Server**-Option ist nur verfügbar, wenn Sie den Arcserve Server als den Download-Server auswählen.

  Wählen Sie Proxy-Einstellungen aus.

  Wenn Sie diese Option aktivieren, wird das Dialogfeld **Proxy-Einstellungen** geöffnet.



Proxy-Einstellungen des Browsers verwenden

Diese Auswahl ist nur unter Windows Internet Explorer (IE) und Google Chrome anwendbar.

Wenn diese Option ausgewählt ist, werden die gleichen Proxy-Einstellungen, die auf den Browser angewendet werden, um eine Verbindung mit dem Arcserve-Server für Arcserve UDP-Aktualisierungsinformationen herzustellen, von Arcserve UDP automatisch erkannt und verwendet.

Proxy-Einstellungen konfigurieren

Wenn diese Option ausgewählt ist, wird der angegebene Proxy-Server aktiviert, um eine Verbindung mit dem Arcserve-Server für Arcserve UDP-Aktualisierungsinformationen herzustellen. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet.

Außerdem können Sie angeben, ob der Proxy-Server Authentifizierung benötigt. Wenn diese Option aktiviert ist, müssen zur Verwendung des Proxy-Servers Authentifizierungsinformationen (Benutzer-ID und Kennwort) angegeben werden.

Hinweis: Als Format für den Benutzernamen sollte ein vollständiger Domänenbenutzername im Format "<Domänenname>\<Benutzername>" verwendet werden.

Verbindung testen

Ermöglicht es Ihnen, die folgenden Verbindungen zu testen, und zeigt bei Abschluss eine Statusmeldung an:

- Wenn Sie "Arcserve-Server" als Download-Server ausgewählt haben, wird die Verbindung zwischen dem Rechner und dem Arcserve-Server über den angegebenen Proxy-Server getestet.
- Wenn Sie "Staging-Server" als Download-Server angegeben haben, wird die Verbindung zwischen dem Rechner und dem angegebenen Staging-Server getestet. Die Schaltfläche "Verbindung testen" wird verwendet, um die Verfügbarkeit der einzelnen aufgelisteten Staging-Server zu testen. Ein entsprechender Status wird im Feld **Verbindungsstatus** angezeigt. Falls keiner der konfigurierten Staging-Server verfügbar ist, erscheint die folgende Meldung oben in der Arcserve UDP Konsole: Update-Server nicht verfügbar.

  Hinweis: Die Verbindungsprüfung wird automatisch durchgeführt, wenn Sie die Seite **Aktualisieren der Konfiguration** unter der Registerkarte **Einstellungen** in der Arcserve UDP Konsole öffnen. Wenn dieser automatische Test ausgeführt wird, wird der neueste Verbindungsstatus des zuvor konfigurierten Download-Servers überprüft (Arcserve-Server oder Staging-Server, je nachdem, welcher ausgewählt ist). Wenn Sie zuvor mehr als einen Staging-Server konfiguriert haben, wird dieser automatische Test auf allen Staging-Servern ausgeführt, um den neuesten Verbindungsstatus abzurufen.

Ablaufplan für Aktualisierungen

Gibt an, wann auf neue Arcserve UDP-Aktualisierungen überprüft werden soll (die anschließend heruntergeladen werden sollen).

4. Klicken Sie auf **Speichern**.

Ihre Voreinstellungen für Aktualisierungen werden gespeichert.

So erstellen Sie einen Staging-Server

Der Staging-Server ist ein Knoten, auf dem derArcserve UDP Agent oder die Konsole installiert ist. Der Knoten muss das Herunterladen von Aktualisierungen vomArcserve Download-Server beenden, um als Staging-Server für das Bereitstellung von Aktualisierungen für andere zu arbeiten.

Hinzufügen eines Staging-Servers:

Staging-Server können Sie auf jedem Knoten hinzufügen, die die folgenden zwei Voraussetzungen erfüllt:

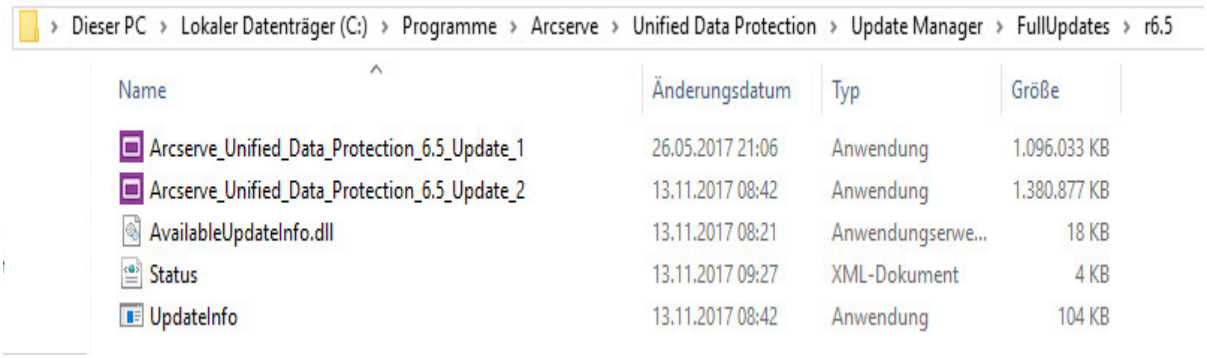
- Auf dem Knoten ist Arcserve UDP entweder Agent oder Arcserve UDP Konsole installiert.
  - Arcserve UDPDie Konsole kann nur Aktualisierungen vom Konsole-Staging-Server herunterladen.
  - Arcserve UDPDer Agent kann Aktualisierungen vom Konsole- oder Agent-Staging-Server herunterladen.
- Der Knoten hat mindestens einmal erfolgreich Aktualisierungen vom Arcserve Download-Server heruntergeladen.

Hinweis: Eine andere Konfiguration ist nicht erforderlich, wenn der Ziel-Staging-Server die Voraussetzungen erfüllt.

Aktualisierung von Staging-Server konfigurieren

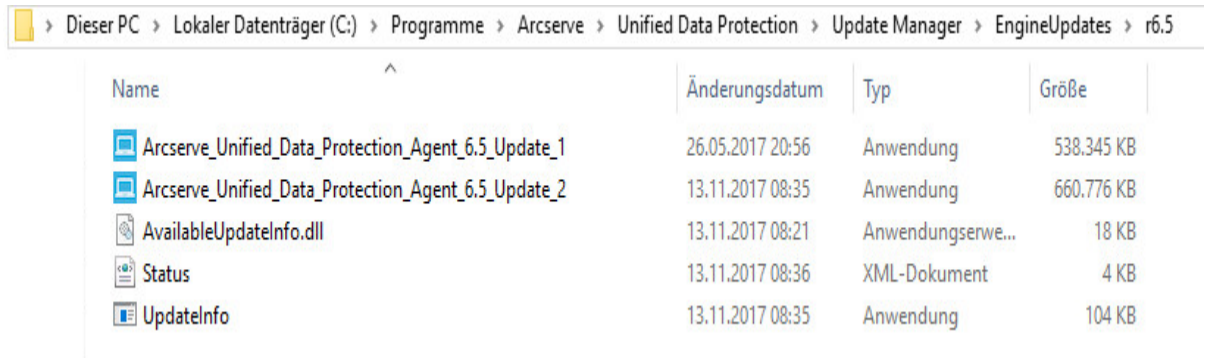
- Wenn der Staging-Server über Arcserve UDP auf diesem Knoten installierte Konsole ausgewählt wird, beachten Sie die folgenden Hinweise:
  - Standard-Port: 8015
  - Arcserve UDPKonsole kann Aktualisierungen von diesem Staging-Server abrufen.
  - Arcserve UDPAgenten kann Aktualisierungen von diesem Staging-Server abrufen.

  Hinweis: Aus dem Verzeichnis < UDP Installed path\Update Manager\FullUpdates> auf dem Ziel-Staging-Server überprüfen Sie die neueste verfügbare Version. Siehe Beispiel unten.



- Wenn der Staging-Server über Arcserve UDP auf diesem Knoten installierten Agenten ausgewählt wird, beachten Sie die folgenden Hinweise:
  - Standard-Port: 8014
  - Arcserve UDPKonsole kann keine Aktualisierungen von diesem Staging-Server abrufen.
  - Arcserve UDPAgenten kann Aktualisierungen von diesem Staging-Server abrufen.

  Hinweis: Aus dem Verzeichnis <UDP Installed path\Update Manager\EngineUpdates> auf dem Ziel-Staging-Server überprüfen Sie die neueste verfügbare Version. Siehe Beispiel unten.



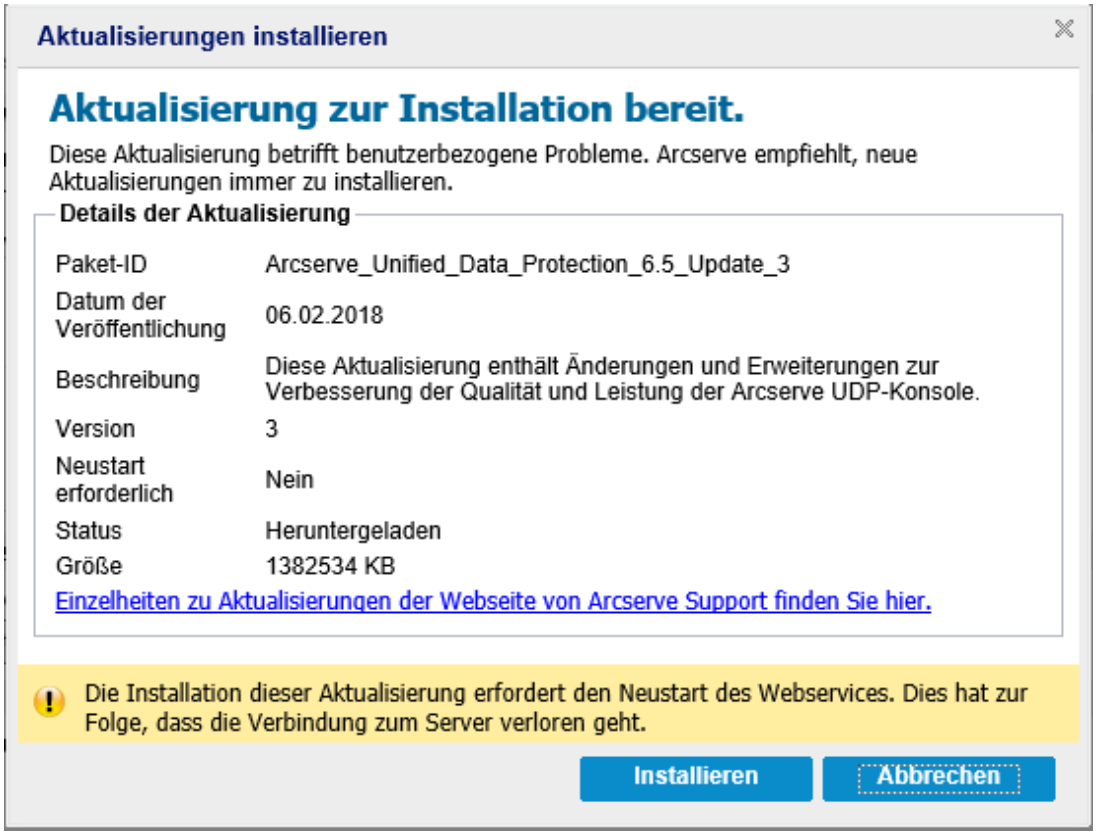
Überprüfen und Installieren der Aktualisierungen

Über die UDP-Konsole können Sie feststellen, ob neue Aktualisierungen verfügbar sind.

Gehen Sie wie folgt vor:

1. Klicken Sie im Drop-down-Menü **Hilfe** auf **Aktualisierungen suchen**. Wenn eine neue Aktualisierung verfügbar ist, wird eine Meldung im oberen Balken angezeigt. Es wird auch das Dialogfeld zur **Installation der Aktualisierung** angezeigt.
2. Wenn Sie den Aktualisierungsablaufplan aktivieren und eine neue Aktualisierung verfügbar ist, dann wird die Aktualisierung automatisch auf den UDP-Server heruntergeladen. Die Verknüpfung **Neue Aktualisierung verfügbar** wird im oberen Balken angezeigt, um visuell darzustellen, dass neue Aktualisierungen zur Installation bereitstehen.
3. Klicken Sie im oberen Balken auf die Verknüpfung **Neue Aktualisierung verfügbar**.

   Das Dialogfeld **Aktualisierungen installieren** wird geöffnet. Es enthält Informationen zur verfügbaren Aktualisierung. Das Dialogfeld enthält Informationen wie Beschreibung, Download-Status und Größe, gibt an, ob ein Neustart erforderlich ist, und enthält einen Link zum Arcserve-Server zum Herunterladen zusätzlicher Aktualisierungsdetails.



4. Klicken Sie auf **Installieren**.

   Die Installation der Aktualisierungen für Arcserve UDP wird gestartet.

Aktualisieren von Agenten auf Remote-Knoten mit Gateway

Die Remote-Knoten und -Server an einem Standort interagieren mit der Konsole mithilfe eines Gateways. Mit Arcserve UDP können Sie die aktuelle Version des Agenten erkennen und für Knoten bereitstellen. Um ein Upgrade oder eine Installation von Arcserve UDP Agent für einen Knoten in einem Standort durchzuführen, verwenden Sie "Agent installieren/aktualisieren".

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Wählen Sie im linken Fensterbereich **Navigation** einen Standort aus der Drop-down-Liste aus.
3. Die Seite **Knoten: Alle Knoten** wird angezeigt.
4. Wählen Sie einen oder mehrere Knoten aus.
5. Klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen** und anschließend auf **Agent installieren/aktualisieren**.

   Die Details der Installation oder des Upgrades werden im mittleren Fensterbereich angezeigt.
6. Überprüfen Sie die Details, und klicken Sie auf **OK**.

   Der Knoten wird mit der aktuellen Version von Arcserve UDP Agent installiert bzw. aktualisiert.

Aktualisieren des RPS auf Remote-Servern mit Gateway

Die Remote-Knoten und -Server an einem Standort interagieren mit der Konsole mithilfe eines Gateways. Mit Arcserve UDP können Sie die aktuelle Version der RPS-Komponente erkennen und für Recovery Point Server bereitstellen. Nachdem Sie die RPS-Komponente bereitgestellt haben, kann der Server Sicherungssitzungen speichern und als Recovery Point Server agieren. Verwenden Sie zum Aktualisieren oder Installieren der Arcserve UDP-RPS-Komponente auf einem Recovery Point Server an einem Standort die Option "Recovery Point Server installieren/aktualisieren".

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Wählen Sie im linken Fensterbereich **Navigation** einen Standort aus der Drop-down-Liste aus.
3. Klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziel:** Die Seite **Recovery Point Server** wird angezeigt.
4. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf einen Recovery Point Server.
   - Wählen Sie einen Recovery Point Server aus, und klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.
5. Klicken Sie auf **Recovery Point Server installieren/aktualisieren**.

   Die Seite **Installation und Upgrade** wird angezeigt.
6. Ändern Sie die Bereitstellungseinstellungen, und klicken Sie auf **OK**, um den Recovery Point Server auf dem ausgewählten Knoten bereitzustellen.

   Die Bereitstellung des Recovery Point Servers startet. Der Fortschritt der Bereitstellung wird im rechten Fensterbereich angezeigt.

(Optional) Automatisches Installieren von Aktualisierungen für Arcserve UDP

Die automatische Installation ermöglicht es Ihnen, eine unbeaufsichtigte Installation der Aktualisierung auszuführen, und erfordert keine Eingaben ihrerseits.

Gehen Sie wie folgt vor:

1. Starten Sie die automatische Installation der Aktualisierung für Arcserve UDP.

   "<UpdateExeFile>" /s /v"<Zusätzliche Argumente>"

2. Konfigurieren Sie die automatische Installation mithilfe folgender Syntax und Argumente:

   UpdateExeFile

   Legt die Ausführung der selbstextrahierenden ausführbaren Datei fest.

   s

   Legt die Ausführung der selbstextrahierenden ausführbaren Datei über den automatischen Modus fest.

   v

   Gibt zusätzliche Argumente für die Aktualisierungsinstallation an.

   Zusätzliche Argumente

   /s

   Führt die Installation der Aktualisierung über den automatischen Modus aus.

   /AutoReboot

   Legt fest, dass nach der Installation der Aktualisierung ein automatischer Neustart ausgeführt werden soll. Wenn ein Neustart erforderlich ist, um die Aktualisierung abzuschließen, dann wird der Rechner ohne Benachrichtigung automatisch neu gestartet.

   Beispiele

   - Um eine Aktualisierung über den automatischen Modus zu installieren und nach Abschluss automatisch neu zu starten, verwenden Sie den folgenden Befehl:

     "<UpdateExeFile>" /s /v"/s /AutoReboot"

   - Um eine Aktualisierung über den automatischen Modus zu installieren und nach Abschluss nicht automatisch neu zu starten, verwenden Sie den folgenden Befehl:

     "<UpdateExeFile>" /s /v"/s"

Überprüfen, ob die Aktualisierungen erfolgreich installiert wurden

Wählen Sie in der Arcserve UDP-Konsole die Option **Hilfe** aus, klicken Sie auf **Info zu**, und überprüfen Sie, ob das Dialogfeld "Info zu Arcserve UDP" die neueste Version anzeigt.

So deinstallieren Sie Arcserve UDP

Sie können Arcserve Unified Data Protection über die folgenden Methoden deinstallieren:

- **Standard Deinstallation**: Verwenden Sie diese Methode, um die Deinstallation über die Windows-Systemsteuerung durchzuführen.
- **Unbeaufsichtigte Deinstallation**: Verwenden Sie diese Methode, um eine unbeaufsichtigte Deinstallation über die Windows-Befehlszeile durchzuführen.

Standardmäßige Deinstallation

Sie können folgende Komponenten deinstallieren.

- Arcserve Unified Data Protection-Konsole
- Arcserve Unified Data Protection-Recovery Point-Server
- Arcserve Unified Data Protection-Agent

Gehen Sie wie folgt vor:

1. Öffnen Sie die Windows-Systemsteuerung.
2. Klicken Sie auf "Programm deinstallieren".

   Das Dialogfeld "Programm deinstallieren oder ändern" wird geöffnet.
3. Wählen Sie Arcserve Unified Data Protection aus, und klicken Sie auf "Deinstallieren".

   Das Dialogfeld "Arcserve Unified Data Protection-Anwendung deinstallieren" wird geöffnet.
4. Wählen Sie die Komponenten aus, die deinstalliert werden sollen, und klicken Sie auf "Weiter".

   Das Dialogfeld **Meldungen** wird geöffnet.
5. Klicken Sie auf "Weiter".

   Das Dialogfeld **Komponenten entfernen** wird geöffnet.
6. Klicken Sie auf **Entfernen**.

   Die ausgewählten Komponenten werden vom Computer deinstalliert.

Automatische Deinstallation

Bei der automatischen Deinstallation ist kein Benutzereingriff erforderlich.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, um Komponenten von Arcserve UDP zu deinstallieren.

   Hinweis: Sie müssen sich mit einem Administratorkonto auf dem Computer anmelden.

2. Öffnen Sie die Windows-Befehlszeile, und führen Sie je nach Betriebssystem den entsprechenden Befehl aus:

   - **x86-Betriebssystem:**

     Um alle Komponenten zu deinstallieren

     %ProgramFiles%\Arcserve\SharedComponents\Arcserve Unified Data Protection\Setup\uninstall /q /ALL

     Um ausgewählte Komponenten zu deinstallieren

     %ProgramFiles%\Arcserve\SharedComponents\Arcserve Unified Data Protection\Setup\uninstall /q /p <Produktcode>

   - **x64-Betriebssystem:**

     Um alle Komponenten zu deinstallieren

     %ProgramFiles(x86)%\Arcserve\SharedComponents\Arcserve Unified Data Protection\Setup\uninstall /q /ALL

     Um ausgewählte Komponenten zu deinstallieren

     %ProgramFiles(x86)%\Arcserve\SharedComponents\Arcserve Unified Data Protection\Setup\uninstall /q /p <Produktcode>

   Die folgenden Werte erklären die Rückgabecodes:

   0 = Die Deinstallation war erfolgreich.

   3010 = Die Deinstallation war erfolgreich, aber ein Neustart ist erforderlich.

   Andere = Die Deinstallation ist fehlgeschlagen.

   Verwendung:

   In der Tabelle unten sind die Produktcodes aufgelistet, die Sie für die Arcserve Unified Data Protection-Komponenten angeben müssen, die Sie deinstallieren möchten.

   Beispiel:

Mit der folgenden Syntax können Sie Arcserve Unified Data Protection-Recovery Point Server automatisch deinstallieren.

"%ProgramFiles(x86)%\Arcserve\SharedComponents\Arcserve Unified Data Protection\Setup\uninstall.exe" /q /p {CAAD8172-1858-4DC7-AE81-C887FA6AFB19}

Komponente	<Produktcode>
Arcserve Unified Data Protection-Agent (x86-Plattformen)	{CAAD8AEA-A455-4A9F-9B48-C3838976646A}
Arcserve Unified Data Protection-Agent (x64-Plattformen)	{CAAD1E08-FC33-462F-B5F8-DE9B765F2C1E}
Arcserve Unified Data Protection Recovery Point-Server	{CAAD8172-1858-4DC7-AE81-C887FA6AFB19}
Arcserve Unified Data Protection Konsole	{CAAD3E40-C804-4FF0-B1C0-26D534D438C0}
Arcserve Unified Data Protection Gateway	{FB95E75D-494F-4146-9B35-F867434B264A}

Nach der Ausführung des Befehls werden die Komponenten von Arcserve UDP deinstalliert.

Entfernen von Komponenten, die nicht durch das Deinstallationsprogramm entfernt wurden

Wichtig!

1. Die Arcserve-Lizenzierung wird von allen Arcserve-Produkten gemeinsam genutzt. Stellen Sie sicher, dass keine anderen Arcserve-Produkte auf Ihrem Rechner installiert sind, da Sie ansonsten die Lizenzierung für alle auf diesem Rechner installierten Arcserve-Produkte verlieren könnten.
2. Programme, die nach Arcserve Unified Data Protection Agent für Windows installiert werden und von diesen entfernten Komponenten abhängen, funktionieren möglicherweise nicht ordnungsgemäß.

   Wenn Sie diese Komponenten manuell entfernen möchten, führen Sie die folgenden Schritte durch:

Arcserve-Lizenzierungskomponente manuell entfernen

1. Gehen Sie zum Verzeichnis *C:\Programme (x86)\Arcserve\SharedComponents\CA_LIC*.
2. Suchen Sie die ZIP-Datei *lic98_uninstaller.zip* und entpacken Sie diese Datei in einem anderen Speicherorten (zum Beispiel: C:\temp).
3. Suchen Sie im Speicherort, an dem die Dateien extrahiert wurden, zwei Skriptdateien mit den Namen *rmlic.exe* und *rmlicense.bat*.
4. Klicken Sie auf *rmlicense.bat*, um das Skript auszuführen, das die Komponenten deinstalliert.
5. Löschen Sie folgende Ordner manuell:
   - C:\Programme (x86)\Arcserve
   - C:\Programme\Arcserve
   - Ordner, in dem Sie die ZIP-Datei extrahiert haben.
6. Entfernen Sie den Registrierungsschlüssel für die Komponente "Arcserve Licensing".
   - Für x64 Plattform: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Arcserve\License
   - Für x86 Plattform: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\License

Manuelles Entfernen von Microsoft Visual C++ und Microsoft SQL Server Express

1. Greifen Sie über die Windows-Systemsteuerung auf die Standardanwendung "Programme hinzufügen oder entfernen" zu (Systemsteuerung, Programme und Funktionen, Programme entfernen).

2. Wählen Sie *Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501* aus, und klicken Sie auf "Deinstallieren".
3. Wählen Sie *Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501* aus, und klicken Sie auf "Deinstallieren".
4. Wählen Sie "Microsoft SQL Server 2014 (64-Bit)" aus, und klicken Sie auf "Deinstallieren".
5. Um nur die Arcserve UDP-Datenbank zu entfernen, wählen Sie "ARCSERVE_APP" aus, und klicken Sie auf "Deinstallieren".

Kapitel 4: Aktualisieren auf Arcserve UDP Version 8.0

In diesem Abschnitt werden die folgenden Themen behandelt:

Hinweis: Empfehlungen zum Schutz des Arcserve UDP-Servers finden Sie unter Schützen eines Arcserve UDP-Servers.

Unterstützte Versionen für Upgrade

Arcserve UDP 8.1 bietet Aktualisierungs- und Abwärtskompatibilität gemäß folgenden Regeln:

- Arcserve UDP 8.1 unterstützt das Upgrade von Arcserve UDP Version 8.0, 7.0 Update 2, 7.0 Update 1, neuester Arcserve UDP 7.0-Version und Version 6.5 Update 4.

  Hinweise: Beachten Sie Folgendes, bevor Sie von anderen früheren Versionen auf Arcserve UDP 8.1 aktualisieren:

  - Aktualisieren Sie für Arcserve UDP 6.5 mit Update 3, Update 2, Update 1 oder der endgültigen Version zuerst auf UDP 6.5 Update 4.
  - Aktualisieren Sie für Arcserve UDP Version 6.0 Update 3 für Windows zuerst auf Arcserve UDP Version 7.0.
  - Aktualisieren Sie für Arcserve UDP Version 6.0 Update 2, Update 1 oder die endgültige Version für Windows zuerst auf Arcserve UDP Version 6.5 Update 4.
  - Aktualisieren Sie für Arcserve UDP Version 6.0 Update 1 oder die endgültige Version für Linux zuerst auf Arcserve UDP Version 6.5 Update 4.
  - Aktualisieren Sie für Arcserve UDP 5.0 Update 4 zuerst auf UDP 6.5 Update 4.
  - Aktualisieren Sie für Arcserve UDP 5.0 mit Update 3, Update 2, Update 1 oder der endgültigen Version zuerst auf UDP 6.0 Update 3 und dann auf UDP 7.0.

- Arcserve UDP 8.1 unterstützt keine Aktualisierungen von Arcserve D2D r16.5, Arcserve Central Protection Management r16.5, Arcserve Data Protection Console r16.5, Arcserve Central Reporting r16.5 und Arcserve Central Virtual Standby r16.5.

  Weitere Informationen finden Sie unter Aktualisieren der Arcserve UDP-Lizenz.

Upgradesequenz auf der Arcserve Appliance

Arcserve Version 8.0 unterstützt Upgrades auf der UDP-Appliance. Das Upgrade kann eine der folgenden Sequenzen umfassen:

- Aktualisieren von Arcserve UDP
  - Aktualisieren der Arcserve Appliance, die als Arcserve UDP-Konsole und RPS ausgeführt wird
  - Aktualisieren der Arcserve Appliance, die nur als Arcserve UDP RPS ausgeführt wird
  - Upgradeschritte bei Verwendung von mindestens zwei Arcserve Appliances in der Umgebung
- Aktualisieren des Arcserve Linux-Agenten auf der Arcserve UDP Appliance
- Aktualisieren von Arcserve Backup auf der Arcserve Appliance

Die Arcserve Appliance aktualisieren, die als Arcserve UDP Console und RPS betrieben wird

Aktualisieren Sie Arcserve Appliance und befolgen Sie dann die beschriebene Aktualisierungssequenz, um die Umgebung zu aktualisieren.

Die Arcserve Appliance aktualisieren, die nur als Arcserve UDP RPS betrieben wird

Aktualisieren Sie die vollständige Produktionsumgebung. Weitere Informationen finden Sie unter Upgradesequenz.

Upgradeschritte bei Verwendung von mindestens zwei Arcserve Appliances in der Umgebung

Aktualisieren Sie die vollständige Produktionsumgebung. Weitere Informationen finden Sie unter Upgradesequenz.

Den Arcserve Linux Agent auf der Arcserve UDP Appliance aktualisieren

1. Aktualisieren Sie die Arcserve UDP-Konsole, die die Linux-Backup-Server-Umgebung verwaltet.
2. Aktualisieren Sie den Linux-Sicherungsserver auf der Arcserve Appliance. Details finden Sie in der *Arcserve Unified Data Protection Agent for Linux – Online-Hilfe*.

Arcserve Backup auf der Arcserve Appliance aktualisieren

Im *Arcserve Backup-Implementierungshandbuch* erfahren Sie, wie Sie ein Upgrade für die Arcserve Appliance durchführen.

Unterstützungsrichtlinie zur Abwärtskompatibilität

Es wird empfohlen, alle Komponenten in der gesamten Umgebung auf Arcserve UDP 8.1 zu aktualisieren, damit die neuen Funktionen in Arcserve UDP 8.1 genutzt werden können. Wenn die Aktualisierung aller Komponenten nicht gleichzeitig abgeschlossen werden kann, wirkt sich dies nicht auf die vorhandenen Sicherungspläne aus.

Die Abwärtskompatibilität unterstützt Arcserve UDP Version 8.0, 7.0, 7.0 Update 1, 7.0 Update 2 und Arcserve UDP 6.5 Update 4.

In diesem Abschnitt werden die folgenden Themen behandelt:

Unterstützungsrichtlinie zur Abwärtskompatibilität für Arcserve UDP Version 8.0

Unterstützung der Abwärtskompatibilität zwischen verschiedenen UDP-Konsolen über den Task "Zu einem remote verwalteten RPS replizieren"

Wenn Sie den Task *Zu einem remote verwalteten RPS replizieren* ausführen möchten, wird empfohlen, zunächst die Konsole und den RPS auf Zielseite zu aktualisieren, bevor Sie die Konsole/den RPS/den Agenten auf Quellseite aktualisieren.

- Die Replikation wird unterstützt, wenn der Quell-RPS UDP 8.1 und der Ziel-RPS noch UDP 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 verwendet.
- Die Replikation wird unterstützt, wenn der Quell-RPS UDP 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 und der Ziel-RPS UDP 8.1 verwendet.
- Replikationsverhalten:
  - Wenn Sie an beiden Standorten ein Upgrade auf UDP 8.1 durchführen, können Sie ohne öffentliche IP von Cloud Hybrid zu einem lokalen Ziel replizieren (neues UDP-Verhalten).
  - Wenn Sie nur an einem der Standorte ein Upgrade auf UDP 8.1 durchführen und der andere Standort eine unterstützte Version von UDP verwendet, können Sie mithilfe der öffentlichen IP von Cloud Hybrid zu einem lokalen Ziel replizieren.

Unterstützung der Abwärtskompatibilität für Windows RPS/Agent (oder agentenlosen Sicherungs-Proxy)

- Die Arcserve UDP 8.1-Konsole unterstützt Recovery Point Server (RPS) und Agenten (oder agentenlose Sicherungs-Proxys) der UDP-Versionen 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 zu Sicherungszwecken, wenn sich der Plan nach

einem Upgrade nicht ändert.

- Die Arcserve UDP 8.1-Konsole und RPS unterstützen Agenten (oder agentenlose Sicherungs-Proxys) der UDP-Versionen 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 zu Sicherungszwecken, wenn sich der Plan nach einem Upgrade nicht ändert.
- Die Arcserve UDP 8.1-Konsole unterstützt die Bereitstellung des vorhandenen Plans ohne jegliche Änderungen, wenn RPS und Agenten (oder agentenlose Sicherungs-Proxys) noch unter UDP 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 ausgeführt werden. Der Agent wird nicht automatisch aktualisiert.
- Die Arcserve UDP 8.1-Konsole unterstützt das Unterbrechen oder Wiederaufnehmen eines vorhandenen Plans ohne jegliche Änderungen, wenn RPS und Agenten (oder agentenlose Sicherungs-Proxys) noch unter UDP 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 ausgeführt werden. Der Agent wird nicht automatisch aktualisiert.
- Die Arcserve UDP 8.1-Konsole unterstützt das Erstellen eines neuen Plans oder das Ändern eines vorhandenen Plans zur Konfiguration von Legacy-Funktionen, die in der vorherigen Version bereits unterstützt wurden, wenn RPS und Agenten (oder agentenlosen Sicherungs-Proxys) noch unter UDP 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 ausgeführt werden. Der Agent wird nicht automatisch aktualisiert.
- Die Arcserve UDP 8.1-Konsole unterstützt das Erstellen eines neuen Plans oder das Ändern eines vorhandenen Plans zur Einbeziehung neuer Funktionen in Version UDP 8.1, wenn der zugehörige RPS, Proxy oder Agent bereits auf die erwartete Version aktualisiert wurde.

  Beispiel:

  - Das Angeben des Netzwerks für die Sicherung wird unterstützt, wenn Konsole, RPS, Proxy und Agent auf UDP 7.0, 7.0 Update 1, 7.0 Update 2, 8.0 und 8.1 aktualisiert werden.
- Die Arcserve UDP 8.1-Konsole unterstützt das Aktualisieren von Knoten, wenn RPS und Agenten (oder agentenlose Sicherungs-Proxys) noch unter UDP 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 ausgeführt werden. Der Plan wird bereitgestellt. Der Agent wird nicht automatisch aktualisiert.
- DieArcserve UDP 8.1-Konsole unterstützt das Hinzufügen eines Version 8.0-RPS-Servers. Der RPS wird beim Hinzufügen jedoch nicht automatisch auf Arcserve UDP Version 8.1 aktualisiert.
- Die Arcserve UDP 8.1 -Konsole unterstützt das Hinzufügen einer früheren Version des Agenten (oder des agentenlosen Sicherungs-Proxys), ohne dass der Agent automatisch aktualisiert wird.

- DieArcserve UDP 8.1-Konsole unterstützt das Hinzufügen von Knoten zu einem vorhandenen Plan.
  - Das Hinzufügen eines neuen Knotens zu einem vorhandenen Plan wird unterstützt, wenn der zugehörige RPS auf Version 8.1 aktualisiert wird. Andernfalls kann der Plan gespeichert werden, die Bereitstellung des Plans schlägt aber fehl.
  - Das Hinzufügen von Knoten vorheriger Versionen zum vorhandenen Plan wird unterstützt, wenn die Version mit der Version des RPS übereinstimmt. Der Agent wird nicht automatisch aktualisiert.
  - Das Hinzufügen eines Arcserve UDP 8.1-Knotens zum vorhandenen Plan wird unterstützt, wenn der zugehörige RPS auf UDP 8.1. aktualisiert wird.
- Gateway wird automatisch aktualisiert, um zur Version der Arcserve UDP-Konsole zu passen.
- Richtlinie zur Abwärtskompatibilität bei der Replikation:
  - Die Replikation wird unterstützt, wenn die Konsole auf Arcserve UDP 8.1 aktualisiert wird, alle zugehörigen Recovery Point Server (RPSs) aber noch unter UDP 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 ausgeführt werden.
    - Die Replikation von einem Quell-RPS mit Arcserve UDP 8.1 zu einem Ziel-RPS mit UDP 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 wird unterstützt.
    - Die Replikation von einem Quell-RPS mit Arcserve UDP UDP 8.0, 7.0, 7.0 Update 1 und 7.0 Update 2 zu einem Ziel-RPS mit UPD 8.1 wird unterstützt.
- Richtlinie zur Abwärtskompatibilität bei Virtual Standby:
  - Die Version des VSB Monitor/Proxys sollte ähnlich der Agentenversion sein, wenn das Sicherungsziel ein freigegebener Ordner ist.
  - Die Version des VSB Monitor/Proxys sollte ähnlich der RPS-Version sein, wenn das Sicherungsziel ein RPS ist.
- Richtlinie zur Abwärtskompatibilität bei Instant VMs:

  Die Version des Instant VM-Wiederherstellungsservers sollte ähnlich der Arcserve UDP Konsolenversion sein.

Unterstützungsrichtlinie zur Abwärtskompatibilität für Arcserve UDP Version 7.x

Unterstützung der Abwärtskompatibilität zwischen verschiedenen UDP-Konsolen über den Task "Zu einem remote verwalteten RPS replizieren"

Wenn Sie den Task *Zu einem remote verwalteten RPS replizieren* ausführen möchten, wird empfohlen, zunächst die Konsole und den RPS auf Zielseite zu aktualisieren, bevor Sie die Konsole/den RPS/den Agenten auf Quellseite aktualisieren.

- Die Replikation wird unterstützt, wenn der Quell-RPS UDP 8.1 und der Ziel-RPS noch UDP 7.0, 7.0 Update 1 und 7.0 Update 2 verwendet.
- Die Replikation wird unterstützt, wenn der Quell-RPS UDP 7.0, 7.0 Update 1 und 7.0 Update 2 und der Ziel-RPS UDP 8.1 verwendet.
- Replikationsverhalten:
  - Wenn Sie an beiden Standorten ein Upgrade auf UDP 8.1 durchführen, können Sie ohne öffentliche IP von Cloud Hybrid zu einem lokalen Ziel replizieren (neues UDP-Verhalten).
  - Wenn Sie nur an einem der Standorte ein Upgrade auf UDP 8.1 durchführen und der andere Standort eine unterstützte Version von UDP verwendet, können Sie mithilfe der öffentlichen IP von Cloud Hybrid zu einem lokalen Ziel replizieren.

Unterstützung der Abwärtskompatibilität für Windows RPS/Agent (oder agentenlosen Sicherungs-Proxy)

- Die Arcserve UDP 8.1-Konsole unterstützt Recovery Point Server (RPS) und Agenten (oder agentenlose Sicherungs-Proxys) der UDP-Versionen 7.0, 7.0 Update 1 und 7.0 Update 2 zu Sicherungszwecken, wenn sich der Plan nach einem Upgrade nicht ändert.
- Die Arcserve UDP 8.1-Konsole und RPS unterstützen Agenten (oder agentenlose Sicherungs-Proxys) der UDP-Versionen 7.0, 7.0 Update 1 und 7.0 Update 2 zu Sicherungszwecken, wenn sich der Plan nach einem Upgrade nicht ändert.
- Die Arcserve UDP 8.1-Konsole unterstützt die Bereitstellung des vorhandenen Plans ohne jegliche Änderungen, wenn RPS und Agenten (oder agentenlose Sicherungs-Proxys) noch unter UDP 7.0, 7.0 Update 1 und 7.0 Update 2 ausgeführt werden. Der Agent wird nicht automatisch aktualisiert.
- Die Arcserve UDP 8.1-Konsole unterstützt das Unterbrechen oder Wiederaufnehmen eines vorhandenen Plans ohne jegliche Änderungen, wenn RPS

und Agenten (oder agentenlose Sicherungs-Proxys) noch unter UDP 7.0, 7.0 Update 1 und 7.0 Update 2 ausgeführt werden. Der Agent wird nicht automatisch aktualisiert.

- Die Arcserve UDP 8.1-Konsole unterstützt das Erstellen eines neuen Plans oder das Ändern eines vorhandenen Plans zur Konfiguration von Legacy-Funktionen, die in der vorherigen Version bereits unterstützt wurden, wenn RPS und Agenten (oder agentenlosen Sicherungs-Proxys) noch unter UDP 7.0, 7.0 Update 1 und 7.0 Update 2 ausgeführt werden. Der Agent wird nicht automatisch aktualisiert.
- Die Arcserve UDP 8.1-Konsole unterstützt das Erstellen eines neuen Plans oder das Ändern eines vorhandenen Plans zur Einbeziehung neuer Funktionen in Version UDP 8.1, wenn der zugehörige RPS, Proxy oder Agent bereits auf die erwartete Version aktualisiert wurde.

  Beispiel:

  - Das Angeben des Netzwerks für die Sicherung wird unterstützt, wenn Konsole, RPS, Proxy und Agent auf UDP 7.0, 7.0 Update 1, 7.0 Update 2, 8.0 und 8.1 aktualisiert werden.
- Die Arcserve UDP 8.1-Konsole unterstützt das Aktualisieren von Knoten, wenn RPS und Agenten (oder agentenlose Sicherungs-Proxys) noch unter UDP 7.0, 7.0 Update 1 und 7.0 Update 2 ausgeführt werden. Der Plan wird bereitgestellt. Der Agent wird nicht automatisch aktualisiert.
- Die Arcserve UDP 8.1-Konsole unterstützt das Hinzufügen eines RPS-Servers mit UDP-Version 7.0, 7.0 Update 1 und 7.0 Update 2. Wenn ein RPS-Server hinzugefügt wird, wird er nicht automatisch auf Arcserve UDP 8.1 aktualisiert.
- Die Arcserve UDP 8.1 -Konsole unterstützt das Hinzufügen einer früheren Version des Agenten (oder des agentenlosen Sicherungs-Proxys), ohne dass der Agent automatisch aktualisiert wird.
- DieArcserve UDP 8.1-Konsole unterstützt das Hinzufügen von Knoten zu einem vorhandenen Plan.

  - Das Hinzufügen eines neuen Knotens zu einem vorhandenen Plan wird unterstützt, wenn der zugehörige RPS auf UDP 8.1 aktualisiert wird. Andernfalls kann der Plan gespeichert werden, die Bereitstellung des Plans schlägt aber fehl.
  - Das Hinzufügen von Knoten vorheriger Versionen zum vorhandenen Plan wird unterstützt, wenn die Version mit der Version des RPS übereinstimmt. Der Agent wird nicht automatisch aktualisiert.

- Das Hinzufügen eines Arcserve UDP 8.1-Knotens zum vorhandenen Plan wird unterstützt, wenn der zugehörige RPS auf UDP 8.1. aktualisiert wird.

- Gateway wird automatisch aktualisiert, um zur Version der Arcserve UDP-Konsole zu passen.
- Richtlinie zur Abwärtskompatibilität bei der Replikation:
  - Die Replikation wird unterstützt, wenn die Konsole auf Arcserve UDP 8.1 aktualisiert wird, alle zugehörigen Recovery Point Server (RPSs) aber noch unter UDP 7.0, 7.0 Update 1 und 7.0 Update 2 ausgeführt werden.
    - Die Replikation von einem Quell-RPS mit Arcserve UDP 8.1 zu einem Ziel-RPS mit UDP 7.0, 7.0 Update 1 und 7.0 Update 2 wird unterstützt.
    - Die Replikation von einem Quell-RPS mit Arcserve UDP UDP 7.0, 7.0 Update 1 und 7.0 Update 2 zu einem Ziel-RPS mit UDP 8.1 wird unterstützt.
- Richtlinie zur Abwärtskompatibilität bei Virtual Standby:
  - Die Version des VSB Monitor/Proxys sollte ähnlich der Agentenversion sein, wenn das Sicherungsziel ein freigegebener Ordner ist.
  - Die Version des VSB Monitor/Proxys sollte ähnlich der RPS-Version sein, wenn das Sicherungsziel ein RPS ist.
- Richtlinie zur Abwärtskompatibilität bei Instant VMs:

  Die Version des Instant VM-Wiederherstellungsservers sollte ähnlich der Arcserve UDP Konsolenversion sein.

Support-Richtlinie zur Rückwärtskompatibilität für Arcserve UDP Version 6.5 Update 4

Unterstützung der Abwärtskompatibilität zwischen verschiedenen UDP-Konsolen über den Task "Zu einem remote verwalteten RPS replizieren"

Wenn Sie den Task *Zu einem remote verwalteten RPS replizieren* ausführen möchten, wird empfohlen, zunächst die Konsole und den RPS auf Zielseite zu aktualisieren, bevor Sie die Konsole/den RPS/den Agenten auf Quellseite aktualisieren.

- Die Replikation wird unterstützt, wenn der Quell-RPS UDP 8.1 und der Ziel-RPS noch Version 6.5 Update 4 verwendet.
- Die Replikation wird unterstützt, wenn der Quell-RPS über Version 6.5 Update 4 und der Ziel-RPS über UDP 8.1 verfügt und das Patch P00001738 angewendet wurde. Wenn die Quell-RPS Version 6.5 Update 1,2,3 ist, aktualisieren Sie zunächst auf Update 4 und wenden Sie Patch P00001738 an.

Unterstützung der Abwärtskompatibilität für Windows RPS/Agent (oder agentenlosen Sicherungs-Proxy)

- Die Arcserve UDP 8.1 -Konsole unterstützt Recovery Point Server (RPS) und Agenten (oder agentenlose Sicherungs-Proxys) der Version 6.5 Update 4 zu Sicherungszwecken, wenn sich der Plan nach einem Upgrade nicht ändert.
- Die Arcserve UDP 8.1 -Konsole und RPS unterstützen Agenten (oder agentenlose Sicherungs-Proxys) der Version 6.5 Update 4 zu Sicherungszwecken, wenn sich der Plan nach einem Upgrade nicht ändert.
- Die Arcserve UDP 8.1-Konsole unterstützt die Bereitstellung des vorhandenen Plans ohne jegliche Änderungen, wenn RPS und Agenten (oder agentenlose Sicherungs-Proxys) noch unter Version 6.5 Update 4 ausgeführt werden. Der Agent wird nicht automatisch aktualisiert.
- Die Arcserve UDP 8.1-Konsole unterstützt das Unterbrechen oder Wiederaufnehmen eines vorhandenen Plans ohne jegliche Änderungen, wenn RPS und Agenten (oder agentenlose Sicherungs-Proxys) noch unter Version 6.5 Update 4 ausgeführt werden. Der Agent wird nicht automatisch aktualisiert.
- Die Arcserve UDP 8.1-Konsole unterstützt das Erstellen eines neuen Plans oder das Ändern eines vorhandenen Plans zur Konfiguration von Legacy-Funktionen, die in der vorherigen Version bereits unterstützt wurden, wenn RPS und Agenten (oder agentenlosen Sicherungs-Proxys) noch unter Version 6.5 Update 4 ausgeführt werden. Der Agent wird nicht automatisch aktualisiert.

- Die Arcserve UDP 8.1-Konsole unterstützt das Erstellen eines neuen Plans oder das Ändern eines vorhandenen Plans zur Einbeziehung neuer Funktionen in Version UDP 8.1, wenn der zugehörige RPS, Proxy oder Agent bereits auf die erwartete Version aktualisiert wurde.

  Beispiel:

  - Das Angeben des Netzwerks für die Sicherung wird unterstützt, wenn Konsole, RPS, Proxy und Agent auf 7.0 Update 1, Update 2 oder UDP 8.1 aktualisiert werden.

- Die Arcserve UDP 8.1-Konsole unterstützt das Aktualisieren von Knoten, wenn RPS und Agenten (oder agentenlose Sicherungs-Proxys) noch unter Version 6.5 Update 4 ausgeführt werden. Der Plan wird bereitgestellt. Der Agent wird nicht automatisch aktualisiert.
- Die Arcserve UDP 8.1-Konsole unterstützt das Hinzufügen eines RPS-Servers mit Version 6.5 Update 4. Wenn ein RPS-Server hinzugefügt wird, wird er nicht automatisch auf Arcserve UDP 8.1 aktualisiert.
- Die Arcserve UDP 8.1 -Konsole unterstützt das Hinzufügen einer früheren Version des Agenten (oder des agentenlosen Sicherungs-Proxys), ohne dass der Agent automatisch aktualisiert wird.
- DieArcserve UDP 8.1-Konsole unterstützt das Hinzufügen von Knoten zu einem vorhandenen Plan.
  - Das Hinzufügen eines neuen Knotens zu einem vorhandenen Plan wird unterstützt, wenn der zugehörige RPS auf UDP 8.1 aktualisiert wird. Andernfalls kann der Plan gespeichert werden, die Bereitstellung des Plans schlägt aber fehl.
  - Das Hinzufügen von Knoten vorheriger Versionen zum vorhandenen Plan wird unterstützt, wenn die Version mit der Version des RPS übereinstimmt. Der Agent wird nicht automatisch aktualisiert.
  - Das Hinzufügen eines Arcserve UDP 8.1-Knotens zum vorhandenen Plan wird unterstützt, wenn der zugehörige RPS auf UDP 8.1. aktualisiert wird.
- Gateway wird automatisch aktualisiert, um zur Version der Arcserve UDP-Konsole zu passen.
- Richtlinie zur Abwärtskompatibilität bei der Replikation:
  - Die Replikation wird unterstützt, wenn die Konsole auf Arcserve UDP 8.1 aktualisiert wird, alle zugehörigen RPS aber noch unter Version 6.5 Update x ausgeführt werden.

        - Die Replikation von einem Quell-RPS mit Arcserve UDP 6.5 Update x zu einem Ziel-RPS mit Version 6.5 Update 4 wird unterstützt.
        - Die Replikation von einem Quell-RPS mit Arcserve UDP 6.5 Update 4 zu einem Ziel-RPS mit Version 6.5 Update x wird unterstützt.
    - Die Replikation von einem Quell-RPS mit Arcserve UDP 6.5 Update x zu einem Ziel-RPS mit UDP 8.1 wird unterstützt.
    - Die Replikation von einem Quell-RPS mit Arcserve UDP 8.1 zu einem Ziel-RPS mit 6.5 Update 4 wird unterstützt.
    - Die Replikation von einem Quell-RPS mit Arcserve UDP 8.1 zu einem Ziel-RPS mit Version 6.5 Update 3, Update 2, Update 1 oder der neuesten Version wird nicht unterstützt.
- Richtlinie zur Abwärtskompatibilität bei Virtual Standby:
    - Die Version des VSB Monitor/Proxys sollte ähnlich der Agentenversion sein, wenn das Sicherungsziel ein freigegebener Ordner ist.
    - Die Version des VSB Monitor/Proxys sollte ähnlich der RPS-Version sein, wenn das Sicherungsziel ein RPS ist.
- Richtlinie zur Abwärtskompatibilität bei Instant VMs:

  Die Version des Instant VM-Wiederherstellungsservers sollte ähnlich der Arcserve UDP Konsolenversion sein.

Unterstützung der Abwärtskompatibilität für Linux-Sicherungsserver

Für Linux-Sicherungsserver 7.x und 6.5.x:

- Die Arcserve UDP 8.1-Konsole unterstützt Linux-Sicherungsserver der Versionen 6.5.x und 7.x, wenn die Recovery Point Server (RPS) unter Arcserve UDP 8.1 ausgeführt werden. Alle Jobs werden reibungslos ausgeführt, mit Ausnahme der neuen Funktion oder Verbesserung in UDP 8.1.
- Die Arcserve UDP 8.1-Konsole unterstützt Recovery Point Server (RPS) und Linux-Sicherungsserver der Versionen 6.5.x und 7.x. Alle Jobs werden reibungslos ausgeführt, mit Ausnahme der neuen Funktion oder Verbesserung in 8.1.
- Nach einem Upgrade des Linux-Sicherungsservers auf Arcserve UDP 8.1 werden alle neue Funktionen für UDP 8.1 unterstützt.

Upgradesequenz für UDP-Konsole, RPS und Agent

Basierend auf der Unterstützungsrichtlinie zur Rückwärtskompatibilität hilft Ihnen die Planung Ihrer Aktualisierung in der folgenden Sequenz bei einer reibungslosen Aktualisierung:

1. Aktualisieren Sie Arcserve UDP-Konsole.
2. Aktualisieren Sie Arcserve UDP-RPS (DR-Standort).
3. Aktualisieren Sie Arcserve UDP-RPS (Rechenzentrum).
4. Aktualisieren Sie Arcserve UDP Agentless Proxy und einige oder alle Agenten im Rechenzentrum.
5. Aktualisieren Sie Arcserve UDP-RPS (Remote-Standort).
6. Aktualisieren Sie Arcserve UDP Agentless Proxy und einige oder alle Agenten am Remote-Standort.

   Hinweis: Wiederholen Sie Schritt 5 und 6 für jeden Standort.

   Hinweise:

   - Aktualisieren Sie zunächst MSP auf der Konsole oder RPS, wenn der MSP-Replikationstask konfiguriert ist.
   - Gateway wird automatisch aktualisiert, um mit der Version der Konsole über-einzustimmen.
   - Aktualisieren Sie gemäß der Support-Richtlinie zur Abwärtskompatibilität von Replikation erst den Ziel-RPS und dann den Quell-RPS.

So aktualisieren Sie auf Arcserve UDP 8.0 von einer früheren Version

Das Aktualisieren einer Installation bedeutet, Funktionen oder Komponenten mit einer höheren Version neu zu installieren. Sie können beim Aktualisierungsvorgang einen Großteil Ihrer aktuellen Einstellungen beibehalten und die in der vorherigen Arcserve UDP-Datenbank gespeicherten Informationen in die neue Arcserve UDP-Datenbank migrieren.

Aktualisierungshinweis

- Überprüfen Sie, ob die Hardware-Voraussetzungen der Arcserve UDP-Version 8.0 erfüllt sind. Weitere Informationen finden Sie unter *System-Informationen* in *Release Hinweise v8.0*.
- Arcserve UDP Version 8.0 unterstützte Plattform, Hypervisor, OS oder Application Version erforderlich. Weitere Informationen finden Sie in der Kompatibilitätsmatrix.
- Bevor Sie von 6.5.3 oder früherne unterstützten Versionen aktualisieren, sollten Sie vermeiden, einen bestehenden Plan anzuhalten. Wenn der Plan vor der Aktualisierung angehalten wurde, kann der Plan nicht fortgesetzt werden, solange nicht alle zugehörigen RPS aktualisiert worden sind.
- Erwerben Sie den Produktschlüssel für Arcserve UDP Version 8.0, und halten Sie ihn bereit.
- Entfernen Sie die vorherige Version der Arcserve Exchange Granular Restore (AEGR) Einzelanwendung für Arcserve UDP Version 5.0. Falls erkannt, fordert Sie der Installationsassistent zum Entfernen auf.
- Im Idealfall sollten ältere Pläne bei jedem der unten beschriebenen Upgrade-Schritte einwandfrei funktionieren.

Führen Sie diese Schritte durch, um zu aktualisieren:

1. Aktualisieren Sie auf MSP-Seite die vorherige Arcserve UDP-Konsole auf Arcserve UDP 8.0.

   Dieser Schritt ist nur erforderlich, wenn **der Task "Von ferngesteuert verwaltetem RPS replizieren"** im vorherigen Release konfiguriert ist.

   Hinweise:

   - Wenn für den Knoten nur die Konsole installiert ist, aktualisieren Sie die Konsole. Das Beenden laufender Aufträge ist nicht erforderlich, um die Konsole zu aktualisieren.

- Wenn die Konsole und RPS auf dem Knoten installiert sind, planen Sie die Aktualisierung der Konsole, wenn vor der Aktualisierung keine Aufträge laufen. Falls erforderlich, halten Sie die Datenspeicher des RPS an, um ausgeführte Jobs abzubrechen, bevor Sie die Konsole aktualisieren.
- Weitere Informationen zur Aktualisierung der Konsole finden Sie unter Installieren von Arcserve Unified Data Protection mit dem Setup-Assistenten oder Installieren von Arcserve UDP mit dem einheitlichen Installationsprogramm.

2. Aktualisieren Sie für MSP den vorherigen Arcserve UDP RPS auf Arcserve UDP Version 8.0.

   Dieser Schritt ist nur erforderlich, wenn **der Task "Von ferngesteuert verwaltetem RPS replizieren"** im vorherigen Release konfiguriert ist.

   Hinweise:

   - Planen Sie die Aktualisierung von RPS, wenn keine Aufträge vor der Aktualisierung ausgeführt werden. Falls erforderlich, halten Sie die Datenspeicher des RPS an, um ausgeführte Jobs abzubrechen, bevor Sie den RPS aktualisieren.
   - Weitere Informationen zum Aktualisieren des RPS finden Sie unter Recovery Point Server installieren/aktualisieren.

3. Aktualisieren Sie für Kunden die vorherige Arcserve UDP Konsole auf Arcserve UDP Version 8.0.

   Hinweise:

   - Wenn für den Knoten nur die Konsole installiert ist, aktualisieren Sie die Konsole. Das Beenden laufender Aufträge ist nicht erforderlich, um die Konsole zu aktualisieren.
   - Wenn auf dem Knoten die Konsole und RPS installiert sind und keine Jobs auf dem RPS laufen, halten Sie die Datenspeicherung auf dem RPS an, um zunächst die laufenden Aufträge abzubrechen. Aktualisieren Sie anschließend die Konsole.
   - Weitere Informationen zur Aktualisierung der Konsole finden Sie unter Installieren von Arcserve Unified Data Protection mit dem Setup-Assistenten oder Installieren von Arcserve UDP mit dem einheitlichen Installationsprogramm.

4. Aktualisieren Sie auf Kundenseite den vorherigen Replikationsziel-RPS für Arcserve UDP auf Arcserve UDP 8.0.

   Hinweise:

   - Arcserve UDP 8.0 unterstützt die Replikation von Arcserve UDP Version 6.5.x Quell-RPS auf Arcserve UDP 8.0 Ziel-RPS. Wenn der Plan mehrere

Replikations-Tasks enthält, aktualisieren Sie zunächst den letzten Replikationsziel-RPS.

- Replikation von Arcserve UDP 8.0 Quell-RPS auf eine niedrigere Version des Ziel-RPS wird nur unterstützt, wenn der Ziel-RPS die Version Arcserve UDP 6.5 Update 4 hat.
- Weitere Informationen zum Aktualisieren des RPS finden Sie unter Recovery Point Server installieren/aktualisieren.

5. Aktualisieren Sie auf Kundenseite den vorherigen Replikationsquell-RPS auf Arcserve UDP 8.0.

   Hinweis: Weitere Informationen zum Aktualisieren des RPS finden Sie unter Recovery Point Server installieren/aktualisieren.

6. Aktualisieren Sie auf Kundenseite den vorherigen Proxy und die vorherigen Agenten auf Arcserve UDP 8.0.

   Hinweise:

   - Weitere Informationen über die Aktualisierung eines agentenlosen Proxy und des Agenten von Windows, finden Sie unter Bereitstellen des Agenten auf Knoten.
   - Weitere Informationen zum Aktualisieren des Linux-Sicherungsservers finden Sie unter So aktualisieren Sie Arcserve UDP Agent (Linux).

7. Aktualisieren Sie auf Kundeseite den vorherigen VSB Monitor oder Instant VM Recovery Server auf Arcserve UDP 8.0.

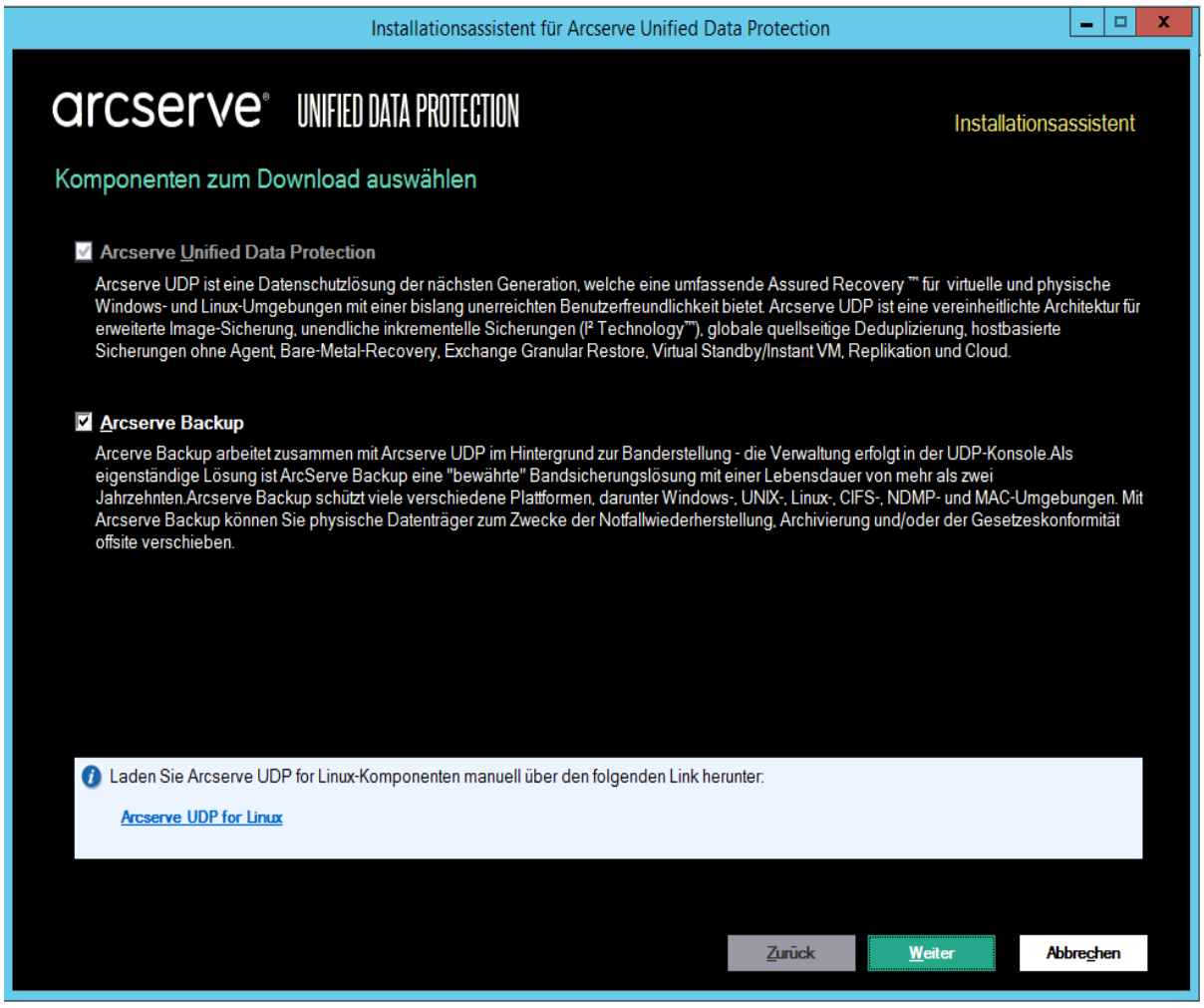
   Hinweis: Weitere Informationen zur Aktualisierung des VSB Monitors finden Sie unter Installieren von Arcserve Unified Data Protection mit dem Setup-Assistenten oder Installieren von Arcserve UDP mit dem einheitlichen Installationsprogramm.

So aktualisieren Sie auf Arcserve UDP 8.0 mit einem Installationsprogramm

Sie können Arcserve UDP Version 8.0 mit dem Installationsprogramm aktualisieren. Überprüfen Sie vor dem Upgrade die unterstützten Versionen.

Gehen Sie wie folgt vor:

1. Laden Sie die Datei "ASDownloader.exe" über den Arcserve-Download-Link herunter.
2. Führen Sie die ASDownloader.exe aus, akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf **Weiter**.
3. Klicken Sie auf **Weiter** auf dem **Erste Schritte** Bildschirm.
4. Wählen Sie auf dem Bildschirm **Komponenten zum Download auswählen** die Komponenten aus, die Sie herunterladen möchten.



Aspekte für die Auswahl der Komponenten:

- Um die Vorgängerversion von Arcserve UDP zu aktualisieren, wählen Sie die Option **Arcserve Unified Data Protection**.
- Um die Vorgängerversion von Arcserve Backup zu aktualisieren, wählen Sie die Option **Arcserve Backup**.

Hinweis: Einige Komponenten werden automatisch nach Abhängigkeit ausgewählt, wenn Sie die Option **Arcserve Backup** auswählen. Wenn Sie die Komponenten nicht auf demselben Rechner installieren möchten, lesen Sie So aktualisieren Sie auf Arcserve UDP 8.0 von einer früheren Version, und verwenden Sie den Setup-Assistenten, um nur die vorhandenen Komponenten zu aktualisieren. Von hier aus können Sie auch das aktuelle Linux Setup für Arcserve UDP auswählen.

5. Nachdem die Komponenten heruntergeladen wurden, wählen Sie die Installationsmethode, um die ausgewählten Komponenten zu aktualisieren.

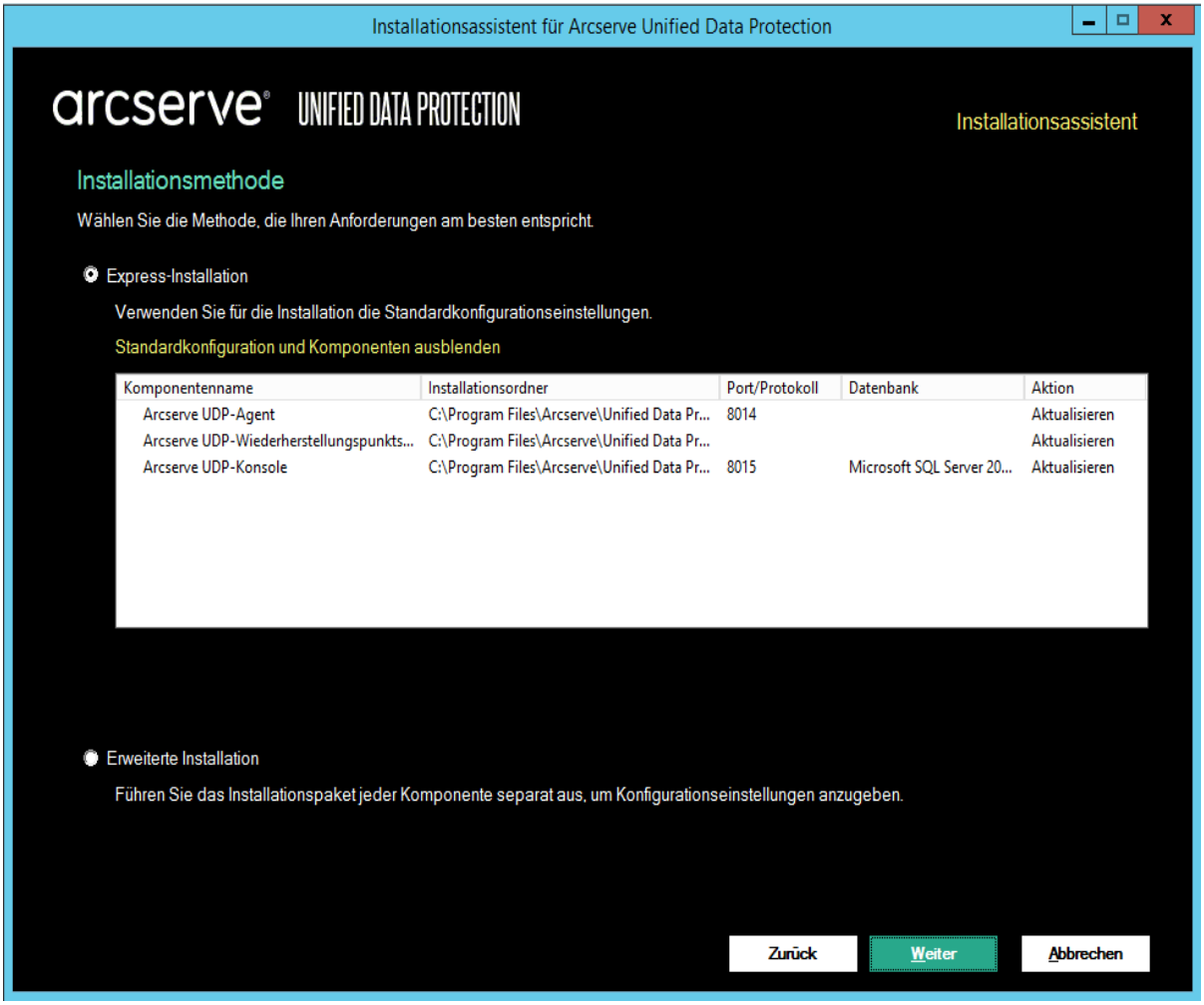
   Express-Installation

   Die Express-Installation wird empfohlen, wenn Sie alle Komponenten mit ihrer Standardkonfiguration auf dem gleichen Rechner installieren möchten.

   Hinweise:

   - Überprüfen Sie die erforderlichen Voraussetzungen für die Aktualisierung. Zum Beispiel ist .Net 4.5.1 für Arcserve Backup erforderlich. Befolgen Sie die Anweisungen, die im Installationsprogramm angezeigt werden, bis alle Voraussetzungen erfüllt sind.
   - Überprüfen Sie die Anforderungen der Kompatibilitätsmatrix.
   - Die Express Installation installiert die Komponenten nach Standardkonfiguration, beispielsweise Pfad, Protokoll, Port und Datenbank. Wenn Sie für die Aktualisierung die Express Installation verwenden, wird die Kon-

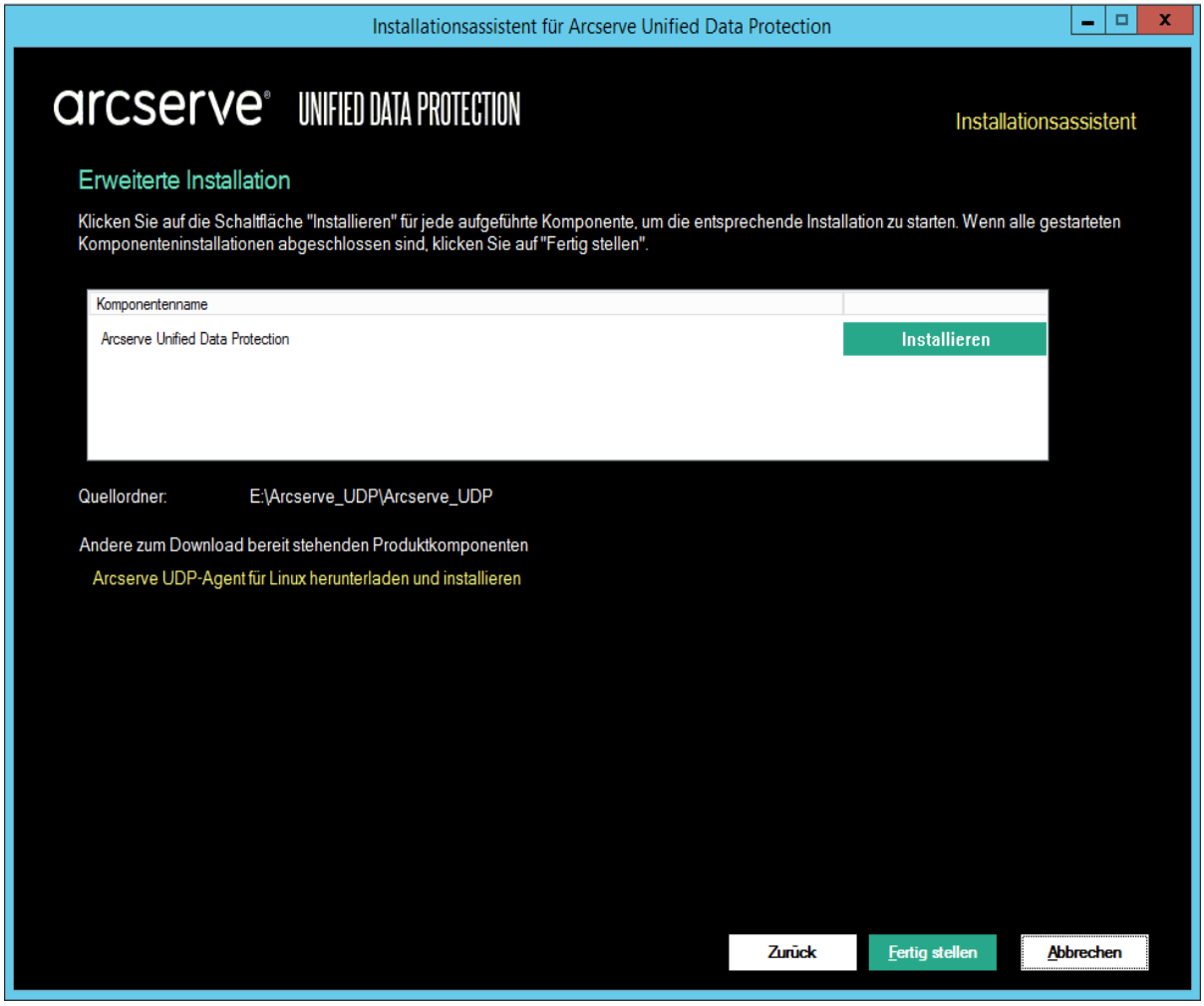
figuration der Vorgängerversion übernommen.



Erweiterte Installation

Wir empfehlen die erweiterte Installation für die Installation oder Aktualisierung einzelner Komponenten auf demselben Rechner. Klicken Sie auf **Installieren**, um jede Komponente separat zu aktualisieren oder zu installieren.

Hinweis: Um Arcserve Unified Data Protection Agent for Linux mithilfe des einheitlichen Installationsprogramms zu aktualisieren, laden Sie die Abbilder über die am Ende des Installers geteilten Links herunter. Befolgen Sie nach dem Kopieren der Bilder auf den Linux-Sicherungsserver die Schritte unter *So aktualisieren Sie Arcserve UDP Agent (Linux)* in der Agent for Linux Online-Hilfe.



Arcserve UDP wurde erfolgreich mit dem einheitlichen Installationsprogramm aktualisiert.

Hinweis: Weitere Informationen finden Sie unter So aktualisieren Sie auf Arcserve UDP 8.0 von einer früheren Version.

So aktualisieren Sie auf Arcserve UDP 8.0 oder Arcserve Backup 18.0, um das Kopieren auf Band zu aktivieren

In diesem Abschnitt wird erläutert, wie Arcserve UDP oder Arcserve Backup 18.0 von einer früheren Version von Arcserve UDP oder Arcserve Backup aktualisiert werden, um Kopie auf Band zu ermöglichen. Arcserve UDP Version 8.0 ist integrierbar in Arcserve Backup 18.0 und ermöglicht das Kopieren von Backup-Daten auf ein Bandmedium. Sie können einen Plan mit dem Task **Kopie auf Band** in der Arcserve UDP-Konsole erstellen oder einen bestehenden Plan erstellen.

Aktualisierungshinweis

- Um sicherzustellen, dass der bestehende Plan mit dem Kopie-auf-Band-Auftrag reibungslos läuft, sollten Sie Arcserve Backup auf 18.0 aktualisieren, bevor Sie Arcserve UDP auf 8.0 aktualisieren.
- Hardwareanforderungen von Arcserve UDP Version 8.0 überprüfen. Ausführliche Informationen zu den Hardwarevoraussetzungen finden Sie in den *Systeminformationen* in *Versionshinweise 8.0*.
- Arcserve UDP Version 8.0 unterstützte Plattform, Hypervisor, OS oder Application Version erforderlich. Weitere Informationen finden Sie in der Kompatibilitätsmatrix.
- Bevor Sie UDP 6.5.3 oder frühere unterstützte Versionen aktualisieren, sollten Sie vermeiden, einen bestehenden Plan anzuhalten. Wenn der Plan vor der Aktualisierung angehalten wurde, kann der Plan nicht fortgesetzt werden, solange der zugehörige RPS nicht aktualisiert wurde.
- Erwerben Sie den Produktschlüssel für Arcserve UDP Version 8.0, und halten Sie ihn bereit.
- Entfernen Sie die vorherige Version der Arcserve Exchange Granular Restore (AEGR) Einzelanwendung für Arcserve UDP Version 5.0. Falls erkannt, fordert Sie der Installationsassistent zum Entfernen auf.
- Im Idealfall sollten ältere Pläne bei jedem der unten beschriebenen Upgrade-Schritte einwandfrei funktionieren.

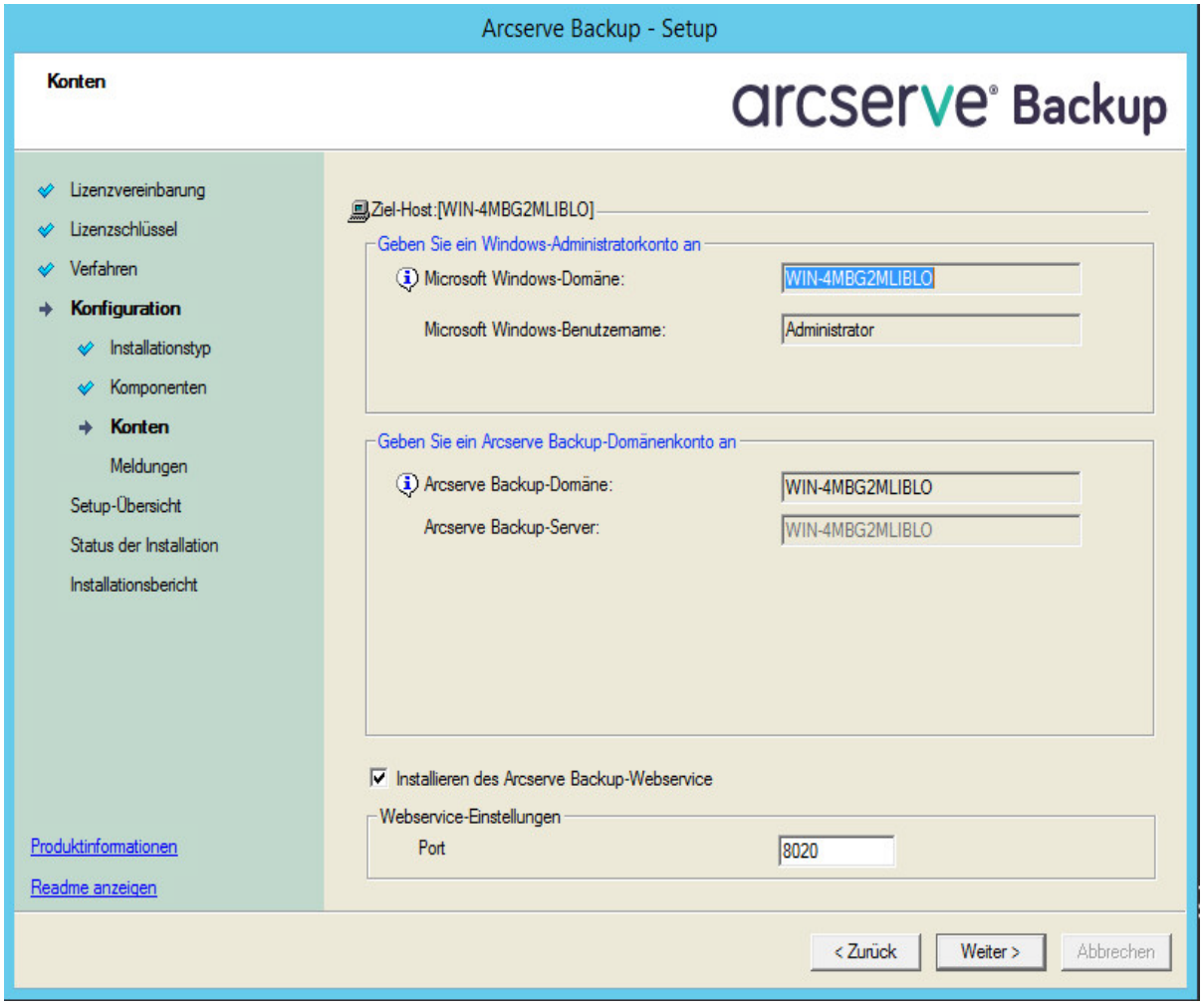
Hinweis zu "Kopie auf Band"

- Bereiten Sie den Arcserve Backup 18.0-Server vor, um von jedem zuvor unterstützten Upgrade-Pfad zu installieren oder zu aktualisieren. Arcserve Backup ist vor der Konfiguration des Tasks **Kopie auf Band** in einem Arcserve UDP-Plan erforderlich.

- Überprüfen Sie, ob die Arcserve Backup 18.0 Anforderung eingehalten wird. Weitere Informationen finden Sie in der Kompatibilitätsmatrix.
- Erwerben Sie den Produktschlüssel für Arcserve Backup 18.0, und bewahren Sie ihn auf.

Befolgen Sie diese Schritte, um eine Kopie auf Band-Funktion zu aktualisieren und zu aktivieren:

1. Aktualisierung auf Arcserve Backup 18.0 von einer vorherigen Version oder Installation von Arcserve Backup 18.0 mit aktivierter **Arcserve Backup Web Service**-Installationsoption.



Hinweis: Weitere Informationen über die Installation und die Aktualisierung von Arcserve Backup finden Sie in der *Arcserve Backup 18.0 Implementationsanleitung*.

Führen Sie nach erfolgreicher Aktualisierung die folgenden Aufgaben aus:

- Überprüfen Sie, ob der Jobprozess im Arcserve Backup-Manager gestartet wurde.

- Verifizieren Sie in der Windows-Dienstkonsole, ob **Arcserve Backup Web Service** ausgeführt wird.

2. Aktualisieren Sie auf Arcserve UDP Version 8.0 von einem älteren Release.

   Hinweis: Weitere Informationen zur Aktualisierung von einem älteren Release finden Sie unter So aktualisieren Sie von einer früheren Version auf Arcserve UDP 8.0.

3. Konfigurieren Sie den **Kopie auf Band**-Task in der Arcserve UDP-Konsole für einen vorhandenen oder einen neuen Plan.

   Hinweis: Weitere Informationen über die Konfiguration des Kopie-auf-Band-Auftrags erhalten Sie unter Erstellen eines Zeitplans für das Kopieren auf Band.

   Der Plan sollte für jede Stufe funktionieren.

So migrieren Sie die Arcserve UDP-Konsole von einem Server auf einen anderen

Weitere Informationen erhalten Sie unter diesem Link.

So aktualisieren Sie das Gateway auf dieselbe Version wie die zugehörige registrierte Konsole

Die Version des Arcserve UDP-Gateway und der zugehörigen registrierten Konsole müssen übereinstimmen. Nachdem die Arcserve UDP-Konsole aktualisiert wurde, wird beim Start des Dienstes die zugehörige Gateway-Version überprüft. Wenn die Gateway-Version nicht mit der Konsolenversion übereinstimmt, löst Arcserve UDP eine automatische Aktualisierung für die Gateway-Server aus.

Wenn das Gateway für die automatische Aktualisierung nicht verfügbar ist, können Sie das Gateway später manuell aktualisieren.

Führen Sie diese Schritte aus, um das Gateway manuell zu aktualisieren:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Klicken Sie auf die Registerkarte **Ressourcen**, navigieren Sie zu **Infrastruktur**, und klicken Sie auf **Standorte**.
3. Wählen Sie die Standorte aus, die aktualisiert werden sollen.
4. Klicken Sie auf die Drop-down-Liste **Aktionen** und anschließend auf **Gateway aktualisieren**.

   Ein Bestätigungsdialogfeld wird geöffnet.
5. Klicken Sie auf **Ja**.

   Das Gateway wird mit der aktuellen Version von Arcserve UDP Gateway aktualisiert.

So migrieren Sie die Arcserve UDP-Konsole

Sie können eine Arcserve UDP-Konsole in eine andere Arcserve UDP-Konsole migrieren, indem Sie *ConsoleMigration.exe* verwenden. Ab Arcserve UDP v6.5 Update 2 können Sie die Arcserve UDP-Konsole zwischen zwei Arcserve UDP-Konsolen migrieren.

Verwenden Sie *ConsoleMigration.exe* für BackupDB und RecoverDB. Der folgende Screenshot zeigt die Verwendung von *ConsoleMigration.exe*:

Gehen Sie zum Abschließen des Migrationsvorgangs folgendermaßen vor:

1. Führen Sie in einer alten Arcserve UDP-Konsole eine Sicherung der Arcserve UDP-Datenbank durch.

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe
-BackupDB

Backed up DB and version files completed.

DB and version files were created at "C:\Program Files\Arcserve\Unified Data
Protection\Management\BIN\Appliance\DB_Migration".
```

   Der Ordner *DB_Migration* wird erstellt.

2. Kopieren Sie in der neuen Arcserve UDP-Konsole den Ordner *DB_Migration* in den folgenden Pfad:

   <UDP_Home> *Management**BIN**Appliance*\

3. Auf der neuen Arcserve UDP-Konsole führen Sie die im Bildschirm unten aufgeführten Schritte durch, um die Datenbank der Arcserve UDPKonsole wiederherzustellen.

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe
-RecoverDB

Are you sure you want to recover the backup DB file? (y/n): y

Stopping Arcserve UDP management service, please wait...

Recovering backup DB file...

Updating nodes, please wait...

Please update nodes manually from UDP console, if you still encounter disconnected nodes.

The disconnected nodes(if exist) will be saved at "C:\Program Files\Arcserve\Unified Data Protec
tion\Management\BIN\Appliance\DB_Migration\logs".

Console migration completed. Console use DB "localhost\ARCSERVE_APP".
```

   Hinweis: Wenn in der Arcserve UDP-Konsole eine andere als die lokale Website vorhanden ist, gehen Sie wie in der Datei *NewRegistrationText.txt* beschrieben vor, um die Website erneut zu registrieren.

Sie haben die Migration der Arcserve UDP-Konsole in die neue Arcserve UDP-Konsole erfolgreich abgeschlossen.

Mit diesem Tool können Sie die Konsolenmigration für die Arcserve UDP-Konsole ausführen, die mit der Remote-SQL-Datenbank verbunden ist. Nach Abschluss der Migration wird die migrierte Arcserve UDP-Konsole so konfiguriert, dass sie sich mit derselben Remote-SQL-Datenbank verbindet.

Hinweis: Wenn Sie in UDP 6.5 Update 2 und Update 3 das Tool für die Konsolenmigration verwenden, um die Migration zwischen zwei Arcserve UDP-Konsolen durchzuführen, muss sowohl die Version der Arcserve UDP-Konsole als auch die Version der SQL-Datenbank auf den beiden Arcserve UDP-Konsolensystemen übereinstimmen. Andernfalls schlägt die Konsolenmigration fehl, und eine Fehlermeldung wird in der Befehlszeile und den Protokolldateien unter dem folgenden Pfad angezeigt:

<UDP_Home> \Management\BIN\Appliance\logs

In Arcserve UDP 6.5 Update 4 wird die Option ***-force*** im Befehl ***ConsoleMigration.exe*** eingeführt, um die Migration der Recovery-Sicherungsdatenbankdateien auf der Zielkonsole unter folgenden Umständen zu erzwingen:

1. Wenn Sie eine Konsolenmigration zwischen zwei Konsolen durchführen möchten, wobei die Quellkonsole SQL Server Enterprise Edition verwendet und die Zielkonsole SQL Server Express Edition. In diesem Fall beträgt die erforderliche Mindestdatenbankgröße der UDP-Quellkonsole 4000 MB.
2. Wenn Sie eine Konsolenmigration von einer Konsole, die eine erweiterte Version der SQL Server-Datenbank verwendet, zu einer Konsole, die eine ältere Version der SQL Server-Datenbank verwendet, durchführen möchten. Beispiel: Eine Migration von einer Konsole mit SQL Server 2016 zu einer Konsole mit SQL Server 2014.

Kapitel 5: Erkennen und Konfigurieren von Arcserve UDP

In diesem Abschnitt werden die folgenden Themen behandelt:

Anmeldung bei der Arcserve UDP-Konsole mit der Multi-Faktor-Authentifizierung

Arcserve UDP unterstützt Multi-Faktor-Authentifizierung (MFA), die eine zusätzliche Sicherheitsebene für alle Benutzer bietet. MFA ist ein Anmeldevorgang, bei dem der Benutzer aufgefordert wird, eine zusätzliche Form der Identifizierung anzugeben. Diese Authentifizierungsmethode erfordert mehr als einen Faktor für die Überprüfung der Benutzeridentität. Im Allgemeinen wird bei der MFA-Anmeldung eine Zwei-Faktor-Authentifizierung verwendet, die zwei Faktoren für die Benutzeridentifizierung zulässt.

Arcserve UDP unterstützt die Zwei-Faktor-Authentifizierung. Es ermöglicht Benutzernamen und Kennwort als erste Faktor-Authentifizierung. Die zweite Faktorauthentifizierung verwendet eine der folgenden Optionen:

- **Zeitbasierter einmaliger Passcode (TOTP):** Im Gegensatz zum herkömmlichen OTP, das an eine E-Mail-Adresse oder SMS gesendet wird, wird ein TOTP mithilfe einer Authentifizierungs-App generiert. Der TOTP ist nur von kurzer Dauer und wird alle 30 Sekunden aktualisiert.
- **E-Mail-OTP:** Diese Funktion authentifiziert sich mit einem OTP, das an die registrierte E-Mail-Adresse gesendet wird, und das OTP ist 30 Sekunden lang gültig. Sie wird nur aktiviert, wenn Sie die E-Mail-Adresse konfiguriert haben.

In diesem Abschnitt werden die folgenden Themen behandelt:

Überprüfen der Voraussetzungen

Berücksichtigen Sie folgende Voraussetzungen:

- Sie müssen die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktivieren. Weitere Informationen zum Aktivieren von MFA finden Sie unter Konfigurieren der Multi-Faktor-Authentifizierung als Administrator.

  Hinweis: Nur Administratoren können die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktivieren.

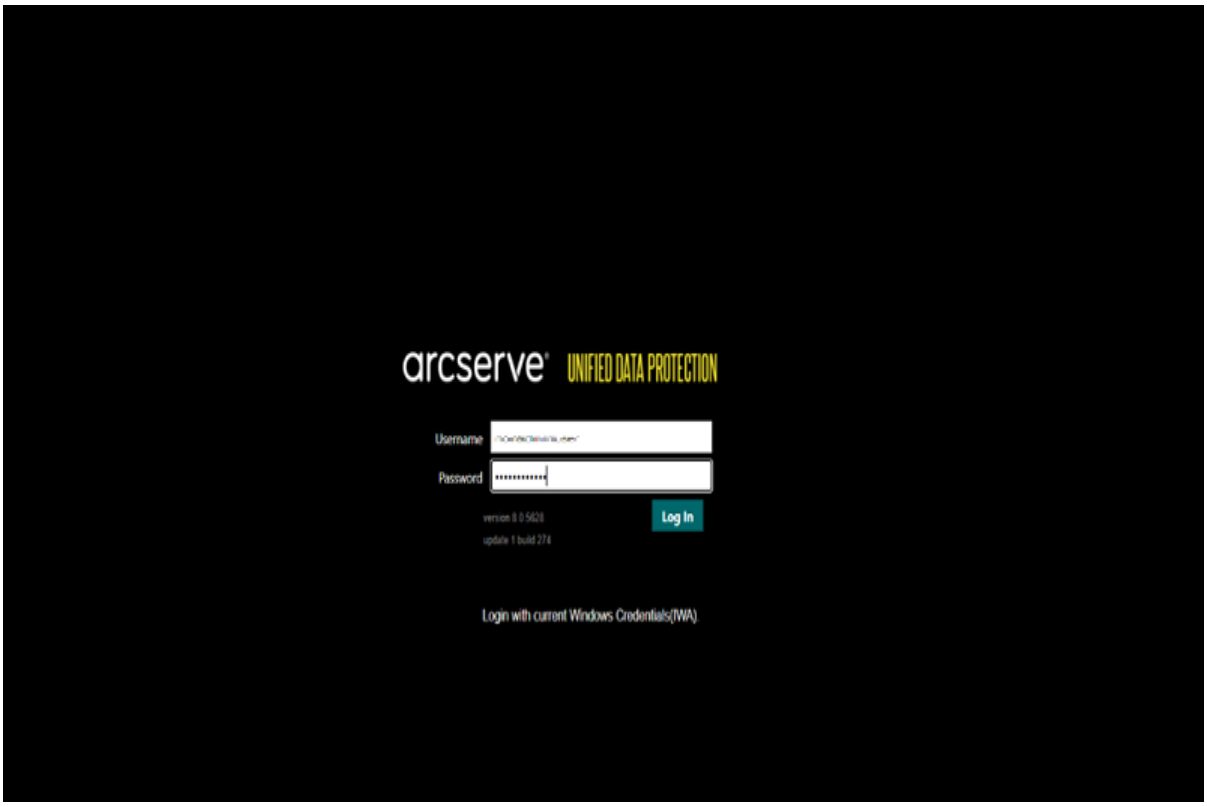
- Installieren Sie eine mobile Authentifizierungs-App auf Ihrem mobilen Gerät. Sie finden die Authentifikator-Apps wie Google Authenticator oder Microsoft Authentication im App-Store Ihres mobilen Geräts.

So melden Sie sich mit MFA bei der Arcserve UDP-Konsole an

Dieser Abschnitt enthält Informationen zur Anmeldung bei der Arcserve UDP-Konsole mithilfe von MFA.

Befolgen Sie diese Schritte:

1. Gehen Sie zur Anmeldeseite der UDP-Konsole.
2. Geben Sie nach Bedarf den Benutzernamen und das Kennwort ein, und klicken Sie dann auf die Schaltfläche **Anmelden**.

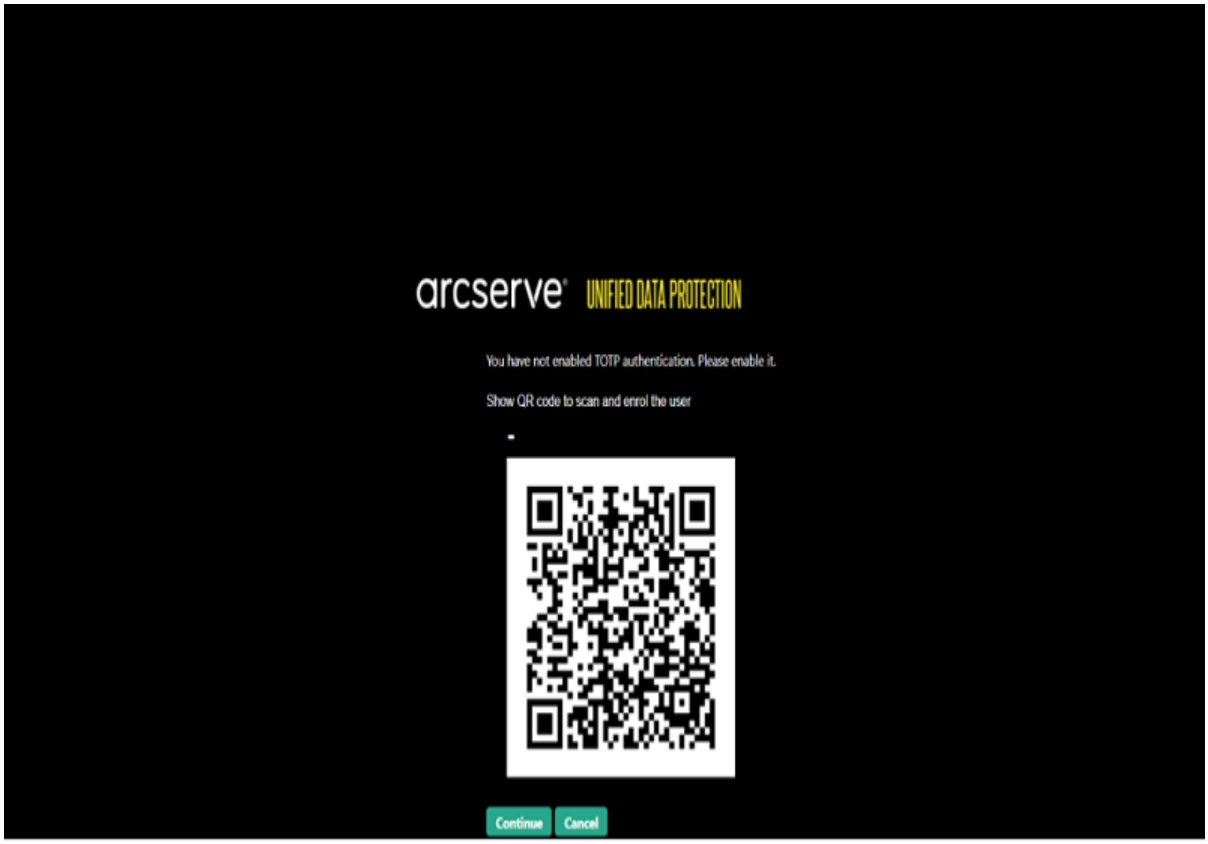


Nach der erfolgreichen Überprüfung der ersten Faktor-Authentifizierung wird die Seite für die zweite Faktor-Authentifizierung angezeigt.

3. Wenn Sie die TOTP-Authentifizierung nicht aktiviert haben, gehen Sie folgendermaßen vor:

a. Klicken Sie auf die Schaltfläche **QR-Code anzeigen**, um den Benutzer zu durchsuchen und zu registrieren.

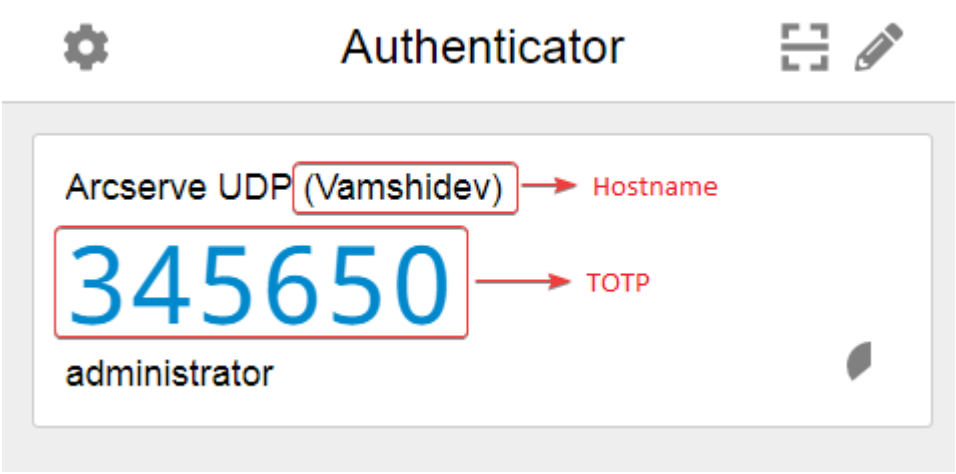
   Das Bild des QR-Codes wird angezeigt.



b. Scannen Sie das QR-Code-Bild mithilfe einer Authentifizierungs-App, um den TOTP zu generieren.

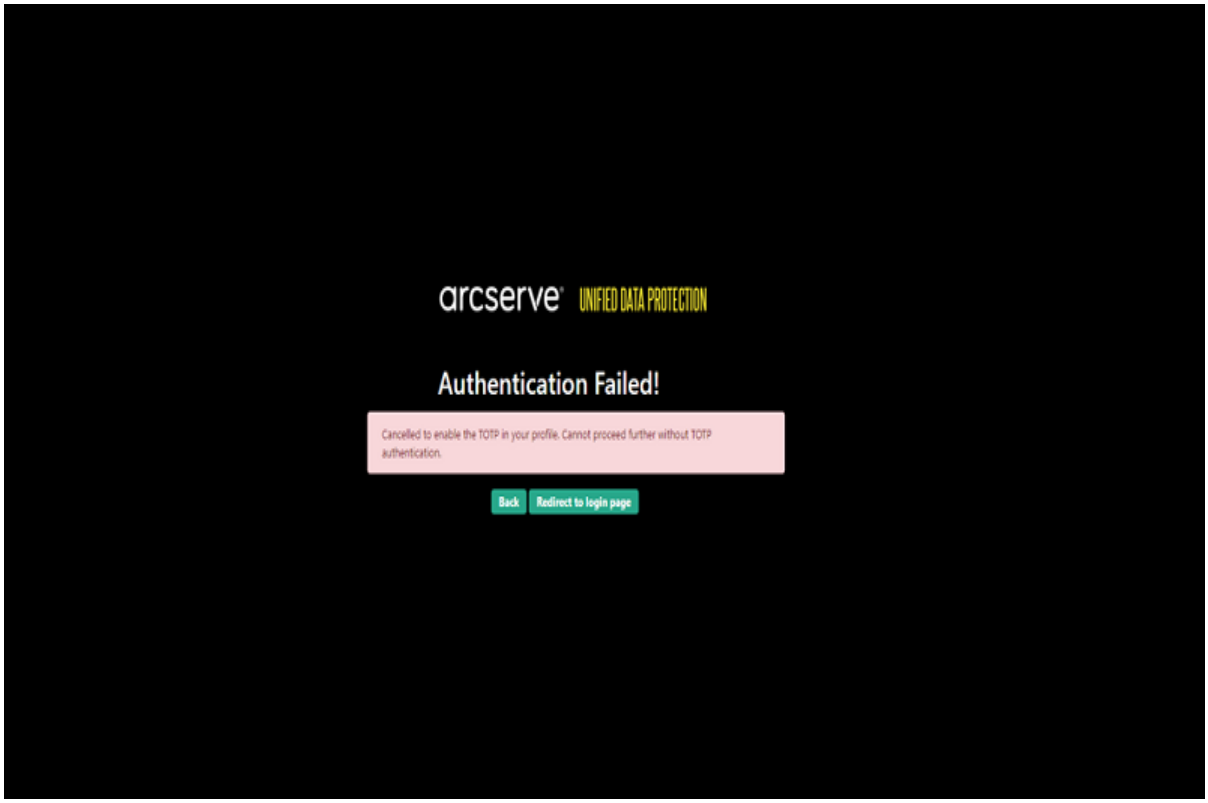
   Hinweise:

   - Sie können jede mobile Authentifizierungs-App wie die Google Authenticator-App oder die Microsoft Authenticator-App auf Ihrem mobilen Gerät verwenden. Alternativ können Sie auch die Authenticator-Erweiterung für den Chrome-Browser verwenden.
   - Wenn Sie eine Authentifizierungs-App für mehrere Benutzerkonten verwenden, unterscheidet der Hostname des Benutzerkontos die TOTPs. In der Authentifikator-App können Sie den Hostnamen und den entsprechenden TOTP anzeigen.



c. Klicken Sie auf die Schaltfläche **Fortfahren**.

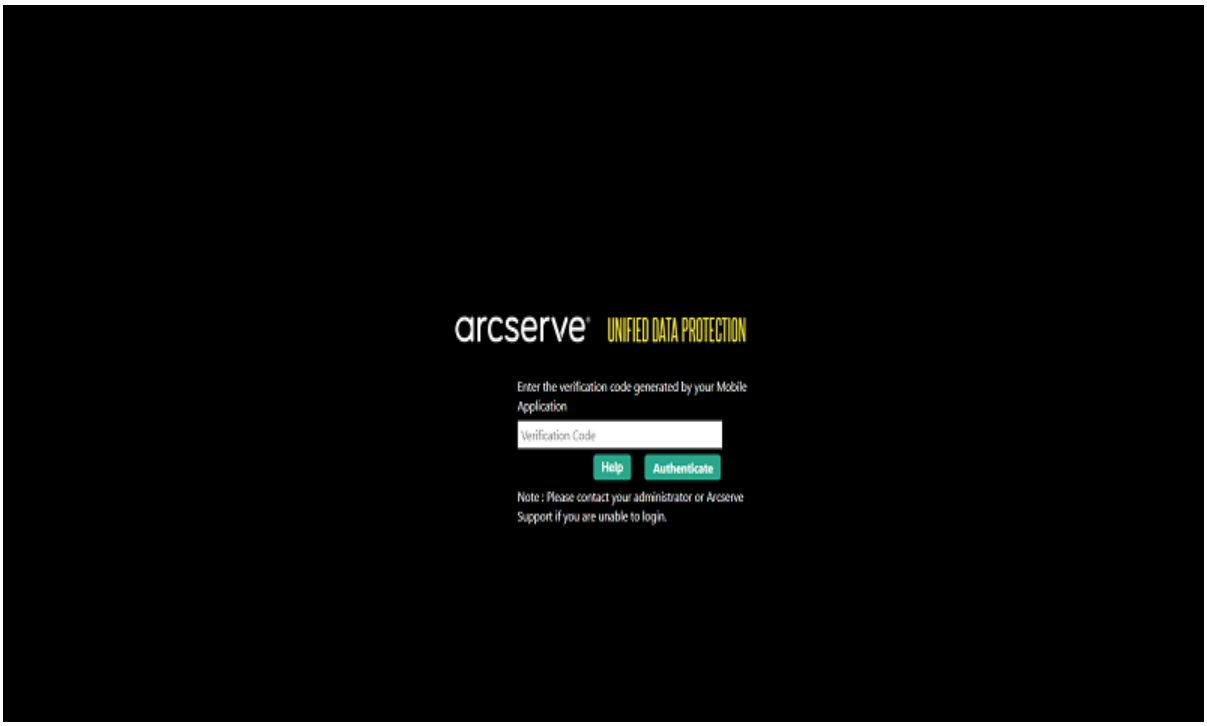
Wenn Sie auf die Schaltfläche **Abbrechen** klicken, schlägt die Authentifizierung fehl.



Hinweis: Wenn Sie zuvor den TOTP-Authentifizierungsfaktor aktiviert haben, werden Sie nicht aufgefordert, Schritt 3 auszuführen.

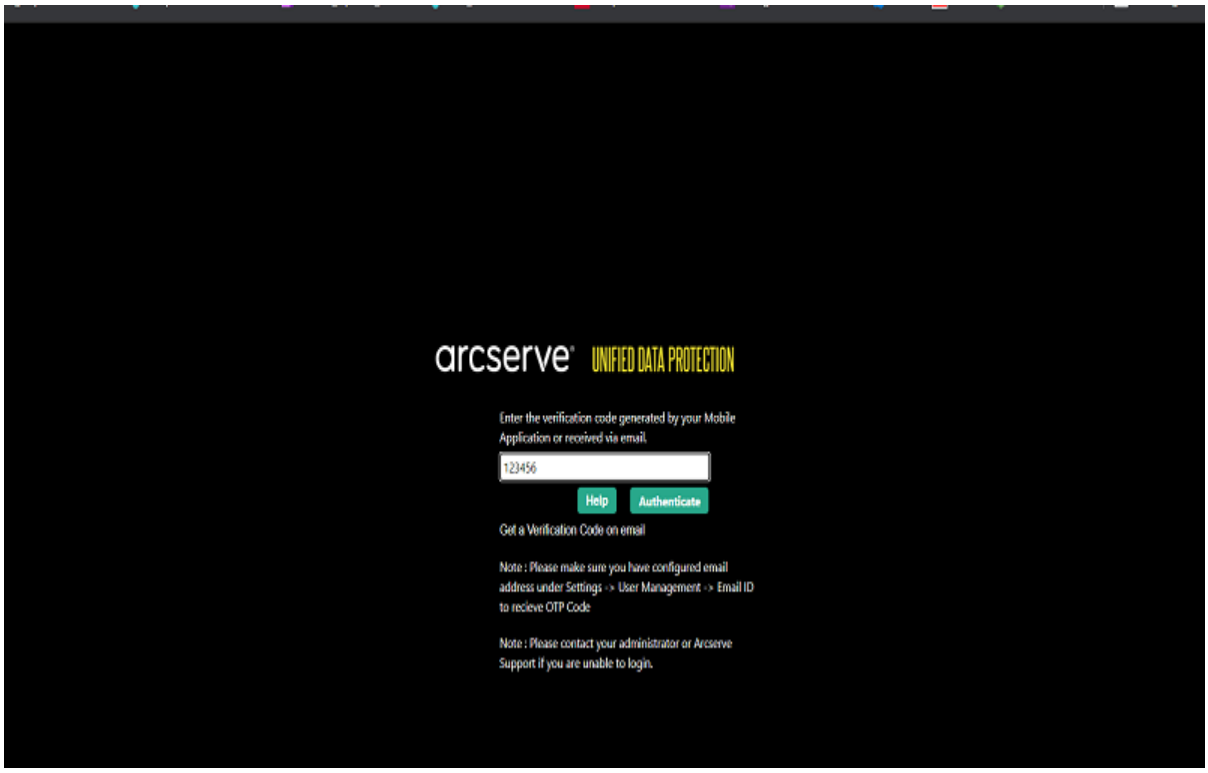
4. Geben Sie im Feld "Bestätigungscode" den TOTP ein.

Öffnen Sie für TOTP die mobile Authentifikator-App auf Ihrem mobilen Gerät oder die Authentifikator-Erweiterung in Ihrem Chrome-Browser. Die Nummer ist 30 Sekunden lang gültig und wird alle 30 Sekunden aktualisiert.



5. (Optional) Wenn Sie nicht über TOTP verfügen, gehen Sie wie folgt vor:
   a. Klicken Sie auf den Link **Verifizierungscode per E-Mail abrufen**.

      Das temporäre E-Mail-OTP wird an Ihre E-Mail-Adresse gesendet.



Hinweise:

- Auf die E-Mail-OTP-Option wird nur zugegriffen, wenn ein Admin-Benutzer E-Mail-OTP aktiviert und E-Mail-Einstellungen konfiguriert. Weitere Informationen finden Sie unter Konfigurieren der Multi-Faktor-Authentifizierung als Admin-Benutzer.
- Stellen Sie sicher, dass Sie die E-Mail-Adresse unter *Einstellungen* > *Benutzerverwaltung* konfigurieren, um die E-Mail-OTP zu empfangen.

b. Geben Sie im Feld für den Bestätigungscode die E-Mail-OTP ein.

6. Klicken Sie auf die Schaltfläche **Authentifizieren**.

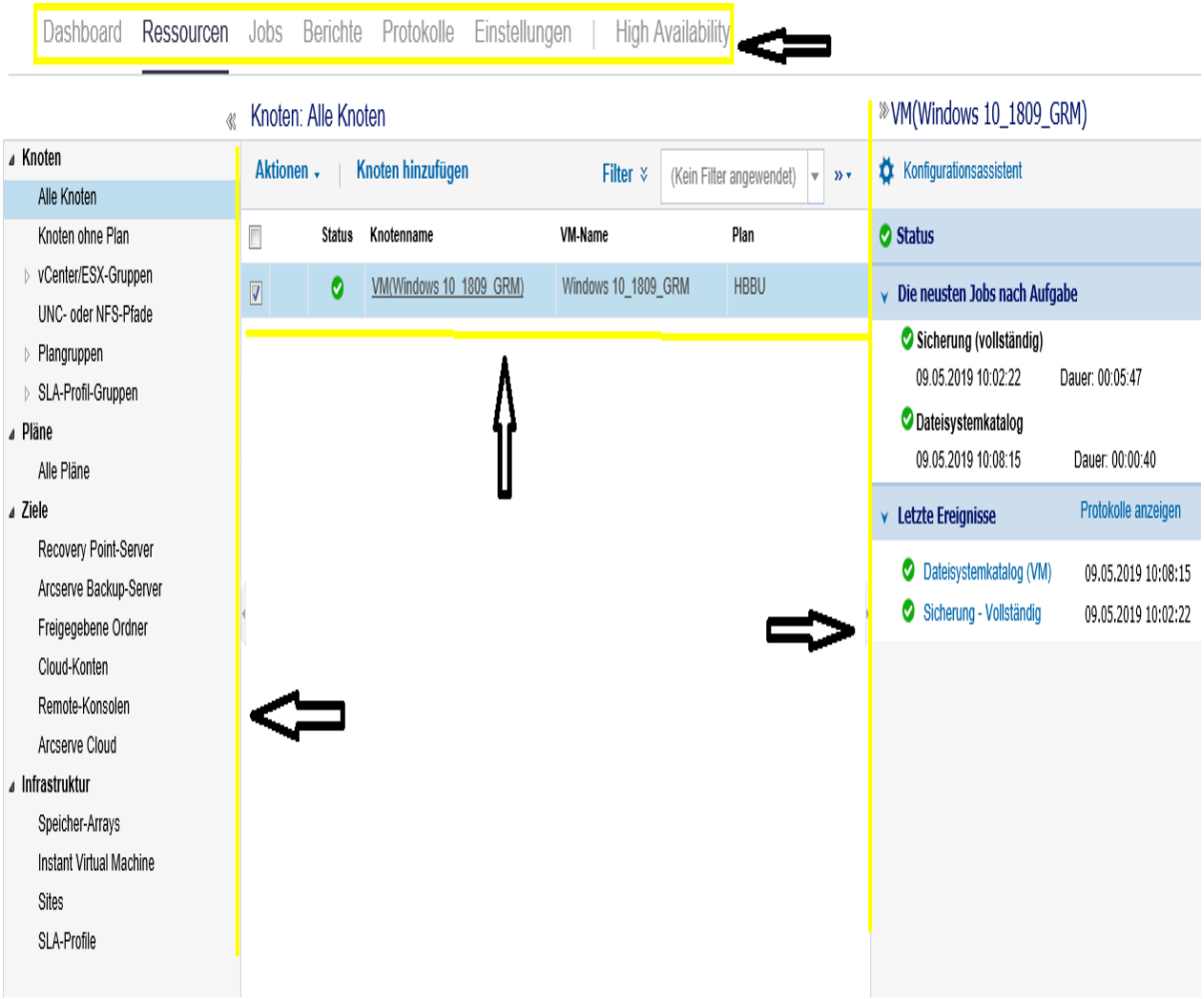
   Sie sind nun erfolgreich bei der UDP-Konsole angemeldet.

Arcserve Unified Data Protection Benutzeroberfläche

Bevor Sie Arcserve Unified Data Protection verwenden, machen Sie sich mit der Benutzeroberfläche vertraut. Auf der Benutzeroberfläche von Arcserve Unified Data Protection können Sie die folgenden Tasks ausführen:

- Verwalten und Überwachen von Jobs
- Hinzufügen und Verwalten von Quellknoten
- Hinzufügen und Verwalten von Ziel-Recovery Point Servern
- Verwalten von Plänen zum Erstellen von Sicherungsablaufplänen
- Abrufen von Datenschutzstatistiken
- Anzeigen von Fehler- und Warnungsprotokollen
- Verwalten und Überwachen von Arcserve High Availability
- Konfigurieren von Datenschutzeinstellungen
- Wiederherstellen von Sicherungsdaten

Navigieren in Arcserve UDP



Registerkarten

Hier können Sie zu den verschiedenen Funktionen von Arcserve Unified Data Protection navigieren.

Fenster

Wenn Sie zu einer Registerkarte navigieren, wird das angezeigte Fenster in die folgenden Bereiche aufgeteilt. Die Fensterbereiche werden verwendet, um zusammengehörende Aktionen auszuführen.

Linker Fensterbereich

Hier können Sie zu verschiedenen Funktionen und Vorgängen navigieren. Das Ergebnis der Klicks wird im mittleren Fensterbereich angezeigt.

Mittlerer Fensterbereich

In diesem Bereich können Sie die meisten Aktionen, beispielsweise Hinzufügen, Löschen, Ändern usw. durchführen. In diesem Bereich werden auch Ergebnis und Status von Aktivitäten wie Jobs, Plänen und Berichten angezeigt. Die meisten Aktionen werden in diesem Bereich ausgeführt. Die Informationen, die auf dieser Seite angezeigt werden, sind in den meisten Fällen das Ergebnis der Optionen, die Sie im linken Fensterbereich aktiviert haben.

Rechter Fensterbereich

Hier wird eine Zusammenfassung der Elemente angezeigt, die Sie im mittleren Fensterbereich ausgewählt haben. Wenn Sie zum Beispiel auf der Registerkarte "Jobs" einen Job im mittleren Fensterbereich ausgewählt haben, wird eine kurze Übersicht des Jobs mit dem Jobüberwachungsserver (sofern ein ausgeführter Job vorhanden ist), den Jobdetails, wie z. B. Quellknotenname, Task, Ziel-Recovery Point Server, sowie dem Zieldatenspeicher im rechten Fensterbereich angezeigt.

Registerkarten

Die Arcserve Unified Data Protection-Lösung enthält die folgenden Registerkarten zum Durchführen von Datenschutzfunktionen:

- Dashboard
- Ressourcen
- Jobs
- Berichte
- Protokoll
- Einstellungen
- High Availability

Dashboard

Auf der Registerkarte **Dashboard** können Sie grafisch den letzten Task-Status und die Datenspeicherung der letzten sieben Tage sehen. Mithilfe der Registerkarte **Dashboard** können Sie folgende Aktionen ausführen:

- Anzeigen des Zeitpunkts der letzten Aktualisierung Das Symbol *Aktualisieren* zeigt die aktuellsten Daten auf dem Dashboard.
- Durch Klick auf das RTO-Balkendiagramm öffnet sich direkt die RTO-Berichtseite.
- Sehen Sie den letzten Task-Status von Knoten oder Plänen gemäß der Filter, die Sie im Diagramm **Letzter Task-Status** auswählen.

Sie können die Diagramme für die folgenden Optionen auf der Registerkarte "Dashboard" anzeigen:

Letzter Task-Status

Letzter Task-Status bezieht sich auf den letzten Task-Status und bietet mehrere Filter, um den Status anzuzeigen. Basierend auf Ihrer Auswahl von Filtern können Sie den letzten Task-Status anzeigen. Beispiel: Wählen Sie **Alle Knoten**, um den letzten Task-Status aller Knoten zu sehen oder wählen Sie einen Plan, um den letzten Task-Status der von diesem Plan geschützten Konten zu sehen. Filtern Sie dann weiter mit einem bestimmten Task-Typ. Wenn Sie **Alle Knoten**auswählen, können Sie den folgenden Status sehen:

- **Erfolgreich** zeigt an, dass die Knoten erfolgreich gesichert wurden.
- **Fehlgeschlagen** zeigt an, dass die letzte Sicherung nicht erfolgreich war.
- **Abgebrochen** zeigt an, dass die letzte Sicherung gestoppt wurde.
- **Versäumt** zeigt an, dass die letzte Sicherung nicht wie geplant durchgeführt wurde.
- **Nicht verbunden** gibt an, dass die Arcserve UDP Konsole nicht mit dem Knoten verbunden wurde.
- **Unvollständig** gibt an, dass der Wiederherstellungsjob nicht abgeschlossen wurde.

Wenn Sie auf einen Abschnitt (den Status) des Kreisdiagramms klicken, wird die Seite **Ressourcen** geöffnet, und die zugeordneten Knoten werden angezeigt. Beispiel: Wenn Sie auf **Erfolgreich** aus dem Kreisdiagramm klicken, öffnet sich die Seite **Ressourcen**. Die Seite **Ressourcen** zeigt die Knoten, die nicht über einen Plan verfügen. Auch der Filter **Erfolgreich** ist auf der Seite **Ressourcen** vorausgewählt.

Tatsächliche, wiederherstellbare und Rohdatengröße: 7 Tage

Die Grafik bezieht sich auf die Rohdaten vs. Wiederherstellbare Daten vs. Tatsächliche Datenspeicherung der letzten sieben Tage.

Größe der wiederherstellbaren Daten

Bezieht sich auf die Größe der Daten, die Sie von den an diesem Tag auf alle Zielspeicher gespeicherten Daten wiederherstellen können. Unabhängig vom Sicherungstyp, Vollsicherung oder inkrementelle Sicherung wird jeder Wiederherstellungspunkt zur Wiederherstellung einer vollständigen Quelle verwendet. Diese Größe ist die Gesamtgröße aller verfügbaren Größen der wiederhergestellten Quelle.

Zum Beispiel: Wenn die Rohdatengröße 30 GB beträgt und nach der Komprimierung und Deduplizierung, beträgt die Größe 22 GB und die wiederherstellbaren Daten 30 GB für die erste vollständige Sicherung. Bei einer Änderung von 4 GB inkrementeller Änderung beträgt die wiederherstellbare Datengröße 30+34 GB= 64 GB.

Tatsächliche Datenspeichergröße

Bezieht sich auf die Größe der endgültigen Daten. Nach dem Komprimieren der Rohdaten und dem Entfernen doppelter Datenblöcke aus den Rohdaten und dem Hinzufügen einiger Metadaten werden die Rohdaten zu den endgültigen Daten und werden auf dem Zielspeicher gespeichert.

Rohdatengröße

Bezieht sich auf die Daten, die aus der Quelle gelesen und an das Ziel übertragen werden.

SLA-Bericht für RTO und RPO

Arcserve UDP hat den SLA-Bericht (Service Level Agreement) eingeführt, um Organisationen bei der Erstellung von Compliance-Berichten im Zusammenhang mit Recovery Point Objective (RPO) und Recovery Time Objective (RTO) zu unterstützen.

RTO-Bericht

Der Arcserve UDP-RTO-Bericht ist ein Compliance-Bericht, der einen Vergleich von Recovery Time Actual- und Recovery Time Objective-Werten für alle ausgeführten Wiederherstellungsjobs anzeigt, wie Dateisystemwiederherstellungen, VM-Wiederherstellungen, BMR, Instant VM und Assured Recovery. Das Balkendiagramm verwendet mehrere Farben zum Anzeigen von Auftragsstatus. Sie können weitere Drill-Down-Funktionen nutzen, um die Knotenebenenstatus "RTO erfüllt", "Nicht erfüllt" und "Nicht definiert" anzuzeigen.

RPO-Bericht

Arcserve UDPDer RPO-Bericht zeigt die Gesamtanzahl der Knoten mit verfügbaren Wiederherstellungspunkten während des angegebenen Zeitraums in einer Balkendiagrammansicht an. Die Kategorisierung erfolgt dabei nach Alter der aktuellsten Wiederherstellungspunkts (15 Minuten, letzte Stunde, 12 Stunden, letzter Tag usw.), Alter des ältesten Wiederherstellungspunkts (30 Tage und älter) und monatlicher Verteilung (Januar bis Dezember). Sie können weitere Drill-Down-Funktionen nutzen, um den Status auf Knotenebene für die ausgewählte Kategorie anzuzeigen.

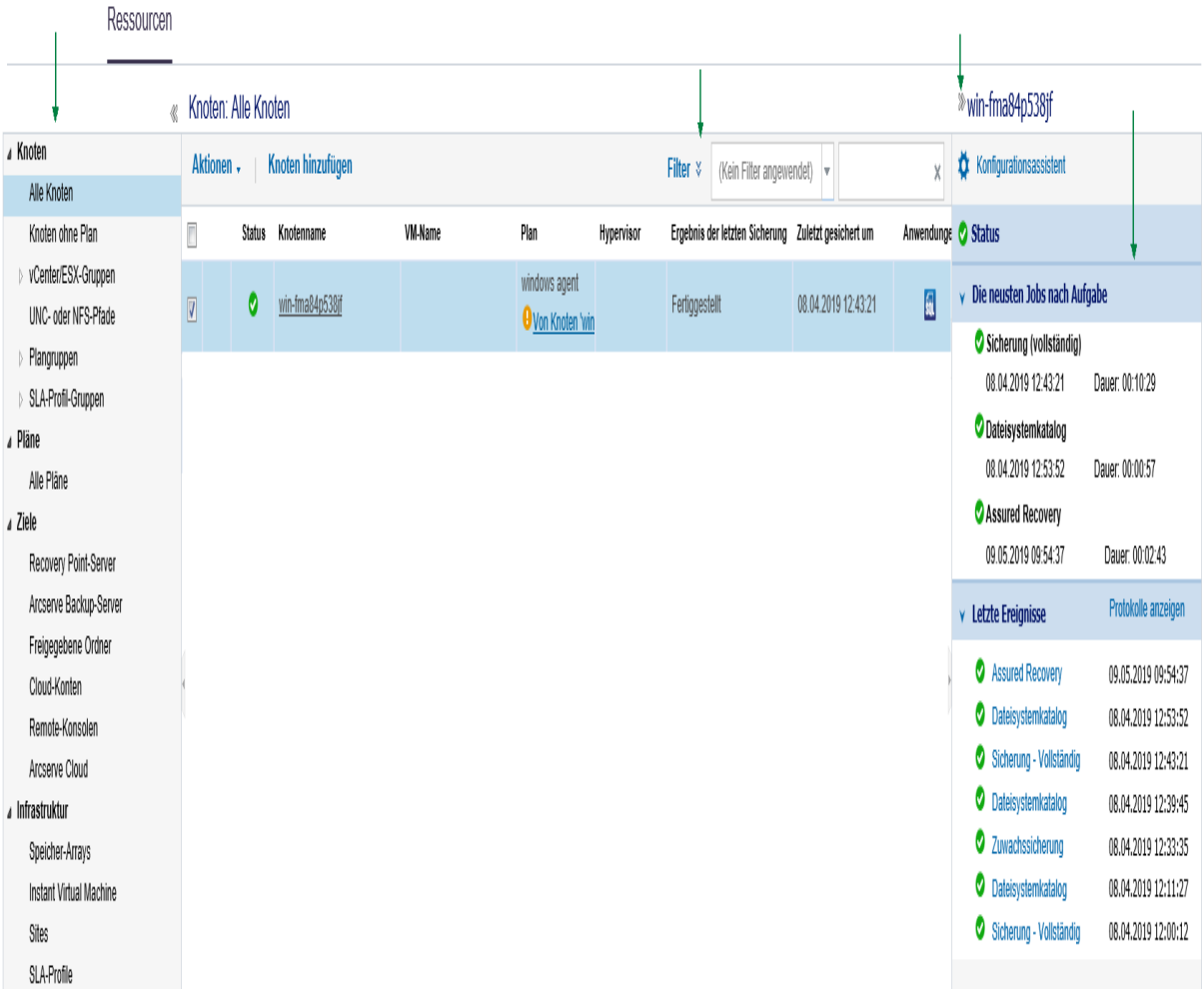
Hinweis: Über das Dashboard können Sie den RPO-Bericht für einen bestimmten Monat direkt aufrufen. Der Bericht wird direkt über das Arcserve UDP-Dashboard befüllt. Wenn Sie innerhalb des RPO-Balkendiagramms auf einem Monat klicken, zeigt das Dashboard den RPO-Berichtsbildschirm für diesen Monat auf dem RPO-Bildschirm an.

Ressourcen

Die Registerkarte **Ressourcen** ermöglicht Ihnen die Verwaltung der Arcserve Unified Data Protection-Ressourcen: Knoten, Ziele, Virtual Standby und Pläne. Verwenden Sie diese Registerkarte, um Ressourcen wie Knoten, die Sie schützen möchten, oder Recovery Point Server für Sicherungen zu Arcserve Unified Data Protection hinzuzufügen. Sie verwenden diese Registerkarte auch, um Pläne und Tasks für Sicherung, Virtual Standby und Replikation zu erstellen. Auf der Registerkarte "Ressourcen" haben Sie folgende Optionen:

- Knotenverwaltung
- Zielverwaltung
- Planverwaltung
- Infrastrukturverwaltung

Hinweis: nur die Registerkarte **Ressourcen** auf der Konsole hat spezifische Standortinformationen. Alle anderen Registerkarten in der Konsole zeigen die konsolidierten Daten für alle Standorte an. Weitere Informationen zu Standorten finden Sie unter So können Sie einen Standort hinzufügen und verwalten.


Ressourcen
Knoten: Alle Knoten
win-fma84p538jf
Knoten
Alle Knoten
Knoten ohne Plan
vCenter/ESX-Gruppen
UNC- oder NFS-Pfade
Plangruppen
SLA-Profil-Gruppen
Pläne
Alle Pläne
Ziele
Recovery Point-Server
Arcserve Backup-Server
Freigegebene Ordner
Cloud-Konten
Remote-Konsolen
Arcserve Cloud
Infrastruktur
Speicher-Arrays
Instant Virtual Machine
Sites
SLA-Profile
Aktionen
Knoten hinzufügen
Filter
(Kein Filter angewendet)
Konfigurationsassistent
Status
Knotenname
VM-Name
Plan
Hypervisor
Ergebnis der letzten Sicherung
Zuletzt gesichert um
Anwendunge
win-fma84p538jf
windows agent
Von Knoten 'win
Fertiggestellt
08.04.2019 12:43:21
Status
Die neusten Jobs nach Aufgabe
Sicherung (vollständig)
08.04.2019 12:43:21
Dauer: 00:10:29
Dateisystemkatalog
08.04.2019 12:53:52
Dauer: 00:00:57
Assured Recovery
09.05.2019 09:54:37
Dauer: 00:02:43
Letzte Ereignisse
Protokolle anzeigen
Assured Recovery 09.05.2019 09:54:37
Dateisystemkatalog 08.04.2019 12:53:52
Sicherung - Vollständig 08.04.2019 12:43:21
Dateisystemkatalog 08.04.2019 12:39:45
Zuwachssicherung 08.04.2019 12:33:35
Dateisystemkatalog 08.04.2019 12:11:27
Sicherung - Vollständig 08.04.2019 12:00:12

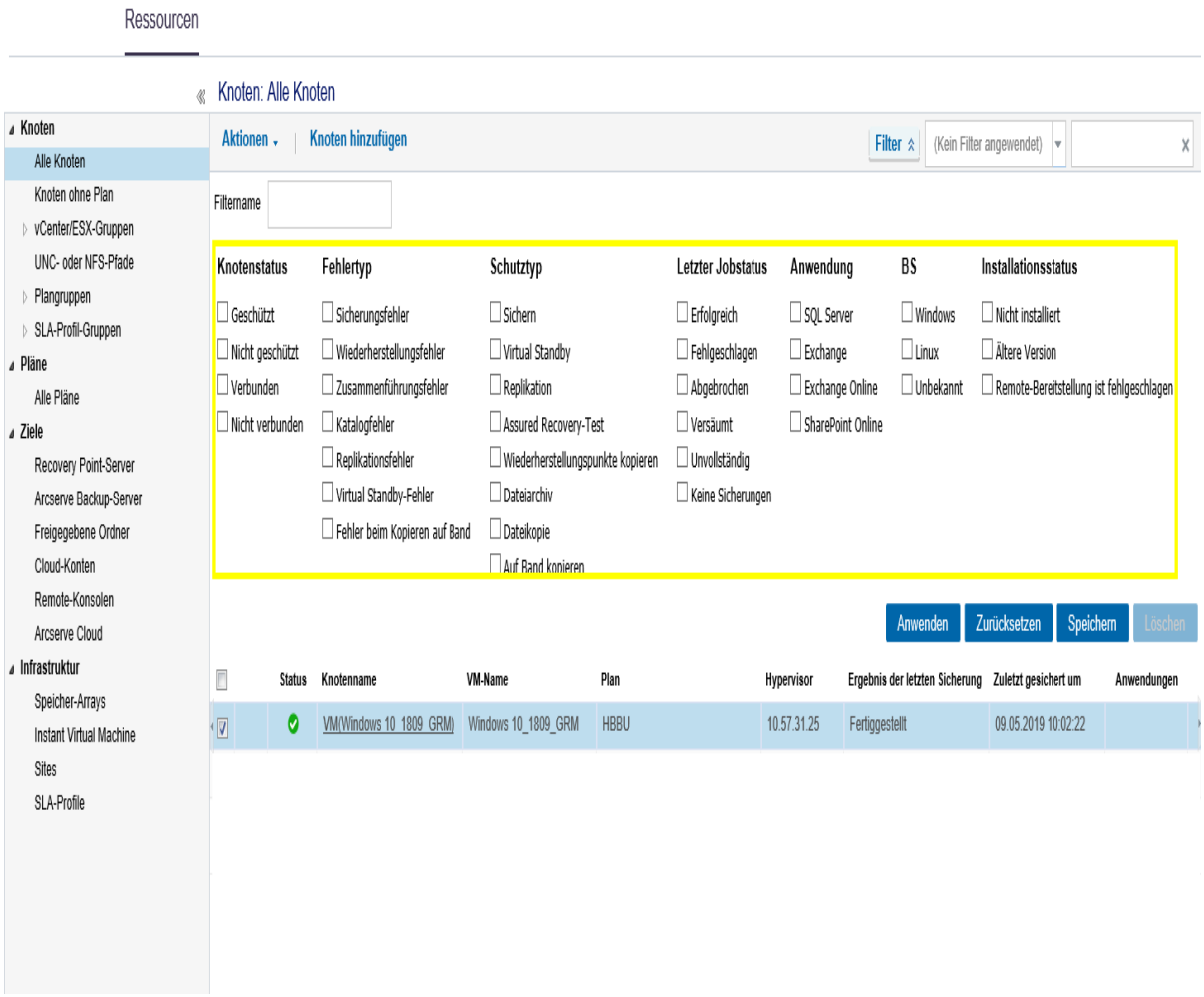
Knotenverwaltung

In der Knotenverwaltungsansicht können Sie alle Knoten verwalten und Filter anwenden, um die Suche nach Knoten zu verfeinern. Wenn Sie einen bestimmten Knoten in mittleren Fensterbereich auswählen, können Sie den Status und die aktuellste Ereignisse über den Knoten im rechten Fensterbereich sehen. Im mittleren Fensterbereich können Sie verschiedene Filter anwenden. Im linken Fensterbereich können Sie Knotengruppen erstellen, um spezifische Knoten in Gruppen zusammenzufassen.

Wenn Sie einen Knoten aus dem mittleren Fensterbereich auswählen, dann werden der Knotenstatus und die aktuellsten Ereignisse im rechten Fensterbereich angezeigt.

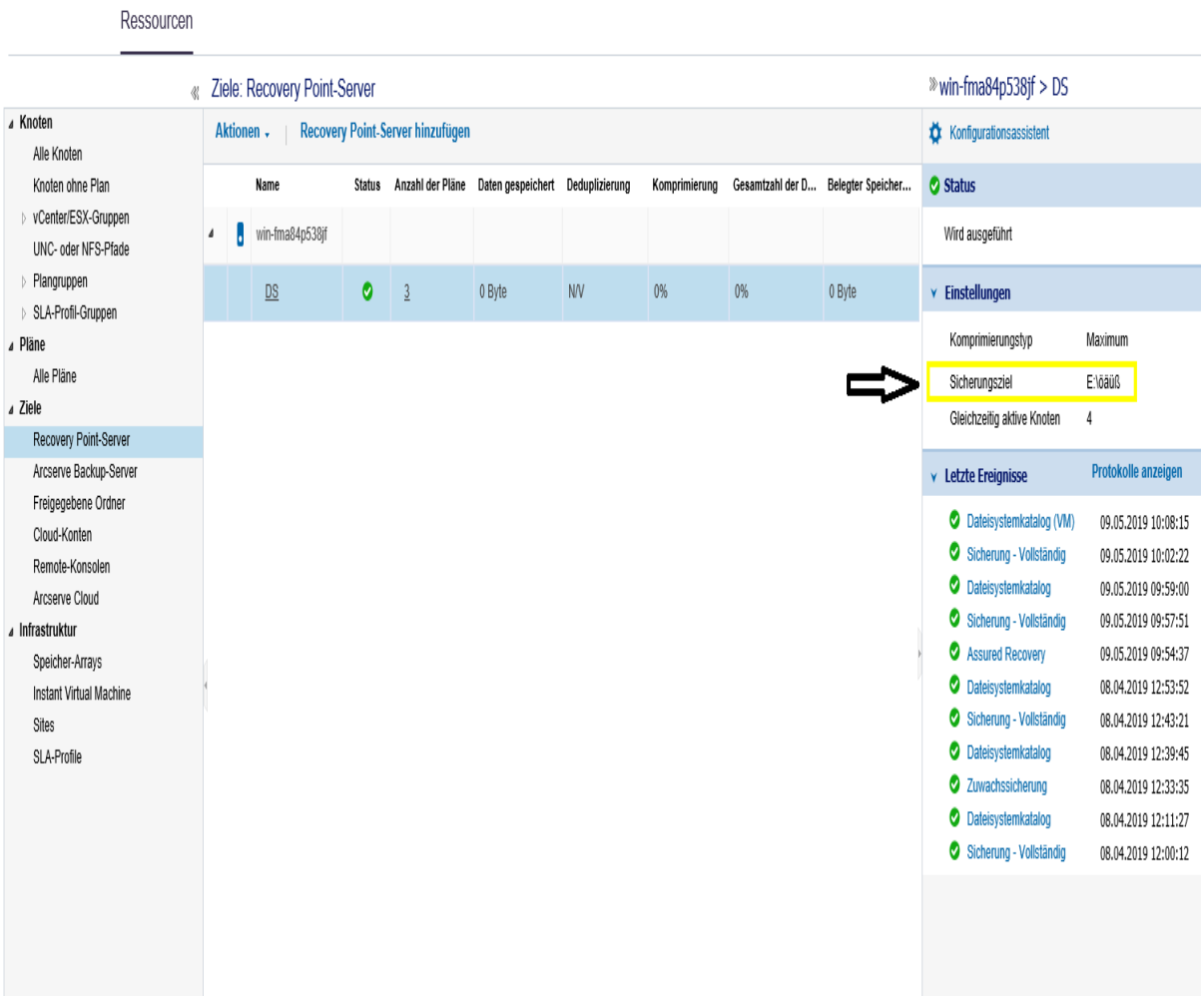
Sie können Vorgänge auf Knoten ausführen, indem Sie auf das Drop-down-Menü "Aktionen" im mittleren Fensterbereich klicken. Die Vorgänge, die Sie im mittleren Fensterbereich über "Aktionen" ausführen können, werden auf alle Quellknoten angewendet. Die Vorgänge, die Sie im rechten Fensterbereich über "Aktionen" ausführen können, werden nur auf den Knoten angewendet, den Sie im mittleren Fensterbereich auswählen.

Klicken Sie in der Registerkarte "Ressourcen" auf **Alle Knoten** unter "Knoten" im linken Bereich. Wählen Sie dann im mittleren Bereich einen Knoten aus und klicken Sie auf **Filter**, um die Optionen für die Knotenverwaltung anzuzeigen. Sie können das Kontrollkästchen der gewünschten Optionen festlegen und dann auf **Übernehmen** klicken.


Ressourcen
Knoten: Alle Knoten
Knoten
Alle Knoten
Knoten ohne Plan
vCenter/ESX-Gruppen
UNC- oder NFS-Pfade
Plangruppen
SLA-Profil-Gruppen
Pläne
Alle Pläne
Ziele
Recovery Point-Server
Arcserve Backup-Server
Freigegebene Ordner
Cloud-Konten
Remote-Konsolen
Arcserve Cloud
Infrastruktur
Speicher-Arrays
Instant Virtual Machine
Sites
SLA-Profile
Aktionen
Knoten hinzufügen
Filter
(Kein Filter angewendet)
Filtername
Knotenstatus
Geschützt
Nicht geschützt
Verbunden
Nicht verbunden
Fehlertyp
Sicherungsfehler
Wiederherstellungsfehler
Zusammenführungsfehler
Katalogfehler
Replikationsfehler
Virtual Standby-Fehler
Fehler beim Kopieren auf Band
Schutztyp
Sichern
Virtual Standby
Replikation
Assured Recovery-Test
Wiederherstellungspunkte kopieren
Dateiarchiv
Dateikopie
Auf Band kopieren
Letzter Jobstatus
Erfolgreich
Fehlgeschlagen
Abgebrochen
Versäumt
Unvollständig
Keine Sicherungen
Anwendung
SQL Server
Exchange
Exchange Online
SharePoint Online
BS
Windows
Linux
Unbekannt
Installationsstatus
Nicht installiert
Ältere Version
Remote-Bereitstellung ist fehlgeschlagen
Anwenden
Zurücksetzen
Speichern
Löschen
Status
Knotenname
VM-Name
Plan
Hypervisor
Ergebnis der letzten Sicherung
Zuletzt gesichert um
Anwendungen
VM(Windows 10_1809_GRM)
Windows 10_1809_GRM
HBBU
10.57.31.25
Fertiggestellt
09.05.2019 10:02:22

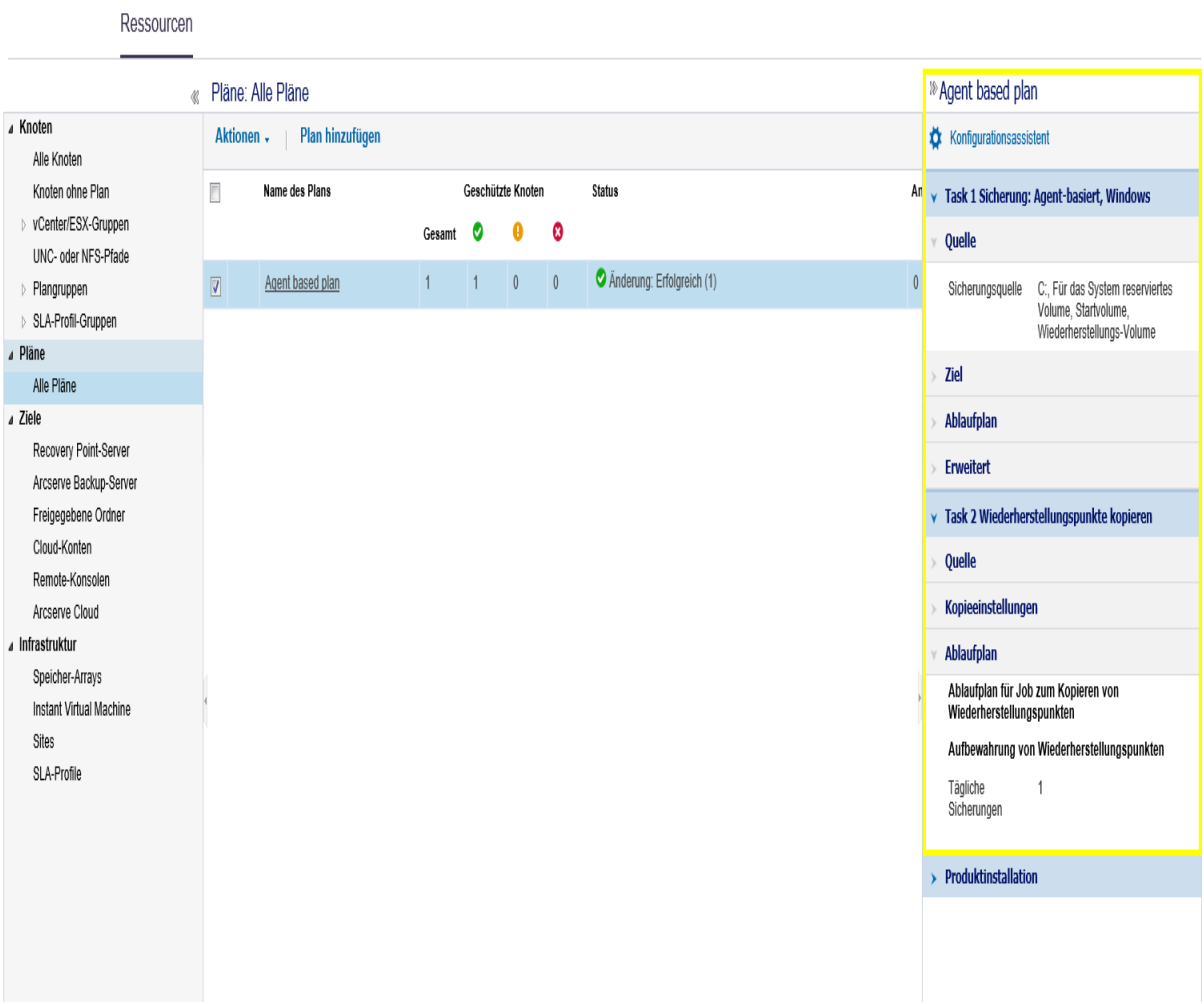
Zielverwaltung

In der Zielverwaltungsansicht können Sie die Ziel-Recovery Point Server verwalten. Wenn Sie einen Server aus dem mittleren Fensterbereich auswählen, werden die neuesten Ereignisse im rechten Fensterbereich angezeigt. Wenn Sie einen Datenspeicher auswählen, dann werden der Status und die Einstellungen im rechten Fensterbereich angezeigt.



Planverwaltung

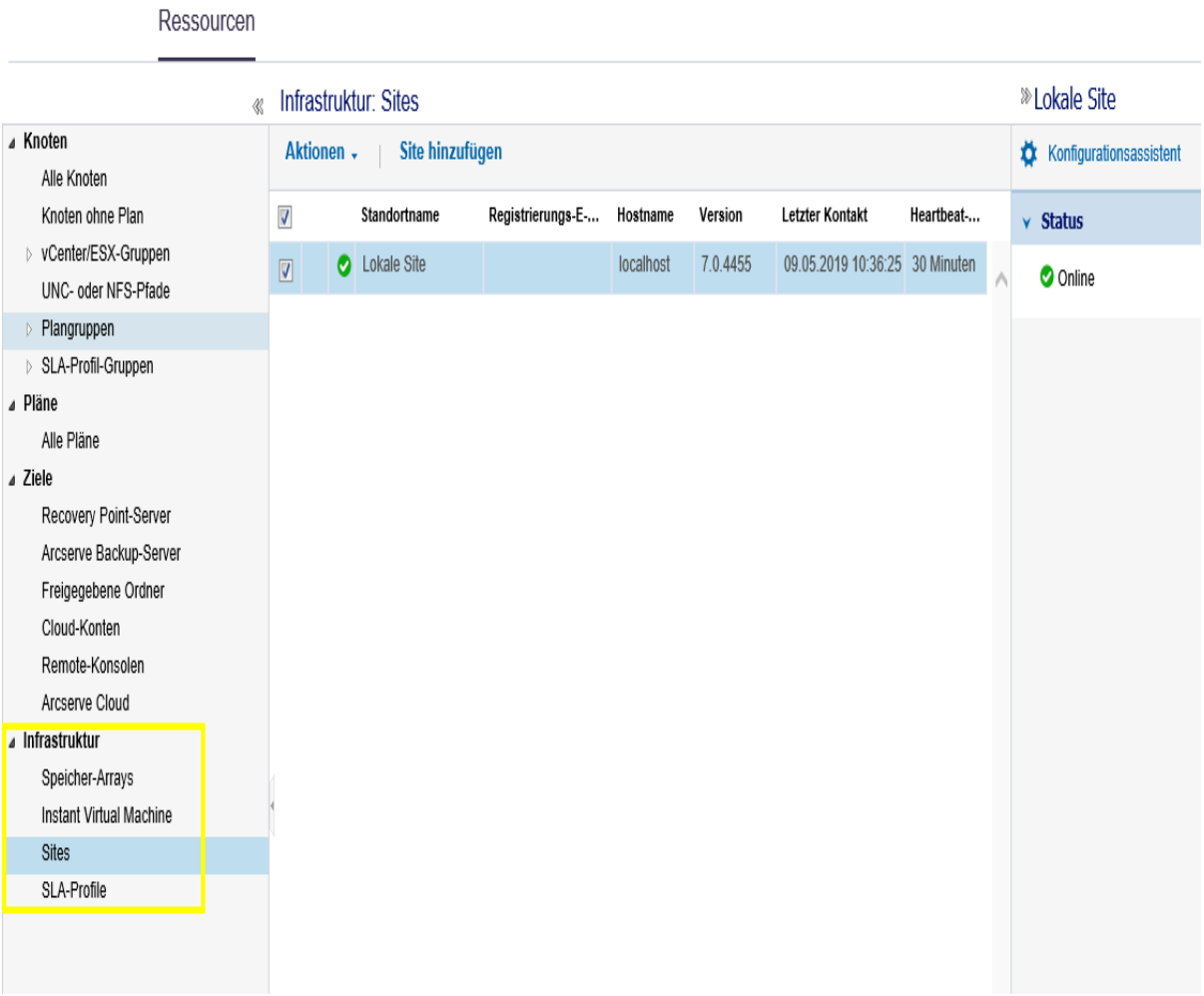
In der Planverwaltungsansicht können Sie alle Pläne verwalten. Über diese Ansicht können Sie Pläne erstellen, ändern, löschen, bereitstellen, unterbrechen und wiederaufnehmen. Die Details des Plans werden im rechten Fensterbereich angezeigt. Sie können auf die erforderlichen Felder klicken, um Details anzuzeigen und zu verwalten.



Infrastrukturverwaltung

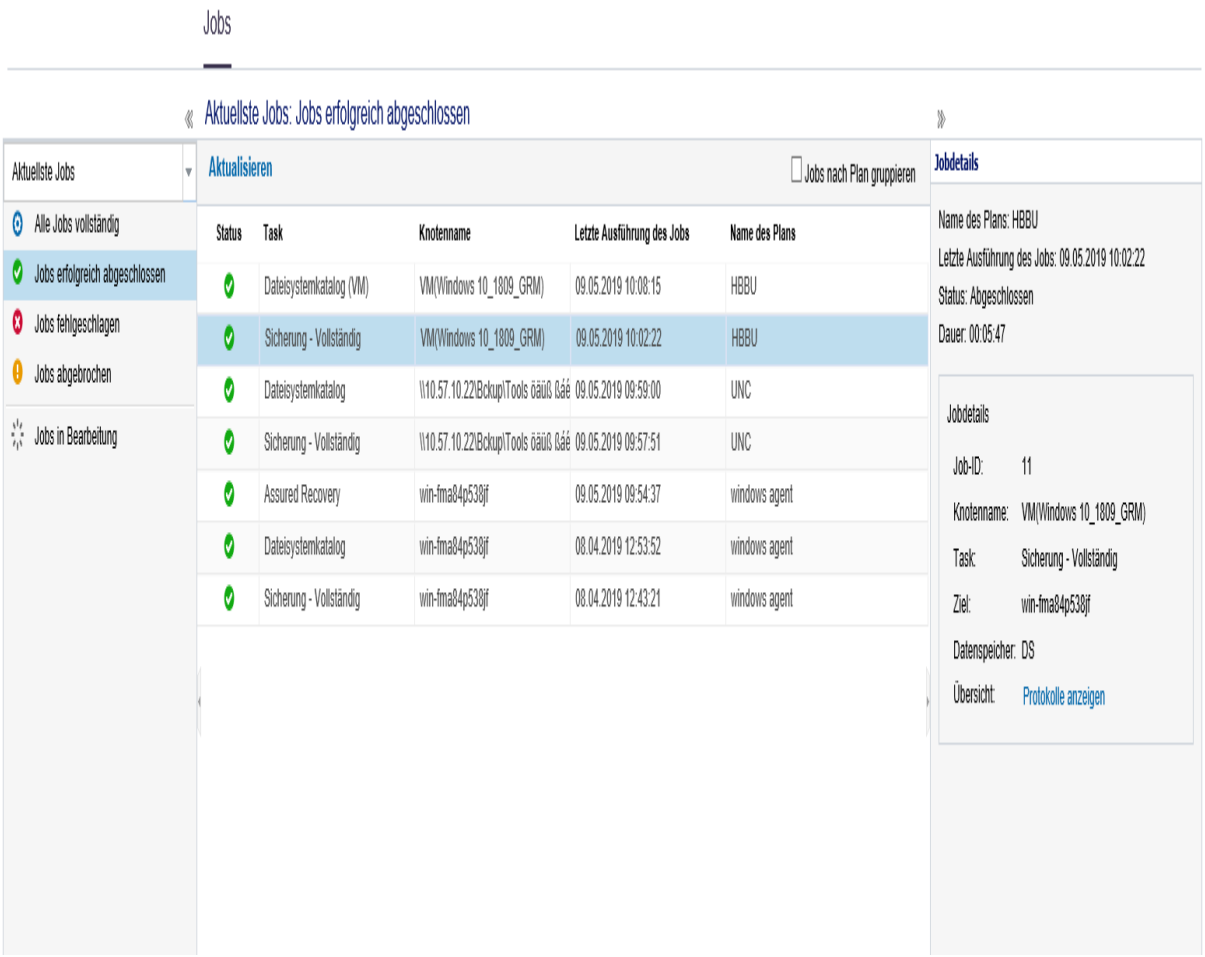
In der Infrastrukturverwaltungsansicht können Sie die Speicher-Arrays, Instant VMs und Remote-Speicherorte verwalten.

Folgender Screenshot zeigt das Fenster für die Infrastrukturverwaltung:



Jobs

Die Registerkarte **Jobs** zeigt den Status der Jobs für einen bestimmten Zeitraum an. Wendet Filter an, um die Ergebnisse zu kategorisieren oder die Jobs nach Plan zu gruppieren.

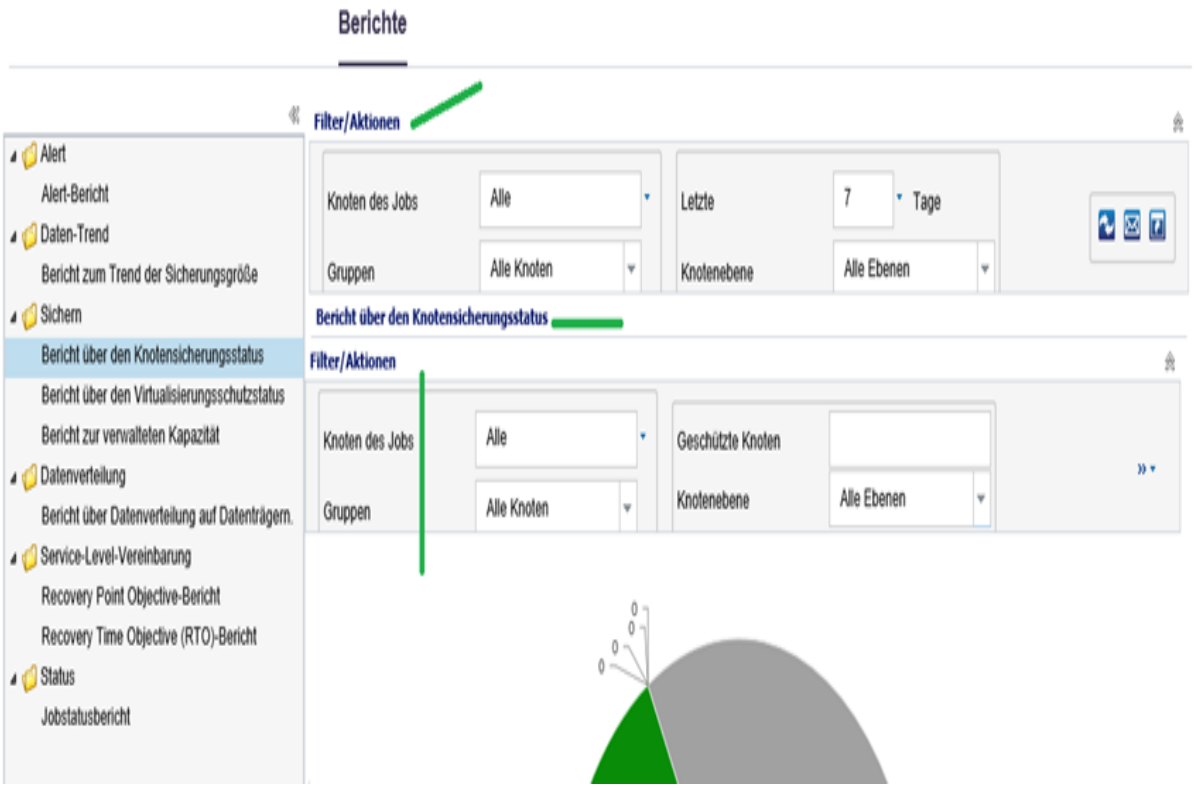


Wenn ein Job ausgeführt wird, zeigt der rechte Fensterbereich den Jobmonitor an, der den Fortschritt des Jobs enthält. Klicken Sie im rechten Fensterbereich auf **Jobdetails**, um den Job-Monitor zu öffnen. Die Job-Monitore werden nur angezeigt, wenn der Job derzeit ausgeführt wird.

Um einen Job abzubrechen, öffnen Sie den Job-Monitor, und klicken Sie auf **Abbrechen**.

Berichte

Auf der Registerkarte **Bericht** wird eine Liste der Berichte, die Sie generieren können, angezeigt. Sie können Filter für Ihre Berichte anwenden, um spezifische Berichte abzurufen. Die Berichte werden im CSV-, PDF- oder HTML-Format generiert. Weitere Informationen zu diesen Berichten finden Sie in So generieren Sie Arcserve UDP-Berichte.



Protokoll

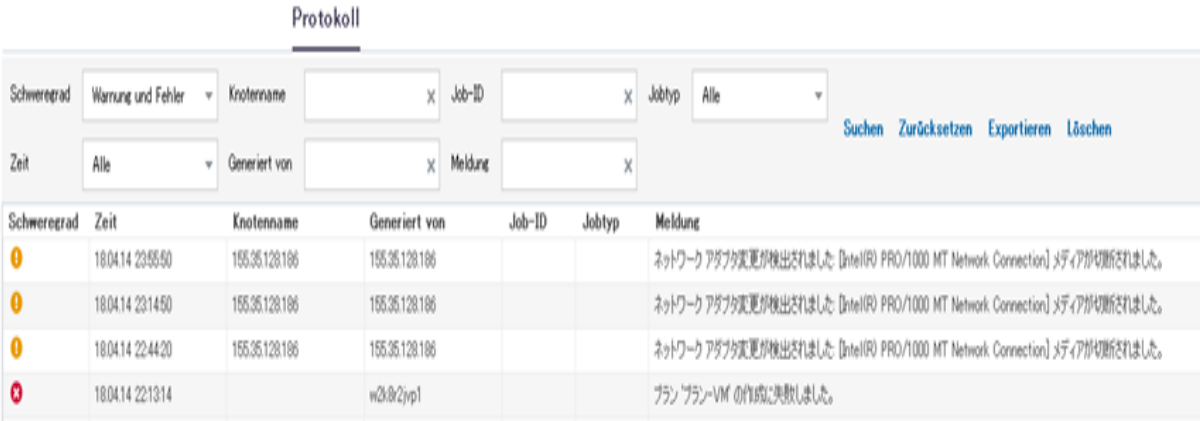
Auf der Registerkarte **Protokoll** werden alle Aktivitätsprotokolle für die geschützten Knoten, Zielserver, Datenspeicher und Pläne angezeigt. Sie können Protokolle anzeigen und verschiedene Filter für Aspekte wie Schweregrad, spezifische Knoten, vom Rechner generierte Protokolle, Job-IDs und Protokollinhalt anwenden.

Die Meldungs-ID enthält einen Hyperlink für den Zugriff auf die detaillierte Dokumentation. Klicken Sie auf den Hyperlink in der Spalte "Meldungs-ID", um die Beschreibung und die Lösung für diese Meldung anzuzeigen.

Hinweis: Die von Konsole und Linux-Sicherungsserver/-Agent generierten Aktivitätsprotokolle und der Job zum Kopieren auf Band weist keine Meldungs-ID auf.

Sie können die Aktivitätsprotokolle über eine Kombination der verfügbaren Filter oder eine der folgenden Optionen suchen:

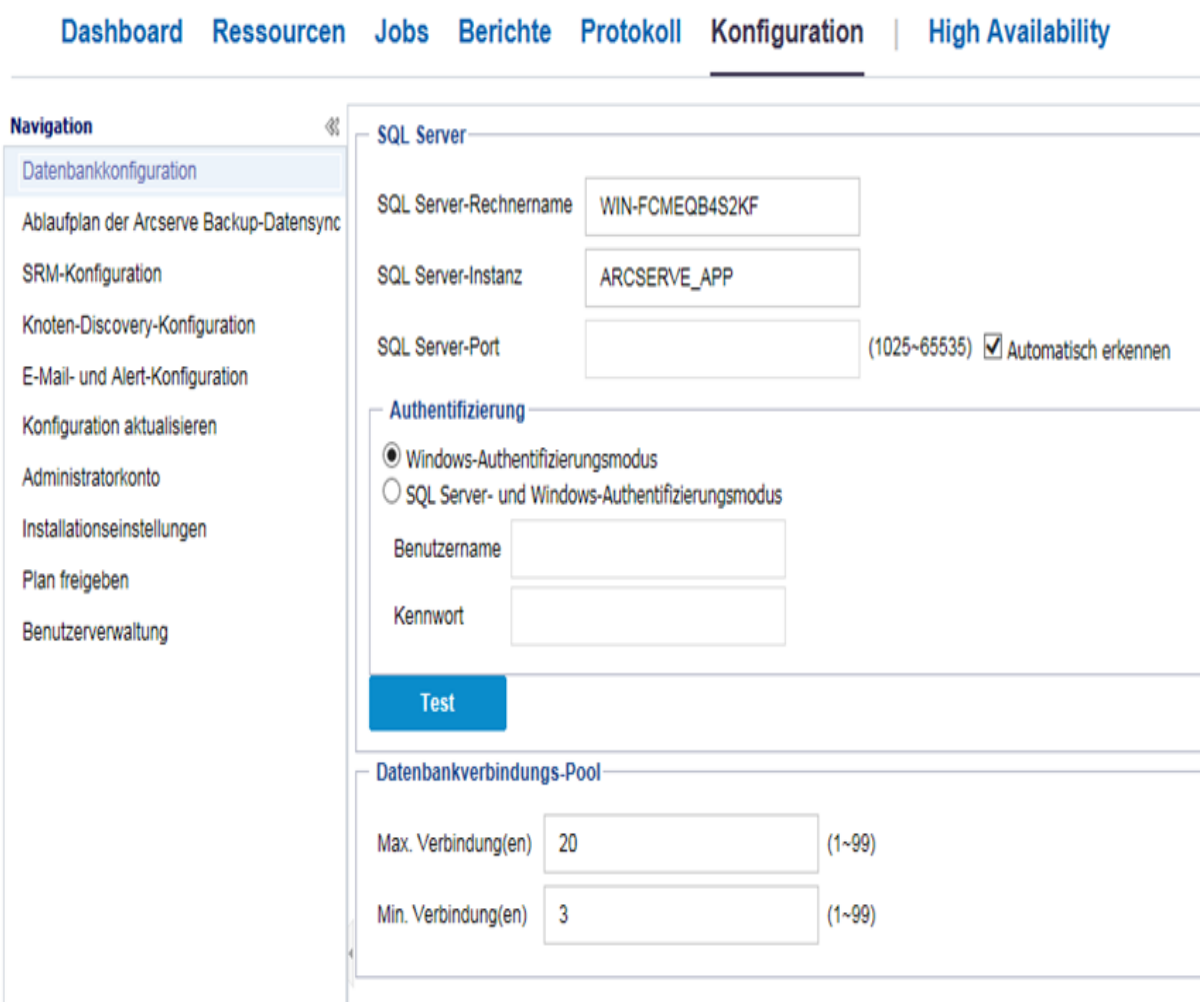
- Wählen Sie Typen für "Schweregrad" aus, um alle Protokolle für den ausgewählten Typ anzuzeigen.
- Geben Sie andere Details ein (wie Knotennamen und Job-ID), und klicken Sie auf **Suchen**.
- **Aktualisierung:** Zeigen Sie die neuesten Protokolle nach definierten Filtern an.
- **Zurücksetzen:** Verwendet nur Standardfilter und zeigt nur Warn- und Fehlermeldungen für alle Jobarten an.
- **Exportieren:** Lädt das aktuelles Jobprotokoll als *.zip(activitylog_export_2017_10_12_15_02_27_586.zip) in das – Downloadverzeichnis des Windowssystems herunter.
- **Löschen:** Löscht alle Datensätze oder alle Protokolleinträge vor dem angegebenen Datum.



Einstellungen

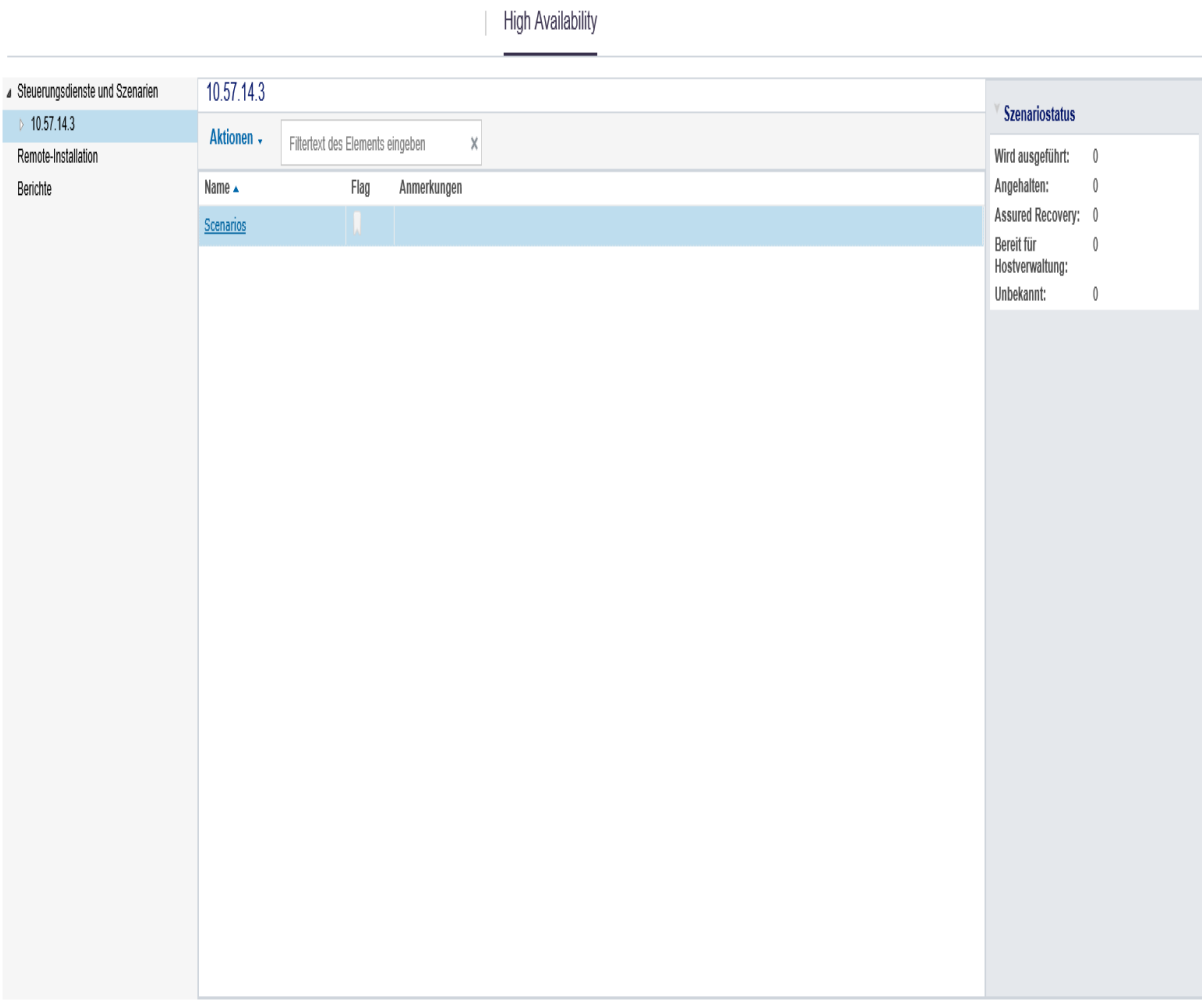
Auf der Registerkarte **Einstellungen** können Sie Voreinstellungen wie beispielsweise den Mailserver, der verwendet werden soll, konfigurieren, Benutzer-ID und Kennwort für den Administrator einrichten und den Standardpfad für die Bereitstellung von Knoten definieren.

Weitere Informationen zur Registerkarte **Einstellungen** finden Sie unter So konfigurieren Sie Arcserve UDP.



High Availability

In der Registerkarte **High Availability** können Sie High Availability-Funktionen von Arcserve verwalten und steuern. Wenn erforderlich, geben Sie die Anmeld-einformationen im **Steuerelement hinzufügen Service** Dialogfeld ein und zeigen die Details an.



Dialogfeld "Job-Monitor"

Im Dialogfeld "Job-Monitor" können Sie den Status eines Jobs anzeigen. Wenn ein Job ausgeführt wird, wird dieser Bereich eingeblendet, um Informationen über das fortlaufende Ereignis anzuzeigen, wie die geschätzte verbleibende Zeit zum Jobabschluss, den Prozentsatz und die Größe des schon abgeschlossenen Jobs, sowie die Gesamtgröße des Jobs, wenn er fertig gestellt ist.

Wenn ein Job ausgeführt wird, blenden Sie im rechten Bereich **Letzte Ereignisse** ein und klicken Sie auf die Schaltfläche **Detail**, um die Statusüberwachungen zu öffnen und ausführlichere Informationen zum derzeit ausgeführten Job anzuzeigen.

Sie können auf die Schaltfläche **Abbrechen** klicken, um den derzeit ausgeführten Job abzubrechen.

So konfigurieren Sie Arcserve UDP

Mit Arcserve Unified Data Protection können Sie folgende Arcserve Unified Data Protection-Konfigurationseinstellungen angeben.

- Server-Kommunikationsprotokoll
- Datenbankeinstellungen
- Datensynchronisation Arcserve Backup
- SRM-Konfiguration
- Knoten-Discovery-Konfiguration
- E-Mail- und Alert-Konfiguration
- Konfigurieren von Proxy-Einstellungen
- Aktualisieren der Konfiguration
- Administratorkonto
- Einstellungen der Remote-Bereitstellung
- Plan freigeben
- Benutzerverwaltung
- Konfigurieren der Zeitüberschreitungsdauer der Konsole

Konfigurieren des Server-Kommunikationsprotokolls

Die Arcserve Unified Data Protection-Lösung verwendet für die Kommunikation zwischen allen Komponenten Hypertext Transfer Protocol (HTTP). Wenn Ihnen eine sichere Übertragung von Kennwörtern zwischen den Komponenten wichtig ist, ändern Sie das HTTP-Protokoll in Hypertext Transfer Protocol Secure (HTTPS) um. Wenn Sie diese zusätzliche Sicherheitsstufe nicht benötigen, können Sie das Protokoll wieder auf HTTP zurücksetzen.

Hinweis: Wenn Sie das Protokoll in HTTPS umändern, wird im Webbrowser eine Warnung angezeigt. Die Ursache für die Warnung ist ein selbstsigniertes Sicherheitszertifikat. Sie werden aufgefordert, die Warnung zu ignorieren und fortzufahren oder das Zertifikat zum Browser hinzuzufügen, damit diese Warnung in Zukunft nicht mehr angezeigt wird.

Gehen Sie wie folgt vor:

1. Melden Sie sich über ein Administratorkonto oder ein Konto mit Administratorrechten bei dem Computer an, auf dem die Arcserve Unified Data Protection-Konsole installiert ist.

   Hinweis: Wenn Sie sich nicht über ein Administratorkonto oder Konto mit Administratorrechten anmelden, konfigurieren Sie die Befehlszeile für die Ausführung mit der Berechtigung "Als Administrator ausführen".
2. Rufen Sie die Windows-Befehlszeile auf.
3. Führen Sie eine der folgenden Aufgaben durch:
   - So ändern Sie das Protokoll von HTTP in HTTP um:

     Starten Sie das Utility-Tool "changeToHttps.bat" an der folgenden Standardstelle.

     Hinweis: Der Speicherort des BIN-Ordners kann abhängig vom Installationsort der Arcserve Unified Data Protection Konsole variieren.

     C:\Programme\Arcserve\Unified Data Protection\Management\BIN

     Wenn das Protokoll erfolgreich geändert wurde, wird die folgende Meldung angezeigt:

     Das Kommunikationsprotokoll wurde auf HTTPS geändert.
   - So ändern Sie das Protokoll von HTTPS auf HTTP:

     Starten Sie das Hilfsprogramm "changeToHttp.bat" an folgendem Standardspeicherort.

Hinweis: Der Speicherort des BIN-Ordners kann abhängig vom Installationsort der Arcserve Unified Data Protection Konsole variieren.

C:\Programme\Arcserve\Unified Data Protection\Management\BIN

Wenn das Protokoll erfolgreich geändert wurde, wird die folgende Meldung angezeigt:

Das Kommunikationsprotokoll wurde auf HTTP geändert.

4. Starten Sie den Browser neu, und stellen Sie erneut eine Verbindung zur Arcserve Unified Data Protection-Konsole her.

   Hinweis: Um das Kommunikationsprotokoll zu aktualisieren, das vom Arcserve Unified Data Protection Recovery Point Server und dem Arcserve Unified Data Protection Agenten verwendet wird, um mit der Arcserve Unified Data Protection Konsole zu kommunizieren, aktualisieren Sie den Knoten direkt aus der Konsole.

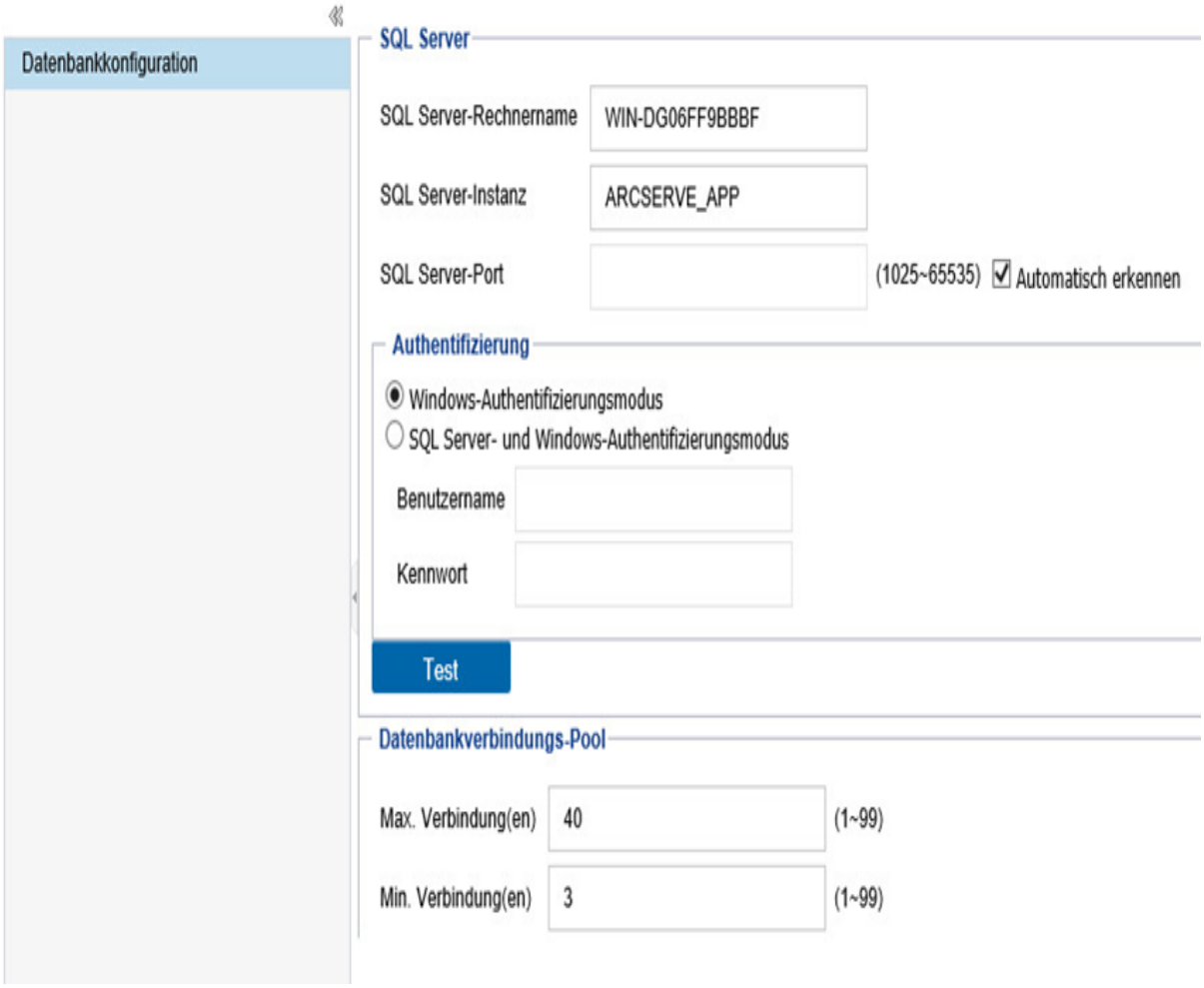
Konfigurieren der Datenbank

Mit der Option **Datenbankkonfiguration** können Sie Details zur Datenbank eingeben. Die Datenbankkonfiguration benötigt Details über SQL Server, Verbindungsanzahl und Authentifizierungsmodus.

Hinweis: Sie können die Datenbank vor der Konfiguration wiedererstellen. Löschen Sie die Arcserve Unified Data Protection-Datenbank über den Vorgang, der unter Erneutes Erstellen der Arcserve Unified Data Protection-Datenbank beschrieben ist.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Datenbankkonfiguration**.



Füllen Sie für die Konfiguration die folgenden Felder auf dem Konfigurationsbildschirm aus, und klicken Sie auf **Speichern**.

SQL Server-Rechnername

Geben Sie den Namen des Servers an, der die SQL Server-Instanz hostet.

SQL Server-Instanz

Geben Sie den Namen der SQL Server-Instanz an.

SQL Server-Port

Geben Sie die Portnummer für diese Instanz an, oder aktivieren Sie die Option **Automatisch erkennen.** 1025 bis 65535 ist der Bereich der Optionen für die Portnummer.

Automatisch erkennen

Wenn Sie dieses Kontrollkästchen aktivieren, kann die Anwendung die Portnummer finden.

Authentifizierung

Wählen Sie einen der Authentifizierungsmodi aus den folgenden Optionen aus:

Windows-Authentifizierungsmodus: Standardmodus:

(Optional) **Test:** Klicken Sie auf "Test", um zu überprüfen, ob die Anwendung mit der Microsoft SQL Serverinstanz kommunizieren kann.

SQL Server- und Windows-Authentifizierungsmodus:

Wählen Sie die Option und geben Sie Daten in die Felder "Benutzername" und "Kennwort" ein.

Werte für Datenbankverbindungs-Pool

Geben Sie für die Höchst- und Mindestanzahl von Verbindungen einen Wert zwischen 1 und 99 ein.

Die Datenbankserver-Konfiguration ist festgelegt.

Verwenden Sie **Zurücksetzen**, um alle festgelegten Werte zu löschen und die ursprünglichen Daten zu laden.

Erneutes Erstellen der Arcserve Unified Data Protection-Datenbank

Aus verschiedenen Gründen möchten Sie die Arcserve Unified Data Protection-Datenbank möglicherweise erneut erstellen. Zum Beispiel verbraucht Ihre aktuelle Datenbank mehr als 10 GB an Daten. Um die Datenbank neu zu erstellen, müssen Sie zunächst die vorhandene Arcserve Unified Data Protection-Datenbank löschen und anschließend eine neue Datenbank konfigurieren, um die gelöschte Datenbank zu ersetzen. Der Vorgang bezieht sich auf Datenbanken von Microsoft SQL Server und Microsoft SQL Server Express Edition.

Wichtig! Wenn Sie die Arcserve Unified Data Protection-Datenbank löschen, gehen alle aktuellen Daten verloren.

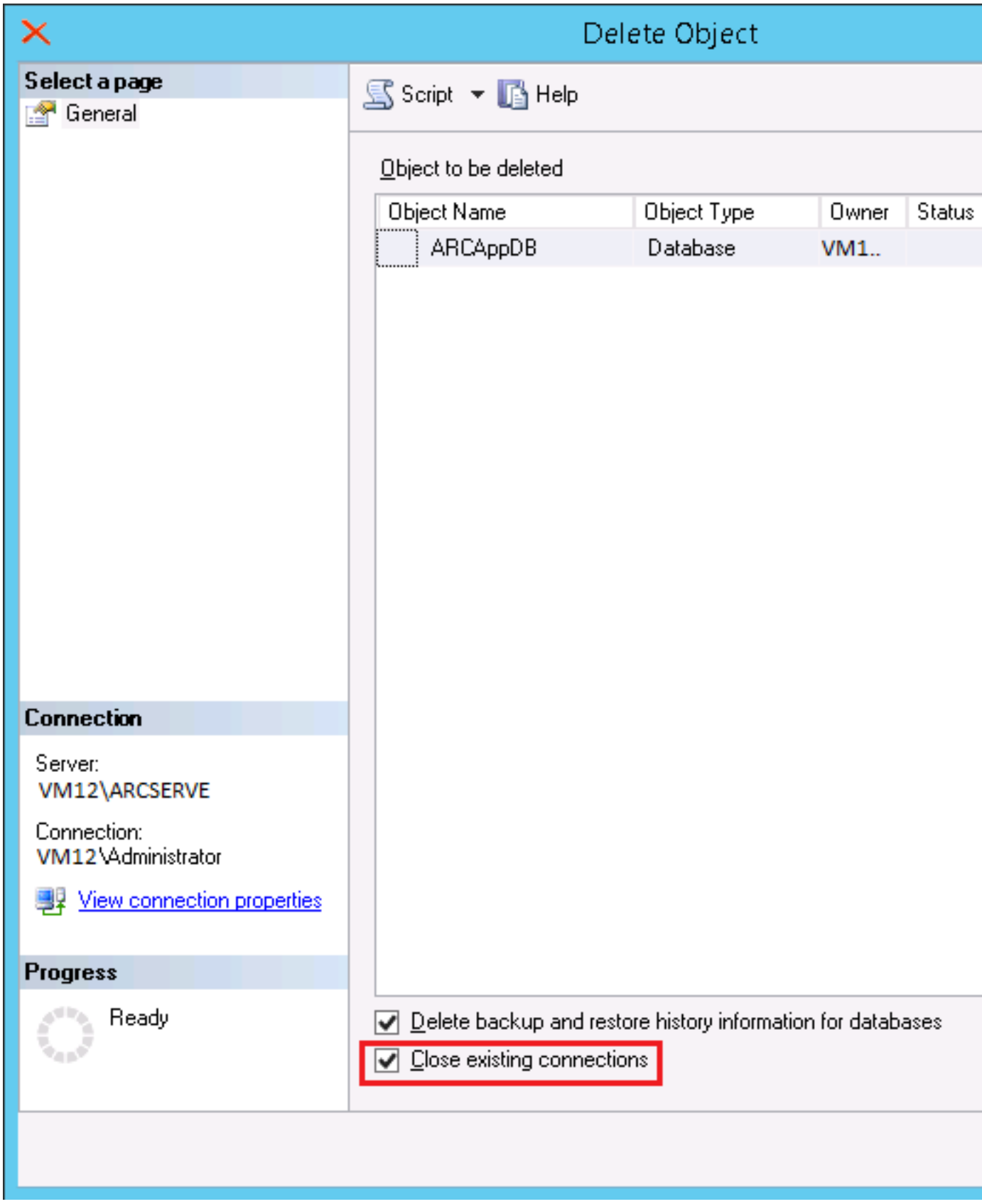
So erstellen Sie die Arcserve Unified Data Protection-Datenbank erneut

1. Öffnen Sie Microsoft SQL Server Management Studio Express und loggen Sie sich in die Instanz ARCSERVE_APP ein.

   Hinweis: Wenn Microsoft SQL Server Management Studio Express nicht auf dem Arcserve Unified Data Protection Server installiert ist, laden Sie die Anwendung im Microsoft Download Center herunter.

2. Klicken Sie mit der rechten Maustaste auf arcserveUDP und klicken Sie anschließend im Pop-up-Dialogfeld auf **Löschen**.

   Das Dialogfeld **Objekt löschen** wird geöffnet.



3. Klicken Sie im Dialogfeld **Objekt löschen** auf die Option **Bestehende Verbindungen schließen** und anschließend auf **OK**.

Die vorhandene Arcserve Unified Data Protection-Datenbank wird gelöscht.

4. Konfigurieren Sie die neue Datenbank. Weitere Informationen finden Sie im Abschnitt Konfigurieren der Datenbank.

   Die Arcserve Unified Data Protection-Lösung erstellt die Datenbank neu. Der Name der Datenbankinstanz lautet **ARCSERVE_APP**.

Konfigurieren der Arcserve Backup-Daten-synchronisation

Sie können den **Arcserve Backup-Datensynchronisierungszeitplan** konfigurieren.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Ablaufplan der Arcserve Backup-Daten-synchronisation**.
3. Klicken Sie im rechten Fensterbereich auf **Aktivieren**.

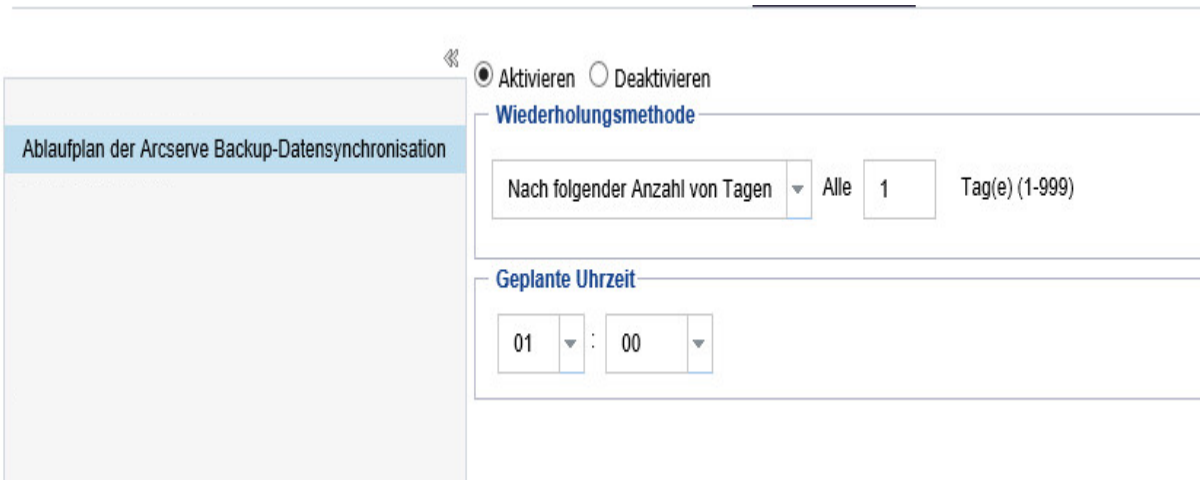
   Standardmäßig ist die Konfiguration für **Arcserve Backup-Datensynchronisation** aktiviert.

   Hinweis: Wenn Sie auf **"Deaktivieren"** klicken, wird die Planung angehalten.
4. Geben Sie folgende Parameter an, um die Arcserve Backup-Datensynchronisation zu planen:
   - **Wiederholungsmethode**
   - **Geplante Uhrzeit**
5. Klicken Sie auf **Speichern**.

   Der Ablaufplan für die Arcserve Backup-Datensynchronisation wird angewendet.

   Hinweis: Klicken Sie nicht auf **Speichern**, wenn Sie die Synchronisierung sofort ausführen möchten.
6. (Optional) Um den Prozess sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

   Das Dialogfeld **Knoten** wird mit der Liste der Knoten angezeigt, die zur Synchronisation verfügbar sind.



7. Wählen Sie die Knoten aus, die Sie für die Synchronisation ausführen möchten, und klicken Sie auf **OK**.

SRM konfigurieren

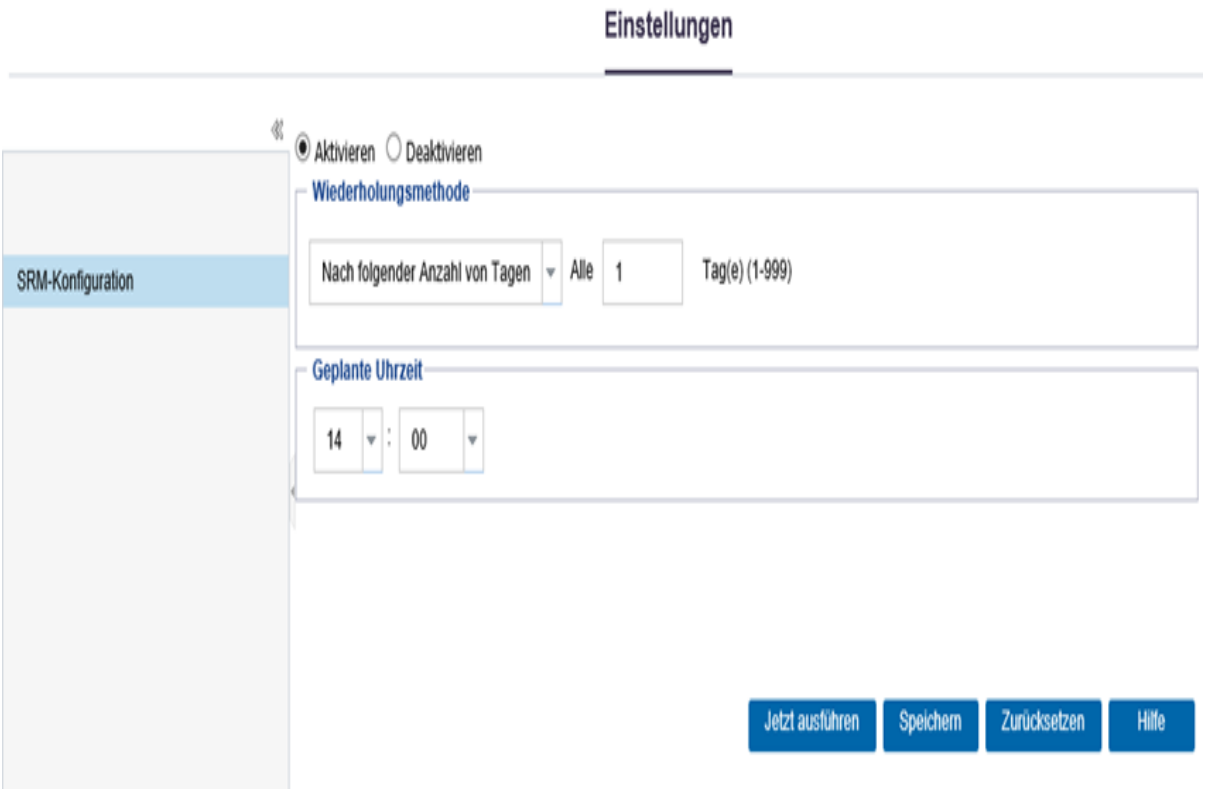
Auf der Seite "SRM-Konfiguration" können Sie einen Ablaufplan für Knoten konfigurieren, der festlegt, wann und wie oft SRM-Daten erfasst werden. SRM (Storage Resource Management, Speicherressourcenverwaltung) ist eine Funktion, die Informationen zu folgenden Daten erfasst:

- Hardware, Software und Anwendungsdaten für Microsoft SQL Server- und Microsoft Exchange Server-Implementierungen
- PKI-Daten (Performance Key Indicators) von Knoten

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **SRM-Konfiguration**.
3. Klicken Sie im rechten Fensterbereich auf **Aktivieren**.

   Standardmäßig ist **SRM-Konfiguration** aktiviert.



Hinweis: Wenn Sie auf **"Deaktivieren"** klicken, wird die Planung angehalten.

4. Geben Sie die folgenden Parameter an, um SRM zu planen:

- **Wiederholungsmethode**
- **Geplante Uhrzeit**

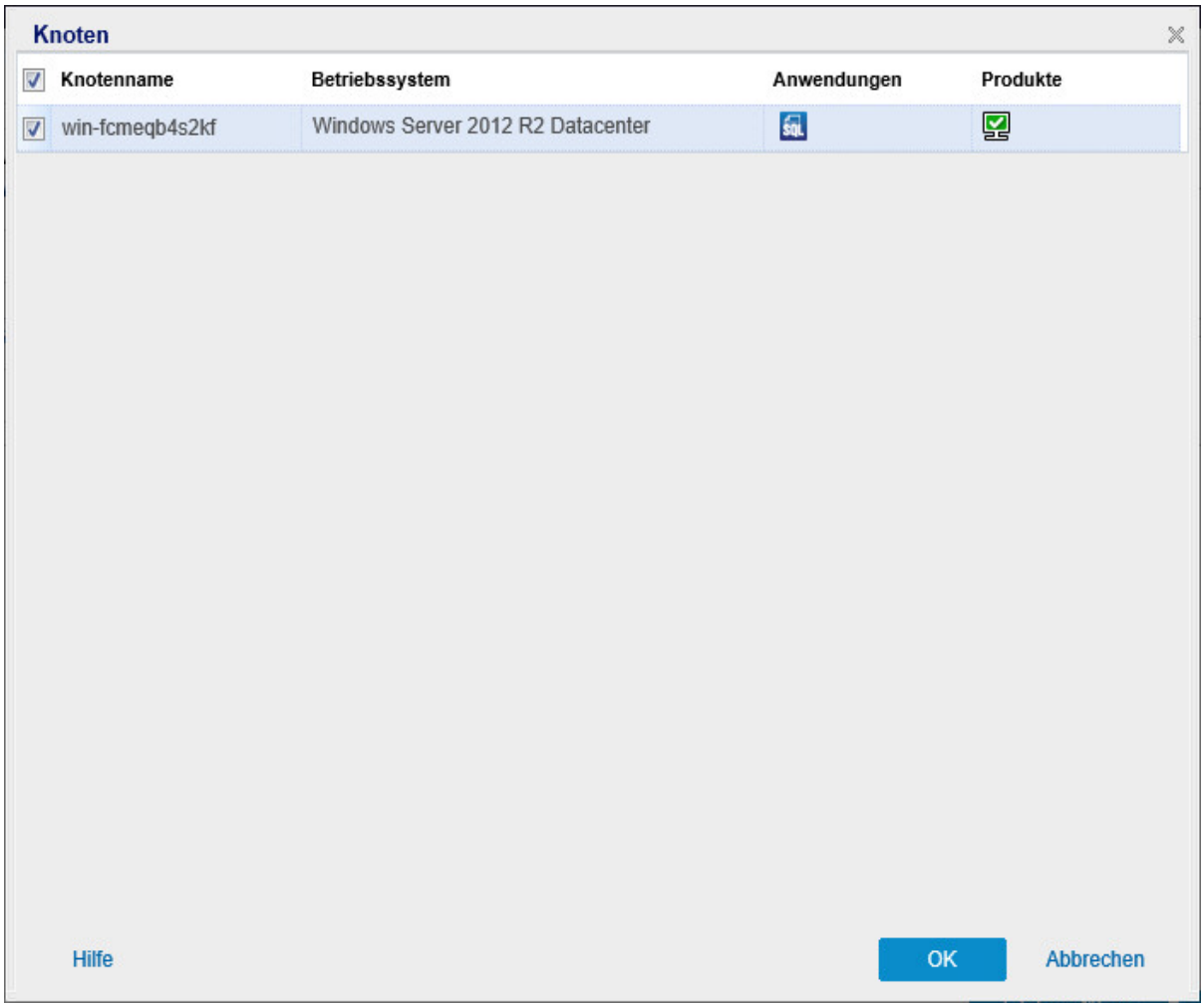
5. Klicken Sie auf **Speichern**.

   Der Ablaufplan für SRM wird angewendet.

   Hinweis: Klicken Sie nicht auf **Speichern**, wenn Sie SRM-Daten sofort erfassen möchten.

6. (Optional) Um den Prozess sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

   Das Dialogfeld **Knoten** wird mit der Liste der Knoten angezeigt, die zur Synchronisation verfügbar sind.



7. Wählen Sie die Knoten aus, die Sie für die Synchronisation ausführen möchten, und klicken Sie auf **OK**.

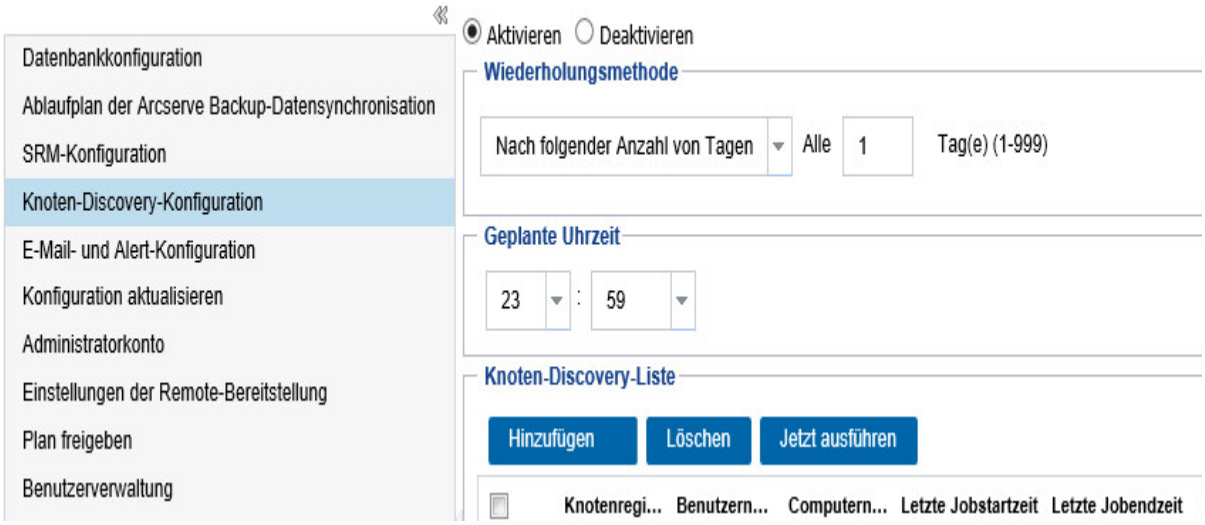
Knoten-Discovery-Konfiguration

Auf der Seite **Knoten-Discovery-Konfiguration** können Sie den Discovery-Ablaufplan für Active Directory-, VMware vSphere- und Microsoft Hyper-V-Knoten in einem Wiederholungsintervall und für einen bestimmten Zeitpunkt konfigurieren. Wenn neue Knoten entdeckt werden, wird an den Administrator eine E-Mail-Benachrichtigung gesendet, damit er die neuen Knoten manuell hinzufügt. Standardmäßig ist **Discovery-Konfiguration** deaktiviert.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Knoten-Discovery-Konfiguration**.

   Wenn Sie die Konfiguration aktivieren möchten, klicken Sie auf die Option **Aktivieren**, um die von Ihnen gewünschte Wiederholungsmethode und einen bestimmten Zeitpunkt für den Beginn der Knoten-Discovery festzulegen.



Sie können die folgenden Parameter festlegen, um Ihren Discovery-Ablaufplan zu konfigurieren:

- **Nach folgender Anzahl von Tagen**: Die Methode wird nach der angegebenen Anzahl von Tagen wiederholt. (Standard)
- **Alle ausgewählten Tage der Woche**: Die Methode wird an den angegebenen Tagen wiederholt. Montag, Dienstag, Mittwoch, Donnerstag und Freitag sind die standardmäßigen Wochentage.
- **Alle ausgewählten Tage des Monats**: Die Methode wird am angegebenen Tag des Monats wiederholt. 1 ist die Standardoption für den Tag des Monats.

- **Geplante Uhrzeit**: Ermöglicht es Ihnen, die Uhrzeit anzugeben, zu der Discovery entsprechend dem Wiederholungsablaufplan ausgeführt wird.
- **Knoten-Discovery-Liste > Hinzufügen:** Wählen Sie aus, woher Sie Knoten hinzufügen möchten. Geben Sie dann die erforderlichen Anmeldeinformationen an.

  Hinweis: Optional klicken Sie auf **Jetzt ausführen**, um Discovery sofort auszuführen.

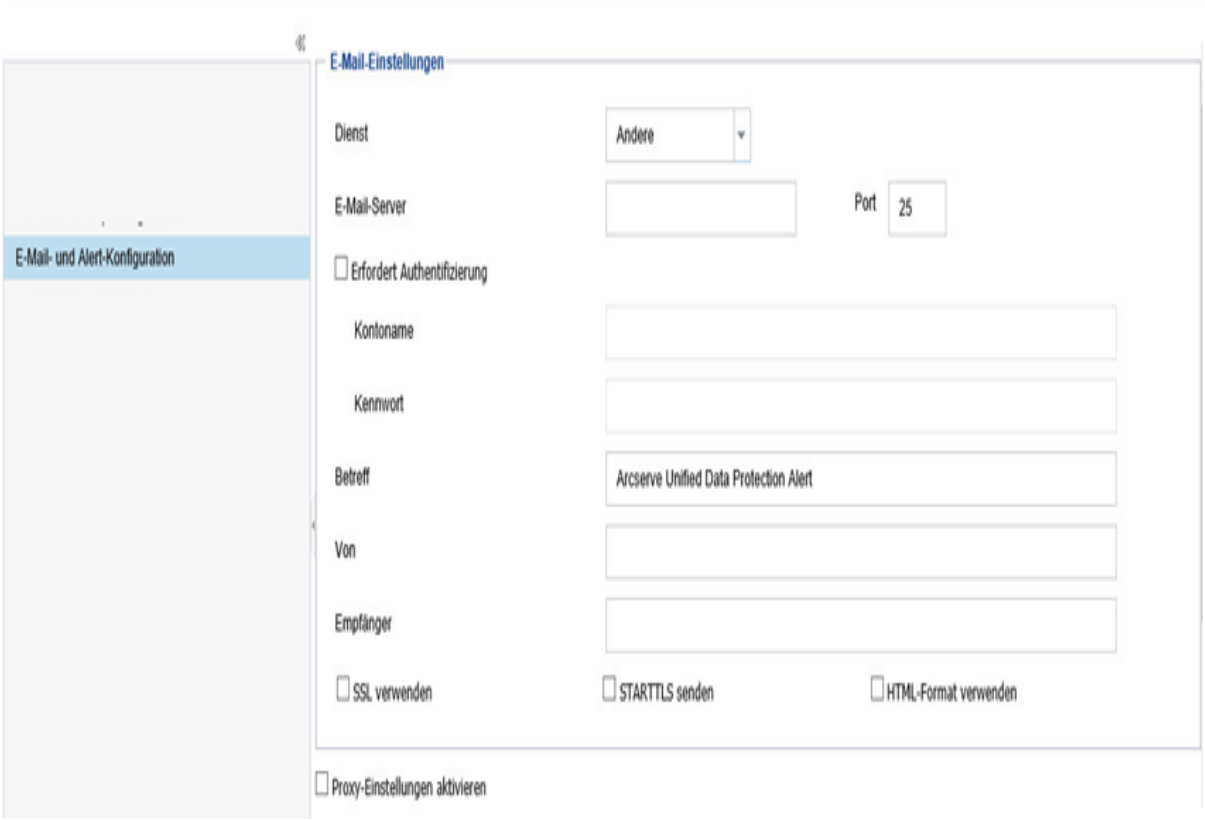
Konfigurieren von E-Mails und Alerts

Auf der Seite **E-Mail- und Alert-Konfiguration** können Sie die Konfigurationen für E-Mail-Einstellungen und E-Mail-Alerts angeben.

Hinweis: Die Installation von Microsoft.NET Framework (Version 2.0 oder höher) auf dem Rechner, auf dem Sie die Konsole für die Berichtsdiagramm-Exportfunktion installiert haben, ist für das erfolgreiche Exportieren von Bildern in einen Bericht Voraussetzung.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **E-Mail- und Alert-Konfiguration**.
3. Geben Sie die Details ein, um Standardeinstellungen festzulegen.



Dienst

Wählen Sie E-Mail-Dienste aus den verfügbaren Optionen aus.

E-Mail-Server

Geben Sie den Hostnamen des SMTP-Servers an, den Sie zur Versendung von Alerts per E-Mail verwenden möchten.

Port

Geben Sie die Portnummer für den E-Mail-Server an.

Authentifizierung erforderlich

Aktivieren Sie das Kontrollkästchen, um Anmeldeinformationen einzugeben.

SSL verwenden/STARTTLS senden/HTML-Format verwenden

Aktivieren Sie die gewünschte Option, um Anforderungen festzulegen.

Proxy-Einstellungen aktivieren

Aktivieren Sie das Kontrollkästchen, um Details für den **Proxy-Server** und die Authentifizierung einzugeben.

Test-E-Mail

Klicken Sie hier, um die Angaben im Abschnitt "E-Mail-Einstellungen" zu überprüfen.

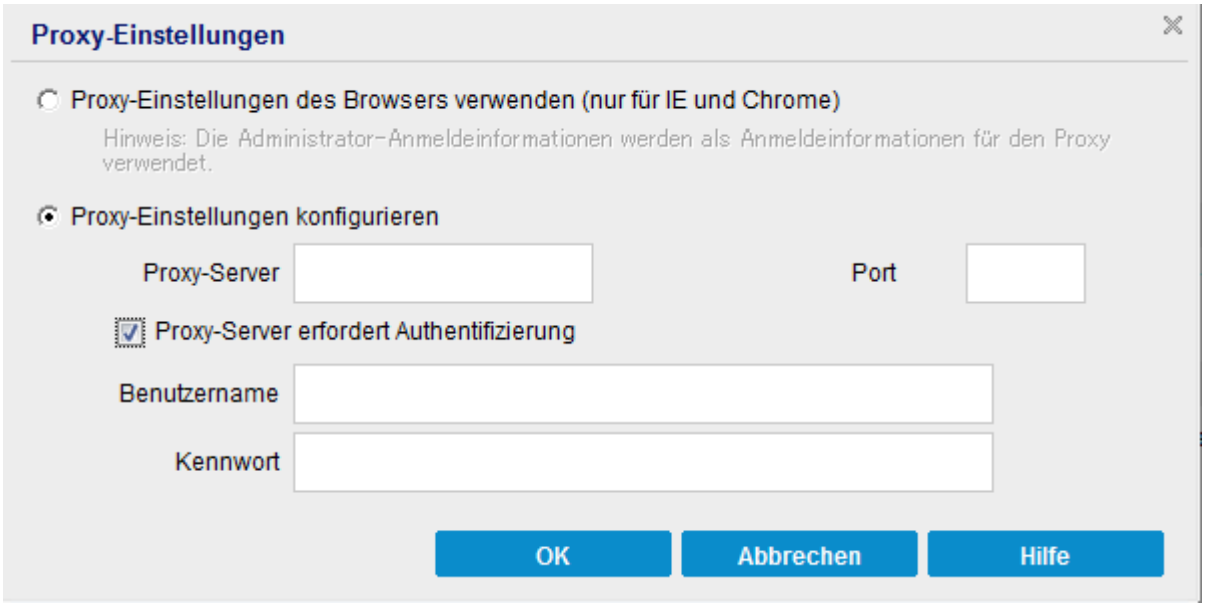
E-Mail-Alerts senden

Wählen Sie **Erkannte Knoten** aus, um **Active Directory**-Knoten zu konfigurieren, die Sie mithilfe der Erkennungsfunktion finden können. Diese Option steht für Knoten auf der Registerkarte **Ressourcen** zur Verfügung.

Proxy-Einstellungen konfigurieren

Klicken Sie auf **Proxy-Einstellungen**, um anzugeben, ob Arcserve UDP über einen Proxy-Server kommunizieren soll. Ein Proxy-Server agiert als Mittelsmann zwischen Ihrem Server und dem Arcserve-Server und bietet damit mehr Sicherheit, erhöhte Leistung und Verwaltungskontrolle. Er fungiert als Verbindung zum Arcserve-Server, von dem Ihr Download-Server die Aktualisierungen abruft.

Wenn Sie den Arcserve-Server als Download-Server auswählen, wird das Dialogfeld **Proxy-Einstellungen** geöffnet.



- **Proxy-Einstellungen des Browsers verwenden**

  Diese Auswahl ist nur unter Windows Internet Explorer (IE) und Google Chrome anwendbar.

  Wenn diese Option ausgewählt ist, werden die gleichen Proxy-Einstellungen, die auf den Browser angewendet werden, um eine Verbindung mit dem Arcserve-Server für Arcserve UDP-Aktualisierungsinformationen herzustellen, von Arcserve UDP automatisch erkannt und verwendet.

- **Proxy-Einstellungen konfigurieren**

  Wenn diese Option ausgewählt ist, wird der angegebene Proxy-Server aktiviert, um eine Verbindung mit dem Arcserve-Server für Arcserve UDP-Aktualisierungsinformationen herzustellen. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet.

Außerdem können Sie angeben, ob der Proxy-Server Authentifizierung benötigt. Wenn diese Option aktiviert ist, müssen zur Verwendung des Proxy-Servers Authentifizierungsinformationen (Benutzer-ID und Kennwort) angegeben werden.

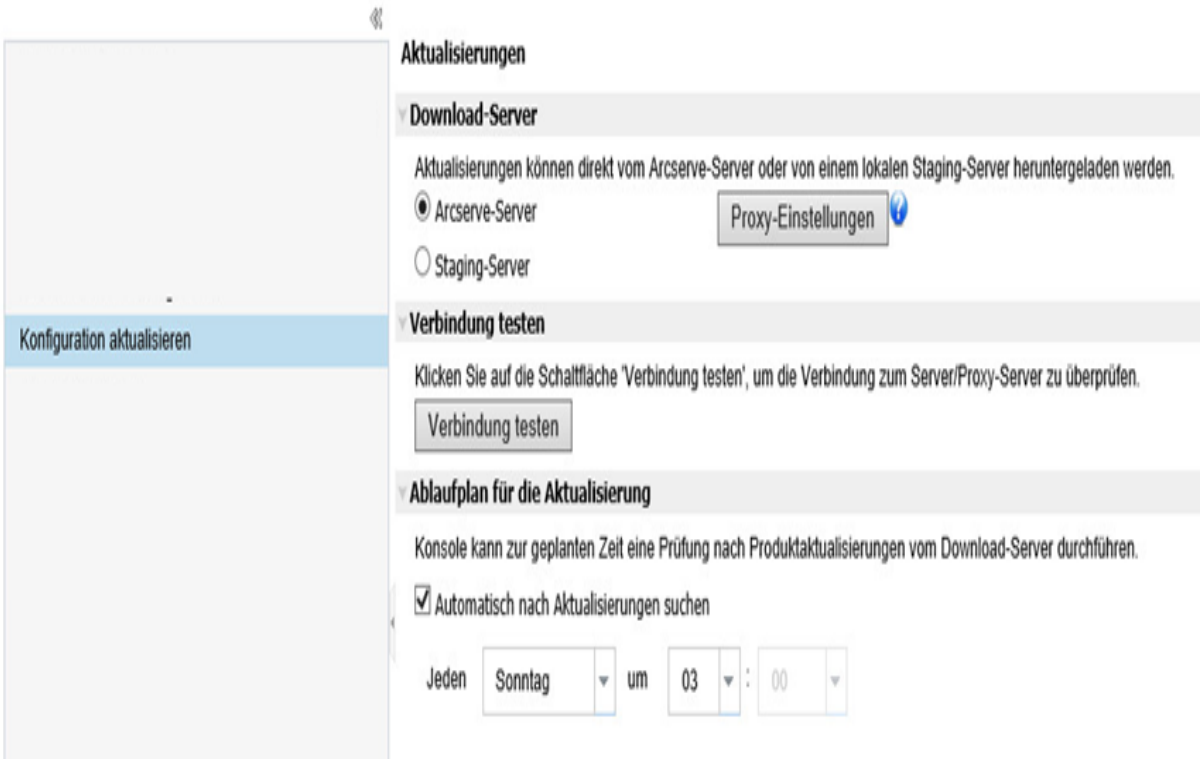
Hinweis: Als Format für den Benutzernamen sollte ein vollständiger Domänenbenutzername im Format "<Domänenname>\<Benutzername>" verwendet werden.

Aktualisieren der Konfiguration

Auf der Seite "Konfiguration aktualisieren" können Sie Download-Server und Aktualisierungspläne für die Konfiguration von Aktualisierungen festlegen. Sie können Details über Arcserve Server-Proxy-Einstellungen oder Staging-Server für "Download-Server" angeben.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Aktualisierungskonfiguration**.



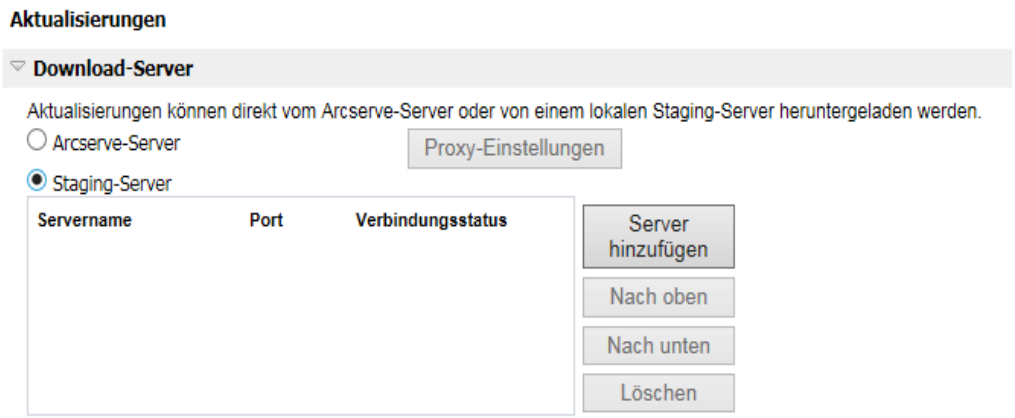
Geben Sie die Details für den Typ des Aktualisierungsservers und des Aktualisierungsablaufplans an. Der Aktualisierungsserver ist entweder Arcserve-Server oder Staging-Server.

3. Wählen Sie für **Download-Server** eine der folgenden Optionen aus:
   - Klicken Sie für **Arcserve-Server** auf **Proxy-Einstellungen**, um das Proxy-Setup abzuschließen.
   - Klicken Sie für "**Staging-Server**" auf "**Server hinzufügen**", um Details des Staging-Servers anzugeben.

Um einem Staging-Server zu erstellen, zeigen Sie So erstellen Sie einen Staging-Server an.

Befindet sich der Staging-Server hinter einer Firewall, bereiten Sie einen Rechner vor, der auf das Internet zugreifen kann, das UDP-Produkt installiert hat und die neuesten Aktualisierungen vom Arcserve-Server erhält. Kopieren Sie dann die Ordner **EngineUpdates** und **FullUpdates** aus folgendem Speicherort auf den Staging-Server-Rechner:

<UDP-Installationspfad>\ Arcserve\Unified Data Protection\Update Manager



Hinweise:

- Da für die Funktion zur automatischen Aktualisierung keine Lizenz erforderlich ist, müssen Sie keine Lizenz auf dem Staging-Server aktivieren.
- Weitere Informationen zu Ports finden Sie unter Von Arcserve UDP verwendete Kommunikationsports.

Sie können mehrere Staging-Server hinzufügen.

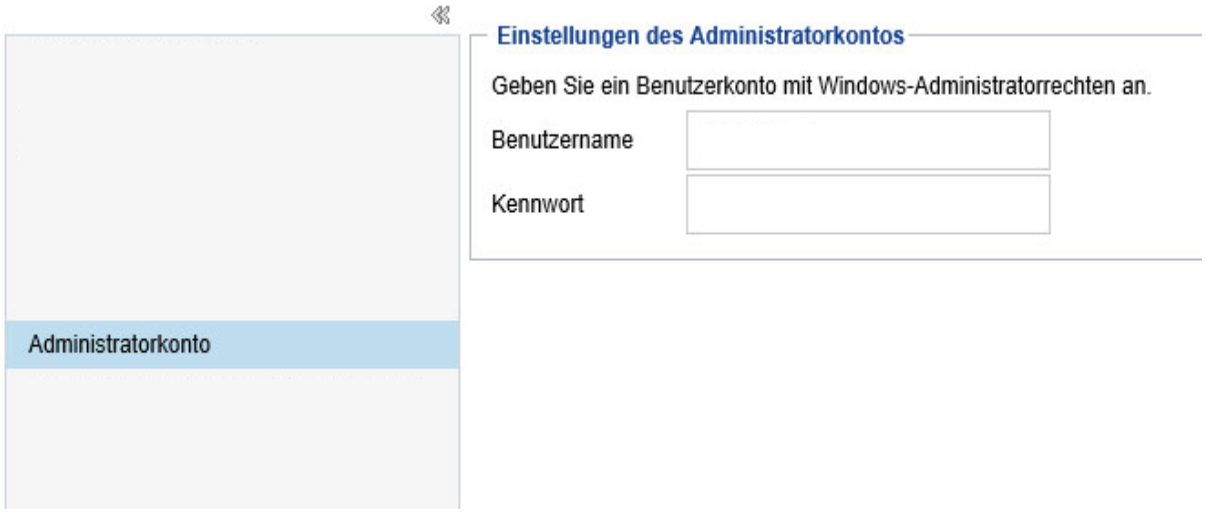
4. Klicken Sie auf **Verbindung testen**, um die Details des **Download-Servers** zu überprüfen.
5. Geben Sie Details für "**Ablaufplan für Aktualisierung**" ein.
6. Wählen Sie "**Automatisch nach Aktualisierungen suchen**" aus.
7. Klicken Sie auf "**Speichern**", um die Aktualisierung fertigzustellen.

Konfigurieren des Administratorkontos

Auf der Seite **Administratorkonto** können Sie ein Benutzerkonto erstellen, indem Sie einen **Benutzernamen** und ein **Kennwort** angeben.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Administratorkonto**.



3. Geben Sie die Anmeldeinformationen Ihres Administrator-Kontos an, und klicken Sie auf **Speichern**.

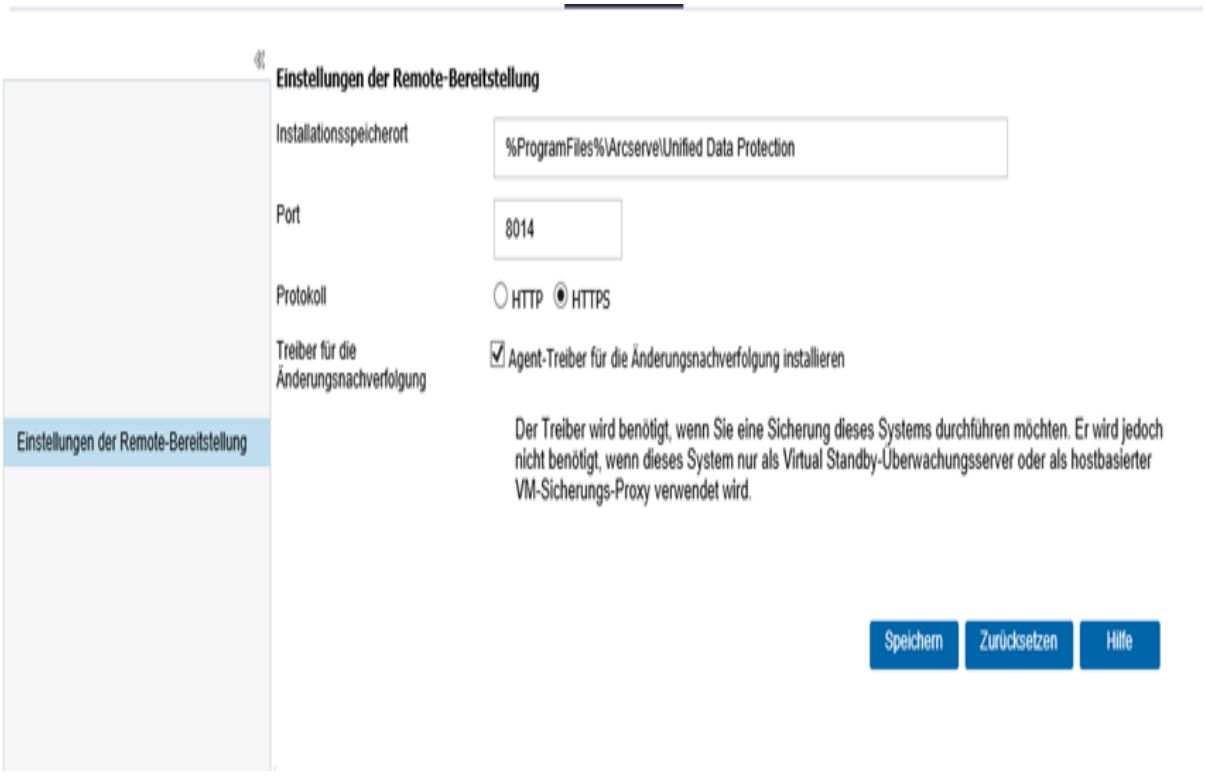
Einstellungen der Remote-Bereitstellung

Auf der Seite **Einstellungen der Remote-Bereitstellung** können Sie Standardeinstellungen für die Installation von Arcserve Unified Data Protection-Agent und Arcserve Unified Data Protection-Recovery Point Server angeben. Geben Sie die standardmäßigen Installationseinstellungen an, um den Speicherort der Installation festzulegen.

Geben Sie die Details für **Installationspfad**, **Protokoll** und **Port** ein, und klicken Sie auf **Speichern**.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Einstellungen der Remote-Bereitstellung**.



3. Geben Sie die erforderlichen Details ein, und klicken Sie auf **Speichern**.

Zuordnen des Plans zum Benutzerkonto

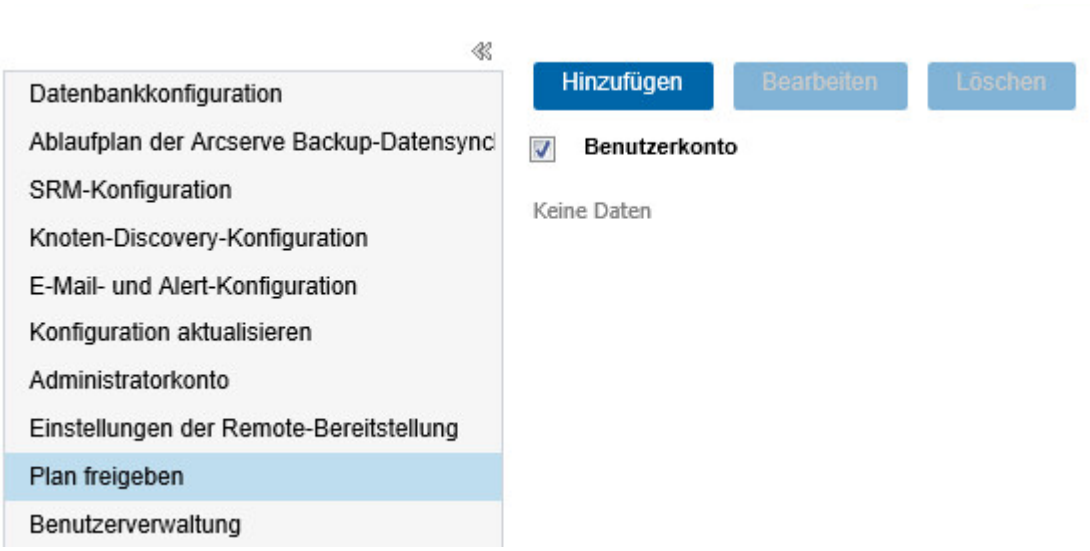
Zieladministrator

Sie haben bereits ein Benutzerkonto und einen Plan für eine Quellkonsole erstellt. Um replizierte Daten zu identifizieren und zu verwalten, weisen Sie den Plan dem Benutzerkonto zu.

Hinweis: Sie können einem Benutzerkonto mehrere Pläne zuweisen, doch ein Plan kann nicht von zwei verschiedenen Konten gemeinsam verwendet werden. Es wird jedoch empfohlen, einem Benutzerkonto jeweils nur einen Plan zuzuweisen, damit Sie die replizierten Daten einfach identifizieren und verwalten können.

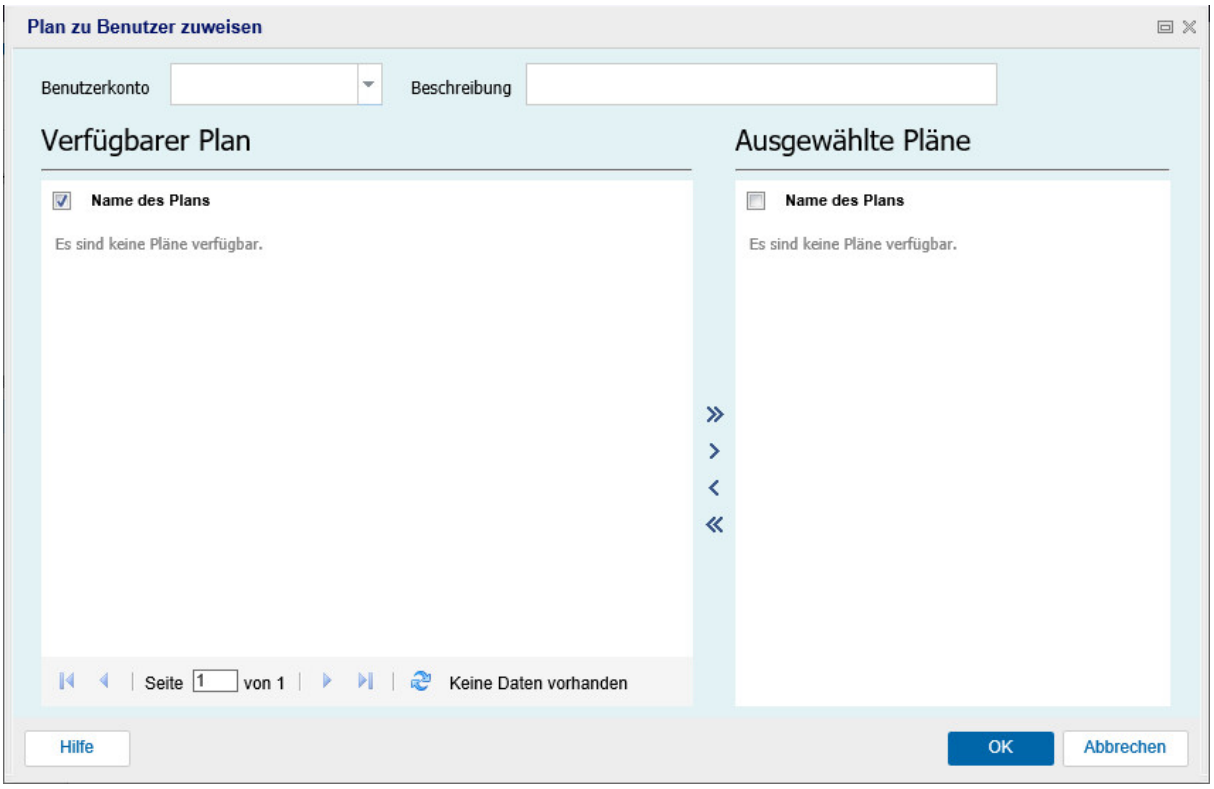
Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Plan freigeben**.



3. Klicken Sie im mittleren Fensterbereich auf **Hinzufügen**.

   Das Dialogfeld **Plan zu Benutzer zuweisen** wird geöffnet.



4. Wählen Sie das **Benutzerkonto** aus.
5. Wählen Sie einen Plan aus der Spalte **Verfügbarer Plan** aus.

   Hinweis: Wenn ein Plan bereits zu einem Benutzernamen hinzugefügt ist, wird dieser Plan nicht in der Spalte "**Verfügbarer Plan**" angezeigt.
6. Klicken Sie auf **Alle Pläne hinzufügen** oder **Ausgewählte Pläne hinzufügen**, um die Pläne in der Spalte **Ausgewählte Pläne** hinzuzufügen.
7. Klicken Sie auf **"OK**".

   Das Dialogfeld **Plan zu Benutzer zuweisen** wird geschlossen. Der Benutzername und die zugeordneten Pläne werden auf der Seite **Plan freigeben** angezeigt.

   Das Benutzerkonto wird dem Plan zugeordnet, der für die Quellkonsole erstellt wurde.

   Sie können **Bearbeiten** verwenden, um die Benutzerkonfiguration zu ändern, oder **Löschen**, um das Benutzerkonto aus der Liste zu entfernen.

Benutzerverwaltung

Auf der Seite "Benutzerverwaltung" haben Sie folgende Möglichkeiten:

- Melden Sie sich über die Arcserve UDP-Konsole bei der Benutzerverwaltungskonsole (Identitätsdienstkonsole) an. Weitere Informationen finden Sie unter Starten der Arcserve UDP-Benutzerverwaltungskonsole.
- Aktivieren und Konfigurieren der Multi-Faktor-Authentifizierung (MFA) für alle Benutzer Weitere Informationen finden Sie unter Konfigurieren der Multi-Faktor-Authentifizierung.

Konfigurieren der Zeitüberschreitungsdauer der Konsole

Wenn die Konsole über eine bestimmte Zeit inaktiv ist, werden Sie von der Konsole automatisch abgemeldet. Sie können den Standard-Zeitlimitwert in der Datei "ConsoleConfiguration.xml" ändern.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Rechner an, auf dem Sie die Konsole installiert haben.
2. Öffnen Sie die Datei "ConsoleConfiguration.xml" von folgendem Speicherort:

   <UDP_Home>\Management\Configuration\ConsoleConfiguration.xml
3. Ändern Sie den Wert für "consoleUISessionTimeout".

   Der Wert wird in Sekunden angegeben.

   Beispiel:

   <consoleUISessionTimeout> 3600 </consoleUISessionTimeout> (Standardwert ist 1 Stunde, Wert wird in Sekunden angegeben)

   3600 bedeutet, dass das Zeitlimit für die Konsole 3600 Sekunden beträgt
4. Speichern Sie die Datei "ConsoleConfiguration.xml".

So migrieren Sie r16.5-Wiederherstellungspunkte zu Arcserve UDP

Wichtig! Hinweise zur Replikation aus einem freigegebenen Ordner in einen auf einem Recovery Point Server ausgewählten Datenspeicher finden Sie unter So führen Sie eine Offline-Datenreplikation mithilfe von RPS-Jumpstart aus.

Um Arcserve r16.5-Wiederherstellungspunkte zu Arcserve UDP migrieren, führen Sie die folgenden Schritte durch:

1. Erstellen eines Datenspeichers zur Replikation von Daten von einem Arcserve r16.5
2. Replizieren von Arcserve r16.5-Daten in den UDP-Datenspeicher

Erstellen eines Datenspeichers zur Replizierung von Daten von einem Arcserve r16.5-Wiederherstellungspunkt

Um Daten von einem vorhandenen Arcserve r16.5 D2D-Wiederherstellungspunkt zu replizieren, erstellen Sie zuerst einen Datenspeicher über die Konsole, wo die Daten repliziert werden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Navigieren Sie zu **Ziele**, **Recovery Point Server**.
3. Wählen Sie den Recovery Point Server aus.
4. Klicken Sie mit der rechten Maustaste, und wählen Sie **Einen Datenspeicher hinzufügen** aus.
5. Geben Sie die Details auf der Seite **Einen Datenspeicher hinzufügen** ein.
6. Speichern Sie den Datenspeicher.

   Der Datenspeicher wurde erstellt.

Replizieren von Arcserve r16.5-Daten in den UDP-Datenspeicher

Nachdem Sie den Datenspeicher erstellt haben, können Sie die Arcserve r16.5-Wiederherstellungspunktdaten mithilfe von RPS-Jumpstart replizieren.

Gehen Sie wie folgt vor:

1. Klicken Sie auf **Aktionen**, und klicken Sie dann auf **RPS-Jumpstart**.

   Der **Assistent für RPS-Jumpstart** wird geöffnet.

2. Wählen Sie "Von einem freigegeb. Ordner zu einem Datenspeicher auf ausgewähltem Recovery Point-Server" aus.

3. Geben Sie "Quelle: Freigegebener Ordner" an.

   Die Wiederherstellungspunktdetails werden angezeigt.

   Hinweis: Wenn die Sitzung und der Zieldatenspeicher unverschlüsselt sind, ist das Sitzungskennwort optional. Wenn die Sitzung unverschlüsselt und die Zieldatenspeicher verschlüsselt ist, müssen Sie auf der Seite "**Zieldatenspeicher auswählen**" ein Sitzungskennwort angeben.

4. Klicken Sie auf **Weiter**.

   Die Seite **Zieldatenspeicher auswählen** wird geöffnet. Wenn die Quelldaten verschlüsselt sind, dann werden nur die verschlüsselten Datenspeicher in der Dropdown-Liste angezeigt.

5. (Optional) Geben Sie das Sitzungskennwort an, wenn die Sitzung in Schritt 3 nicht verschlüsselt ist.

6. Klicken Sie auf **Weiter**.

7. Klicken Sie auf **Fertig stellen**.

   Die Wiederherstellungspunktdaten von Arcserve r16.5 werden in den Arcserve UDP-Datenspeicher repliziert.

Einrichten des Konfigurationsassistenten

Mit dem Konfigurationsassistenten konfigurieren Sie Ihre Datenschutzumgebung, sobald Sie sich an der Konsole angemeldet haben. Wenn Sie Arcserve UDP zum ersten Mal verwenden, ist der Konfigurationsassistent ein idealer Weg, um Ihren ersten Sicherungsplan zu erstellen. Der Assistent erstellt Pläne, um zu definieren, wie man Daten schützt. Ein Plan besteht aus einem oder mehreren Tasks zum Definieren von Quelle, Ziel, Ablaufplan und erweiterten Parametern. Mit der ersten Anmeldung an der Konsole öffnet sich der Konfigurationsassistent. Sie können die Willkommensseite des Assistenten ausblenden, indem Sie **Diese Seite beim nächsten Mal nicht anzeigen** auswählen.

Sie können einen Plan zum Schutz Ihrer physischen Knoten wie Windows- und Linux-Knoten und virtuellen Rechner wie VMware und Hyper-V erstellen.

Die folgenden Schritte enthalten eine allgemeine Beschreibung zum Erstellen eines Windows-Agenten-basierten Plans mithilfe des Konfigurationsassistenten.

1. Melden Sie sich bei der Konsole an.

   Wenn Sie sich zum ersten Mal anmelden, wird der Konfigurationsassistent geöffnet.

2. Wenn der Assistent nicht geöffnet wird, klicken Sie auf die Registerkarte **Ressourcen** und dann im rechten Bereich auf **Konfigurationsassistent**.

   Die Willkommensseite des Assistenten wird geöffnet.

3. Klicken Sie auf **Weiter**.

   Die Seite **Plan erstellen** wird geöffnet.

4. Geben Sie den Namen des Plans ein.

5. Wählen Sie den zu schützenden Knotentyp aus.

   Wählen Sie z. B. **Agentenbasierte Sicherung Windows**.

6. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Zu schützende Knoten hinzufügen** wird geöffnet. Die Felder auf der Seite **Zu schützende Knoten hinzufügen** sind optional.

7. Wählen Sie die Methode zum Hinzufügen von Knoten aus der Drop-down-Liste aus.

   Die Felder variieren je nach Ihrer Auswahl.

8. Geben Sie die Knotendetails an, klicken Sie auf **Zur Liste hinzufügen**, und klicken Sie dann auf **Weiter**.

   Die Seite "**Sicherungsziel**" wird geöffnet.

9. Wählen Sie in der Drop-down-Liste den Zieltyp aus.

Die übrigen Felder auf der Seite **Sicherungsziel** variieren je nach dem Zieltyp. Sie können auch das Sitzungskennwort aktivieren.

Informationen zum Erstellen eines Datenspeichers finden Sie unter Hinzufügen von Datenspeichern.

10. Geben Sie die übrigen Ziel-Details an, und klicken Sie auf **Weiter**.

    Die Seite **Sicherungsablaufplan** wird geöffnet.

11. Geben Sie den Sicherungsablaufplan an, und klicken Sie auf **Weiter**.

    Die Seite **Bestätigung des Plans** wird geöffnet.

12. Überprüfen Sie den Plan.

13. (Optional) Klicken Sie auf **Plan erstellen**, um einen anderen Plan hinzufügen.

14. Klicken Sie auf **Weiter**

    Die Ressourcenkonfiguration ist abgeschlossen.

15. Klicken Sie auf **Fertig stellen**.

    Der Assistent wird geschlossen und ein neuer Plan erstellt.

    Sie können den Plan unter **Ressourcen**, **Pläne**, **Alle Pläne** sehen.

Kapitel 6: Wichtige Funktionen von Arcserve UDP

In diesem Abschnitt werden die folgenden Themen behandelt:

Informationen zur Nutanix Funktion in Arcserve UDP

Um die Funktionen zu erkunden, die für das Nutanix-Feature in Arcserve UDP verfügbar sind, lesen Sie bitte So arbeiten Sie mit Nutanix mithilfe von Arcserve UDP.

Informationen zur OneDrive Funktion in Arcserve UDP

Entdecken Sie die Funktionen, die für die OneDrive Funktion in Arcserve UDP verfügbar sind.

- Verwalten von OneDrive Knoten
- So erstellen Sie einen Sicherungsplan für Microsoft Office 365 OneDrive
- So stellen Sie OneDrive Daten wieder her

Grundlegendes zur Exchange Online-Funktion in Arcserve UDP

Exchange Online ist eine E-Mail-Anwendung, die in der Microsoft-Cloud gehostet wird. Um Ihre Exchange Online-E-Mail-Elemente (E-Mails, Kalenderelemente, Kontakte usw.) aus der Microsoft-Cloud zu sichern, müssen Sie einen Plan in Arcserve UDP erstellen. Erfahren Sie mehr über die für die Exchange Online-Funktion verfügbaren Funktionen in Arcserve UDP.

- Benutzerrechte für Exchange Online in Arcserve UDP
- Hinzufügen eines Exchange Online-Knotens
- Verwalten von Exchange Online-Knoten
- Hinzufügen der erforderlichen Rolle und Gruppe zum Exchange Online-Sicherungskonto zur Durchführung von Sicherungen und Wiederherstellungen
- Erstellen eines Exchange Online-Sicherungsplans
- So stellen Sie Exchange Online-Postfachdaten wieder her
- Best Practices

Grundlegendes zur Hardware-Snapshot-Funktion in UDP

Arcserve UDP bietet die Möglichkeit, Hardwarespeicher-Snapshots für die Sicherung zu nutzen. Sie können angeben, ob Sie einen Hardware-Snapshot verwenden möchten, wenn Sie einen Sicherungstask erstellen. Wenn Sie den Hardware-Snapshot auswählen, versucht Arcserve UDP zuerst, einen Hardware-Snapshot zu erstellen. Wenn der Hardware-Snapshot fehlschlägt, kehrt Arcserve UDP automatisch zum Software-Snapshot zurück, ohne dass der Sicherungsjob fehlschlägt.

- Verwenden von Hardware-Snapshots für Sicherungen
- Unterstütztes Speicher-Array in Arcserve UDP
- Verwenden von Hardware-Snapshots für die agentenlose VMware-Sicherung
- Verwenden von Hardware-Snapshots für die agentenlose Hyper-V-Sicherung
- Verwenden von Hardware-Snapshots für die agentenbasierte Sicherung
- Überprüfen, ob die Sicherung Hardware-Snapshots verwendet hat

Nimble

- Hinzufügen eines Speicher-Arrays
- Hinweise zu Nimble-Speicher bei aktivierter CHAP-Authentifizierung
- Verwenden von Hardware-Snapshots für die agentenlose VMware-Sicherung

HPE 3PAR Storeserve

- Hinzufügen eines Speicher-Arrays
- Verwenden von Hardware-Snapshots für die agentenlose VMware-Sicherung

NetApp

- Hinzufügen eines Speicher-Arrays
- Hinweise für den NetApp iSCSI/FC-Support für VMware
- Auf Hardware-Snapshot für NetApp NFS VMware angewandte Bedingungen
- Verwenden von Hardware-Snapshots für die agentenlose VMware-Sicherung

Grundlegendes zur Cloud-Funktion in UDP

Arcserve UDPDie Cloud-Funktion gewährleistet, dass Ihre Daten bei versehentlichem Löschen in der Cloud für Sie geschützt sind. Die Arcserve UDP Cloud-Funktionen ermöglichen Ihnen u. a. die angegebenen Dateien und Wiederherstellungspunkte zu kopieren sowie Instanzen mithilfe von Wiederherstellungspunkten und virtuelle Standby VMsin der Cloud zu erstellen.

Links zum Verwenden der Cloud anzeigeninArcserve UDP:

- Hinzufügen eines Cloud-Kontos
- Verwalten von Knoten für die Cloud
  - Herunterladen von Wiederherstellungspunkten aus der Cloud
  - Hochladen von Wiederherstellungspunkten in die Cloud
  - Kopieren von Wiederherstellungspunkten auf einen lokalen Datenträger oder eine Netzwerkfreigabe
- So konfigurieren Sie einen RPS in der Cloud
  - Bestimmen einer Cloud-Konfiguration zur Wiederherstellung von einem Cloud-Dateikopiespeicherort.
  - Bestimmen einer Cloud-Konfiguration zur Wiederherstellung von einem Cloud-Dateiarchivspeicherort.
- So sichern Sie Daten in der Cloud
  - Erstellen eines Plans für ein Virtual Standby in AWS EC2
  - Erstellen und Verwalten von Instant VMs auf Amazon EC2
  - Erstellen eines Ablaufplans für das Kopieren von Wiederherstellungspunkten
- Cloud für Linux
  - Installieren von Arcserve UDP Agent (Linux) in AWS Cloud
  - Ausführen einer Bare-Metal-Recovery (BMR) für Linux-Rechner in der AWS-Cloud
  - So führen Sie eine Migrations-BMR von Amazon EC2 auf einen lokalen Linux-Rechner durch
  - So führen Sie eine IVM-Migration aus der Cloud auf einen lokalen Rechner durch
- Microsoft Office 365-Sicherungsplan

- Erstellen eines Exchange Online-Sicherungsplans
- So stellen Sie Exchange Online-Postfachdaten wieder her
- So erstellen Sie einen Sicherungsplan für Microsoft Office 365 OneDrive
- So stellen Sie OneDrive Daten wieder her
- Erstellen eines SharePoint Online-Sicherungsplans (Video ansehen)
- So stellen Sie Restore SharePoint Online-Websitesammlungsdaten wieder her

- Microsoft Azure
  - Erstellen eines Plans für ein Virtual Standby auf Microsoft Azure
  - So erstellen und verwalten Sie eine Instant VM auf Microsoft Azure
- Fehlerbehebung
  - Hinzufügen eines Verschlüsselungskennworts für ein vorhandenes verschlüsseltes Ziel
  - Konfigurieren der Registrierung für das Kopieren von Wiederherstellungspunkten
  - Bandbreitenüberlastung bei Jobs zum Kopieren von Wiederherstellungspunkten in die Cloud
  - Verbindung zur Cloud kann nicht hergestellt werden.

Grundlegendes zur UNC/NFS-Pfad-Funktion in UDP

Der UNC-Pfad/NFS-Pfad wird als neuer Knotentyp eingeführt. Informationen zur Verwendung der Funktion finden Sie in den folgenden Abschnitten:

- Benutzerrechte für UNC/NFS-Pfade in Arcserve UDP
- Hinzufügen und Verwalten eines UNC/NFS-Pfades
- Erstellen eines Sicherungsplans für UNC/NFS-Pfade
- Wiederherstellen von einem UNC/NFS-Pfad aus

Grundlegendes zur SharePoint Online-Funktion in UDP

Arcserve UDP v6.5 Update 2 und höher unterstützt die Arbeit mit der Microsoft SharePoint-Online-Umgebung. Informationen zur Verwendung der Funktion finden Sie in den folgenden Abschnitten:

- Voraussetzungen
- Hinzufügen eines SharePoint-Knotens
- Verwalten von SharePoint Online-Knoten
- Erstellen eines SharePoint Online-Sicherungsplans
- So stellen Sie Restore SharePoint Online-Websitesammlungsdaten wieder her

Voraussetzungen

Arcserve UDP 8.0 hat die folgende Voraussetzung, um mit der Microsoft SharePoint Online Umgebung zu arbeiten:

Stellen Sie sicher, dass Sie über die entsprechenden Benutzerberechtigungen für die Arcserve UDP-Funktionen verfügen. Weitere Informationen finden Sie unter Benutzerberechtigungen für SharePoint Online in Arcserve UDP.

Kapitel 7: Verwenden der rollenbasierten Arcserve UDP-Verwaltung

Mit der rollenbasierten Verwaltung (RBAC) können Administratoren die verschiedenen Rollen und Berechtigungen für die verschiedenen Benutzer zuweisen, für die Verwendung der Arcserve UDP-Konsole. Jede Rolle kann über eigene Berechtigungen verfügen. Eine Superadministrator-Rolle kann benutzerdefinierte Rollen und Berechtigungen für andere Benutzer der Arcserve UDP-Konsole erstellen.

Mit RBAC können Sie den einzelnen Rollen verschiedene Sicherheitsebenen zuweisen.

In diesem Abschnitt werden die folgenden Themen behandelt:

Zugriff auf die Benutzerverwaltungskonsole

Auf der Seite "Benutzerverwaltung" haben Sie folgende Möglichkeiten:

- Melden Sie sich über die Arcserve UDP-Konsole bei der Benutzerverwaltungskonsole (Identitätsdienstkonsole) an.
- Aktivieren und Konfigurieren der Multi-Faktor-Authentifizierung (MFA) für alle Benutzer

In diesem Abschnitt werden die folgenden Themen behandelt:

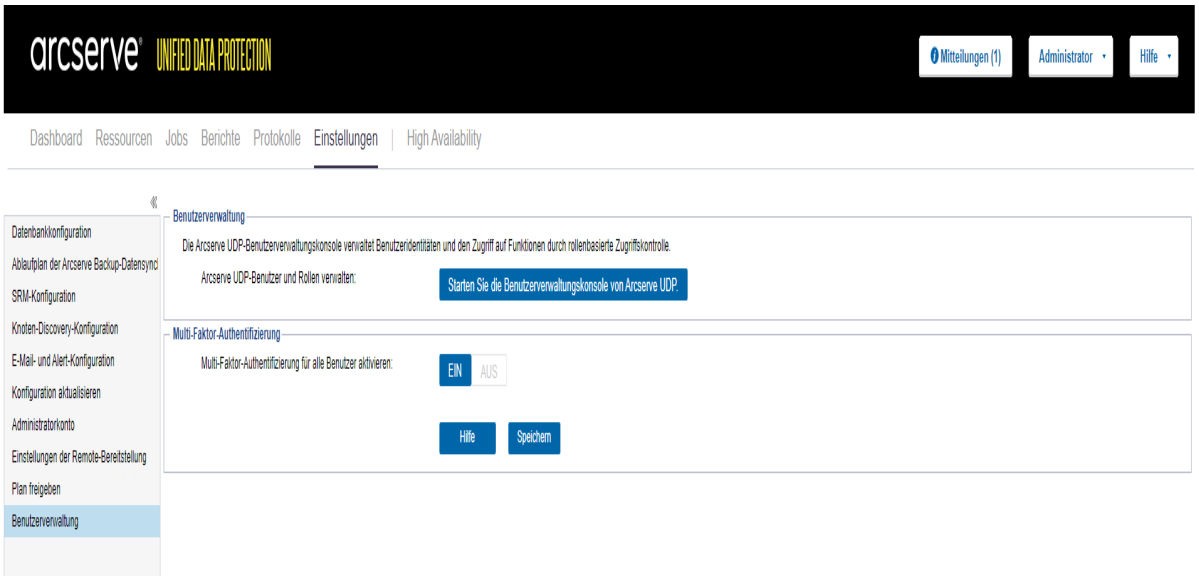
Die Arcserve UDP-Benutzerverwaltungskonsole starten

Die Arcserve UDP-Benutzerverwaltungskonsole verwaltet Benutzeridentitäten und steuert den Zugriff auf Funktionen mithilfe der rollenbasierten Zugriffssteuerung. Dieser Abschnitt enthält Informationen zum Starten der Arcserve UDP-Benutzerverwaltungskonsole.

Gehen Sie wie folgt vor:

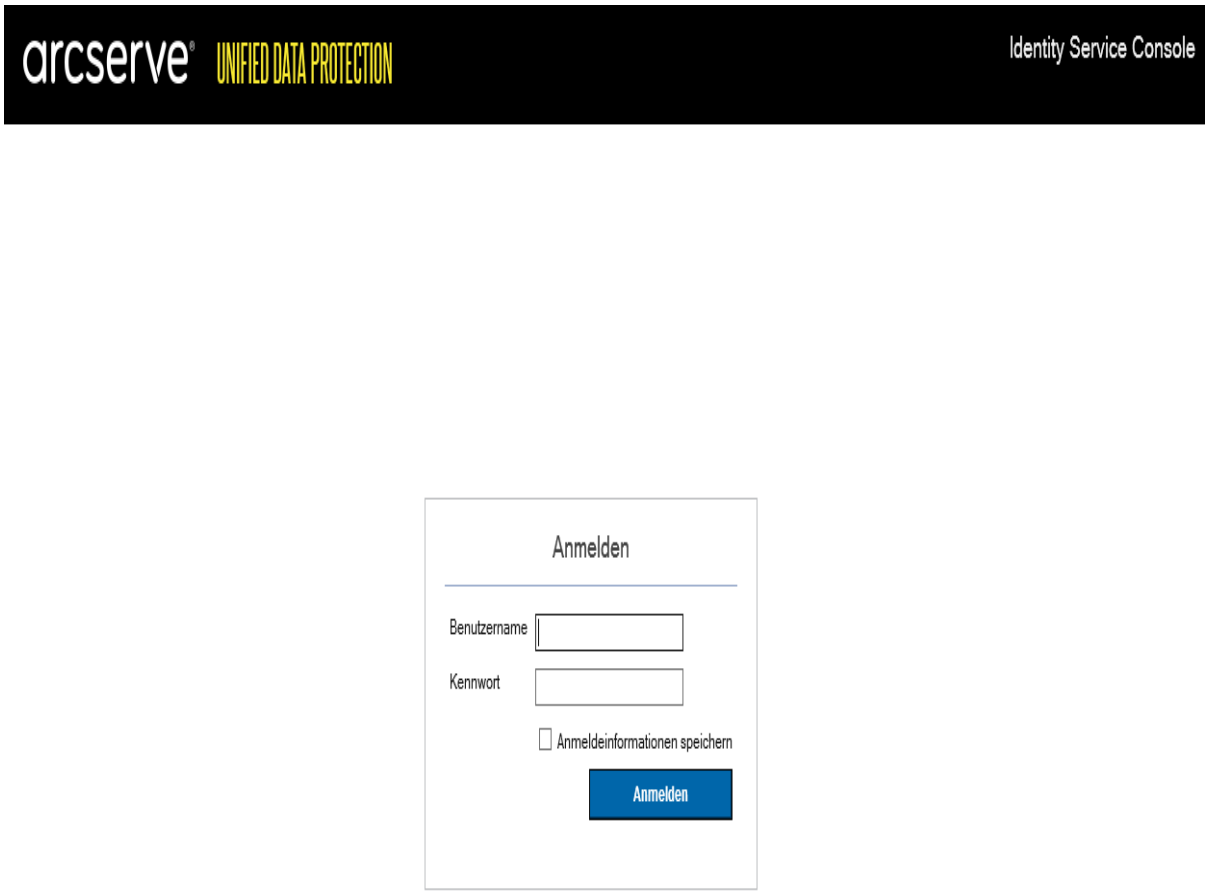
1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung**.

   Die Seite Benutzerverwaltung wird im mittleren Fensterbereich angezeigt.



3. Klicken Sie auf **Starten Sie die Arcserve UDP-Benutzerverwaltungskonsole**.

   Die Identitätsdienstkonsole wird in einem neuen Fenster angezeigt.



4. Geben Sie den Benutzernamen und das Kennwort ein, und klicken Sie dann auf **Anmelden**.

   Die Startseite der Identitätsdienstkonsole wird angezeigt.

   Sie haben erfolgreich auf die Arcserve UDP-Benutzerverwaltungskonsole zugegriffen.

   Alternativ können Sie sich auch bei der Identity Service-Konsole anmelden. Geben Sie die Adresse im folgenden Format in das neue Fenster ein, um sich anzumelden:

   HTTP (oder HTTPS)://(IP-Adresse oder Hostname): (Konsolen-Portnummer)/carbon

Multi-Faktor-Authentifizierung konfigurieren

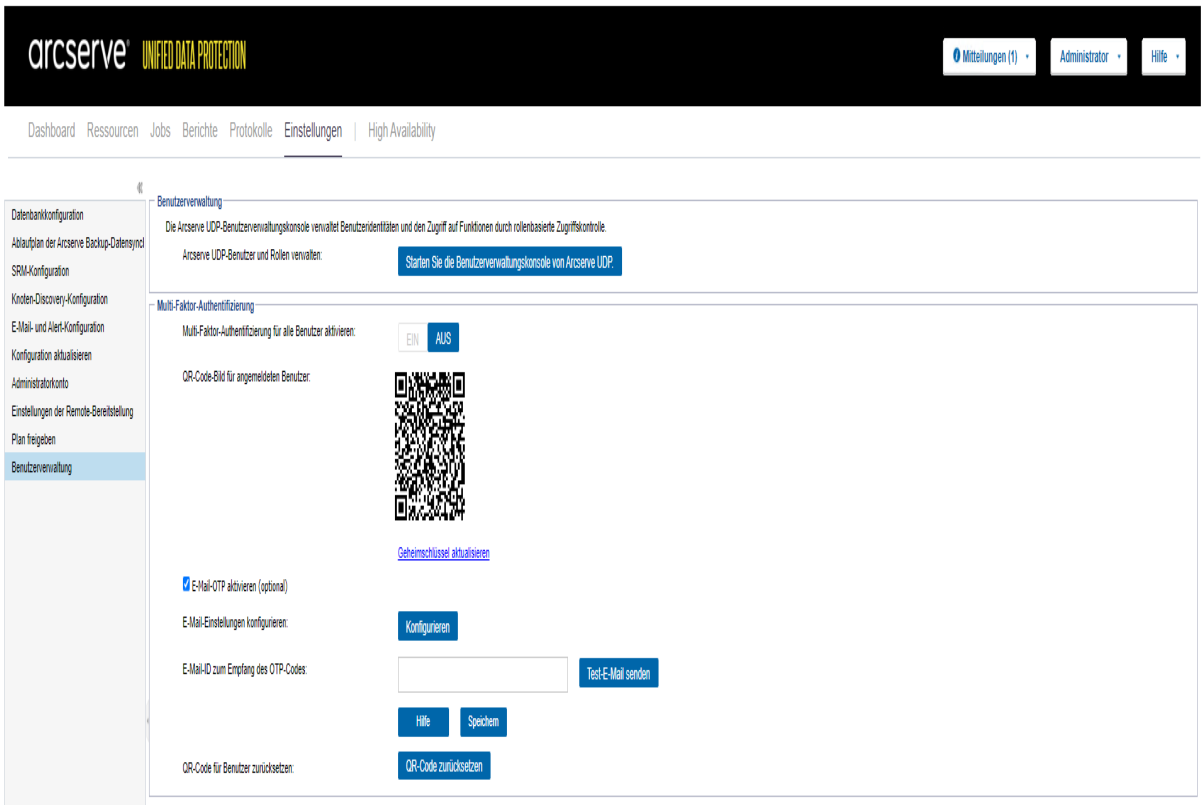
Dieser Abschnitt enthält die folgenden Themen:

Konfigurieren der Multi-Faktor-Authentifizierung als Admin-Benutzer

Dieser Abschnitt enthält Informationen zum Konfigurieren der Multi-Faktor-Authentifizierung für alle Benutzer.

Befolgen Sie diese Schritte:

1. Melden Sie sich mit Administrator-Anmeldeinformationen bei der Arcserve UDP-Konsole an.
2. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung**.



3. Um die Multi-Faktor-Authentifizierung für alle Benutzer zu aktivieren, **aktivieren** Sie im Abschnitt "Multi-Faktor-Authentifizierung" die Einstellung.

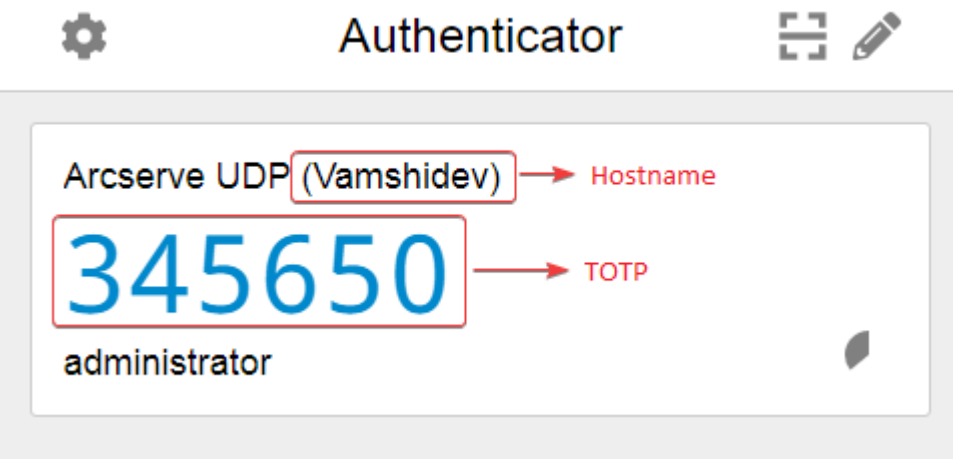
   Das QR-Code-Bild für den angemeldeten Benutzer wird angezeigt.

   Hinweis: Wenn Sie die Multi-Faktor-Authentifizierung für alle Benutzer deaktivieren möchten, **deaktivieren** Sie die Einstellung.

4. Scannen Sie das QR-Code-Bild mithilfe einer Authentifizierungs-App, um den TOTP zu generieren.

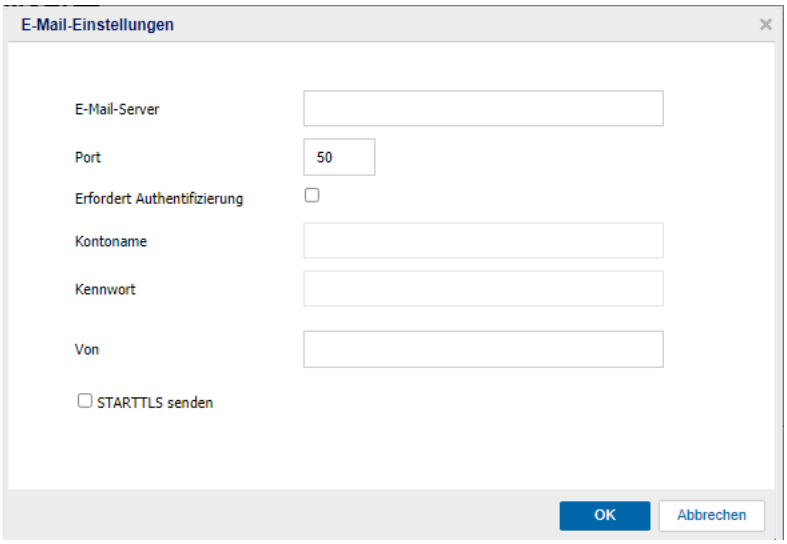
   Hinweise:

- Sie können jede mobile Authentifizierungs-App wie die Google Authenticator-App oder die Microsoft Authenticator-App auf Ihrem mobilen Gerät verwenden. Alternativ können Sie auch die Authenticator-Erweiterung in Ihrem Chrome-Browser verwenden.
- Klicken Sie unter dem QR-Code-Bild auf den Link **Geheimen Schlüssel aktualisieren**, um einen neuen TOTP zu generieren.
- Wenn Sie eine Authentifizierungs-App für mehrere Benutzerkonten verwenden, unterscheidet der Hostname des Benutzerkontos die TOTPs. In der Authentifikator-App können Sie den Hostnamen und den entsprechenden TOTP anzeigen.



5. (Optional) Wenn Sie E-Mail-OTP aktivieren möchten, wählen Sie **E-Mail-OTP aktivieren** (Optional), und gehen Sie dann wie folgt vor:
   a. Um die E-Mail-Einstellungen zu konfigurieren, klicken Sie auf die Schaltfläche **Konfigurieren**.

      Das Dialogfeld "E-Mail-Einstellungen" wird angezeigt.

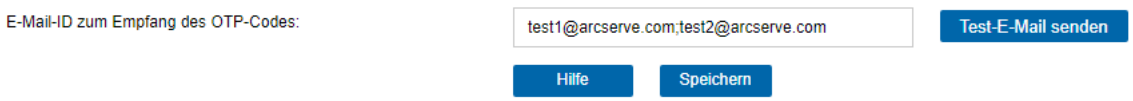


b. Führen Sie im Dialogfeld zur Tabellenauswahl die folgenden Schritte aus, und klicken Sie dann auf **OK**:

   - **E-Mail-Server:** Geben Sie die Adresse des E-Mail-Servers ein.
   - **Port:** Geben Sie die Portnummer für den E-Mail-Server ein.
   - Wenn der angegebene E-Mail-Server eine Authentifizierung erfordert, aktivieren Sie das Kontrollkästchen **Authentifizierung erforderlich**.
   - **Kontoname:** Geben Sie den Benutzernamen oder die E-Mail-Adresse des angegebenen E-Mail-Servers ein.
   - **Kennwort:** Geben Sie das zu authentifizierende Kennwort ein.
   - **Von:** Geben Sie nach Bedarf die E-Mail-Adresse des Absenders ein.
   - Wenn der angegebene E-Mail-Server den Befehl STARTLS-Protokoll erfordert, aktivieren Sie das Kontrollkästchen **STARTLS senden**.

c. Damit *E-Mail-ID den OTP-Code erhält*, geben Sie eine oder mehrere E-Mail-Adressen ein.

   Hinweis: Sie müssen eine E-Mail-Adresse angeben, um das OTP während der Anmeldung zu erhalten. Wenn Sie mehrere E-Mail-Adressen angeben möchten, trennen Sie sie durch ein Semikolon (;).



d. Um zu überprüfen, ob die konfigurierten E-Mail-Adressen OTP empfangen, klicken Sie auf **Test-E-Mail senden**.

6. Klicken Sie auf **Speichern**.

   Das Dialogfeld "Bestätigen" wird angezeigt.

   Hinweis: Das Bestätigungsdialogfeld wird angezeigt, um den Identitätsdienst nur neu zu starten, wenn Sie die E-Mail-Einstellungen konfigurieren, ändern oder entfernen.

7. Klicken Sie im Dialogfeld "Bestätigen" auf **Ja**, um den Identitätsdienst neu zu starten.

   Nachdem der Identitätsdienst neu gestartet wurde, aktualisieren Sie den Browser. Dies ist erforderlich, damit die E-Mail-Einstellungen angewendet werden.

Informationen zum Zurücksetzen von QR-Codes finden Sie unter Zurücksetzen von QR-Codes.

So setzen Sie den QR-Code zurück

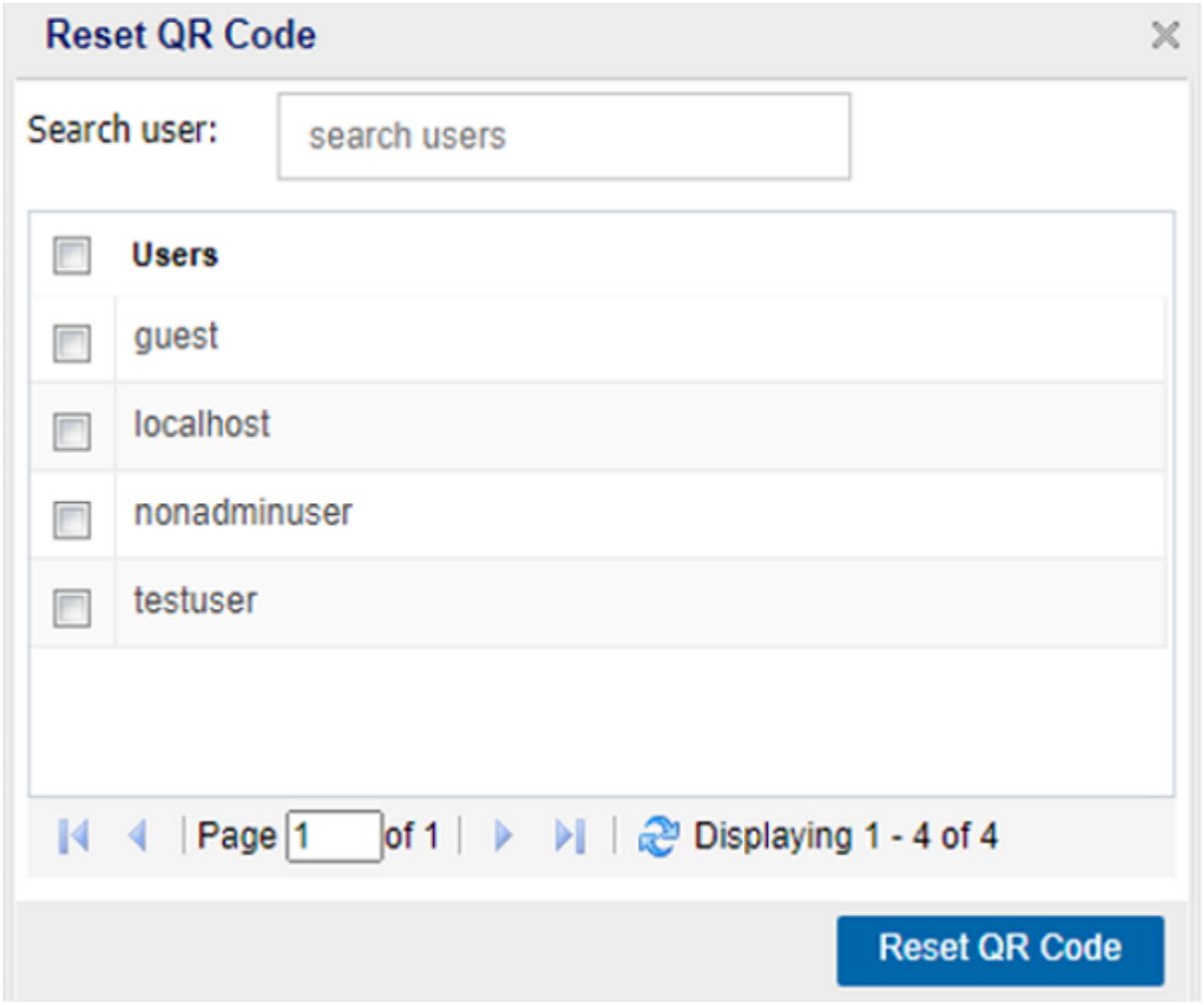
Dieser Abschnitt enthält Informationen zum Zurücksetzen des QR-Codes für Benutzer.

Hinweis: Ein Admin-Benutzer kann den QR-Code für alle Benutzer mit Ausnahme seines eigenen zurücksetzen.

Befolgen Sie diese Schritte:

1. Melden Sie sich mit Administrator-Anmeldeinformationen bei der Arcserve UDP-Konsole an.
2. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung**.
3. Klicken Sie für *QR-Code zurücksetzen* auf die Schaltfläche **QR-Code zurücksetzen**.

   Das Dialogfeld "QR-Code zurücksetzen" wird angezeigt.



4. **Wählen Sie im Dialogfeld "QR-Code zurücksetzen" aus der Liste der Benutzer die Benutzer aus, für die Sie den QR-Code zurücksetzen möchten, und klicken Sie dann auf QR-Code zurücksetzen**.

Hinweis: Nach dem Zurücksetzen des QR-Codes müssen die ausgewählten Benutzer bei der nächsten Anmeldung den QR-Code erneut nach einem neuen TOPT durchsuchen und sich erneut registrieren.

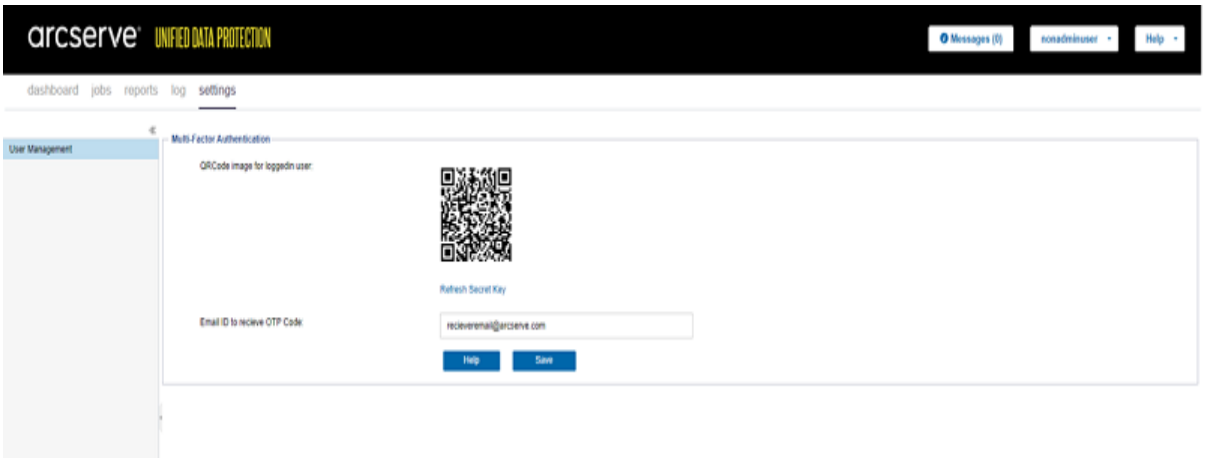
Konfigurieren der Multi-Faktor-Authentifizierung als Nicht-Administrator

Dieser Abschnitt enthält Informationen zum Konfigurieren der Multi-Faktor-Authentifizierungseinstellungen für das eigene Benutzerprofil.

Befolgen Sie diese Schritte:

1. Melden Sie sich mit Nicht-Administrator-Anmeldeinformationen bei der Arcserve UDP-Konsole an.

2. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung**.



Hinweis: Die Seite *Einstellungen> Benutzerverwaltung* ist nicht für Benutzer verfügbar, die nicht über die Berechtigung Benutzerverwaltung verfügen. Allerdings kann der Administrator diese Berechtigung allen Benutzern ohne Administratorrechte oder anderen Benutzern zuweisen. Weitere Informationen finden Sie unter Zuweisen einer vordefinierten Rolle.

3. Klicken Sie unter dem QR-Code-Bild auf den Link **Geheimschlüssel aktualisieren**, um einen neuen TOTP zu generieren.
4. Damit *E-Mail-ID den OTP-Code erhält*, geben Sie eine oder mehrere E-Mail-Adressen ein.

   Hinweis: Sie müssen eine E-Mail-Adresse angeben, um das OTP während der Anmeldung zu erhalten. Wenn Sie mehrere E-Mail-Adressen angeben möchten, trennen Sie sie durch ein Semikolon (;).

5. Klicken Sie auf **Speichern**.

   Die geänderten Einstellungen werden übernommen.

Hinzufügen von Benutzern, Löschen von Benutzern und Ändern des Kennworts

Über die Windows-Benutzersteuerung können Sie lokale Benutzer oder Domänenbenutzer hinzufügen oder löschen. Die Benutzerverwaltungsliste in der Identitätsdienstkonsole wird automatisch aktualisiert.

Verwenden Sie die Windows-Benutzersteuerung, um das Benutzerkennwort zu ändern. Wenn Sie das Kennwort eines Benutzers aktualisieren, muss der Benutzer sich mit dem aktuellen Kennwort an der Identitätsdienstkonsole anmelden. Die Rolle des Benutzers wird beibehalten.

Konfigurieren der Benutzerverwaltung

Sie können anderen Benutzern verschiedene Rollen zuweisen und verschiedene Rollen mit unterschiedlichen Berechtigungen ausstatten. Durch das Konfigurieren der Benutzerverwaltung können Sie die folgenden Optionen ausführen:

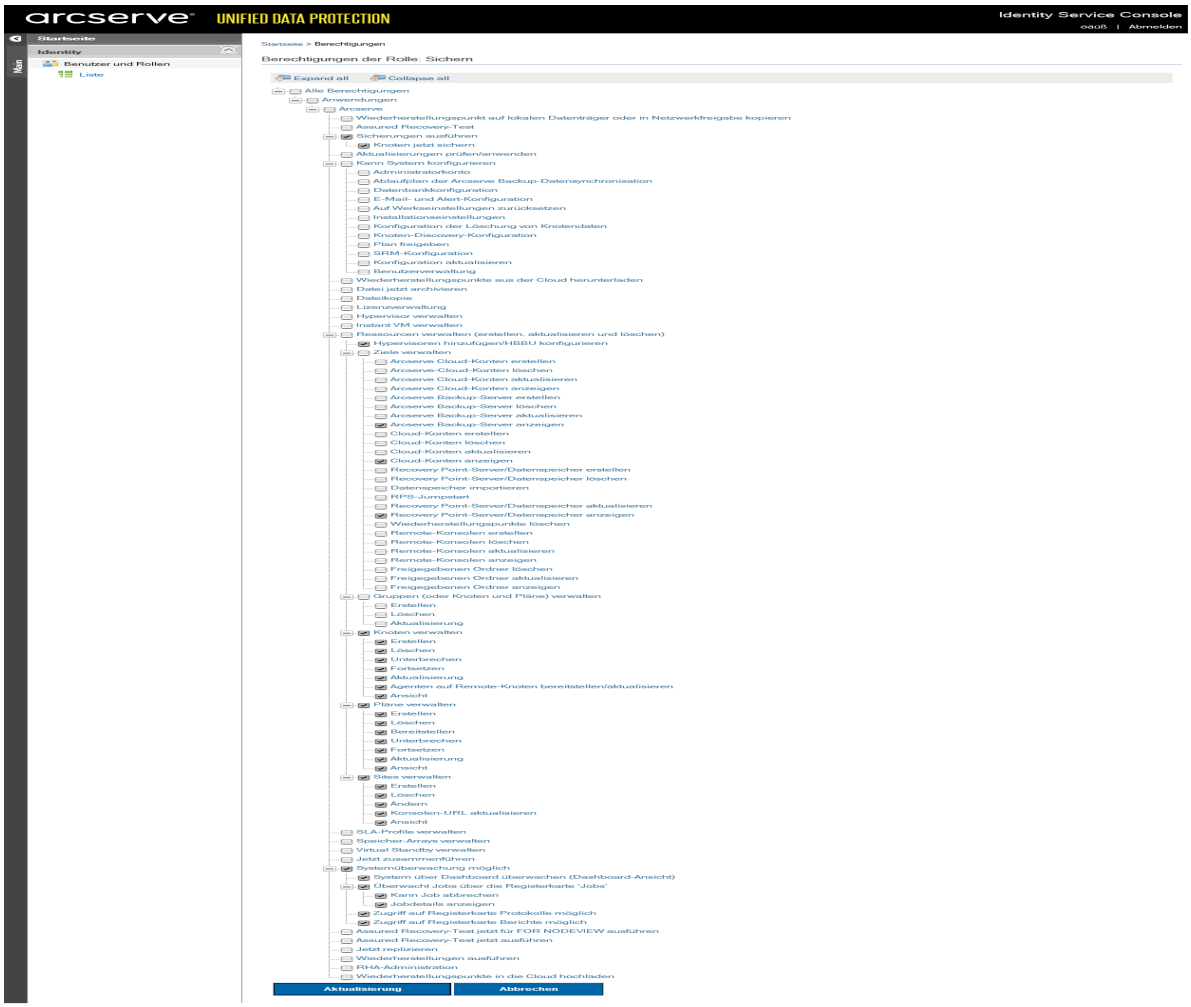
- Vordefinierte Rollen
- Zuweisen einer vordefinierten Rolle
- Anzeigen und Abbrechen einer Rolle
- Neue Rolle hinzufügen
- Suchen von Benutzern und Rollen

Vordefinierte Rollen

Die Funktion einer vordefinierten Rolle ist die Bereitstellung einer Referenz für eine typische Rollendefinition. Jeder Rolle ist ein vordefinierter Satz von Berechtigungen zugewiesen.

Für die Administratorrolle werden alle Berechtigungsoptionen ausgewählt. Benutzer mit Administratorrolle können auf alle Funktionen von Arcserve UDP zugreifen.

Klicken Sie auf die Berechtigung für die Sicherungsrolle, und die folgenden ausgewählten Berechtigungen werden vordefiniert:


arcserve
UNIFIED DATA PROTECTION
Identity Service Console
aaa5 | Abmelden
Startseite
Identity
Benutzer und Rollen
Liste
Main
Startseite > Berechtigungen
Berechtigungen der Rolle: Sichern
Expand all
Collapse all
Alle Berechtigungen
Anwendungen
Arcserve
Wiederherstellungspunkt auf lokalen Datenträger oder in Netzwerkfreigabe kopieren
Assured Recovery-Test
Sicherungen ausführen
Knoten jetzt sichern
Aktualisierungen prüfen/anwenden
Kann System konfigurieren
Administratorkonto
Ablaufplan der Arcserve Backup-Datensynchronisation
Datenbankkonfiguration
E-Mail- und Alert-Konfiguration
Auf Werkseinstellungen zurücksetzen
Installationseinstellungen
Konfiguration der Löschung von Knotendaten
Knoten-Discovery-Konfiguration
Plan freigeben
SRM-Konfiguration
Konfiguration aktualisieren
Benutzerverwaltung
Wiederherstellungspunkte aus der Cloud herunterladen
Datei jetzt archivieren
Dateikopie
Lizenzverwaltung
Hypervisor verwalten
Instant VM verwalten
Ressourcen verwalten (erstellen, aktualisieren und löschen)
Hypervisoren hinzufügen/HBBU konfigurieren
Ziele verwalten
Arcserve Cloud-Konten erstellen
Arcserve-Cloud-Konten löschen
Arcserve Cloud-Konten aktualisieren
Arcserve Cloud-Konten anzeigen
Arcserve Backup-Server erstellen
Arcserve Backup-Server löschen
Arcserve Backup-Server aktualisieren
Arcserve Backup-Server anzeigen
Cloud-Konten erstellen
Cloud-Konten löschen
Cloud-Konten aktualisieren
Cloud-Konten anzeigen
Recovery Point-Server/Datenspeicher erstellen
Recovery Point-Server/Datenspeicher löschen
Datenspeicher importieren
RPS-Jumpstart
Recovery Point-Server/Datenspeicher aktualisieren
Recovery Point-Server/Datenspeicher anzeigen
Wiederherstellungspunkte löschen
Remote-Konsolen erstellen
Remote-Konsolen löschen
Remote-Konsolen aktualisieren
Remote-Konsolen anzeigen
Freigegebenen Ordner löschen
Freigegebenen Ordner aktualisieren
Freigegebenen Ordner anzeigen
Gruppen (oder Knoten und Pläne) verwalten
Erstellen
Löschen
Aktualisierung
Knoten verwalten
Erstellen
Löschen
Unterbrechen
Fortsetzen
Aktualisierung
Agenten auf Remote-Knoten bereitstellen/aktualisieren
Ansicht
Pläne verwalten
Erstellen
Löschen
Bereitstellen
Unterbrechen
Fortsetzen
Aktualisierung
Ansicht
Sites verwalten
Erstellen
Löschen
Ändern
Konsolen-URL aktualisieren
Ansicht
SLA-Profile verwalten
Speicher-Arrays verwalten
Virtual Standby verwalten
Jetzt zusammenführen
Systemüberwachung möglich
System über Dashboard überwachen (Dashboard-Ansicht)
Überwacht Jobs über die Registerkarte 'Jobs'
Kann Job abbrechen
Jobdetails anzeigen
Zugriff auf Registerkarte Protokolle möglich
Zugriff auf Registerkarte Berichte möglich
Assured Recovery-Test jetzt für FOR NODEVIEW ausführen
Assured Recovery-Test jetzt ausführen
Jetzt replizieren
Wiederherstellungen ausführen
RHA-Administration
Wiederherstellungspunkte in die Cloud hochladen
Aktualisierung
Abbrechen

Für die Sicherungsrolle sind folgende Berechtigungen vordefiniert:

- Sicherung durchführen
- Ziel anzeigen
- Knoten/Pläne/Standorte verwalten
- Systemfunktion überwachen

Die Administratorrolle kann ganz flexibel die ausgewählten Berechtigungen löschen oder neue Berechtigungen auswählen. Wenn Sie auf "Aktualisieren" klicken, wird die neu hinzugefügte Berechtigung zur Standardberechtigung für die Sicherungsrolle. Sie können die Rolle auch umbenennen.

Für die Überwachungsrolle sind der Dashboard-Job-Monitor und die Protokollierungs-/Berichterstellungsberechtigung vorausgewählt.

Für die Wiederherstellungsrolle sind die folgenden Berechtigungen vorausgewählt:

- Instant VM verwalten
- Ziel anzeigen
- Knoten anzeigen
- Plan anzeigen
- Virtual Standby verwalten
- Jobs überwachen
- Auf Protokolle zugreifen
- Wiederherstellung durchführen

Wenn Sie die Wiederherstellungsrolle einem Benutzer zuweisen, kann sich der Benutzer anmelden und verfügt dann über die entsprechenden Berechtigungen. Wenn einem Benutzer zum Beispiel die Wiederherstellungsrolle zugewiesen ist und ein Knoten erfolgreich gesichert wurde, kann der Benutzer eine Instant VM erstellen oder wiederherstellen und dann mit der nächsten Aktivität fortfahren.

Für die Rolle _Admin hat die Berechtigung der RHA-Administration Zugriff auf die High Availability-Funktion.

Zuweisen einer vordefinierten Rolle

Wenn ein Superadministrator einem Benutzer eine Rolle zuweist, kann nur dieser Benutzer sich an der Konsole anmelden. Mit der Schaltfläche "Benutzer" wird die vollständige Benutzerliste einschließlich der Domänenbenutzer und lokalen Benutzer angezeigt.

Sie können lokalen Benutzern oder Domänenbenutzern die verfügbaren (vordefinierten) Rollen oder selbst definierte Rollen zuweisen.

Hinweis: Nur ein Super-Administrator (ein Administrator, der Arcserve UDP installiert) kann anderen Benutzern die Administratorrolle zuweisen. Administratoren können anderen Benutzern nur Nicht-Administrator-Rollen zuweisen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf **Benutzer und Rollen** im Fensterbereich **Konfigurieren**.

   Auf der Seite "Benutzerverwaltung" werden Benutzer und Rollen angezeigt.

2. Klicken Sie auf der Seite "Benutzerverwaltung" auf **Benutzer**.

   Eine Liste der Benutzer wird angezeigt.

3. Klicken Sie auf **Rolle zuweisen** für einen Benutzer.

   Die Seite **Rollenliste des Benutzers** wird geöffnet.

4. Wählen Sie eine oder mehrere Rollen aus, und klicken Sie auf **Aktualisieren**.

   Die Rolle für den Benutzer wird erfolgreich aktualisiert.

5. Klicken Sie auf **Fertig stellen**, um zum vorherigen Bildschirm zurückzukehren.

   Sie haben einem Benutzer erfolgreich eine Rolle zugewiesen.

Anzeigen und Abbrechen einer Rolle

Sie können die aktuelle Rolle anzeigen, die einem Benutzer zugewiesen wurde. Sie können die Zuweisung einer Rolle aufheben, indem Sie das Kontrollkästchen für diese Rolle deaktivieren.

Gehen Sie wie folgt vor:

1. Klicken Sie auf **Benutzer und Rollen** im Fensterbereich **Konfigurieren**.

   Auf der Seite **Benutzerverwaltung** werden Benutzer und Rollen angezeigt.

2. Klicken Sie auf der Seite "Benutzerverwaltung" auf "Benutzer".

   Eine Liste der Benutzer wird angezeigt.

3. Deaktivieren Sie das Kontrollkästchen, um die Zuweisung einer Rolle aufzuheben, und klicken Sie auf **Aktualisieren**.

   Die Rollen werden vom Benutzer entfernt.

   Hinweis: Ein Benutzer kann sich nicht in der Arcserve UDP Konsole anmelden, wenn ihm keine Rolle zugeteilt wurde.

4. Klicken Sie auf **Fertig stellen**, um zu vorherigen Seite zurückzukehren.

   Sie haben erfolgreich eine Rolle angezeigt und abgebrochen.

Hinzufügen einer neuen Rolle

Sie können eine benutzerdefinierte Rolle erstellen und Berechtigungen für diese Rolle auswählen.

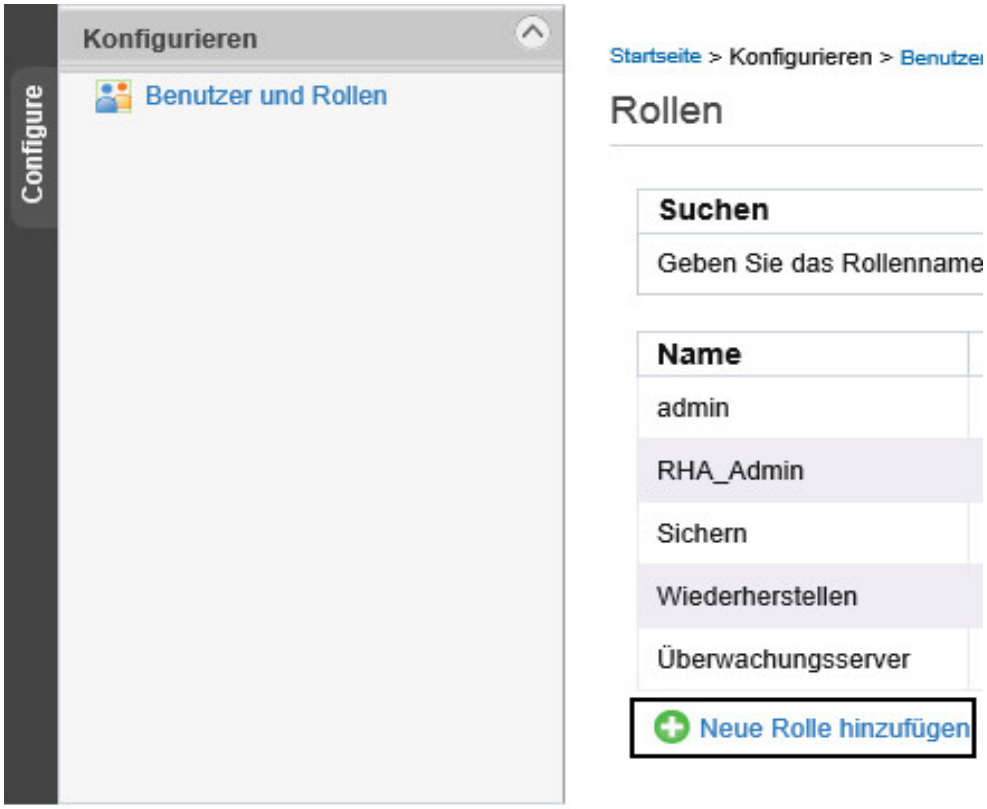
Gehen Sie wie folgt vor:

1. Klicken Sie auf **Benutzer und Rollen** auf der Seite **Konfigurieren**.

   Es werden Benutzer und Rollen auf der Seite **Benutzerverwaltung** angezeigt.

2. Klicken Sie auf **Rollen**.

   Die Seite **Rollen** wird angezeigt, und es werden alle verfügbaren Rollen aufgelistet.



3. Klicken Sie auf **Neue Rolle hinzufügen**.

   Die Seite **Rolle hinzufügen** wird geöffnet.

4. Geben Sie einen Rollennamen ein, und klicken Sie auf **Weiter**.

   Hinweis: Verwenden Sie keine Sonderzeichen wie **~!@#$%^&*** und andere im Namen einer Rolle.

5. Aktivieren Sie die erforderlichen Berechtigungskontrollkästchen, und klicken Sie auf **Weiter**.

6. Wählen Sie die Benutzer für diese Rolle aus.

7. Klicken Sie auf **Fertig stellen**.

   Eine neue Rolle und zu dieser Rolle zugewiesene Berechtigungen werden erstellt.

   Hinweis: Einige Berechtigungen funktionieren nur, wenn die damit verbundenen Berechtigungen auch ausgewählt werden. Um beispielsweise eine Rolle für die Verwaltung des virtuellen Standby-Modus zu konfigurieren, wählen Sie die Berechtigung zum Verwalten des virtuellen Standby-Modus aus und wählen Sie "Berechtigung zum Anzeigen des Knotens" aus, um sicherzustellen, dass die Rolle normal funktionieren kann.

Suchen von Benutzern und Rollen

Sie können Benutzer und Rollen filtern, um den benötigten Benutzer oder die benötigte Rolle zu finden. Geben Sie * ein, um nach allen Benutzern und Rollen zu suchen.

Um nach einer Rolle zu suchen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **Benutzer und Rollen** auf der Seite **Konfigurieren**.

   Es werden Benutzer und Rollen auf der Seite **Benutzerverwaltung** angezeigt.

2. Klicken Sie auf **Rollen**.

   Die Seite **Rollen** wird geöffnet.

3. Geben Sie das Rollennamenmuster an, und klicken Sie auf **Suchen**.

   Das gefilterte Ergebnis wird angezeigt.

Um nach einem Benutzer zu suchen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **Benutzer und Rollen** auf der Seite **Konfigurieren**.

   Es werden Benutzer und Rollen auf der Seite **Benutzerverwaltung** angezeigt.

2. Klicken Sie auf **Benutzer**.

   Die Seite **Benutzer** wird geöffnet.

3. Geben Sie das Benutzernamenmuster an, und klicken Sie auf **Suchen**.

   Das gefilterte Ergebnis wird angezeigt.

Integrieren von Arcserve UDP in Active Directory

Arcserve UDP unterstützt die Active Directory (AD)-Integration mithilfe von Windows und Active Directory-Gruppen.

Dieser Abschnitt enthält folgende Themen:

- So integrieren Sie Arcserve UDP 8.0 in Active Directory unter Verwendung von Windows-Gruppen
- So integrieren Sie Arcserve UDP 8.0 in Active Directory unter Verwendung von Active Directory-Gruppen

So integrieren Sie Arcserve UDP 8.0 in Active Directory unter Verwendung von Windows-Gruppen

Die vorhandene Funktion für rollenbasierte Verwaltung (UDP-RBA) ermöglicht die Verwaltung von UDP-Berechtigungen auf Basis von Active Directory (AD)-Gruppen. Die vorherige Version von UDP-RBA hat nur einzelne AD-Benutzerkonten unterstützt. Jetzt können auch AD-Gruppen als RBA-Rollen fungieren.

Der schreibgeschützte sekundäre LDAP-Benutzerspeicher lässt sich durch Ausführen eines Hilfsprogramms automatisch hinzufügen.

Gehen Sie wie folgt vor:

1. Starten Sie die Befehlszeile, und führen Sie *C:\Program Files\Arcserve\Unified Daten Protection\Management\BIN* aus.
2. Führen Sie das Dienstprogramm *DomainAuthTool.bat* aus.

   Die folgenden Informationen werden auf dem Bildschirm angezeigt:

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>DomainAuti
log4j:WARN No appenders could be found for logger (com.ca.arcserve.edge.ap
log4j:WARN Please initialize the log4j system properly.


Nutzung: DomainAuthTool.bat <Vorgang> <Voraussetzungen> [Optionen]

        Vorgang (Kleinschreibung):
                Create          Erstellen oder Aktualisieren der Einstellu

                Remove          Entfernen der Einstellung des schreibgesch

        Erforderliche Parameter (Groß-/Kleinschreibung beachten):
                -Username:<username>    Das Format des Administrator- oder
äne\Benutzername oder Benutzername@Domäne.com.
                -Password:<password>    Administratorkennwort von Arcserve

        Optionaler Parameter (Groß-/Kleinschreibung beachten):
                -DCName:<DC name>       Name oder IP des Domänen-Controlle
dern.
                -Protocol:<protocol>    Protokoll für AD, LDAP oder LDAPS
                -Port:<port>            Port für AD (Standard: 389). Diese

Beispiele:
        DomainAuthTool.bat Create -Username:administrator -Password:1234
        DomainAuthTool.bat Create -Username:administrator -Password:1234 -
        DomainAuthTool.bat Remove -Username:administrator -Password:1234

C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>
```

3. Erstellen Sie einen schreibgeschützten sekundären LDAP-Benutzerspeicher, und ändern Sie gleichzeitig die optionalen Parameter. Beispiel: Sehen Sie sich den gelb markierten Befehl im Screenshot unten an.

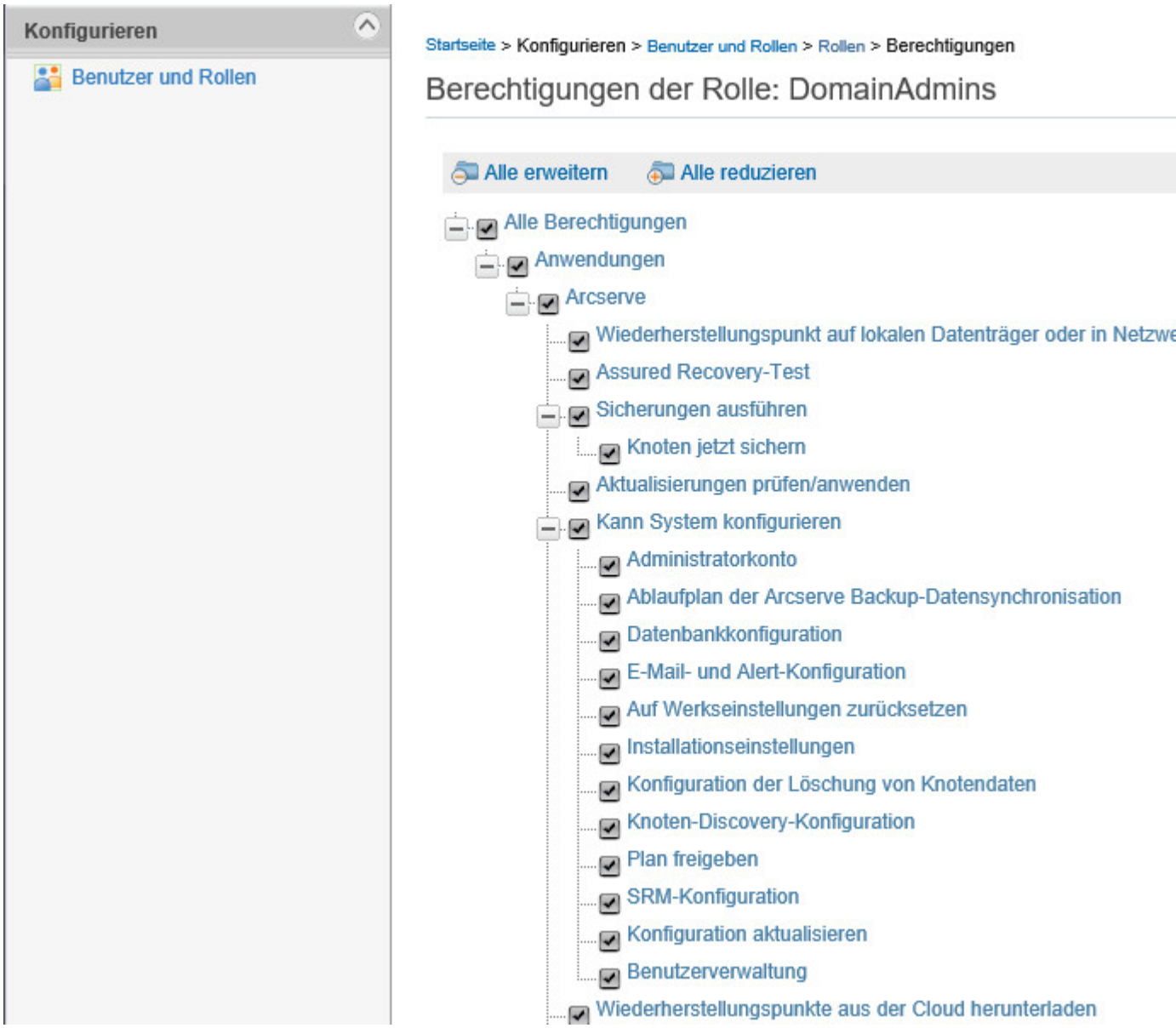
```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>DomainAuthTool.bat Create -Username:grmarchive16\administrator -
Password:Arcserve
log4j:WARN No appenders could be found for logger (com.ca.arcserve.edge.app.base.util.CommonUtil).
log4j:WARN Please initialize the log4j system properly.
Um den schreibgeschützten LDAP-Benutzerspeicher zu konfigurieren, müssen Sie den Domänenbenutzer und die Beziehung zwischen Domän
enbenutzer und Rolle löschen. Möchten Sie fortfahren? (J/N) y
Der schreibgeschützte LDAP-Benutzerspeicher wurde erfolgreich erstellt.
ConsoleConfiguration.xml erfolgreich aktualisiert.
Domänenbenutzer und Beziehung zwischen Domänenbenutzer und Rolle wird gelöscht...
Der Domänenbenutzer und die Beziehung zwischen Domänenbenutzer und Rolle wurden erfolgreich gelöscht.

C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>
```

4. Weisen Sie die lokale Benutzerrolle zu.

Weitere Informationen finden Sie unter Zuweisen einer vordefinierten Rolle.

5. Um den schreibgeschützten LDAP-Domänenbenutzern eine Berechtigung hinzuzufügen, führen Sie die folgenden Schritte durch:
   a. Treten Sie der Gruppe über den Domänencontroller bei.
   b. Fügen Sie die Arcserve UDP-Berechtigung für die entsprechende Gruppe hinzu, wie im folgenden Screenshot gezeigt.

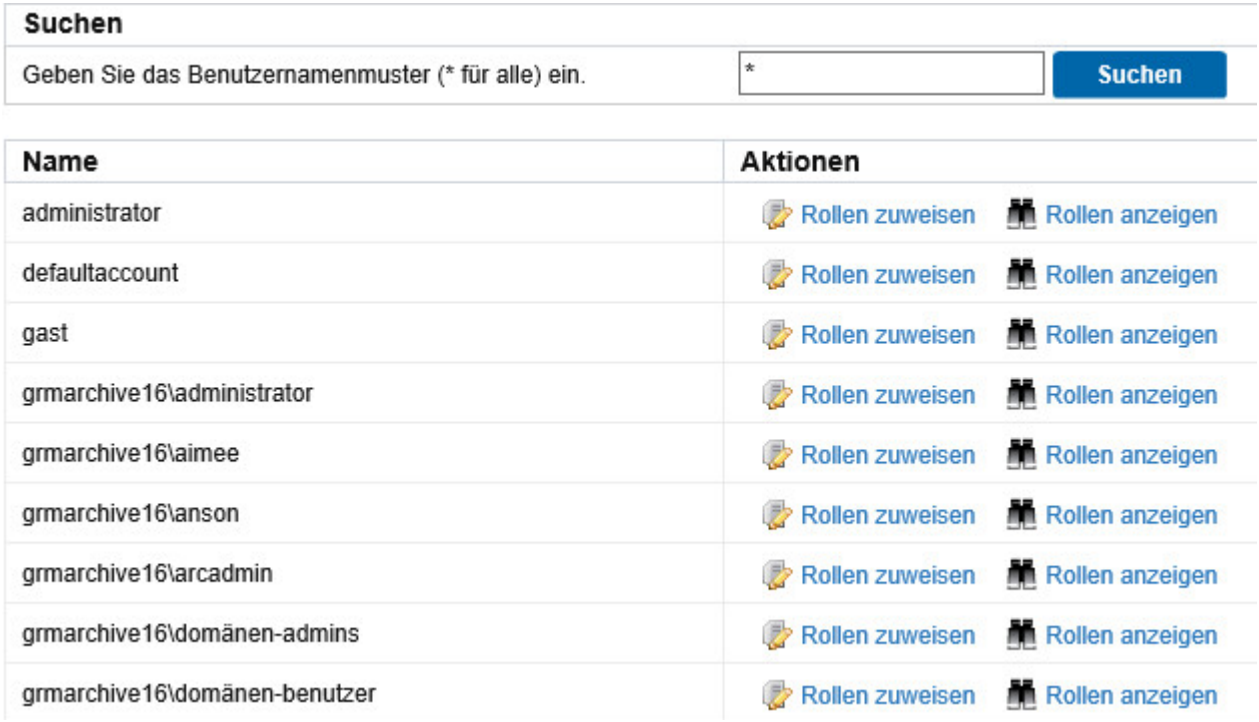
   Hinweis: Das direkte Zuweisen der lokalen Standardrolle zu schreibgeschützten Domänenbenutzern ist nicht möglich.



Der Benutzer kann sich nun bei der Arcserve UDP-Konsole mit einer speziellen Berechtigung anmelden.

6. (Optional) Entfernen Sie den LDAP-Benutzerspeicher mit dem Dienstprogramm.

Führen Sie das Dienstprogramm aus, um den LDAP-Benutzerspeicher zu entfernen. Starten Sie dann den Verwaltungsdienst neu. Der vorherige Domänenbenutzer wird wie unten angezeigt aufgelistet.



So integrieren Sie Arcserve UDP 8.0 in Active Directory unter Verwendung von Active Directory-Gruppen

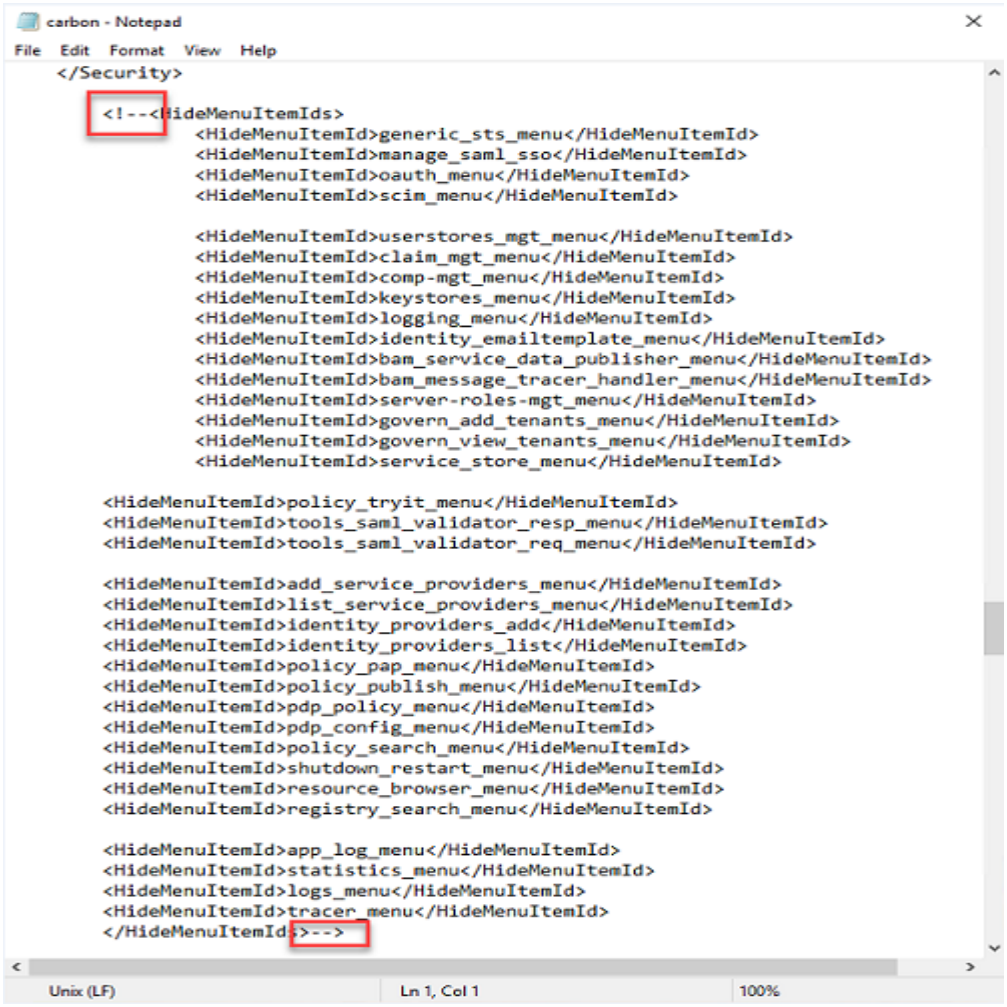
Die rollenbasierte Verwaltung von Arcserve UDP 8.0 ermöglicht Berechtigungen auf Benutzerebene, wenn die Azure Active (AD)-Funktion nicht standardmäßig aktiviert ist. Die WSO2 Carbon-Plattform in Arcserve UDP 8.0 unterstützt jedoch keine AD-Gruppen, die über sekundären Benutzerspeicher verfügen. Sie können die Erweiterung für Arcserve UDP 8.0 aktivieren, mit der die AD-Gruppe als Arcserve UDP-Rollen konfiguriert wird und die Berechtigungen für die Mitglieder der AD-Gruppe automatisch zugewiesen werden.

Gehen Sie wie folgt vor:

1. Navigieren Sie zum folgenden Installationspfad von Arcserve UDP, und öffnen Sie die Datei *carbon.xml*:

   …\Programme\Arcserve\Unified Data Protection\Management\IdentityServer\repository\conf\carbon.xml

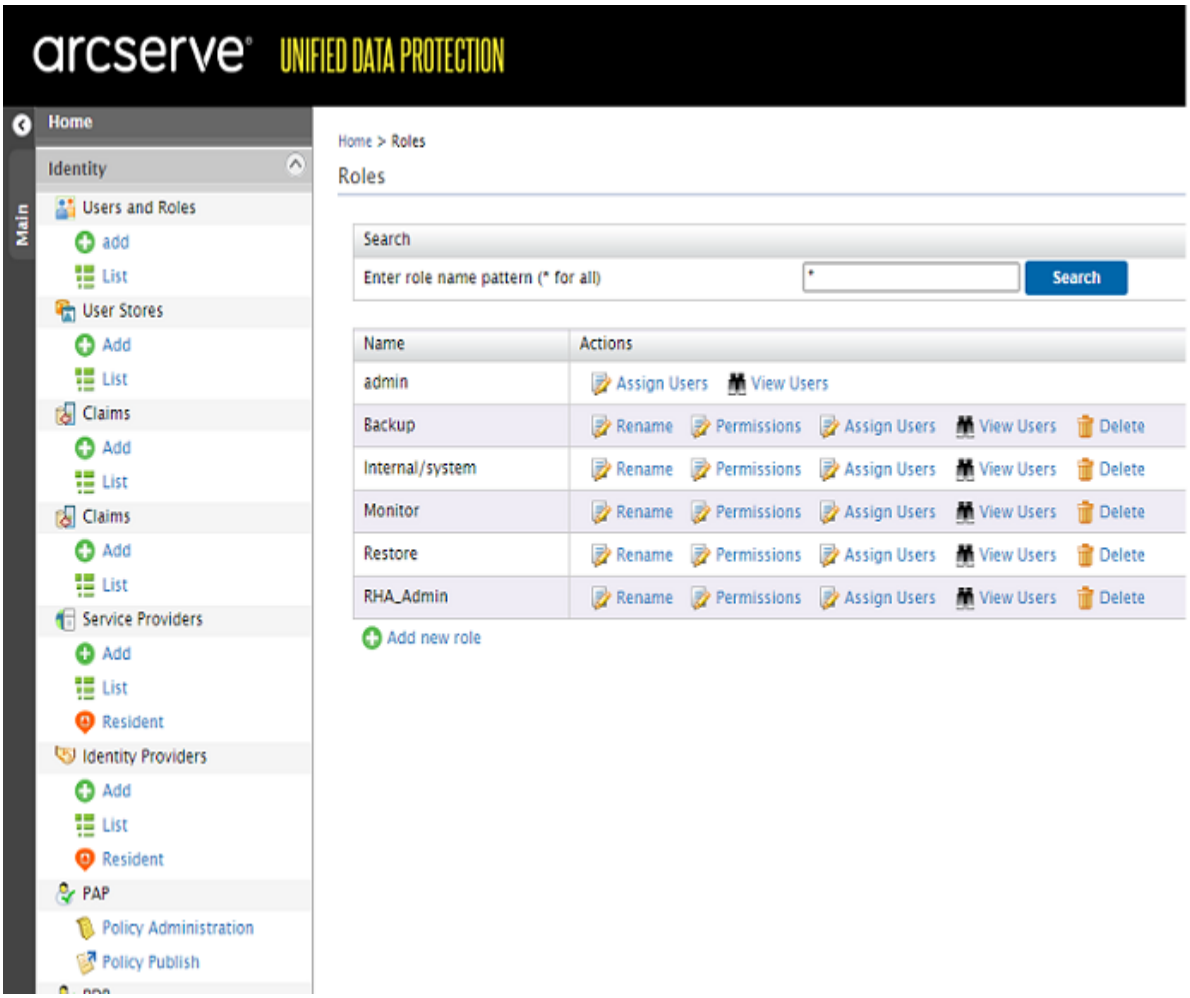
2. Deaktivieren Sie in der Datei *carbon.xml* die Inhalte von HideMenuItemIds mithilfe von <!-- und --> wie im folgenden Screenshot dargestellt.



3. Speichern Sie die Datei *carbon.xml*, und starten Sie den Arcserve UDP-Verwaltungsdienst neu.
4. Öffnen Sie die Benutzerverwaltungskonsole über den folgenden Link:

   https://localhost:8015/carbon

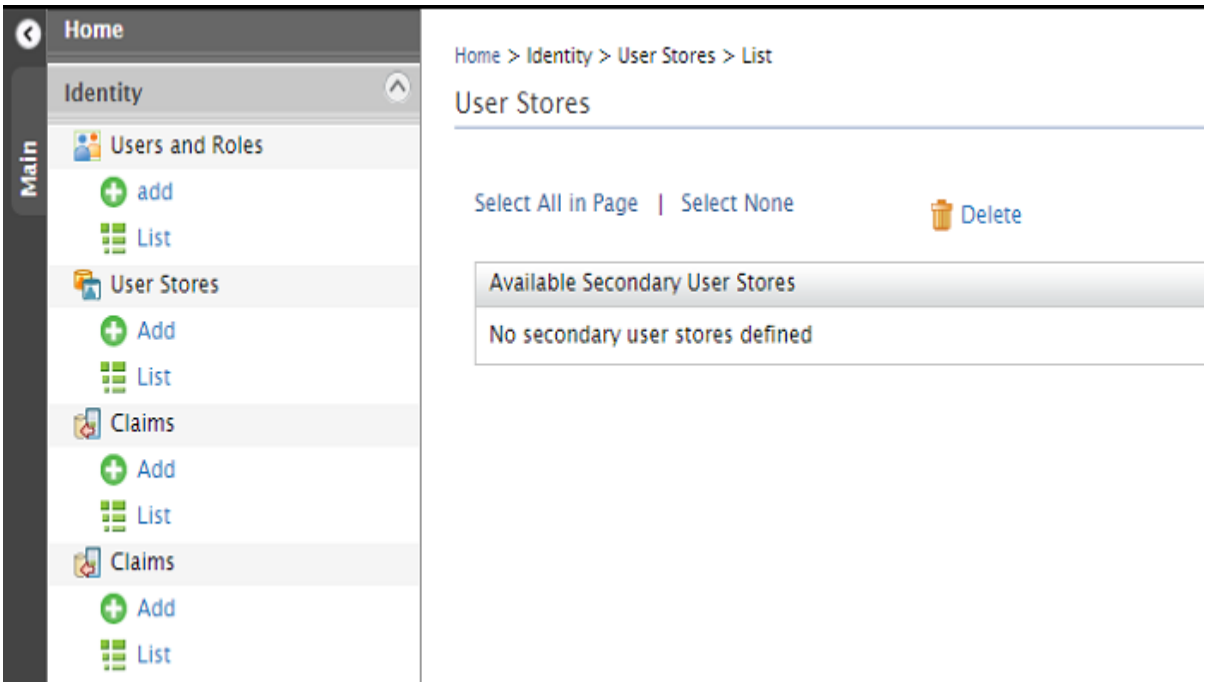
   Die Seite *Arcserve UDP – rollenbasierte Zugriffssteuerung – Verwaltung Home* wird angezeigt.



5. Klicken Sie im linken Bereich auf die Option **Benutzerspeicherverwaltung**.

   Die Seite **Benutzerspeicherverwaltung** wird angezeigt.

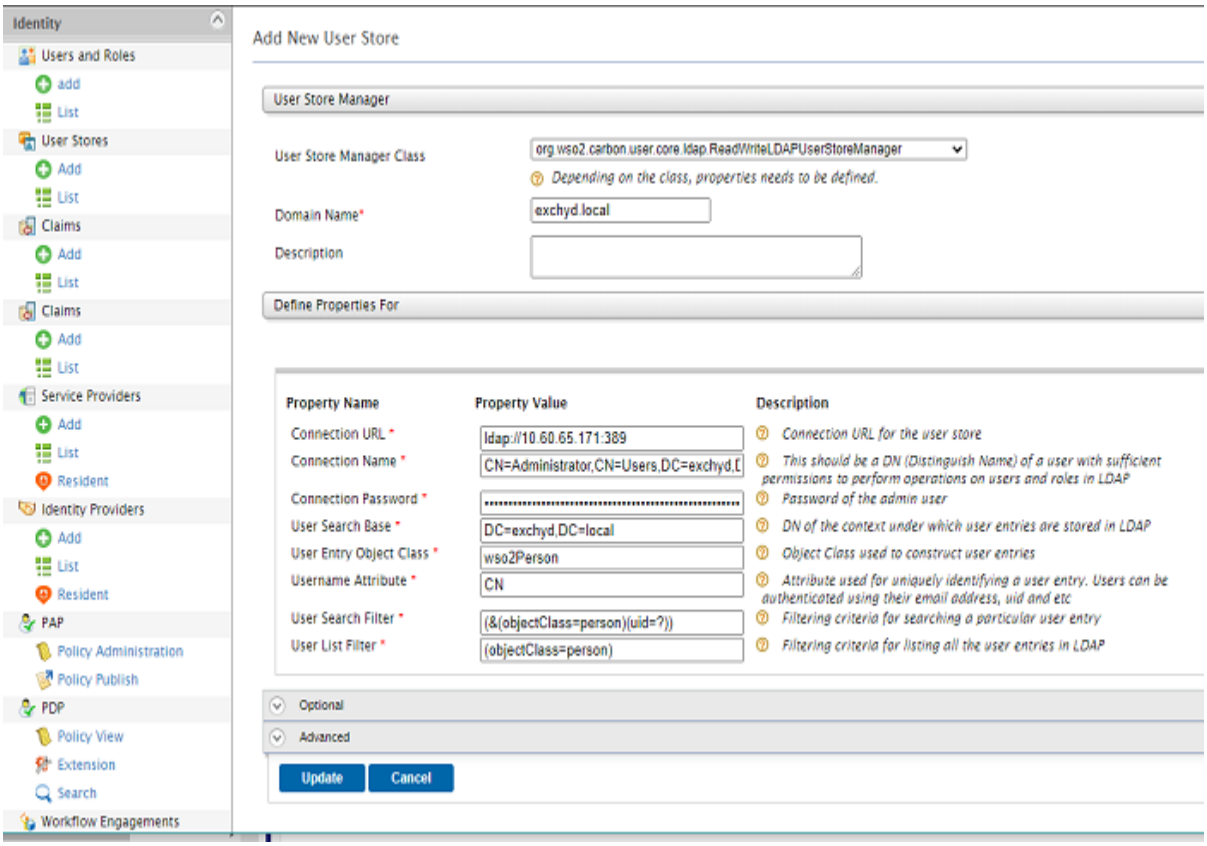
6. Klicken Sie auf **Sekundären Benutzerspeicher hinzufügen**.



Die Seite **Benutzerspeicher-Manager** wird angezeigt.

7. Wählen Sie die benötigte Option **Benutzerspeicher-Manager-Klasse** aus der Drop-down-Liste aus, und geben Sie den Domänennamen in das Feld **Domänenname** ein.
8. Geben Sie bei Bedarf die Details für die Felder unter **Eigenschaften definieren für** und **Optional** ein.

   Im folgenden Screenshot finden Sie ein Beispiel für die Seite "Benutzerspeicher-Manager" nach Eingabe der Informationen.

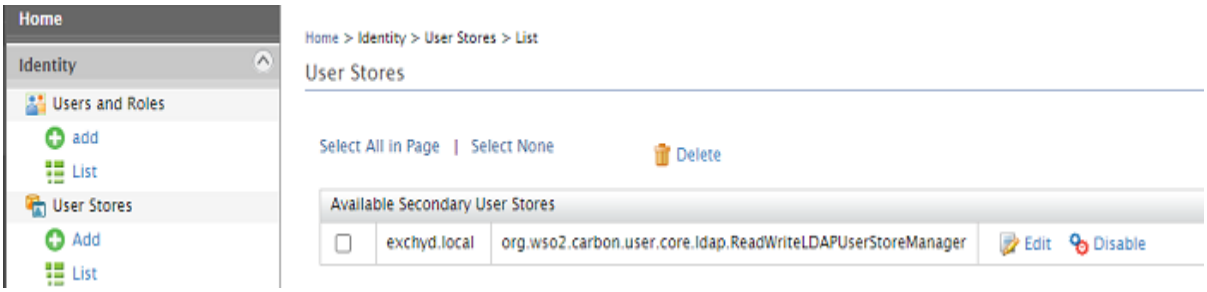


9. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **UDP-Benutzerverwaltung** wird angezeigt.

10. Klicken Sie auf **OK**.

    Die Seite "Benutzerspeicherverwaltung" wird angezeigt. Hier wird der hinzugefügte sekundäre Benutzerspeicher angezeigt.



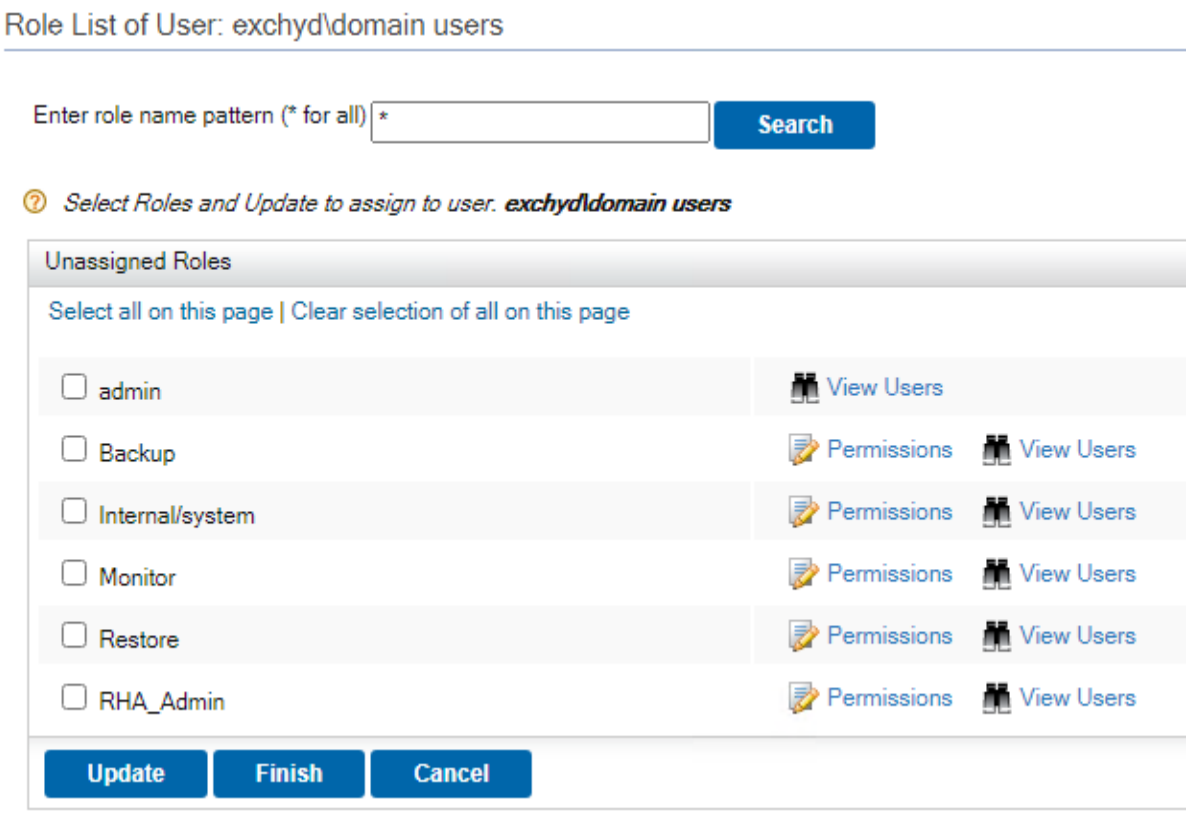
Hinweis: Wenn kein sekundärer Benutzerspeicher angezeigt wird, aktualisieren Sie den Browser.

11. (Optional) Klicken Sie im linken Bereich auf die Option **Benutzer und Rollen**, um die Liste der Benutzer und Rollen anzuzeigen.

    Hinweis: Sie müssen die Rollen in der Domäne mithilfe von AD definieren.

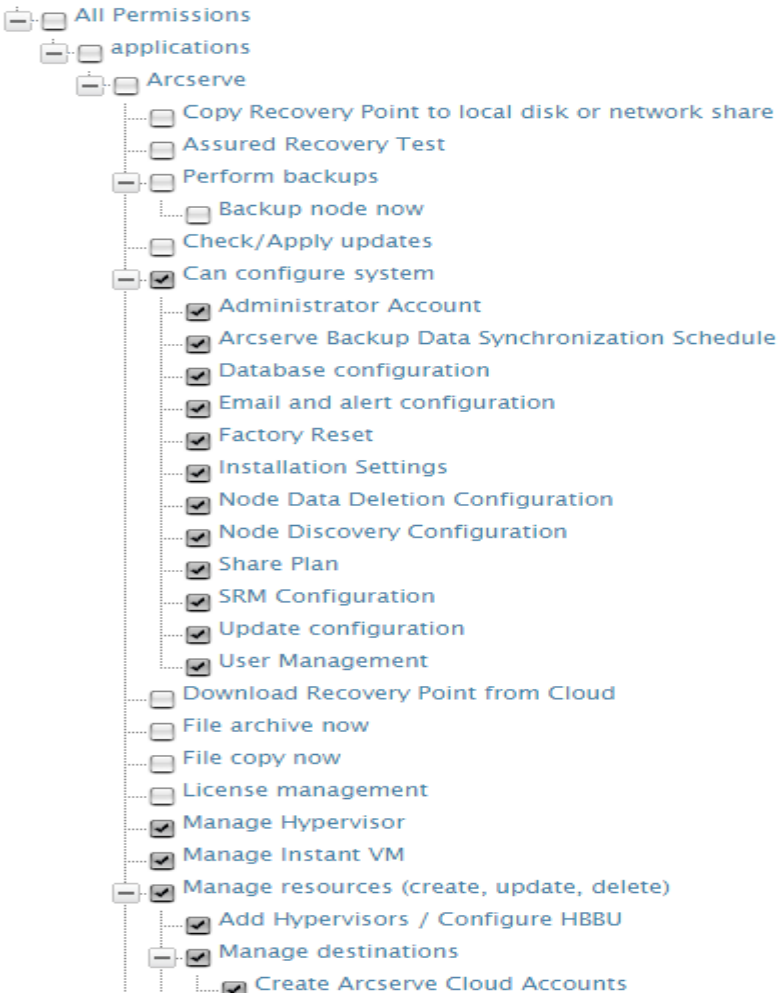
12. Gehen Sie nun wie folgt vor, um die UDP-Rollenberechtigungen hinzuzufügen:
    a. Wählen Sie einen AD-Benutzer oder eine AD -Gruppe aus.
    b. Weisen Sie eine Rolle aus der Liste der verfügbaren Rollen zu.
    c. Klicken Sie auf **Rolle anzeigen**.

       Die Seite **Rollenliste des Benutzers** wird angezeigt.



    d. Klicken Sie auf **Berechtigungen**.

       Die Liste der Berechtigungen wird angezeigt.



e. Wählen Sie nach Bedarf die Berechtigungen aus.

Nun kann sich der sekundäre Benutzer mit den zugewiesenen Berechtigungen bei der Arcserve UDP-Konsole anmelden.

Zugreifen auf Arcserve UDP mithilfe der integrierten Windows-Authentifizierung

Arcserve UDP-Benutzer können sich jetzt auch über die integrierte Windows-Authentifizierung (IWA) anmelden. IWA macht die browserbasierte Anmeldung einfacher. Wurde ein Benutzer unter Windows einmal authentifiziert, erlaubt es IWA dem Webbrowser, die Anmeldeinformationen des Benutzers zu speichern. Sie müssen dann im Browser nur die URL der geschützten Webanwendung eingeben. Browser und Server authentifizieren und melden den Benutzer automatisch an.

Hinweis: Die Arcserve UDP-Konsole unterstützt keine IWA, wenn die Datenbank-Konsolenverbindung den Windows-Authentifizierungsmodus verwendet. Um dieses Problem zu umgehen, lesen Sie die Tipps zur Fehlerbehebung unter dem Link.

Mit der Einführung von IWA können Sie jetzt dieselbe Funktion für den Zugriff auf Arcserve UDP verwenden.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Anmeldeseite der Arcserve UDP-Konsole.

   Der IWA-Link wird auf der Anmeldeseite angezeigt.

2. Klicken Sie auf den Link: **Anmeldung mit den aktuellen Windows-Anmeldeinformationen (IWA)**.

   Sie werden auf die Startseite geführt.

   Um Probleme zu beheben, siehe Problembehandlung.

Fehlerbehebung für die integrierte Windows-Authentifizierung (IWA)

Falls der IWA-Link die Konsolenseite nicht öffnet, können Sie die folgenden Schritte zur Fehlerbehebung durchführen:

1. Überprüfen Sie, ob Sie IWA auf Ihrem lokalen Rechner verwenden und nicht auf einem Remote-Rechner.
2. Wenn Sie nach einem Klick auf den IWA-Link einen weißen Bildschirm sehen, überprüfen Sie, ob dem Benutzer in der Konsole für die rollenbasierte Verwaltung die entsprechende Rolle zugewiesen ist.

   Hinweis: Wenn die Datenbank-Konsolenverbindung den Windows-Authentifizierungsmodus verwendet, siehe den Link.
3. Konfigurieren Sie anhand der folgenden Schritte, wenn während der IWA-Anmeldung mit Firefox Probleme auftreten, die Konsolen-URL zu öffnen.

   Gehen Sie wie folgt vor:

   a. Geben Sie in die Adressleiste des Browsers "about:config" ein.

   b. Klicken Sie auf **Ich werde vorsichtig sein, versprochen!**, um fortzufahren und zur Seite "about:config" zu gelangen.

   c. Legen Sie Werte für die folgenden Optionen fest, sodass der Browser der ProxySG-Appliance vertraut und die Authentifizierung aushandelt:

      network.automatic-ntlm-auth.trusted-uris, network.negotiate.auth.delegation-uris, network.negotiate-auth.trusted-uris

      Führen Sie für jede Option die folgenden Schritte aus:

      - Suchen Sie die Option, für die Sie eine Einstellung vornehmen möchten, indem Sie scrollen oder den Namen der Option ins das Feld "Filter" eingeben.
      - Doppelklicken Sie auf die Option, um das Dialogfeld "Zeichenfolgenwert eingeben" zu öffnen.
      - Geben Sie dir virtuelle URL (für transparente Bereitstellungen) ein.

        Wenn Sie mehrere ProxySG-Appliances haben, die Anmeldeinformationen für die Authentifizierung verlangen, trennen Sie die Eingaben durch Kommas. Angenommen, Ihre geöffnete URL

für die Konsole ist "https://localhost:8015", dann können Sie als Zeichenfolgenwert "localhost" eingeben. Wenn die URL " https://10.57.60.9:8015" ist, dann geben Sie "10.57.60.9" als Zeichenfolgenwert ein.

- Klicken Sie auf **"OK**".

4. Beim Öffnen der Konsole in Internet Explorer mit IWA auf dem Remote-Rechner, dessen Windows-Anmeldeinformationen exakt die gleichen wie auf dem lokalen Rechner sind, auf dem UDP installiert ist, müssen Sie möglicherweise folgende Schritte vornehmen:
   a. Wählen Sie Extras > Internetoptionen.
   b. Wählen Sie die Registerkarte "Sicherheit" aus.
   c. Wählen Sie die lokale Intranet-Zone und klicken Sie auf Websites > **Erweitert**.
   d. Geben Sie den vollständig qualifizierten Domänennamen der Appliance ProxySG (für explizite Bereitstellung) oder die virtuelle URL (für transparente Bereitstellung) in das Feld "Diese Website dem Zonenfeld hinzufügen" ein und klicken Sie dann auf Hinzufügen > Schließen > OK.
   e. Wählen Sie die Registerkarte "Erweitert" und stellen Sie sicher, dass die Option "Sicherheit > Integrierte Windows-Authentifizierung aktivieren" ausgewählt ist.
   f. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld "Internetoptionen" zu schließen.

Die Arcserve UDP-Konsole unterstützt IWA nicht, wenn für die Verbindung zur Konsolendatenbank der Windows-Authentifizierungsmodus verwendet wird.

Um die integrierte Windows-Authentifizierung (IWA) zu verwenden, müssen Sie den Authentifizierungsmodus der Verbindung zur Konsolendatenbank in den SQL Server- und Windows-Authentifizierungsmodus ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie in den SQL Server-Verwaltungstools, ob die Konsolendatenbank den SQL Server- und Windows-Authentifizierungsmodus unterstützt. Wenn die Konsolendatenbank den Modus nicht unterstützt, wechseln Sie in den SQL Server- und Windows-Authentifizierungsmodus, und starten Sie SQL Server neu.
2. Führen Sie die folgenden Schritte aus, um das Arcserve UDP-Konto in SQL Server zu erstellen:
   a. Klicken Sie im folgenden Ordner mit der rechten Maustaste auf **DBAccountUpdate.bat** und klicken Sie auf die Option **Als Administrator ausführen**:

      <UDP-Installationsordner>\Management\BIN

      Die Befehlszeilenschnittstelle wird geöffnet.

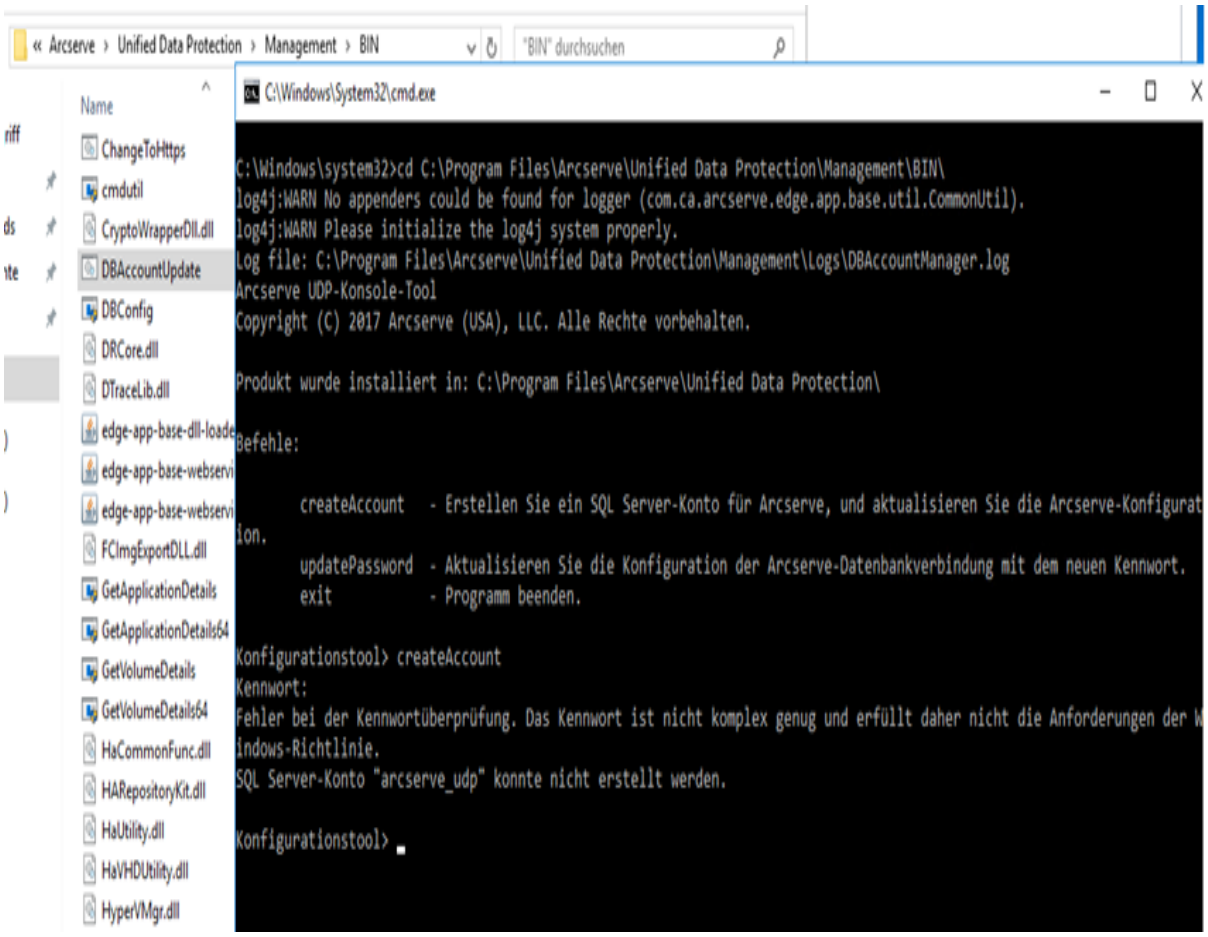
   b. Geben Sie in der Befehlszeilenschnittstelle *createAccount* ein und drücken Sie die Eingabetaste.

      Die Befehlszeilenschnittstelle fordert Sie zur Angabe eines Kennworts auf.

   c. Geben Sie das gewünschte Kennwort für das Konto *arcserve_udp* ein und drücken Sie die Eingabetaste.

      Die Arcserve UDP-Konsole erstellt das SQL Server-Konto *arcserve_udp*.

   d. Geben Sie *Exit* ein, um die Befehlszeilenschnittstelle zu schließen.



3. Starten Sie den Arcserve UDP-Verwaltungsdienst neu.

Fehlerbehebung

Die folgende Liste liefert mögliche Lösungswege für Fehler, die bei der Benutzerverwaltungskonsole auftreten können:

- **Problem**

  Login in die Benutzerverwaltungskonsole ist fehlgeschlagen

  Lösung

  Stellen Sie sicher, dass Sie als Administrator angemeldet haben. Benutzer ohne Administratorrechte verfügen nicht über die Zugriffsrechte für die Benutzerverwaltungskonsole. Stellen Sie sicher, dass Benutzername und Kennwort korrekt sind,

- **Problem**

  Authentifizierungsfehler: Der Benutzer kann sich nicht in die Konsole einloggen

  Lösung

  Überprüfen Sie, ob dem Benutzer eine Rolle zugewiesen wurde. Ein Benutzer kann sich nicht in der Arcserve UDP Konsole anmelden, wenn ihm keine Rolle zugeteilt wurde.

- **Problem**

  Die Seite der Benutzerverwaltungskonsole ist abgelaufen.

  Lösung

  Die Zeitspanne für die Anmeldung an der Seite "Benutzerverwaltungskonsole" beträgt 15 Minuten. Wenn die Konsole 15 Minuten lang keinen Vorgang auf der Seite in die Konsole feststellt, wird der Benutzer automatisch abgemeldet.

Kapitel 8: Hinzufügen und Verwalten von Quellknoten

In diesem Abschnitt werden die folgenden Themen behandelt:

Hinzufügen von Knoten zur Konsole

Ein Knoten ist ein physischer Quellrechner oder ein virtueller Quellrechner auf einem Hypervisor, den Sie schützen möchten. Sie können einen Knoten schützen, indem Sie Daten in einem Ziel sichern. Mit Arcserve Unified Data Protection können Sie folgende Arten von Knoten hinzufügen:

- Windows
- Linux
- Virtuelle Rechner in VMware-ESX/vCenter und Microsoft Hyper-V-Servern

Sie können Knoten hinzufügen, indem Sie die Knotendetails manuell angeben, Discovery von Active Directory durchführen oder einen Import aus einer Datei oder einem Hypervisor ausführen.

Hinweis: Sie können Knoten auch hinzufügen, während Sie einen Plan erstellen.

Der nächste Schritt?

- Überprüfen der Voraussetzungen
- Hinzufügen von Knoten
- Erkennen von Knoten
- Importieren von Knoten

Überprüfen der Voraussetzungen

Erfüllen Sie folgende Voraussetzungen, bevor Sie mit dem Hinzufügen eines Knoten beginnen:

1. Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.
2. Melden Sie sich bei der Konsole an.
3. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite "**Knoten: Alle Knoten**" wird angezeigt.
4. Klicken Sie im mittleren Fensterbereich auf **Knoten hinzufügen**.

   Das Dialogfeld **Knoten zu Arcserve UDP-Konsole hinzufügen** wird geöffnet.

   Das Dialogfeld stellt mehrere Optionen bereit, um einen Knoten hinzuzufügen.

Hinzufügen von Knoten

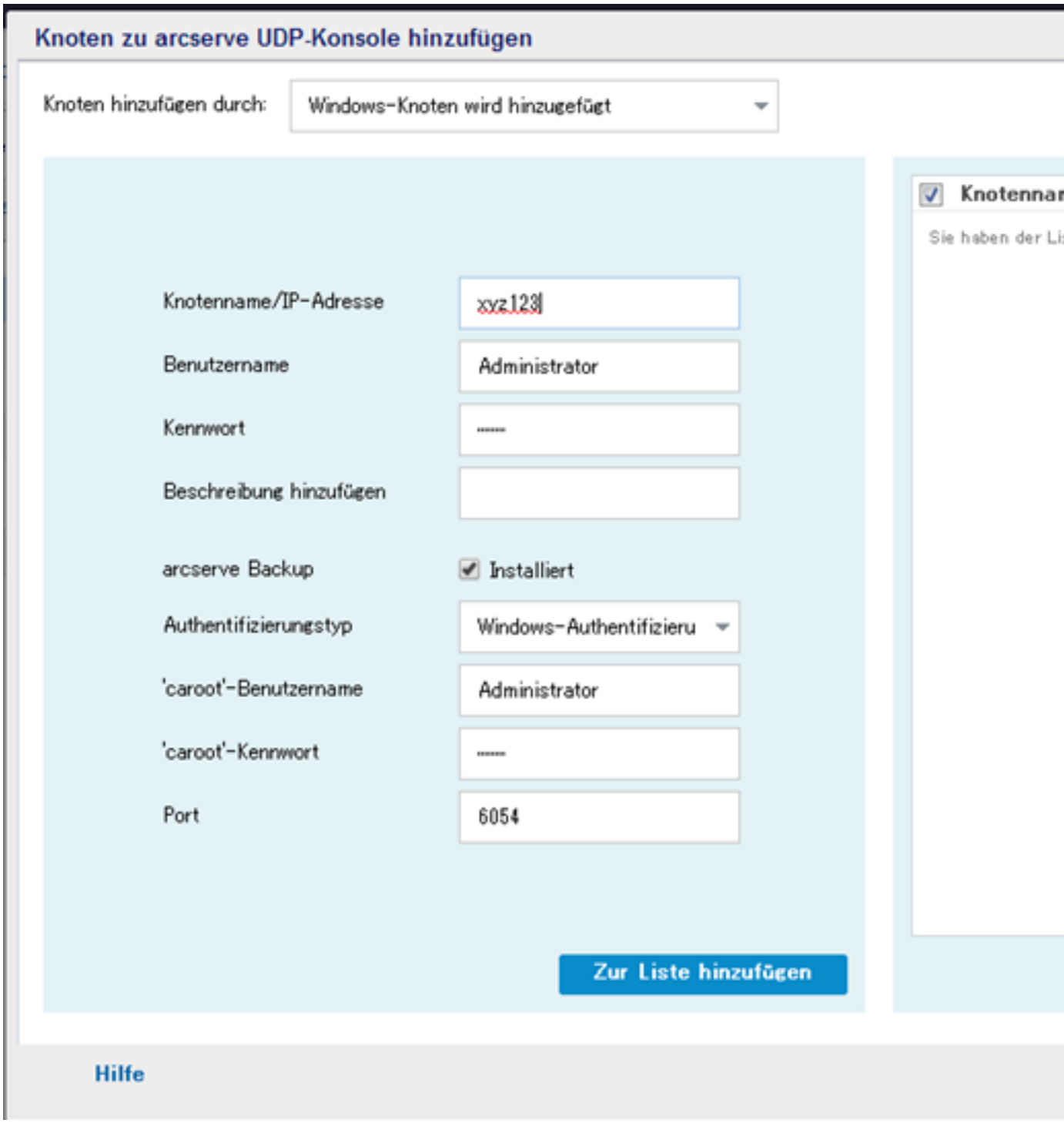
Wenn Sie IP-Adresse oder Namen eines Knotens oder Knotensatzes kennen, können Sie diese zur Konsole hinzufügen, indem Sie die entsprechenden Details manuell angeben. Sie können folgende Arten von Knoten hinzufügen:

- **Windows:** Windows-Quellknoten, die Sie schützen möchten. Wenn der Windows-Quellknoten mit dem SMB-Port blockiert ist, wird Arcserve UDP Agent (Windows) auf diesem Knoten installiert.
- **Linux:** Linux-Quellknoten, die Sie schützen möchten. Arcserve Unified Data Protection Agent for Linux ist auf dem Linux-Sicherungsserver und nicht auf den Linux-Quellknoten installiert.
- **Linux-Sicherungsserver:** Ein Linux-Server, der Linux-Quellknoten verwaltet. Arcserve Unified Data Protection Agent for Linux ist auf diesem Server installiert.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Drop-down-Liste **Knoten hinzufügen durch** eine der folgenden Optionen aus:

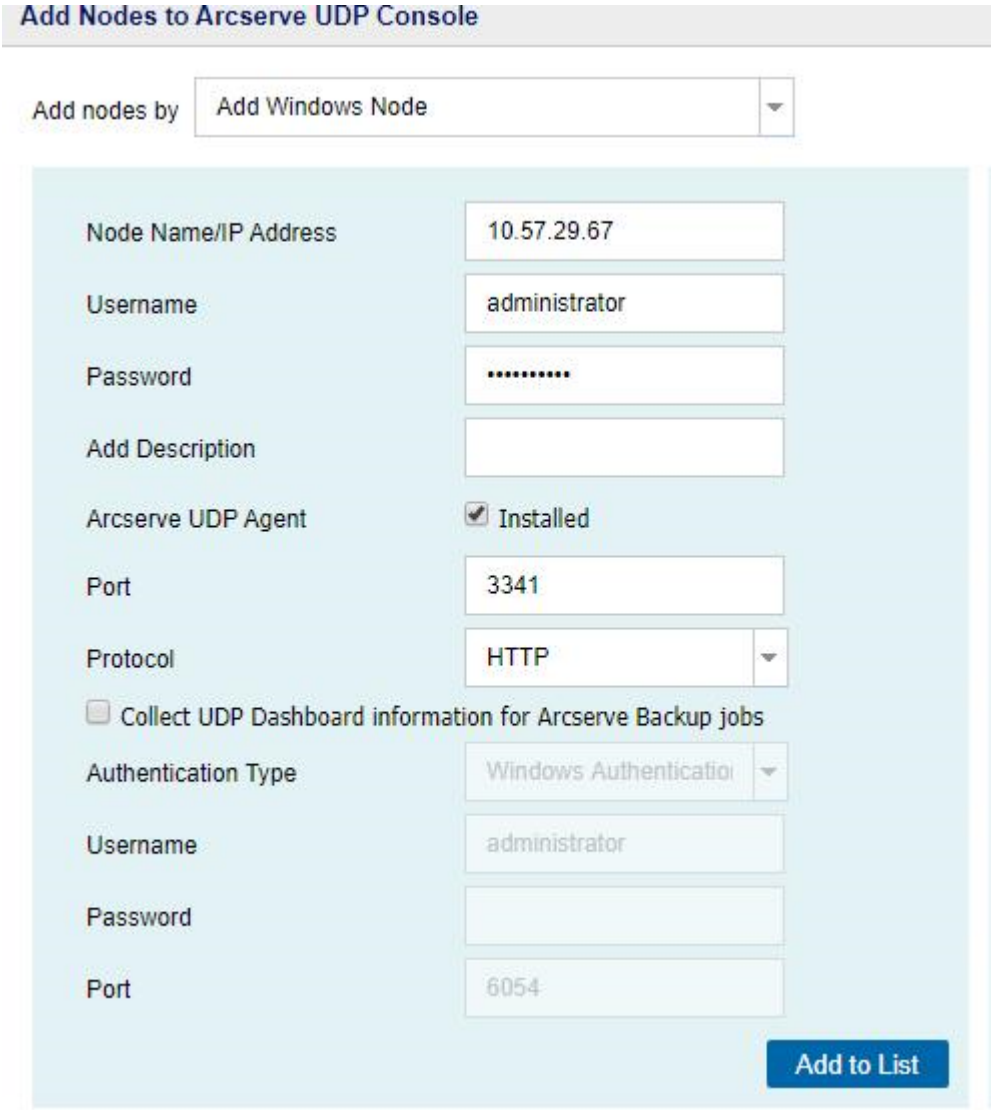
   Hinzufügen von Windows-Knoten



Hinweis: Um die Details für Arcserve Backup zu aktivieren, wählen Sie **Installiert** aus.

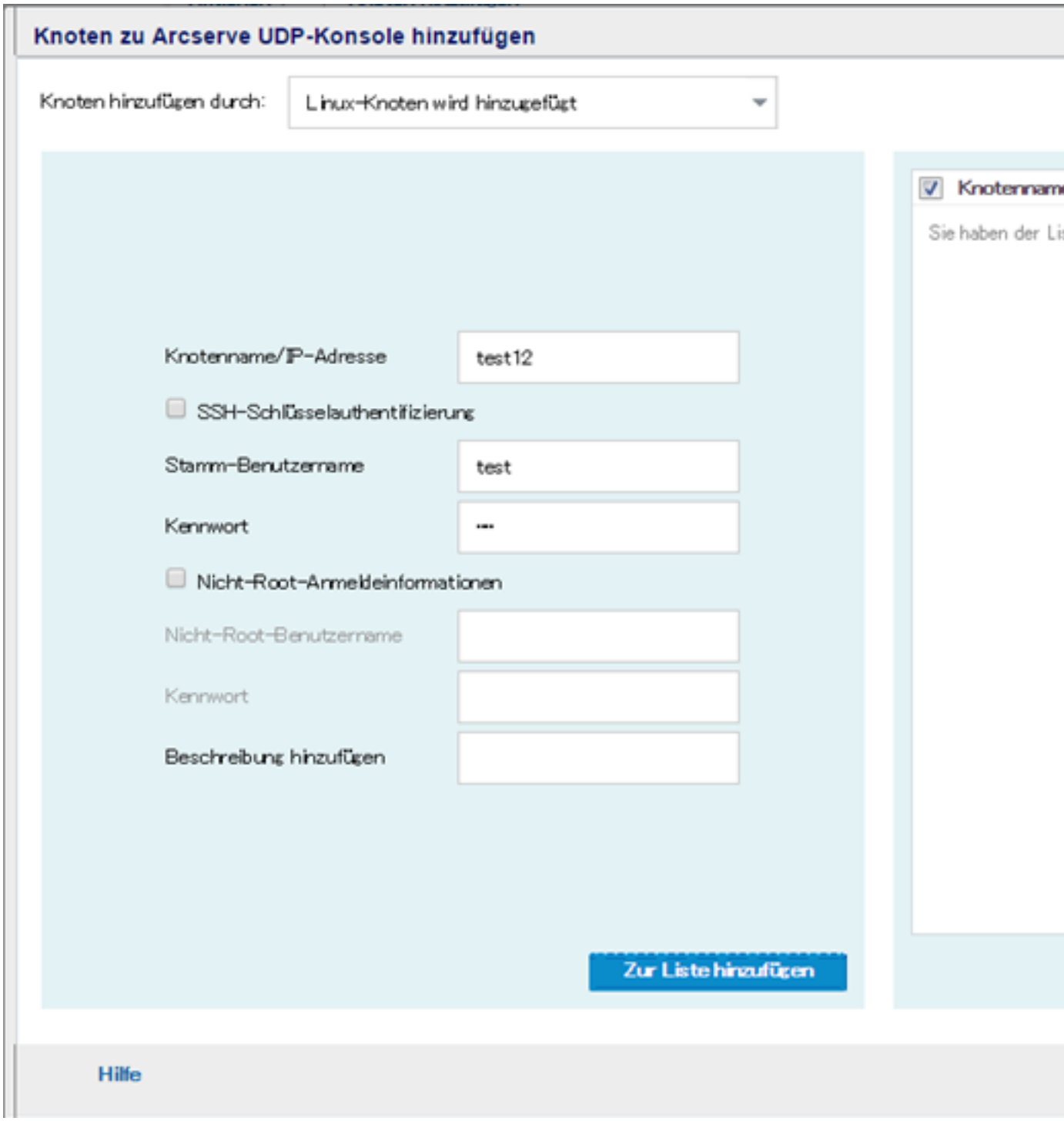
2. Um einen gesperrten Knoten des SMB-Ports hinzuzufügen, gehen Sie zur Drop-Down-Liste **Knoten hinzufügen durch**, und wählen Sie eine der folgenden Optionen aus:

   Hinzufügen von Windows-Knoten



Hinweis: Geben Sie den benutzerdefinierten Port und Protokolldetails an, und wählen Sie dann "Installiert" aus.

Linux-Knoten wird hinzugefügt

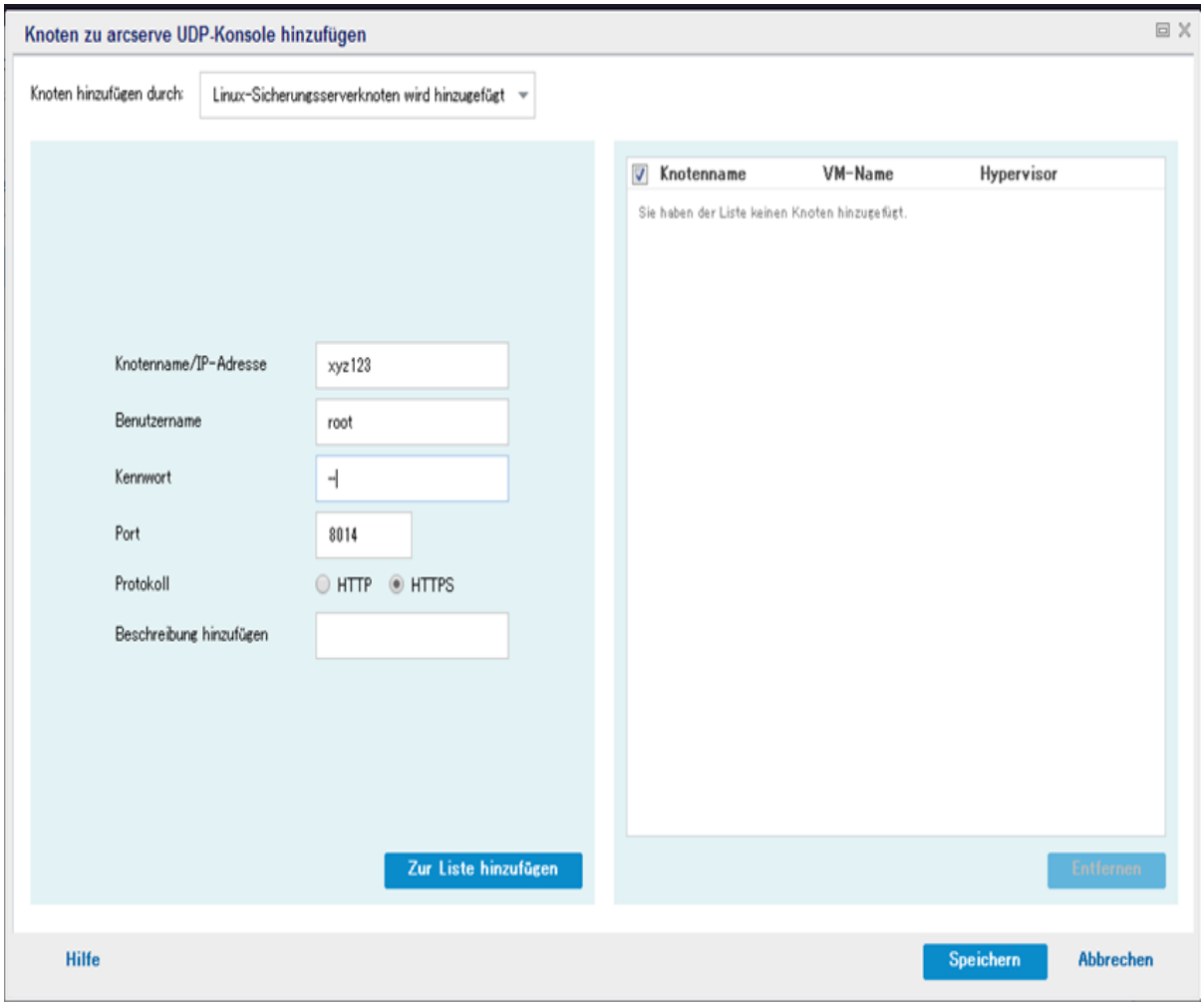


Hinweise:

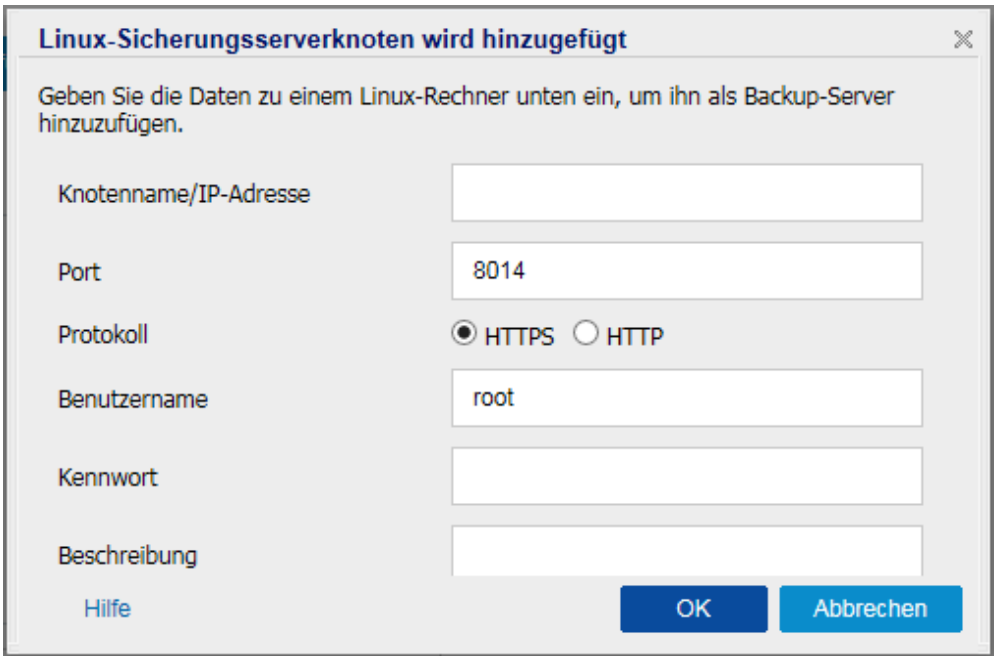
- Unter Linux müssen Sie bei der Auswahl der **SSH-Schlüsselauthentifizierung** keine Kennwortdetails eingeben, der Benutzername ist jedoch erforderlich. Weitere Informationen über das Konfigurieren des SSH-Schlüssels finden Sie unter Konfigurieren der Authentifizierung für private und öffentliche Schlüssel.

- Bevor Sie einen Linux-Knoten hinzufügen, müssen Sie einen **Linux-Sicherungsserver** hinzufügen, der die Linux-Knoten verwaltet.
- Knoten mit Debian Linux unterstützen ausschließlich Root-Anmeldeinformationen. Um Debian Linux mit Nicht-Root-Benutzer hinzuzufügen, verwenden Sie sudoers. Weitere Informationen zur Konfiguration von sudo finden Sie unter Konfigurieren von sudo unter Debian.
- Sie können sich am Linux Backup-Server von der Arcserve UDP Konsole aus nur anmelden, wenn Sie eine Wiederherstellung durchführen.

Hinzufügen von Linux-Sicherungsserverknoten



Das folgende Dialogfeld wird angezeigt, wenn Sie den Linux-Sicherungsserverknoten über den Task **Sicherung: Agentenbasierte Linux-Sicherung** hinzufügen:



Die Details für die ausgewählte Option werden angezeigt.

3. Geben Sie die Details des Knotens ein, und klicken Sie auf **Zur Liste hinzufügen**.

   Der Knoten wird im rechten Fensterbereich hinzugefügt. Um weitere Knoten hinzuzufügen, führen Sie die Schritte erneut durch. Alle hinzugefügten Knoten werden im rechten Fensterbereich aufgelistet.

4. (Optional) Um die hinzugefügten Knoten aus der Liste im rechten Fensterbereich zu entfernen, wählen Sie die Knoten aus, und klicken Sie auf **Entfernen**.

5. Wählen Sie die hinzuzufügenden Knoten aus, und klicken Sie auf **Speichern**.

   Die Knoten werden hinzugefügt und sind auf der Seite "**Knoten: Alle Knoten**" verfügbar.

   Wenn sich Ihr Linux Backup-Server in der NAT-Umgebung befindet, führen Sie folgende Schritte aus, bevor Sie die Arcserve UDP-Konsole hinzufügen:

   1. Erstellen Sie die Datei *server.cfg* im folgenden Linux-Sicherungsserver-Ordner:

      /opt/Arcserve/d2dserver/configfiles/.

   2. Fügen Sie der Datei "server.cfg" folgende Zeile hinzu:

      nat_enable=true

   3. Starten Sie den Linux-Agent mit folgendem Befehl neu:

      /opt/Arcserve/d2dserver/bin/d2dserver restart

   Hinweis: Wenn dieser Linux-Sicherungsserver bereits hinzugefügt ist, aktualisieren Sie den Linux-Sicherungsserver auf der UDP-Konsole.

Erkennen von Knoten

Um Knoten hinzuzufügen, die sich in einem Active Directory-Verzeichnis befinden, können Sie zunächst durch das Angeben der Active Directory-Details Discovery für die Knoten durchführen und sie anschließend zur Konsole hinzufügen.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Drop-down-Liste **Knoten hinzufügen durch Knoten werden von Active Directory erkannt** aus.
2. Geben Sie die Benutzeranmeldeinformationen an, und klicken Sie auf **Hinzufügen**.

   Benutzername

   Gibt Domäne und Benutzernamen im Format Domäne\Benutzername an.

   Kennwort

   Gibt das Benutzerkennwort an.

   Computernamenfilter

   Gibt den Filter zum Erkennen der Knotennamen an.

   Nach der Validierung wird der Benutzername zur Liste hinzugefügt.
3. Wählen Sie den hinzugefügten Benutzernamen aus, und klicken Sie auf **Durchsuchen**.

   Bei einer erfolgreichen Knoten-Discovery wird das Dialogfeld **Bestätigen** angezeigt, in dem Sie aufgefordert werden, die Knoten aus dem **Discovery**-Ergebnis hinzuzufügen.

   Hinweis: Der Discovery-Prozess kann abhängig von Faktoren wie Netzwerk und Anzahl von Computern im Netzwerk eine gewisse Zeit in Anspruch nehmen.
4. Klicken Sie auf **Ja**.

   Die erkannten Knoten werden aufgelistet.
5. Wählen Sie den Knoten aus, geben Sie Benutzernamen und Kennwort ein, und klicken Sie auf **Anwenden**.

   Hinweis: Wenn Sie auf "Anwenden" klicken, werden die Anmeldeinformationen überprüft. Sie müssen jeden Knoten überprüfen, bevor Sie ihn zur Liste hinzufügen.

   Für überprüfte Knoten wird ein grünes Häkchen angezeigt.
6. Klicken Sie auf **Zur Liste hinzufügen**.

   Der ausgewählte Knoten wird im rechten Fensterbereich angezeigt.

7. Um die Knoten der Konsole hinzuzufügen, wählen Sie im rechten Feld den Knoten aus und klicken Sie auf **Speichern**. Hinweis: Um alle Knoten hinzuzufügen, aktivieren Sie das Kontrollkästchen **Knotenname**.

   Die bestätigten Knoten werden hinzugefügt und sind auf der Seite "**Knoten: Alle Knoten**" verfügbar.

Fehlerbehebung: Die angegebene Domäne ist nicht vorhanden oder konnte nicht kontaktiert werden

Problem

Beim Hinzufügen von Knoten über Discovery aus Active Directory erhalte ich die folgende Fehlermeldung angezeigt:

"The specified domain either does not exist or could not be contacted. Verify that the Console server can access the domain controller through the network."

Lösung

Überprüfen Sie zunächst die Verbindung zwischen dem Arcserve UDP und dem Domänencontroller. Wenn die Konnektivität in Ordnung ist, verwenden Sie den folgenden Befehl mit dem Argument "dsgetdc", um zu überprüfen, ob Windows den Domänencontroller anhand des Domänennamens finden kann:

nltest.exe

Beispiel: "nltest /dsgetdc:sample_domain", wobei "sample_domain" der Domänenname ist.

Wenn der Befehl fehlschlägt, dann liegt möglicherweise ein DNS-Problem in Ihrer Umgebung vor.

Hinweis: Sie sollten den oben genannten Befehl auf dem UDP-Rechner ausführen. Weitere Informationen finden Sie im folgenden Artikel von Microsoft.

Importieren von Knoten

Mit der Importmethode von Arcserve Unified Data Protection können Sie mehrere physische und virtuelle Knoten gemeinsam hinzufügen. Je nach Bedarf können Sie eine der folgenden Importmethoden verwenden:

- Importieren von Knoten aus CSV- oder TXT-Dateien
- Importieren von Knoten von einem vCenter/ESX-Server
- Importieren von Knoten von einem Hyper-V-Server

Importieren von Knoten von einem vCenter/ESX-Server

Mit dieser Importmethode können Sie virtuelle Rechnerknoten aus dem ESX-Server oder vCenter-Server importieren. Diese Option listet alle virtuellen Rechner auf, die auf dem angegebenen Server erkannt werden, auch wenn sie bereits in Arcserve Unified Data Protection verwaltet werden.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Drop-down-Liste **Knoten hinzufügen durch** die Option **Aus vCenter/ESX importieren** aus.
2. Geben Sie die Details zum vCenter/ESX-Server an, und klicken Sie auf "**Verbinden**".

   Im linken Fensterbereich wird eine Knotenstruktur angezeigt.

   Hinweis: VMware Virtual Disk Development Kit (VDDK) 6.x.x ist in Arcserve UDP Version 7.0 enthalten. VDDK 6.x.x bietet jedoch keine Unterstützung für HTTP. Außerdem unterstützen vCenter und ESX in der Regel standardmäßig nur HTTPS-Verbindungen. Wählen Sie HTTPS aus, es sei denn, Sie ersetzen das integrierte VDDK 6.x.x durch eine andere Version und konfigurieren vCenter/ESX manuell zum Zulassen von HTTP-Verbindungen.
3. Erweitern Sie die Knotenstruktur.

   (Optional) Sie können den Knotennamen im Filterfeld eingeben, um den Knoten in der Struktur zu finden.
4. Wählen Sie die Knoten aus, die hinzugefügt werden sollen.

   Hinweis: Arcserve UDP ermöglicht es Ihnen, die folgenden Optionen auszuführen:

   - Hinzufügen und Schützen von Containerobjekten in vSphere-Infrastrukturen (z. B. Rechenzentren und Ressourcenpools)
   - Hinzufügen und Schützen von VM-Vorlagen sowie Tag-basierte Sicherung von VMs

   Allerdings können Sie diese Aktion derzeit nur mithilfe des Plan-Assistenten ausführen. Weitere Informationen finden Sie unter *Knoten aus vCenter/ESX hinzufügen* im Thema Angeben der Quelle.
5. Aktivieren Sie das Kontrollkästchen **Anmeldeinformationen für die ausgewählten Knoten angeben**, und geben Sie die Benutzeranmeldeinformationen an.

   Hinweis: Für Funktionen wie Pre Flight Check (PFC), Anwendungsprotokollkürzung und Befehle vor/nach der Sicherung sind Benutzeranmeldeinformationen erforderlich.

6. Klicken Sie auf **Zur Liste hinzufügen**.

   Die ausgewählten Knoten werden im rechten Fensterbereich hinzugefügt.

7. Wählen Sie die Knoten aus, und klicken Sie auf **Speichern**.

   Die Knoten werden hinzugefügt und auf der Seite **Knoten: Alle Knoten** angezeigt.

Importieren von Knoten von einem Hyper-V-Server

Mit dieser Importmethode können Sie virtuelle Rechnerknoten aus Microsoft Hyper-V-Servern importieren.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Drop-down-Liste **Knoten hinzufügen durch** die Option **Aus Hyper-V importieren** aus.
2. Füllen Sie die folgenden Felder aus, und klicken Sie auf **Verbinden**.

   Hyper-V

   Gibt den Namen oder die IP-Adresse des Hyper-V-Servers an. Um virtuelle Rechner zu importieren, die in Hyper-V-Clustern sind, geben Sie entweder den Cluster-Knotennamen oder den Hyper-V-Hostnamen an.

   Benutzername

   Gibt den Namen eines Hyper-V-Benutzers mit Administratorrechten an.

   Hinweis: Verwenden Sie für Hyper-V-Cluster ein Domänenkonto mit Administratorrechten des Clusters. Für eigenständige Hyper-V-Hosts empfehlen wir, ein Domänenkonto zu verwenden.

   Kennwort

   Gibt das Kennwort für den Benutzernamen an.

   Die Arcserve Unified Data Protection-Lösung durchsucht die Knotenstruktur und zeigt sie im linken Fensterbereich an.
3. Erweitern Sie die Knotenstruktur.

   (Optional) Sie können den Knotennamen im Filterfeld eingeben, um den Knoten in der Struktur zu finden.

   Hinweis: Die als Clusterrolle konfigurierten virtuellen Rechner werden in der Struktur direkt unter dem Cluster-Knotennamen aufgelistet. Die virtuellen Rechner, die nicht Teil des Clusters sind, werden unter dem Hostnamen des individuellen Hyper-V-Hosts aufgelistet.
4. Wählen Sie die Knoten aus, die hinzugefügt werden sollen.
5. Aktivieren Sie das Kontrollkästchen **Anmeldeinformationen für die ausgewählten Knoten angeben**, und geben Sie die Benutzeranmeldeinformationen an.

   Hinweis: Für Funktionen wie Pre Flight Check (PFC), Anwendungsprotokollkürzung und Befehle vor/nach der Sicherung sind Benutzeranmeldeinformationen erfor-

derlich. Ohne Benutzeranmeldeinformationen schlägt der PFC für die ausgewählten Knoten fehl.

6. Klicken Sie auf **Zur Liste hinzufügen**.

   Die ausgewählten Knoten werden im rechten Fensterbereich hinzugefügt.

7. Wählen Sie die Knoten aus, und klicken Sie auf **Speichern**.

   Die Knoten werden hinzugefügt und auf der Seite **Knoten: Alle Knoten** angezeigt.

Importieren von virtuellen Rechnern mit einem zusätzlichen Administratorkonto

Zusätzliche Administratorkonten sind jene Konten, bei denen es sich nicht um Standardadministratoren handelt. Solche Konten werden auch als nicht integrierte Administratorkonten bezeichnet. Um einen virtuellen Rechner von einem Hyper-V-Host zu importieren, können Sie das integrierte Administratorkonto des Hyper-V-Hosts, ein Domänenkonto in der lokalen Administratorengruppe des Hyper-V-Hosts oder einen nicht integrierten Administratorbenutzer verwenden.

Der Benutzer des zusätzlichem Administratorkontos kann die unten beschriebenen Vorgänge zum Deaktivieren des Remote-Zugriffs auf UAC durchführen.

Hinweise:

- Dieser Vorgang weicht vom Deaktivieren von UAC grundsätzlich ab. Mit diesem Vorgang können Sie bestimmte Funktionen von UAC deaktivieren.
- Da für den Import die Technologie von Windows-Verwaltungsinstrumentation (WMI) eingesetzt wird, überprüfen Sie, ob WMI nicht durch die Firewall blockiert ist.

Gehen Sie wie folgt vor:

1. Klicken Sie auf "Start", geben Sie "regedit" im Feld "Programme/Dateien durchsuchen" ein, und drücken Sie die Eingabetaste.

   Der Registrierungs-Editor von Windows wird geöffnet.

   Hinweis: Möglicherweise müssen Sie Admin-Anmeldeinformationen angeben, um den Windows-Registrierungs-Editor zu öffnen.

2. Suchen Sie den folgenden Registrierungsschlüssel, und klicken Sie darauf:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. Klicken Sie im Menü "Bearbeiten" auf "Neu" und anschließend auf "DWORD-Wert (32-Bit)".
4. Geben Sie "LocalAccountTokenFilterPolicy" als Namen des neuen Eintrags ein, und drücken Sie die Eingabetaste.
5. Klicken Sie mit der rechten Maustaste auf "LocalAccountTokenFilterPolicy" und anschließend auf "Ändern".
6. Geben Sie in das Datenfeld "Wert" 1 ein, und klicken Sie auf OK.
7. Verlassen Sie den Registrierungseditor.

Weitere Informationen zum Verhalten von Windows finden Sie in der Microsoft-Dokumentation.

Importieren von Knoten aus CSV- oder TXT-Dateien

Wenn Sie mehrere physische Knoten hinzufügen möchten, können Sie, statt sie jeweils einzeln hinzuzufügen, eine CSV- oder TXT-Datei im Format <Knotenname>, <Benutzername>, <Kennwort> erstellen. Anschließend können Sie die TXT- oder CSV-Datei mithilfe der Such- und Upload-Optionen auswählen und in die Konsole importieren.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Dropdown-Liste **Aktionen** den Befehl **importieren**.
2. Klicken Sie auf **Durchsuchen**, um die gespeicherte Datei im TXT- oder CSV-Format auszuwählen.
3. Klicken Sie auf **Upload**.

   Die Knoten werden hinzugefügt und auf der Seite **Knoten: Alle Knoten** angezeigt.

So verwalten Sie Knoten

Mit Arcserve UDP können Sie mehrere Aktionen für die Verwaltung von Knoten ausführen. Sie können beispielsweise Knoten und Hypervisor aktualisieren, Knoten exportieren und löschen und Preflight-Checks durchführen.

Der nächste Schritt?

- Überprüfen der Voraussetzungen
- Aktualisieren der Hypervisor-Informationen
- Angeben des Hypervisor
- Aktualisieren der VM-Informationen
- Aktualisieren von Knoten
- Exportieren von Knoten
- Anhalten von Knoten
- Fortsetzen von Knoten
- Synchronisieren von Daten
- Löschen von Knoten aus der Konsole
- Bereitstellen des Agent auf Knoten
- Durchführen von Preflight-Checks für Ihre Sicherungsjobs

Überprüfen der Voraussetzungen

Bevor Sie mit der Verwaltung von Knoten beginnen, müssen Sie folgende Voraussetzungen erfüllen:

- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.
- Melden Sie sich bei der Konsole an.
- Fügen Sie einen Knoten hinzu.

Aktualisieren der Hypervisor-Informationen

Wenn ein VM-Knoten zu Arcserve Unified Data Protection hinzugefügt wird, können sich die Informationen zur Verbindung wie Hostname oder Anmeldeinformationen für den Hypervisor der VM ändern. In solchen Fällen können Sie die Hypervisor-Informationen in Arcserve Unified Data Protection aktualisieren.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Klicken Sie mit der rechten Maustaste auf die Knotengruppe unter **vCenter/ESX Groups** oder **Hyper-V Groups**.
3. Klicken Sie auf **vCenter/ESX aktualisieren** oder **Hyper-V aktualisieren**.

   Das Dialogfeld **vCenter/ESX aktualisieren** bzw. **Hyper-V aktualisieren** wird angezeigt.
4. Geben Sie die neuen Details im Dialogfeld ein, und klicken Sie auf **OK**.

   Das Dialogfeld **vCenter/ESX aktualisieren** bzw. **Hyper-V aktualisieren** wird geschlossen.

   Die Hypervisor-Informationen wurden erfolgreich aktualisiert.

Angeben des Hypervisor

Geben Sie die Hypervisor-Details an, um für den Schutz einer VM keine zusätzliche Lizenz verwenden zu müssen. Wenn Sie einen virtuellen Rechner (Virtual Machine, VM) über einen Plan für hostbasierte agentenlose Sicherungen schützen, wird für den Schutz der VM die Lizenz des Hypervisor-Host verwendet. Sie müssen keinen Agent auf der VM installieren. In gewissen Fällen ziehen Sie es möglicherweise vor, den Agenten auf der VM zu installieren und einen agentenbasierten Sicherungsplan für den Schutz der VM zu erstellen. In solchen Fällen verwendet die VM eine andere Lizenz als jene des Hypervisor-Hosts. Geben Sie in solchen Fällen die Hypervisor-Details an, und die VM nutzt die Hypervisor-Hostlizenz statt einer weiteren Lizenz.

Beispiele, wann die Hypervisor-Informationen angegeben werden sollten:

- Sie verwenden einen Plan für hostbasierte agentenlose Sicherungen, um die VMs von ESX-Servern oder Hyper-V-Servern zu schützen. Der Plan verwendet für den Schutz der VM die Hypervisor-Lizenz. Jetzt müssen Sie den UDP Agent auf einer VM des angegebenen Hypervisors installieren und einen agentbasierten Plan zum Schutz der VM erstellen. Normalerweise verwendet der Plan eine zusätzliche Lizenz für den Schutz der VM. Wenn Sie den Hypervisor für die VM angeben, verwendet der Plan die Lizenz des Hypervisor.
- Sie haben einen agentbasierten Linux Plan zum Schutz der Linux VM Agent-Knoten. Wenn Sie den Hypervisor für die VM angeben, verwenden alle VMs auf demselben Hypervisor die Hypervisor-Lizenz.

Beachten Sie folgende Punkte, bevor Sie den Hypervisor angeben:

- Der Hypervisor für einen physischen Knoten kann nicht spezifiziert werden.
- Der Hypervisor kann nicht für einen VM-Knoten spezifiziert werden, der von vCenter/ESX oder Hyper-V importiert wird.
- Der Hypervisor kann für mehrere VMs spezifiziert werden, die gleichzeitig zu demselben Hypervisor gehören.
- Stellen Sie sicher, dass die aktuellste Version von VMware Tools bzw. Hyper-V-Integrationsdienst installiert und die VM eingeschaltet ist. Stellen Sie auch sicher, dass Windows Management Instrumentation (WMI) in der Ausnahmeliste der Firewalls auf dem Knoten des VM-Agent enthalten ist.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

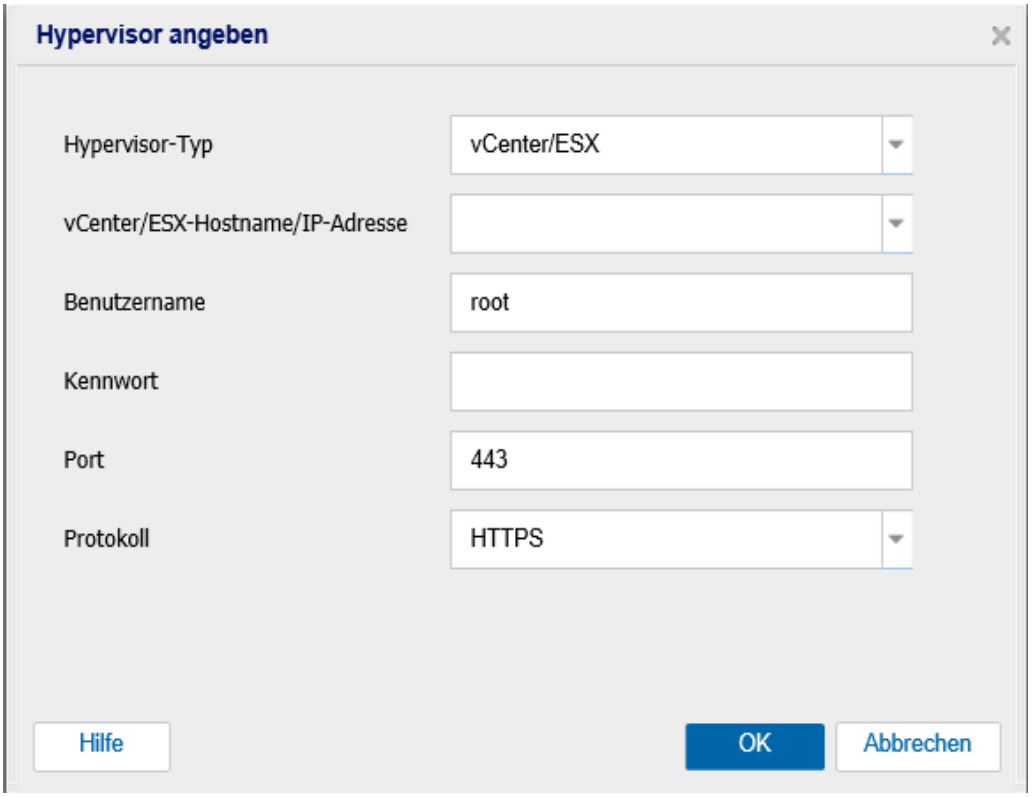
Die Seite "**Knoten: Alle Knoten**" wird angezeigt.

3. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf den Knotennamen.
   - Wählen Sie den Knotennamen aus, und klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.

4. Klicken Sie auf **Hypervisor angeben**.

   Das Dialogfeld "Hypervisor angeben" wird geöffnet. Als **Hypervisor-Typ** kann **Hyper-V**, **vCenter/ESX** oder **Anderer** (Xen, Kernel-basierter virtueller Rechner, Red Hat Enterprise Virtualization) verwendet werden.



5. Geben Sie die Hypervisor-Details ein, und klicken Sie auf **OK**.

   Die Hypervisor-Informationen sind nun angegeben.

Aktualisieren der VM-Informationen

Mit Arcserve Unified Data Protection können Sie bestimmte Eigenschaften der VM-Knoten direkt auf den Hypervisoren aktualisieren. Sie können die Aktualisierung manuell oder automatisch auslösen. Folgende Eigenschaften der VM-Knoten werden mit ihren entsprechenden VMs im Hypervisor aktualisiert und synchronisiert:

- Knotenname
- VM-Name
- BS

Um die Aktualisierung manuell auszulösen, verwenden Sie die Option **VM-Informationen aktualisieren**.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

2. Klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen** und anschließend auf **VM-Informationen aktualisieren**.

   Das Dialogfeld **VM-Informationen aktualisieren** wird geöffnet.

3. Klicken Sie auf **OK**.

   Sie haben eine manuelle Discovery ausgelöst, und dadurch werden die virtuellen Rechnerknoten aktualisiert.

   Die Funktion zur automatischen Aktualisierung wird automatisch ausgelöst, wenn Sie folgende Aktionen ausführen:

   - Öffnen Sie in der Konsole die Registerkarte **Ressource**.
   - Versenden Sie einen geplanten Bericht.

   Hinweis: Auch wenn Sie mehrere automatische Aktualisierungen auslösen, es wird nur eine automatische Aktualisierung gleichzeitig ausgeführt. Die verbleibenden automatischen Aktualisierungen werden in eine Warteschlange gestellt.

Aktualisieren von Knoten

Sie können Informationen aktualisieren, die sich auf die vorhandenen Knoten beziehen. Sie können den Knoten jederzeit aktualisieren. Situationen, in denen das Aktualisieren eines Knotens erforderlich ist, sind beispielsweise folgende:

- Ein neues Produkt wurde auf dem Knoten installiert, nachdem der Knoten bei Arcserve Unified Data Protection registriert wurde.
- Der Benutzername oder das Kennwort für den Knoten wurden aktualisiert, nachdem der Knoten mit Arcserve Unified Data Protection registriert wurde.

Hinweis: Wenn ein Knoten sowohl als Recovery Point Server als auch als Agent eingesetzt wird und Sie die Anmeldeinformationen oder das Protokoll dieses Knotens ändern, aktualisieren Sie den Knoten über die Seite **Ziele: Recovery Point Server**. Nachdem Sie den Recovery Point Server aktualisiert haben, wird der Plan automatisch für den Agent bereitgestellt. Wenn Sie den Knoten über die Seite **Knoten: Alle Knoten** aktualisieren, werden die Pläne, in denen diese Knoten verwendet werden, nicht erfolgreich bereitgestellt. Um den Plan bereitzustellen, aktualisieren Sie den Knoten über die Seite **Ziele: Recovery Point Server** erneut.

Gehen Sie wie folgt vor:

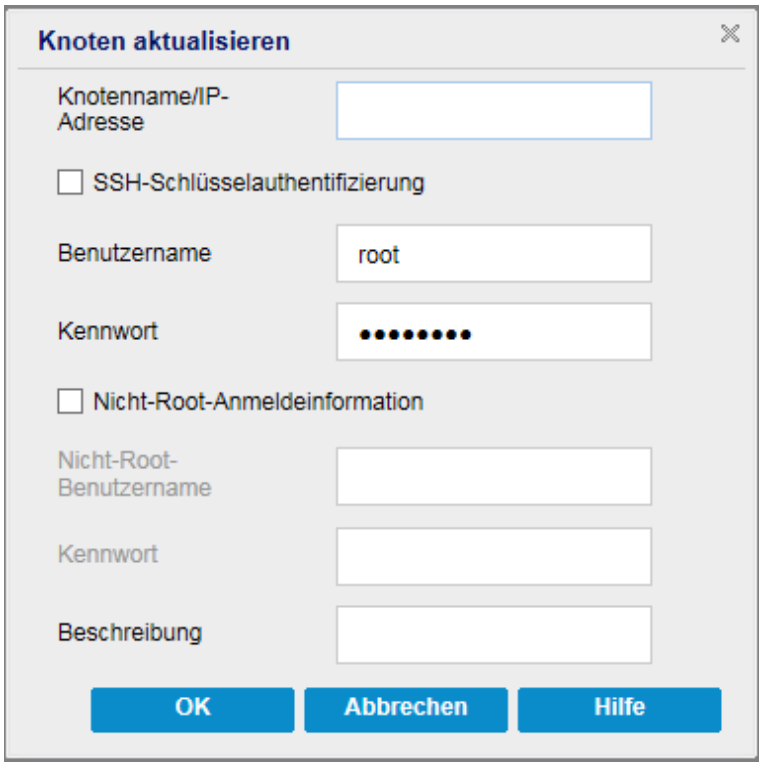
1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

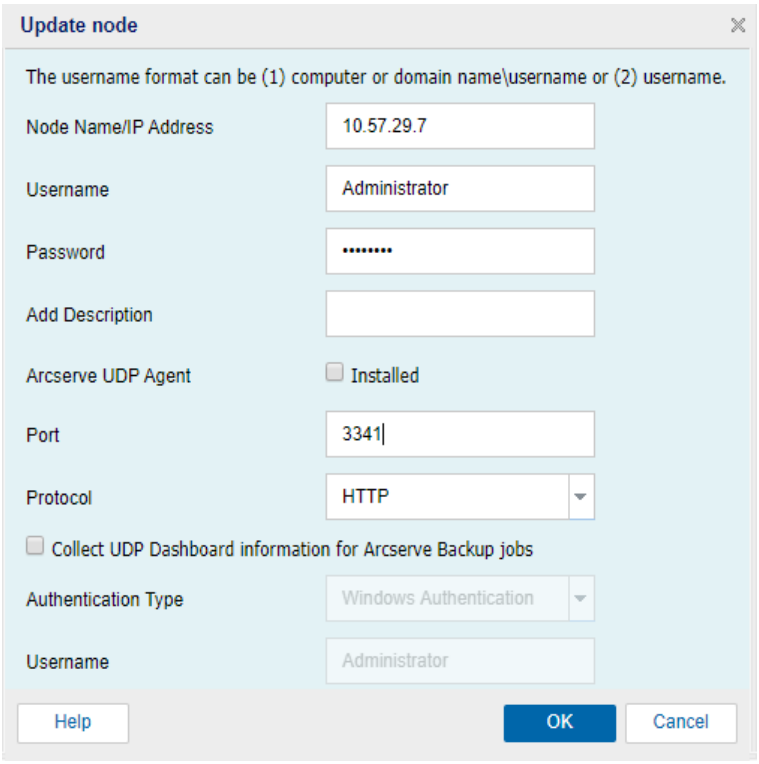
2. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf den Knotennamen.
   - Wählen Sie den Knotennamen aus, und klicken Sie im mittleren Fensterbereich auf das Drop-down-Menü **Aktionen**.
3. Klicken Sie auf **Aktualisieren**.

   Das Dialogfeld "**Knoten aktualisieren**" wird geöffnet.

   Das folgende Dialogfeld gilt für Linux-Knoten:



Das folgende Dialogfeld für Windows-Knoten (wenn der SMB-Port gesperrt ist) mit benutzerdefiniertem Port wird angezeigt:



4. Aktualisieren Sie die Details, und klicken Sie auf "**OK**".

   Die Knoteninformationen wurden aktualisiert.

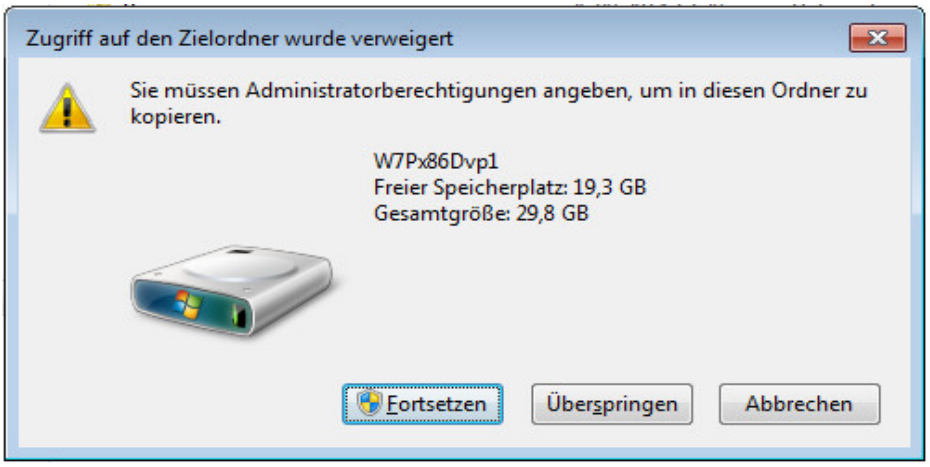
Aktualisieren von Knoten mithilfe eines zusätzlichen Administratorkontos

Zusätzliche Administratorkonten sind Konten, die keine Standardadministratoren verwenden. Solche Konten werden auch als nicht integrierte Administratorkonten bezeichnet. Die Funktionen "Knoten aktualisieren" und "Preflight-Check" (PFC) verwenden das in "Knoten aktualisieren" angegebene Konto, um eine Verbindung mit einem virtuellen Rechner herzustellen und Tests durchzuführen.

Hinweis: Für die Funktion "Knoten aktualisieren" sollten Sie entweder den integrierten Administrator oder ein integriertes Domänen-Administratorkonto verwenden. Bei Bedarf können Sie einen nicht integrierten Administrator verwenden. Zuvor sollten Sie jedoch überprüfen, ob das Konto, das Sie verwenden, über die erforderlichen Administratorrechte verfügt.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie mit dem zusätzlichen Administratorkonto von einem anderen Rechner auf \\[VM-Hostname]\ADMIN$ zugreifen können. Wenn Sie dabei ein Problem haben, überprüfen Sie, ob "Datei- und Druckerfreigabe" durch die Firewall blockiert ist. Wenn die Firewalleinstellungen in Ordnung sind, müssen Sie möglicherweise den Remote-Zugriff auf UAC deaktivieren. Informationen zum Deaktivieren des Remote-Zugriffs auf UAC finden Sie in Importieren von virtuellen Rechnern mit einem zusätzlichen Administratorkonto.
2. Wenn Sie Knoten in VMware aktualisieren, installiert Arcserve UDP für die Ausführung von PFC automatisch einige Tools in der VM. Um zu überprüfen, ob das Konto über die erforderlichen Berechtigungen verfügt, führen Sie folgende Schritte aus:
    a. Melden Sie sich mit dem nicht integrierten Administratorkonto beim virtuellen Rechner an.
    b. Kopieren Sie eine Datei von C:\Windows nach C:\, und stellen Sie sicher, dass die folgende Meldung nicht angezeigt wird:



c. Wenn ein Problem auftritt, können Sie die Konfigurationen der Benutzerkontensteuerung (User Account Control, UAC) ändern. Deaktivieren Sie dazu **Ausführung aller Administratoren im Administrator-Genehmigungsmodus** in der lokalen Sicherheitsrichtlinie, indem Sie die UAC-Einstellungen unter secpol.msc -> Lokale Richtlinien -> Sicherheitsoptionen ändern. (Secpol.msc ist der Editor für Sicherheitsrichtlinien von Microsoft).

Hinweis: Versuchen Sie nicht, die UAC im Dialogfeld "Einstellungen zur Benutzerkontensteuerung" zu deaktivieren, das über die Systemsteuerung geöffnet wird.

Weitere Informationen zum Ändern der UAC-Konfigurationseinstellungen finden Sie in der entsprechenden Microsoft-Dokumentation.

3. Für Hyper-V-VMs muss das zusätzliche Administratorkonto ähnliche Berechtigungen haben wie in Importieren von virtuellen Rechnern mit einem zusätzlichen Administratorkonto beschrieben.

Exportieren von Knoten

Sie können die Knoten als ZIP (.zip)-Dateien exportieren. Bei Bedarf können Sie die ZIP-Datei importieren, um die Knoten aufzubewahren. Wenn Sie zum Beispiel die Knoten vor den Upgrades oder vor dem Neustart exportieren, ist dies für das Importieren des gleichen Satzes an Knoten hilfreich.

Sie können nur Knoten exportieren, die über gültige Anmeldeinformationen verfügen und unter Windows ausgeführt werden.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

2. Wählen Sie einen Knoten aus.

3. Klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen** und anschließend auf **Exportieren**.

   Ein Dialogfeld wird geöffnet, in dem Sie dazu aufgefordert werden, eine Aktion für die Datei "list.zip" durchzuführen.

4. Klicken Sie auf **Öffnen** oder **Speichern**.

   Die Knotenliste wird exportiert.

Anhalten von Knoten

Mit Arcserve UDP können Sie anstelle des gesamten Plans nur ausgewählte Knoten anhalten. Um zu verhindern, dass ein geplanter Job ausgeführt wird, müssen Sie jetzt nicht mehr den kompletten Plan unterbrechen und wiederaufnehmen, was alle zugehörigen Knoten stoppt.

Wichtig: Das Anhalten einer Knotenfunktion funktioniert nur, wenn dieser Knoten mit einem agentenbasierten Windows-Plan oder einem hostbasierten agentenlosen Plan verknüpft ist. Für andere Pläne können Sie einen Knoten nicht anhalten.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

2. Wählen Sie die gewünschten Knoten aus, die einem Plan zugeordnet sind.

3. Klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen** und anschließend auf **Anhalten**.

   Ein Bestätigungsdialogfeld wird angezeigt, in dem Sie darüber informiert werden, dass nur manuelle Jobs für angehaltene Knoten ausgeführt werden können.

4. Klicken Sie auf **Ja**.

   Die Knoten werden angehalten. Wenn ein Knoten nicht angehalten werden kann, wird eine Meldung mit dem Grund angezeigt.

Fortsetzen von Knoten

Mit Arcserve UDP können Sie einen angehaltenen Knoten wieder aufnehmen. Nun können Sie anstatt einen Plan auszusetzen und wiederaufzunehmen, bestimmte Knoten, die diesem Plan zugeordnet sind, aussetzen und wiederaufnehmen.

Wichtig: Das Anhalten und Fortsetzen einer Knotenfunktion funktioniert nur, wenn der Knoten entweder einem agentenbasierten Windows-Plan oder einem host-basierten agentenlosen Plan zugeordnet ist. Für andere Pläne können Sie einen Knoten nicht aussetzen oder wiederaufnehmen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

2. Wählen Sie die ausgesetzten Knoten aus.

3. Klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen** und anschließend auf **Wiederaufnehmen**.

   Es wird ein Dialogfeld angezeigt, in dem Sie Ihre Aktion bestätigen müssen.

4. Klicken Sie auf **Ja**.

   Der Knoten wird erneut ausgeführt.

Synchronisieren von Daten

Durch das Synchronisieren bleiben Daten in unterschiedlichen Datenbanken konsistent und aktuell.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.
3. (Gruppenebene) Wählen Sie eine der Knotengruppen aus, die im linken Fensterbereich angezeigt werden, und klicken Sie mit der rechten Maustaste darauf.
4. Aktivieren Sie eine der folgenden Optionen:

   Hinweis: Es werden nur jene Optionen angezeigt, die Sie bereits für die Synchronisation mit Arcserve Unified Data Protection hinzugefügt haben.

   - Vollständige Synchronisation von Arcserve Backup
   - Inkrementelle Synchronisation für Arcserve Backup

   Im Dialogfeld **Informationen** wird angezeigt, dass die ausgewählte Synchronisationsmethode übergeben wird.

Löschen von Knoten aus der Konsole

Arcserve Unified Data Protection verfügt über eine Option zum Löschen von Knoten. Wenn Sie die Knoten löschen, werden auch die zugeordneten Protokolle und Jobübersichten gelöscht. Sie können gelöschte Knoten bei Bedarf zu einem späteren Zeitpunkt wieder hinzufügen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

2. Wählen Sie einen Knoten aus, der gelöscht werden soll.

3. Führen Sie eine der folgenden Aktionen durch:

   - Klicken Sie mit der rechten Maustaste auf den Knotennamen.
   - Wählen Sie den Knotennamen aus, und klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen**.

4. Klicken Sie auf **Löschen**.

   Ein **Bestätigungsdialogfeld** wird geöffnet.

5. Klicken Sie auf **Ja**.

   Der Knoten wird aus der Konsole gelöscht.

Bereitstellen des Agent auf Knoten

Um ein Upgrade oder eine Installation von Arcserve Unified Data Protection-Agent für einen Knoten durchzuführen, verwenden Sie **Agent installieren/aktualisieren**. Wenn der Zielrechner eine frühere Version von Arcserve Unified Data Protection-Agent enthält, verwenden Sie die Upgrade-Option, um die aktuelle Version zu erhalten. Anderenfalls verwenden Sie die Installationsoption.

Hinweis: Sie können Arcserve Unified Data Protection-Agents für mehrere Knoten bereitstellen. Sie können maximal 16 Bereitstellungsaufgaben gleichzeitig ausführen. Wenn mehr als 16 Aufgaben vorliegen, bleiben weitere Aufgaben im ausstehenden Status und werden erst ausgeführt, wenn ein Teil der 16 standardmäßigen Bereitstellungsaufgaben abgeschlossen ist. Um die Höchstanzahl von Tasks zu ändern, aktualisieren Sie folgenden Registrierungsschlüssel:

deployMaxThreadCount

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

2. Wählen Sie einen oder mehrere Knoten aus.

3. Klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen** und anschließend auf **Agent installieren/aktualisieren**.

   Die Details zur Installation oder zum Upgrade werden über dem Namen des Knotens im mittleren Fensterbereich angezeigt.

4. Überprüfen Sie die Details.

5. Geben Sie den **Ablaufplan** für die Installation bzw. für das Upgrade an, und klicken Sie auf "OK".

   Der Knoten ist mit der aktuellen Version von Arcserve Unified Data Protection Agent installiert bzw. aktualisiert.

   Hinweis: Sie können eine Agent-Bereitstellung abbrechen, wenn sie für einen späteren Zeitpunkt geplant ist. Um eine Agent-Bereitstellung abzubrechen, wählen Sie den Agenten aus und klicken auf **"Aktionen", "Agentbereitstellung abbrechen"**.

Durchführen von Preflight-Checks für Ihre Sicherungsjobs

Die Arcserve Unified Data Protection-Lösung enthält ein Hilfsprogramm namens "Preflight-Check" (PFC), mit dem Sie wichtige Überprüfungen auf spezifischen Knoten ausführen können, um Bedingungen zu erkennen, die Fehler bei Sicherungsjobs verursachen können. PFC ist nur auf Knoten virtueller Maschinen anwendbar, die von vCenter/ESX oder Hyper-V oder Nutanix AHV importiert werden. PFC funktioniert nicht für die VMware-VM Vorlage. Der Preflight-Check wird automatisch ausgeführt, wenn Sie die folgenden Aktionen ausführen:

- Importieren Sie virtuelle Maschinen von einem vCenter Server/ESX Server system oder Hyper-V oder Nutanix AHV
- Führen Sie einen Sicherungsjob aus.

Andere Verweise:

- Lösungen für Preflight-Check-Elemente von VMware-VMs
- Lösungen für Preflight-Check-Elemente von Hyper-V VMs
- Lösungen für die Preflight-Prüfelemente von Nutanix AHV VMs

Außerdem können Sie einen Preflight-Check auch manuell ausführen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Die Seite **Alle Knoten: Knoten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Namen eines Knotens und anschließend auf **Preflight-Check**.

   Hinweis: Sie können **Preflight-Checks** auch mithilfe einer der folgenden Optionen ausführen:

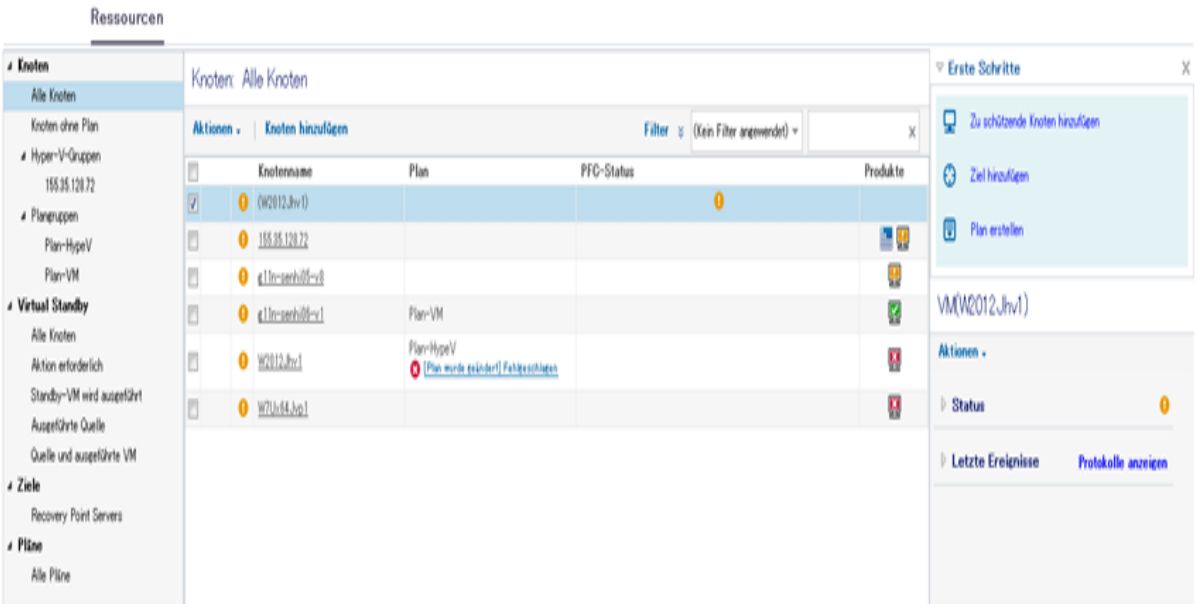
   - (Knotenebene) Klicken Sie auf die Kontrollkästchen der Knoten, für die Sie Preflight-Checks ausführen möchten, klicken Sie anschließend auf das Menü **Aktionen**, und wählen Sie **Preflight-Check** aus.
   - (Gruppenebene) Klicken Sie mit der rechten Maustaste auf die Gruppe, die die Knoten enthält, und anschließend auf **Preflight-Check**.

   Die folgende Meldung wird angezeigt: **Preflight-Check des virtuellen Rechners wird gestartet**.

4. Navigieren Sie zur Spalte **PFC-Status**, um den Status des Preflight-Checks anzuzeigen.

   Hinweis: Die Spalte "PFC-Status" wird standardmäßig nicht in der Benutzeroberfläche angezeigt. Sie müssen die Spalte "PFC-Status" manuell in der Benutzeroberfläche aktivieren.

   Sie können den Status des Preflight-Checks auch anzeigen, indem Sie im rechten Fensterbereich auf **Protokolle anzeigen** klicken.



In der folgenden Tabelle sind die Überprüfungen beschrieben, die von PFC für VMware-VMs ausgeführt werden:

Element	Beschreibung
Verfolgung geänderter Blöcke (CBT)	Eine Funktion zur Verfolgung von Datenträgersektoren, die sich auf einem virtuellen Rechner befinden, der geändert wurde. Dies hilft dabei, die Größe der Sicherungen zu minimieren. Dieses Element stellt sicher, dass CBT aktiviert ist.
VMware-Tools	Dieses Element stellt sicher, dass VMware Tools auf jedem virtuellen Rechner installiert sind.
Festplatte	Dieses Element überprüft die Datenträger des virtuellen Rechners.
Power-Status	Dieses Element stellt sicher, dass der virtuelle Rechner eingeschaltet ist.
Datenkonsistenz	Dieses Element überprüft, ob für die VM ein anwendungskonsistenter Snapshot erstellt werden kann.
ESX Server	Dieses Element überprüft, ob ein Server die virtuelle Maschine erkennen kann. Die Option ist nur sichtbar, wenn der Knoten in ESX nicht verfügbar ist.

In der folgenden Tabelle sind die Überprüfungen beschrieben, die von PFC für Hyper-V-VMs ausgeführt werden:

Element	Beschreibung
Hyper-V-Anmeld-einformationen	Das Produkt muss ein Sicherungshilfsprogramm und ein Hilfsprogramm zur Verfolgung geänderter Blöcke auf Hyper-V-Server über die Systemfreigabe ADMIN$ bereitstellen. Über diese Aktion können Sie überprüfen, ob das Produkt die erforderlichen Berechtigungen für die Freigabe hat. Der Sicherungs- bzw. Wiederherstellungsjob schlägt fehl, wenn die Hyper-V-Anmeldeinformationen nicht richtig sind oder wenn die ADMIN$-Freigabe vom Administrator geschlossen wurde.
Integrationsdienste	Dieses Element stellt sicher, dass Hyper-V-Integrationsdienste auf jedem virtuellen Rechner installiert und aktiviert sind. Ohne die Integrationsdienste kann Arcserve Unified Data Protection die folgenden Aktionen nicht durchführen: ▪ Ausführen von zuvor bzw. danach auszuführende Befehle und Aktionen der Anwendungsprotokollbereinigung. ▪ Ausführen von anwendungskonsistenter Sicherung. Integrationsdienste enthalten mehrere Dienste. Die Arcserve Unified Data Protection-Lösung überprüft die Status der folgenden beiden Dienste: ▪ Hyper-V Data Exchange Service: Ist erforderlich, um VM-Informationen zu erfassen und um zuvor bzw. danach auszuführende Befehle und Aktionen der Anwendungsprotokollbereinigung auszuführen. ▪ Hyper-V Volume Shadow Copy Requestor: Ist für die anwendungskonsistente Sicherung erforderlich.
Power-Status	Dieses Element stellt sicher, dass der virtuelle Rechner eingeschaltet ist. Die Warnung "Unterbrochen" wird angezeigt, wenn sich die VM in einem Status befindet, der nicht "Eingeschaltet" oder "Ausgeschaltet" ist, wie z. B. der Status "Gespeichert". Die Arcserve Unified Data Protection-Lösung kann zuvor bzw. danach auszuführende Befehle und Aktionen der Anwendungsprotokollbereinigung nicht ausführen, wenn sich die VM nicht im eingeschalteten Status befindet. Außerdem kann Arcserve Unified Data Protection die anwendungskonsistente Sicherung nicht ausführen, wenn sich die VM im Status "Unterbrochen" befindet.
Festplatte	Dieses Element überprüft, ob nicht unterstützte Datenträger an die VM angehängt sind.
Datenkonsistenz	Dieses Element überprüft, ob anwendungskonsistente Snapshots für die VM erstellt werden können.

Die folgende Tabelle beschreibt die Prüfungen, die PFC für Nutanix AHV VM durchführt:

Element	Beschreibung
Power-Status	Dieses Element stellt sicher, dass der virtuelle Rechner eingeschaltet ist.
Datenkonsistenz	Dieses Element überprüft, ob für die VM ein anwendungskonsistenter Snapshot erstellt werden kann.
AHV Server	Dieses Element überprüft, ob ein Server die virtuelle Maschine erkennen kann. Die Option ist nur sichtbar, wenn der Knoten in Nutanix AHV nicht verfügbar ist.

Lösungen für Preflight-Check-Elemente von VMware-VMs

Andere Verweise:

- Lösungen für Preflight-Check-Elemente von Hyper-V VMs
- Lösungen für die Preflight-Prüfelemente von Nutanix AHV VMs

Folgende Tabellen beschreiben die Lösungen, die Ihnen dabei helfen, Fehler und Warnungen aus Ihren Preflight-Check-Ergebnissen für VMware-VMs zu beheben:

Verfolgung geänderter Blöcke (CBT)

Status	Meldung	Lösung
Fehler	Verfolgung geänderter Blöcke kann nicht aktiviert werden.	Wenn der virtuelle Rechner nicht über Version 7 oder höher der Hardware verfügt, führen Sie ein Upgrade der Hardwareversion des virtuellen Rechners durch, oder erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection und verwenden Sie Arcserve Unified Data Protection Agent für Windows, um die VM zu sichern.
Warnung	"Verfolgung geänderter Blöcke" ist aktiviert, und Snapshots sind vorhanden. Eine vollständige Sicherung wird für vollständige oder Überprüfungs-Sicherungsjobs angewendet.	**Hinweis:** Dies betrifft nur Voll- und Verifizierungs-Sicherungsaufträge. Für eine Zuwachssicherung werden nur geänderte Daten gesichert. Um die Sicherung verwendeter Blöcke für vollständige oder Überprüfungs-Sicherungsjobs anzuwenden, führen Sie die folgenden Schritte aus: 1. Löschen Sie alle Snapshots, die der virtuellen Maschine zugeordnet sind. 2. Melden Sie sich am Sicherungs-Proxy-Server an. 3. Öffnen Sie den Registrierungseditor und suchen Sie den folgenden Schlüssel: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\ARCserve Unified Data Protection\Engine\AFBackupDll\<VM-InstanceUUID>* **Hinweis:** Ersetzen Sie <VM-InstanceUUUID> durch den UUID-Wert der virtuellen Maschine, bei der CBT ausfällt. Sie finden den Wert in der URL des virtuellen Rechners, der verwendet wird, wenn eine Verbindung mit Arcserve UDP Agent (Windows) hergestellt wird. 4. Stellen Sie den Registrierungsschlüssel auf "Full disk backupForFullBackup"=0 ein. 5. Erstellen oder setzen Sie die Registrierung auf

		ResetCBT=1. 6. Senden Sie den Sicherungsauftrag.

VMware-Tools

Status	Meldung	Lösung
Warnung	Veraltet.	Installieren Sie die aktuelle Version von VMware-Tools.
Warnung	Nicht installiert oder nicht ausgeführt.	Installieren Sie die aktuelle Version von VMware-Tools und stellen Sie sicher, dass das Tool ausgeführt wird.

Festplatte

Status	Meldung	Lösung
Fehler	VM-Snapshots werden nicht für den virtuellen Rechner unterstützt, weil er über einen SCSI-Controller verfügt, der so konfiguriert ist, dass er sich einen Bus teilen kann.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent für Windows , um die VM zu sichern.
Warnung	Der physische Raw Device Mapping-Datenträger (RDM) wird nicht gesichert.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent für Windows , um die VM zu sichern.
Warnung	Die virtuelle Raw Device Mapping-Datenträger (RDM) wird als vollständiger Datenträger gesichert.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent für Windows , um die VM zu sichern.
Warnung	Der unabhängige Datenträger wird nicht gesichert.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent für Windows , um die VM zu sichern.
Warnung	Für vollständige und Überprüfungs-Sicherungsjobs wird der Datenträger im NFS-Datenspeicher als vollständiger Datenträger gesichert.	**Hinweis**: Dies betrifft nur Voll- und Verifizierungs-Sicherungsaufträge. Für eine Zuwachssicherung werden nur geänderte Daten gesichert. Verschieben Sie den virtuellen Datenträger in einen Datenspeicher auf einem Blockspeichergerät, oder erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection oder verwenden Sie Arcserve Unified Data Protection Agent für Windows, um die VM zu sichern.

Power-Status

Status	Meldung	Lösung

Warnung	Ausgeschaltet	Starten Sie den virtuellen Rechner.
Warnung	Unterbrochen	Starten Sie den virtuellen Rechner.

Datenkonsistenz

Status	Meldung	Lösung
Warnung	VMware unterstützt das Stilllegen auf Anwendungsebene nicht für eine VM, die IDE-Datenträger besitzt.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent für Windows, um die Microsoft SQL Server- und Exchange Server-Daten zu sichern.
Warnung	VMware unterstützt das Stilllegen auf Anwendungsebene nicht für eine VM, die SATA-Datenträger besitzt.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent, um die Microsoft SQL Server- und Exchange Server-Daten zu sichern.
Warnung	VMware unterstützt das Stilllegen auf Anwendungsebene nicht, weil die Version des ESX-Servers < 4.1 ist.	Führen Sie ein Upgrade auf ESX Server 4.1 oder höher durch, oder erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection bzw. verwenden Sie Arcserve Unified Data Protection Agent für Windows, um die Microsoft SQL Server-Daten und Exchange Server-Daten zu sichern.
Warnung	VMware unterstützt das Stilllegen auf Anwendungsebene nicht, weil es nicht genug verfügbare SCSI-Slots gibt.	Fügen Sie einen SCSI-Controller vom vSphere Web Client zur VM hinzu, oder erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection oder verwenden Sie Arcserve Unified Data Protection Agent für Windows, um die Microsoft SQL Server- und Exchange Server-Daten zu sichern.
Warnung	VMware unterstützt das Stilllegen auf Anwendungsebene nicht für eine VM, wenn das Gast-BS dynamische Festplatten besitzt.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent für Windows, um die Microsoft SQL Server- und Exchange Server-Daten zu sichern. **Hinweis**: Auf virtuellen Rechnern, auf denen Windows Server 2008 mit ein-

		fachen oder dynamischen Datenträgern ausgeführt wird, unterstützt VMware den inaktiven Modus auf Anwendungsebene nicht.
Warnung	Nicht überprüft, da die Anwendung nicht auf den virtuellen Rechner zugreifen konnte. Stellen Sie sicher, dass die Benutzeranmeldeinformationen korrekt sind und mit Administratorberechtigungen verknüpft sind.	Geben Sie die mitgelieferten Anmeldeinformationen des lokalen Administrators oder die Anmeldeinformationen des Domänenadministrators an, um sich beim Gastbetriebssystem des virtuellen Rechners anzumelden. Stellen Sie außerdem sicher, dass die VMware Tools im virtuellen Rechner aktualisiert sind und ausgeführt werden. Aufgrund einer VMware-Beschränkung werden Sicherungen nur auf VMs unterstützt, die auf einem ESX-Server ausgeführt werden, für die eine bezahlte Lizenz vorliegt. Auf ESXi-Servern mit freier Lizenz werden Sicherungen nicht unterstützt. **Hinweis:** Die Datenkonsistenzprüfung wird unter Windows Server 2008 und höher unterstützt.
Warnung	Es kann nicht überprüft werden, ob datenkonsistente Sicherung möglich ist, weil der virtuelle Rechner nicht eingeschaltet ist.	Weitere Informationen finden Sie in der Spalte "Power-Status".
Warnung	VMware unterstützt das Stilllegen auf Anwendungsebene nicht, wenn beim Gast-BS Speicherplätze aktiviert sind. Wiederherstellung auf Dateiebene wird nur für Volumes unterstützt, bei denen Speicherplätze nicht aktiviert sind. (Die vollständige VM-Wiederherstellung wird über 'VM wiederherstellen' unterstützt).	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent für Windows, um die Microsoft SQL Server- und Microsoft Exchange Server-Daten zu sichern.

Erstellen von anwendungskonsistenten Snapshots für VMware

In einigen Fällen erstellt der VMware-VSS-Writer keine anwendungskonsistenten Snapshots auf einigen virtuellen Rechnern (VM). Dadurch befinden sich die gesicherten Daten möglicherweise nicht in einem anwendungskonsistenten Status.

Überprüfen der Voraussetzungen:

Es müssen folgende Voraussetzungen erfüllt sein, um anwendungskonsistente Snapshots erstellen zu können:

- Die neuesten VMware-Tools müssen installiert sein und innerhalb des Gast-BS der VM ausgeführt werden. Stellen Sie außerdem sicher, dass der VMware Snapshot Provider-Dienst installiert ist und ausgeführt wird.
- Die VM muss unter ESXi 4.1 oder höher ausgeführt werden.
- Die VM darf nur SCSI-Datenträger verwenden. Die VM muss über dieselbe Anzahl von freien SCSI-Slots wie Datenträgern verfügen.
- Anwendungskonsistentes Stilllegen wird für VMs mit IDE- oder SATA-Datenträgern nicht unterstützt.
- Alle Volumes in der VM sind Basisdatenträger, und es sind keine dynamischen Festplatten vorhanden.
- Im Gastbetriebssystem der VM sind keine Speicherplätze aktiviert.
- Der Parameter "disk.EnableUUID" der VM muss konfiguriert sein. Für VMs, die unter Version 4.1 oder höher erstellt wurden, ist dieser Parameter standardmäßig aktiviert. Die folgenden Konfigurationen werden vom Sicherungsjob automatisch ausgeführt, damit Dateninkonsistenzen vermieden und anwendungskonsistente Sicherungen ausgeführt werden. Wenn der Sicherungsjob "disk.EnableUUID" nicht aktivieren kann, konfigurieren Sie den Parameter wie folgt manuell:
  - Wenn der Parameter "disk.EnableUUID" vorhanden ist und auf FALSE gesetzt ist, ändern Sie ihn in TRUE um.
  - Wenn der Parameter "disk.EnableUUID" nicht vorhanden ist, erstellen Sie ihn, und setzen Sie ihn auf TRUE.
  - Wenn der Parameter "disk.EnableUUID" vorhanden ist und auf TRUE gesetzt ist, belassen Sie ihn, wie er ist.

  Hinweis: Weitere Informationen zum Erstellen von anwendungskonsistenten Sicherungen finden Sie im entsprechenden Artikel der VMware-KB.

Betroffene Funktionen:

Wenn eine der Anforderungen nicht erfüllt wird, bleiben die Sitzungsdaten absturzkonsistent. Dadurch sind folgende Funktionen betroffen:

- Gesicherte Daten, die Anwendungsdaten für VMs wie beispielsweise SQL, Exchange und SharePoint enthalten, bleiben möglicherweise in einem absturzkonsistenten Status.
- Der Katalogjob kann möglicherweise fehlschlagen.

Lösungen für Preflight-Check-Elemente von Hyper-V VMs

Andere Verweise:

- Lösungen für Preflight-Check-Elemente von VMware-VMs
- Lösungen für die Preflight-Prüfelemente von Nutanix AHV VMs

Folgende Tabellen beschreiben die Lösungen, die Ihnen dabei helfen, Fehler und Warnungen aus Ihren Preflight-Check-Ergebnissen für Hyper-V-VMs zu beheben:

Hyper-V-Anmeldeinformationen

Status	Meldung	Lösung
Fehler	Es konnte nicht auf die ADMIN$-Freigabe des Hyper-V-Servers zugegriffen werden, oder es liegen nicht die erforderlichen Berechtigungen dazu vor.	■ Stellen Sie sicher, dass der Hyper-V-Server ausgeführt wird. ■ Stellen Sie sicher, dass eine Verbindung zum Netzwerk des Hyper-V-Servers hergestellt werden kann. ■ Stellen Sie sicher, dass die ADMIN$-Freigabe des Hyper-V-Servers aktiviert ist. ■ Geben Sie Administratorrechte von Hyper-V an, wenn Sie VM daraus importiert.

Integrationsdienste

Status	Meldung	Lösung
Warnung	Nicht installiert, wird ausgeführt, betriebsbereit.	Integrationsdienste installieren/aktualisieren/aktivieren. **Hinweise:** ■ Wenn die Integrationsdienste installiert sind, stellen Sie für Windows-VMs sicher, dass die folgenden beiden erforderlichen Dienste auf der VM ausgeführt werden: Hyper-V Data Exchange Service und Hyper-V Volume Shadow Copy Requestor. Überprüfen Sie auch, ob im Ereignisprotokoll Fehler von Hyper-V-Diensten gemeldet werden. ■ Stellen Sie für Linux-VMs sicher, dass auf der spe-

		zifischen Linux-VM die aktuellsten Versionen der Integrationsdienste installiert sind und die Funktionen für *Key-Value Pair* und *Live virtual machine backup* verfügbar sind. Weitere Informationen zu Diensten mit Linux-Integration für Hyper-V-VMs finden Sie im entsprechenden Artikel der Microsoft-KB.
Warnung	Keine Antwort	Starten Sie die Integrationsdienste auf dem Gastbetriebssystem auf der VM neu.
Warnung	Der Integrationsservice im virtuellen Rechner ist nicht kompatibel mit dem Integrationsservice im Hyper-V-Server.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent, um die VM zu sichern.
Warnung	Veraltet.	Führen Sie ein Upgrade der Integrationsdienste durch.

Power-Status

Status	Meldung	Lösung
Warnung	Ausgeschaltet.	Starten Sie den virtuellen Rechner.
Warnung	Unterbrochen.	Starten Sie den virtuellen Rechner.

Festplatte

Status	Meldung	Lösung
Warnung	Der physische, am virtuellen Rechner angehängte Datenträger wird nicht gesichert.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent, um den virtuellen Rechner zu sichern.
Warnung	Virtueller Rechner konnte nach Instanzen-UUID nicht abgerufen werden.	Überprüfen Sie, ob der virtuelle Rechner auf dem Hyper-V-Server vorhanden ist.

Datenkonsistenz

Status	Meldung	Lösung
Warnung	Ein anwendungskonsistenter Snapshot wird nicht unterstützt. Der virtuelle Rechner hat eine dynamische Festplatte.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent, um den virtuellen Rechner zu sichern.
Warnung	Ein anwendungskonsistenter Snapshot wird nicht unterstützt,	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve UDP, oder verwenden Sie Arcserve UDP Agent, um den virtuellen Rechner zu sichern.

	da die VM über Speicherplätze verfügt.	
Warnung	Ein anwendungskonsistenter Snapshot wird nicht unterstützt, da die VM über ein Volume verfügt, dessen Schattenkopie-Speicherplatz sich auf einem anderen Volume befindet.	Ändern Sie den Speicherbereich der Schattenkopie zum Volume selbst. **Hinweis:** Für VMs unter Hyper-V 2012 R2 werden auch in solchen Fällen anwendungskonsistente Snapshots unterstützt, sofern das jeweils aktuelle Update von Microsoft auf den Hyper-V-Host aufgespielt ist.
Warnung	Ein anwendungskonsistenter Snapshot wird nicht unterstützt. Der virtuelle Rechner hat andere Dateisysteme als NTFS/Refs.	Wenn Sie den virtuellen Rechner sichern möchten und Dateisysteme, die nicht NTFS/Refs sind, überspringen möchten, erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve Unified Data Protection, oder verwenden Sie Arcserve Unified Data Protection Agent, um den virtuellen Rechner zu sichern. **Hinweis:** Für VMs unter Hyper-V 2012 R2 werden auch in solchen Fällen anwendungskonsistente Snapshots unterstützt, sofern das jeweils aktuelle Update von Microsoft auf den Hyper-V-Host aufgespielt ist.
Warnung	Ein anwendungskonsistenter Snapshot wird nicht unterstützt. Die "ScopeSnapshot"-Funktion ist im virtuellen Rechner aktiviert.	Deaktivieren Sie "ScopeSnapshot" in der VM, indem Sie dem DWORD-Registrierungsschlüssel "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\ScopeSnapshots" den Wert 0 hinzufügen.
Warnung	Ein anwendungskonsistenter Snapshot wird nicht unterstützt. Der Integrationsservice ist nicht betriebsbereit (Status "Fehlgeschlagen").	Weitere Informationen finden Sie in der Spalte "Integrationsdienste".
Warnung	Nicht überprüft, da die Anwendung den virtuellen Rechner nach Instanzen-UUID nicht abrufen konnte.	Überprüfen Sie, ob der virtuelle Rechner auf dem Hyper-V-Server vorhanden ist.
Warnung	Nicht überprüft, weil der virtuelle Rechner nicht eingeschaltet ist.	Weitere Informationen finden Sie in der Spalte "Power-Status".
Warnung	Ein anwendungskonsistenter Snapshot wird nicht unterstützt. Anmeldung beim virtuellen	Geben Sie die mitgelieferten Anmeldeinformationen des lokalen Administrators oder die Anmeldeinformationen des Domänenadministrators an, um sich beim Gastbetriebssystem des virtuellen Rechners

	Rechner zur Überprüfung des Grunds nicht möglich.	anzumelden. Stellen Sie außerdem sicher, dass der virtuelle Rechner mit dem Netzwerk verbunden ist.
Warnung	Ein anwendungskonsistenter Snapshot wird aus unbekanntem Grund nicht unterstützt.	Um herauszufinden, warum ein anwendungskonsistenter Snapshot nicht erstellt werden konnte, überprüfen Sie die Ereignisprotokolle. Das Ereignisprotokoll befindet sich im folgenden Speicherort: In der VM: "Ereignisanzeige" > "Windows-Protokolle" > "Anwendung" und "System". Suchen Sie in der Protokolldatei nach Fehlern, die von Datenträger, VSS und VolSnap stammen. Auf dem Hyper-V-Server: "Ereignisanzeige" > "Windows-Protokolle" > "Anwendungs- und Dienstprotokolle" > "Microsoft" > "Windows" > "Hyper-V-*". Suchen Sie im Protokoll nach Fehlern für die jeweilige VM.

Erstellen von anwendungskonsistenten Snapshots für Hyper-V

In einigen Fällen erstellt der Hyper-V-VSS-Writer keine anwendungskonsistente Snapshots auf einigen virtuellen Rechnern (VM). Dadurch befinden sich die gesicherten Daten möglicherweise nicht in einem anwendungskonsistenten Status.

Überprüfen der Voraussetzungen:

Es müssen folgende Voraussetzungen erfüllt sein, um anwendungskonsistente Snapshots erstellen zu können:

- In der untergeordneten VM ist der Integrationsdienst mit dem Namen "Hyper-V-Volumeschattenkopie-Anforderer" installiert, und der Integrationsdienst wird ausgeführt.
- Die untergeordnete VM wird ausgeführt.
- Der Speicherort der Snapshot-Datei für die VM ist so festgelegt, dass das Volume im Hostbetriebssystem den VHD-Dateien für die VM entspricht.
- Alle Volumes in der untergeordneten VM sind Basisdatenträger, und es sind keine dynamischen Festplatten vorhanden.
- Alle Datenträger in der untergeordneten VM müssen ein Dateisystem verwenden, das Snapshots unterstützt (zum Beispiel NTFS).

Hinweise zur Überprüfung:

Sie müssen folgende Hinweise beachten, um anwendungskonsistente Snapshots zu erstellen:

- Der Integrationsdienst, der in der untergeordneten VM installiert ist, muss mit dem Hyper-V-Host kompatibel sein.
  - Beispiel: Windows 8.1/2012R2-Integrationsdienst in VM ist nicht kompatibel mit Windows 2008R2-Hyper-V-Host.
- Für Windows 8, 2012 und später sowie die auf dem Windows 2008 R2 Hyper-V-Host ausgeführte VM muss die "ScopeSnapshot"-Funktion in der VM deaktiviert sein. Um die "ScopeSnapshot"-Funktion zu deaktivieren, führen Sie diese Schritte aus:
  1. Melden Sie sich bei der VM an.
  2. Navigieren Sie zu folgendem Speicherort:

     HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
  3. Öffnen Sie den Schlüssel "SystemRestore".

Hinweis: Erstellen Sie den Schlüssel, falls er nicht vorhanden ist.

4. Fügen Sie einen 32-Bit-DWORD-Registrierungswert mit dem Namen "ScopeSnapshots" hinzu, und legen Sie den Wert auf 0 fest.

Betroffene Funktionen:

Wenn eine der Anforderungen nicht erfüllt ist, sind die Sitzungsdaten absturzkonsistent. Dadurch sind folgende Funktionen betroffen:

- Gesicherte Daten, die Anwendungsdaten für VMs wie beispielsweise SQL, Exchange und SharePoint enthalten, bleiben möglicherweise in einem absturzkonsistenten Status.
- Der Katalogjob kann möglicherweise fehlschlagen.

Lösungen für die Preflight-Prüfelemente von Nutanix AHV VMs

Andere Verweise:

- Lösungen für Preflight-Check-Elemente von VMware-VMs
- Lösungen für Preflight-Check-Elemente von Hyper-V VMs

Die folgenden Tabellen beschreiben die Lösungen, die Ihnen helfen sollen, Fehler und Warnungen aus Ihren Preflight-Prüfergebnissen für Nutanix AHV-VMs zu beheben:

Nutanix Guest Tools (NGT)

Status	Meldung	Lösung
Warnung	Wird nicht ausgeführt	Aktivieren Sie die Nutanix Guest Tools für die VM.
Warnung	Tools aktiviert	Guest Tools aktiviert, aber nicht ausgeführt. Installieren Sie die Guest Tools in der VM.

Power-Status

Status	Meldung	Lösung
Warnung	Ausgeschaltet	Starten Sie den virtuellen Rechner.
Warnung	Unterbrochen	Fahren Sie mit der virtuellen Maschine fort.

Datenkonsistenz

Status	Meldung	Lösung
Warnung	Nutanix AHV unterstützt keine anwendungskonforme Suche für eine VM mit IDE-Laufwerken.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve UDP oder verwenden Sie Arcserve UDP Agent (Windows), um die Daten von Microsoft SQL Server und Exchange Server zu sichern.
Warnung	Nutanix AHV unterstützt keine anwendungskonforme Suche für eine VM mit SATA-Laufwerken.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve UDP oder verwenden Sie Arcserve UDP Agent, um die Daten von Microsoft SQL Server und Exchange Server zu sichern.
Warnung	Nutanix AHV unterstützt kein anwendungskonformes Stilllegen, da nicht genügend SCSI-Slots zur Verfügung stehen.	Erstellen Sie einen agentenbasierten Sicherungsplan in Arcserve UDP oder verwenden Sie Arcserve UDP Agent (Windows), um die Daten von Microsoft SQL Server und Exchange Server zu sichern.
Warnung	Nicht überprüft, da die Anwendung nicht	Geben Sie die integrierten lokalen

	auf den virtuellen Rechner zugreifen konnte. Stellen Sie sicher, dass die Benutzeranmeldeinformationen korrekt sind und mit Administratorberechtigungen verknüpft sind.	Administrator- oder Domänenadministrator-Anmeldeinformationen an, um sich am Gastbetriebssystem der virtuellen Maschine anzumelden.
Warnung	Es kann nicht überprüft werden, ob datenkonsistente Sicherung möglich ist, weil der virtuelle Rechner nicht eingeschaltet ist.	Weitere Informationen finden Sie in der Spalte "Power-Status".

Hinzufügen und Verwalten eines UNC/NFS-Pfades

Der UNC/NFS-Pfad wird als Knotentyp in Arcserve UDP eingeführt. Im Gegensatz zu anderen Knoten können Sie den Knoten UNC/NFS Path nicht aus dem Abschnitt "Alle Knoten" hinzufügen. Wie beim Exchange Online-Knoten können Sie den UNC/NFS-Pfad-Knoten nur hinzufügen, wenn Sie einen Plan erstellen. Nach dem Hinzufügen können Sie den UNC/NFS-Pfad-Knoten im Bereich "Alle Knoten" verwalten, wenn Sie eine Aktualisierung vornehmen oder einen Löschvorgang ausführen möchten.

Der nächste Schritt?

- Hinzufügen eines UNC/NFS-Pfades
- Aktualisieren eines UNC/NFS-Pfades
- Löschen eines UNC/NFS-Pfades

Hinzufügen eines UNC/NFS-Pfades

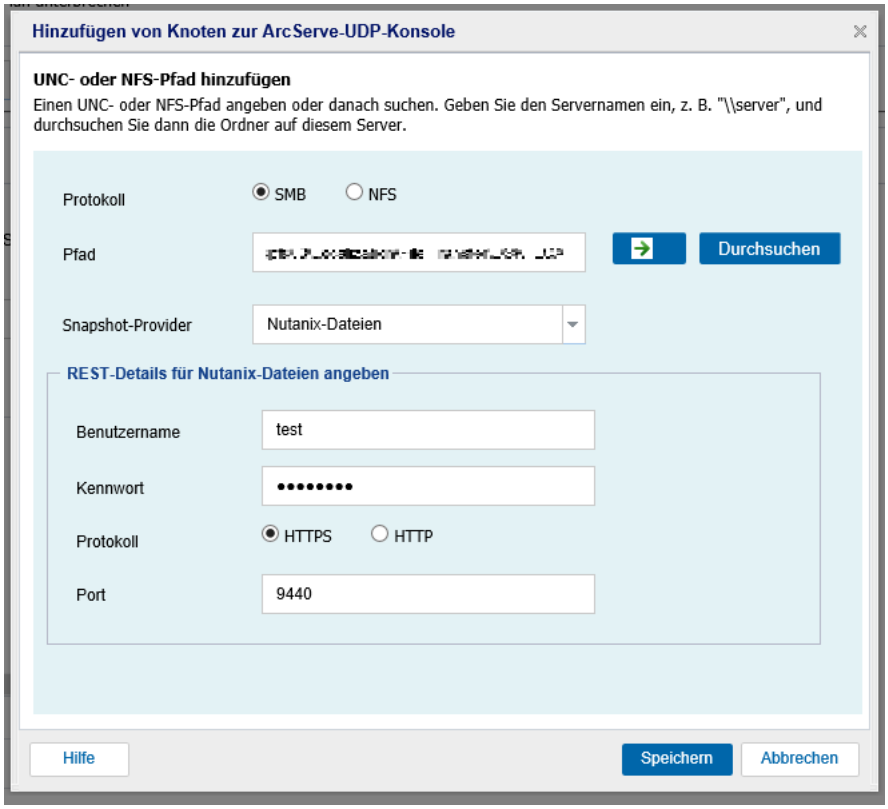
Sie können einen UNC/NFS-Pfad nur dann hinzufügen, wenn Sie einen UNC/NFS-Pfad-Sicherungsplan erstellen. Beim Erstellen des Plans können Sie auf der Registerkarte **Quelle** einen UNC/NFS-Pfad-Knoten hinzufügen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte **Quelle** des UNC-Pfad-Sicherungsplans auf die Option **UNC- oder NFS-Pfad hinzufügen**.

   Das Dialogfeld Knoten zur Arcserve UDP-Konsole hinzufügen wird angezeigt.

2. Führen Sie auf der Seite "UNC- oder NFS-Pfad hinzufügen" die folgenden Schritte aus:



   a. Wählen Sie **SMB** oder **NFS** als Protokoll aus.

      - Wenn Sie **SMB** auswählen, gehen Sie folgendermaßen vor:

        1. Geben Sie den UNC-Pfad im folgenden Format ein:

           *Hostname**share*

           Hinweise:

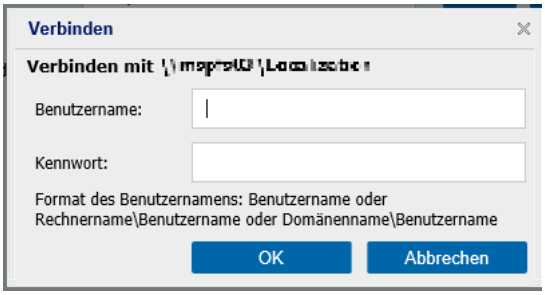
- Während die Nutanix-Dateifreigabe als Quelle für die Sicherung mit Nutanix-Dateien als Snapshot-Provider bereitgestellt wird, können Sicherungen nur auf Freigabeebene, jedoch nicht auf Unterordnerebene durchgeführt werden.
- Gehen Sie folgendermaßen vor, um den UNC-Pfad abzurufen:
  a. Wählen Sie die neu erstellte Freigabe im mittleren Fensterbereich aus.
  b. Navigieren Sie in der Spalte SHARE/EXPORT DETAILS im Fensterbereich "Zusammenfassung" zu **Mount Path**, und kopieren Sie dann den Ladepfad.

     Wenn der UNC-Pfad gültig ist, werden ein Nach-rechts-Pfeil und die Option "Durchsuchen" aktiviert.

2. Klicken Sie auf den Pfeil nach rechts (>), um den UNC-Pfad zu validieren.

   Das Dialogfeld Verbinden wird angezeigt.

3. Geben Sie den Benutzernamen und das Kennwort nach Bedarf ein, und klicken Sie auf **OK**.



   Im Dialogfeld Knoten zu Arcserve UDP-Konsole hinzufügen wird der verifizierte UNC-Pfad angezeigt.

- Wenn Sie "NFS" auswählen, gehen Sie folgendermaßen vor:

  1. Geben Sie den UNC-Pfad im folgenden Format ein:

     *Hostname**share*

  2. Wählen Sie die Codierung aus den verfügbaren Optionen aus: "ANSI", "GB2312-80", "KSC5601", "BIG5", "SHIFT-JIS", "EUC-KR", "EUC-TW" und "EUC-JP".

     Der Standardwert ist ANSI.

Hinweis: Während der Sicherung eines freigegebenen NFS-Ordners werden alle entsprechenden Dateien/Ordner, deren Name eine nicht unterstützte Sprachcodierung verwendet, übersprungen, oder es werden unbrauchbare Namen angezeigt.

b. Wählen Sie in der Drop-down-Liste "Snapshot Provider" die Option **Nutanix-Dateien** aus.

c. Geben Sie im Feld "REST-Details für Nutanix-Dateien angeben" die folgenden Anmeldeinformationen an:

Benutzername

Bezieht sich auf den Benutzernamen, der vom REST-API-Benutzer mithilfe von Nutanix Prism erstellt wurde.

Hinweis: Wählen Sie für sichere Kommunikation das HTTPS-Protokoll aus.

Kennwort

Bezieht sich auf das Kennwort für den Benutzernamen.

Protokoll

Gibt das Protokoll an, das Sie für die Kommunikation mit dem Zielserver verwenden möchten. Die verfügbaren Optionen sind HTTP und HTTPS.

Port

Bezieht sich auf die Portnummer. Der Standardwert für den Port ist 9440; hiermit kann auf die REST-API-Aufrufe und Prism zugegriffen werden.

3. Klicken Sie auf **Speichern**.

Sie können den UNC/NFS-Pfad-Knoten aktualisieren oder löschen.

Aktualisieren eines UNC/NFS-Pfades

Sie können Informationen aktualisieren, die sich auf die vorhandenen Knoten beziehen. Wenn Sie die Anmeldeinformationen des UNC/NFS-Pfads ändern, müssen Sie den UNC/NFS-Pfad auf der Konsole aktualisieren.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

2. Navigieren Sie im linken Fensterbereich zu **Knoten** und wählen Sie **UNC/NFS-Pfade** aus.

   Die vorhandenen UNC/NFS-Pfade werden im mittleren Fensterbereich angezeigt.

3. Wählen Sie im mittleren Fensterbereich einen UNC/NFS-Pfad aus und klicken Sie auf **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.

4. Klicken Sie in der Liste auf **Aktualisieren**.

   Das Dialogfeld "**Knoten aktualisieren**" wird geöffnet.

5. Aktualisieren Sie die Details, und klicken Sie auf "**OK**".

   Die Knoteninformationen wurden aktualisiert.

Löschen eines UNC/NFS-Pfades

Sie können einen vorhandenen UNC/NFS-Pfad-Knoten auf der Registerkarte **Ressourcen** löschen:

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

2. Navigieren Sie im linken Fensterbereich zu **Knoten** und wählen Sie **UNC/NFS-Pfade** aus.

   Die vorhandenen UNC/NFS-Pfade werden im mittleren Fensterbereich angezeigt.

3. Wählen Sie den gewünschten UNC/NFS-Pfad aus und klicken Sie auf **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.

4. Klicken Sie auf **Löschen**.

   Ein Bestätigungsdialogfeld wird angezeigt.

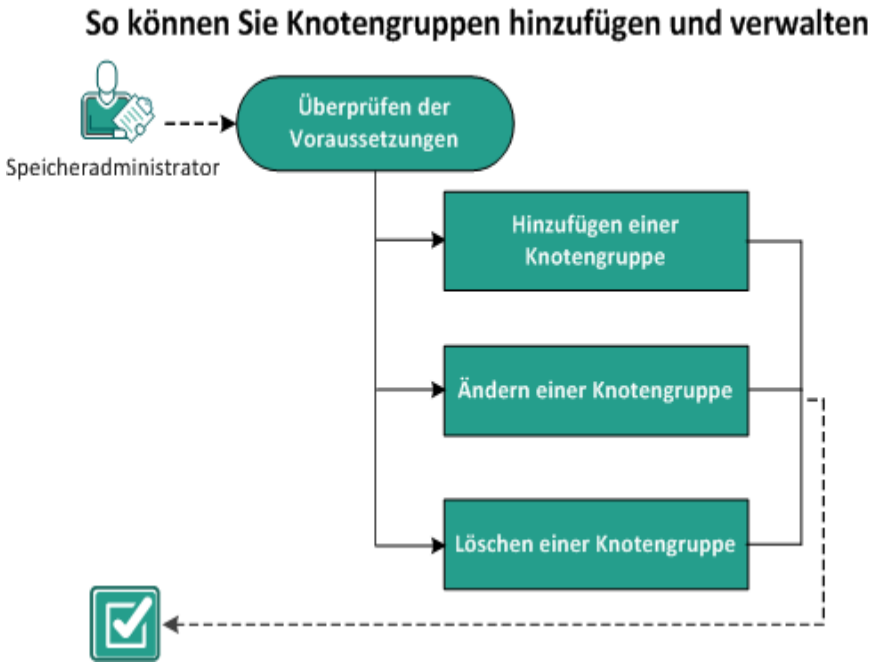
5. Klicken Sie auf **"OK"**.

   Der UNC/NFS-Pfad wird erfolgreich gelöscht.

Hinzufügen und Verwalten von Knotengruppen

Mit Arcserve Unified Data Protection können Sie mehrere Knoten zu einer Gruppe hinzufügen. Sie können Knotengruppen hinzufügen, um Ihre physische und virtuelle Rechnerumgebung zu verwalten.

Folgendes Diagramm beschreibt, wie Sie die Knotengruppen hinzufügen und verwalten können:



Die Arcserve Unified Data Protection-Lösung enthält folgende Knotengruppen:

- Standardgruppen:
  - **Alle Knoten**: Zeigt alle Knoten an, die zur Konsole hinzugefügt werden.
  - **Knoten ohne Plan**: Zeigt die Knoten an, denen kein Plan zugewiesen ist.

  Hinweis: Sie können die Standardknotengruppen nicht ändern oder löschen.
- Gruppen, die angezeigt werden, wenn Sie untergeordnete Gruppen hinzufügen:
  - **Plangruppen**: Zeigt die Liste der Pläne an, die Sie erstellt haben. Wählen Sie die einzelnen Pläne unter der Gruppe aus, um jeweils alle Knoten anzuzeigen, die mit einem Plan verknüpft sind.
  - **Benutzerdefinierte Gruppen**: Zeigt die Liste er benutzerdefinierten Knotengruppen an, die Sie erstellt haben. Ein Beispiel ist die Knotengruppe, die Sie im mittleren Fensterbereich über **Aktionen**, **Knotengruppe**, **Hinzufügen** erstellt haben.

- **vCenter/ESX-Gruppen**: Zeigt die Knoten an, die Sie über die Option **Aus vCenter/ESX importieren** hinzufügen.
- **Linux-Sicherungsservergruppen**: Zeigt die Knoten des Linux-Sicherungsservers an.
- **Exchange Online Knoten**: Zeigt die Exchange Online-Knoten an.
- **UNC-Pfade**: Zeigt UNC-Knoten an.
- **SLA Profilgruppen**: Zeigt Service Level Agreement- (SLA-) bezogene Knoten an.
- **Hyper-V-Gruppen**: Zeigt die Knoten an, die Sie mit der Option **Aus Hyper-V importieren** hinzufügen.
- **Globale Dashboard-Gruppen**: Zeigt alle primären Arcserve Backup-Zweigstellenserver unter dem GDB-Server an. Die globale Dashboard-Gruppe wird hinzugefügt, wenn Sie einen globalen Arcserve Backup Dashboard-Server der Konsole hinzufügen und eine vollständige Arcserve Backup-Synchronisation für den hinzugefügten GDB-Server ausführen.
- **Oracle-Datenbankgruppe**: Zeigt die Oracle-Datenbankknoten an.

Der nächste Schritt?

- Überprüfen der Voraussetzungen
- Hinzufügen von Knotengruppen
- Ändern von Knotengruppen
- Löschen von Knotengruppen

Überprüfen der Voraussetzungen

Bevor Sie an den Knotengruppen arbeiten, müssen Sie folgende Voraussetzungen erfüllen:

- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.
- Melden Sie sich bei der Konsole an.
- Fügen Sie einen Knoten hinzu.

Hinzufügen von Knotengruppen

Sie können eine Gruppe für ausgewählte Knoten erstellen, um die Knotenliste zu verwalten. Sie können Knoten beispielsweise nach Geschäftsfunktion oder nach installierten Anwendungen gruppieren. Sie können Knoten auch zu einem späteren Zeitpunkt zu benutzerdefinierten Gruppen hinzufügen, wenn Sie zuvor eine leere Gruppe hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen**.
4. Klicken Sie auf **Knotengruppe erstellen**.

   Das Dialogfeld **Gruppe hinzufügen** wird geöffnet. Es enthält alle verfügbaren Knoten.
5. Führen Sie folgende Aktionen durch, um Knoten zur Gruppe hinzuzufügen, und klicken Sie auf **OK**.
   - Wählen Sie Knoten aus, die Sie zu einer Gruppe hinzufügen möchten.
   - Geben Sie einen Namen für die Gruppe an.

     Im rechten Fensterbereich werden Sie im Dialogfeld **Informationen** darüber benachrichtigt, dass die Knotengruppe erstellt wurde.

   Die hinzugefügte Gruppe wird im linken Fensterbereich unter **Benutzerdefinierte Gruppen** angezeigt.

   Hinweis: Die Optionen **Ändern** und **Löschen** sind nur aktiviert, wenn Sie eine Gruppe hinzugefügt haben.

Ändern von Knotengruppen

Mit der Arcserve Unified Data Protection-Lösung können Sie die Knotengruppen, die Sie erstellt haben, ändern. Sie können Knoten zu Knotengruppen hinzufügen und aus ihnen entfernen und den Namen von Knotengruppen ändern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.
3. Wählen Sie unter "**Benutzerdefinierte Gruppen**" im linken Fensterbereich eine Gruppe aus.

   Die Details der ausgewählten Gruppe werden im mittleren Fensterbereich angezeigt.
4. Klicken Sie auf die Drop-down-Liste **Aktionen** und anschließend auf **Diese Knotengruppe aktualisieren**.

   Das Dialogfeld "**Gruppe ändern**" wird geöffnet.
5. Aktualisieren Sie die Details, und klicken Sie auf "**OK**".

   Die Knotengruppe wurde aktualisiert.

Löschen von Knotengruppen

Sie können bei Bedarf eine Gruppe löschen. Wenn Sie eine manuell hinzugefügte Gruppe löschen, werden die virtuellen oder physischen Rechner nicht aus Arcserve Unified Data Protection entfernt. Wenn Sie allerdings eine Gruppe löschen, die über ESX- oder vCenter Server-Discovery automatisch erstellt wurde, werden die Gruppe und alle virtuellen Rechner aus der Konsole gelöscht.

Wichtig! Sie können die standardmäßigen Knotengruppen nicht löschen.

Hinweis: Das Löschen der Knotengruppen löscht keine einzelnen Knoten aus der Konsole.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.
3. Wählen Sie unter **Benutzerdefinierte Gruppen** im linken Fensterbereich einen Gruppennamen aus.

   Die Details der ausgewählten Gruppe werden im mittleren Fensterbereich angezeigt.
4. Klicken Sie auf die Drop-down-Liste **Aktionen** und anschließend auf **Diese Knotengruppe löschen**.

   Das Dialogfeld **Bestätigen** wird geöffnet.
5. Klicken Sie auf **Ja**.

   Im rechten Fensterbereich werden Sie im Dialogfeld **Informationen** darüber benachrichtigt, dass die Knotengruppe gelöscht wurde.

Verwalten von Knoten für die Cloud

Mit Arcserve UDP können Sie verschiedene Aktionen ausführen, um Knoten für die Cloud zu verwalten.

Der nächste Schritt?

- Herunterladen von Wiederherstellungspunkten aus der Cloud
- Hochladen von Wiederherstellungspunkten in die Cloud
- Kopieren von Wiederherstellungspunkten auf einen lokalen Datenträger oder eine Netzwerkfreigabe

Herunterladen von Wiederherstellungspunkten aus der Cloud

Mit dieser Funktion können Sie Wiederherstellungspunkte aus der Cloud in lokale Freigaben oder Netzwerkfreigaben herunterladen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

2. Führen Sie eine der folgenden Aktionen durch:

   - Klicken Sie mit der rechten Maustaste auf den Knotennamen.
   - Wählen Sie den Knotennamen aus, und klicken Sie im mittleren Fensterbereich auf das Drop-down-Menü **Aktionen**.

3. Klicken Sie auf **Herunterladen von Wiederherstellungspunkten aus der Cloud**.

   Die Seite **Herunterladen von Wiederherstellungspunkten** aus der Cloud wird geöffnet.

   Sie können den gewünschten Wiederherstellungspunkt in zwei Schritten aus der Cloud herunterladen.

4. Gehen Sie in Schritt 1 wie folgt vor, um einen Wiederherstellungspunkt auszuwählen, und klicken Sie dann auf **Weiter**.

a. Wählen Sie im Drop-down-Menü "Cloud-Dienst" einen Cloud-Dienst aus.

b. Wählen Sie im Drop-down-Menü "Cloud-Speicher" einen Cloud-Speicher aus.

c. Wählen Sie in der Drop-down-Liste "Bucket-Namen" einen Bucket-Namen aus, der einen Wiederherstellungspunkt enthält.

   Die Details zum Wiederherstellungspunkt werden nur angezeigt, wenn Sie einen CRP-Task für den Plan konfigurieren.

Der Bildschirm "Ziel auswählen" wird angezeigt.

5. Geben Sie in Schritt 2 die nachfolgenden Informationen an, und klicken Sie auf **Fertigstellen**.

   a. Geben Sie ein **Ziel** ein.

      Hinweis: Wenn Sie ein Remote-Ziel eingegeben haben, das validiert werden muss, wird nach Klicken auf **Fertig stellen** das Dialogfeld **Verbinden** angezeigt. Geben Sie Details ein, damit das Ziel validiert wird.

   b. Wählen Sie eine Art von **Komprimierung** aus.

   c. Wählen Sie die Art des **Verschlüsselungsalgorithmus** aus.

   d. Geben Sie zweimal das **Verschlüsselungskennwort** ein.

Der Wiederherstellungspunkt wird von der Cloud heruntergeladen.

Hochladen von Wiederherstellungspunkten in die Cloud

Mithilfe dieser Funktion können Sie Wiederherstellungspunkte von Sicherungszielen wie RPS\lokalen Freigaben\Remote-Freigaben in die Cloud hochladen.

Wichtig! Sie benötigen einen Knoten, der einen Sicherungsplan und eine qualifizierte Sicherungssitzung für das Kopieren in die Cloud hat.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

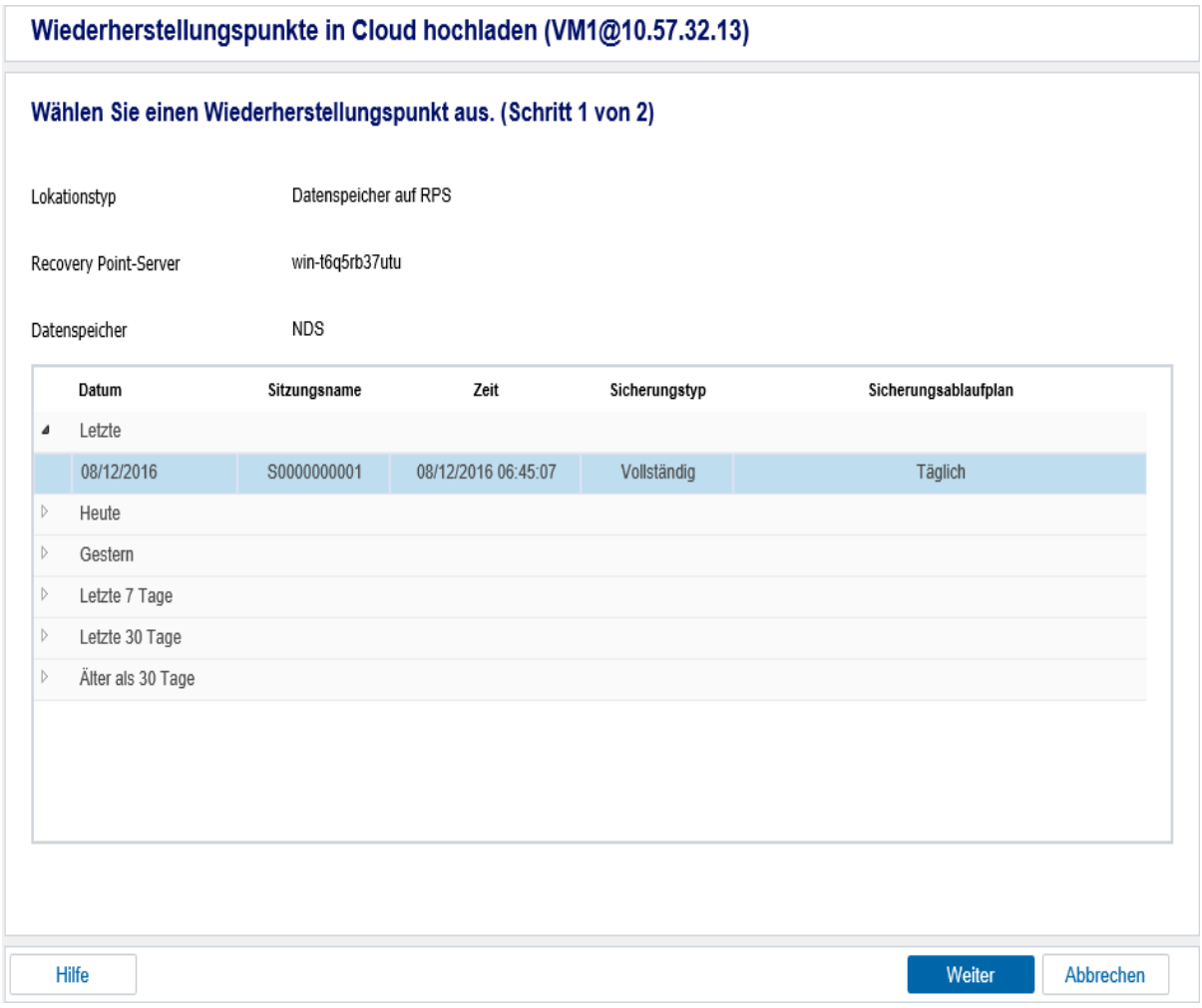
2. Führen Sie eine der folgenden Aktionen durch:

   - Klicken Sie mit der rechten Maustaste auf den Knotennamen.
   - Wählen Sie den Knotennamen aus, und klicken Sie im mittleren Fensterbereich auf das Drop-down-Menü **Aktionen**.

3. Klicken Sie auf **Hochladen von Wiederherstellungspunkten in die Cloud**.

   Das Dialogfeld **Hochladen von Wiederherstellungspunkten in die Cloud** wird geöffnet.

   Sie können den gewünschten Wiederherstellungspunkt in zwei Schritten in die Cloud hochladen.



4. In Schritt 1 wählen Sie einen **Wiederherstellungspunkt** aus und klicken dann auf **Weiter**.

   Der nächste Bildschirm des Uploads wird angezeigt.

5. Geben Sie in Schritt 2 die nachfolgenden Informationen an, und klicken Sie auf **Fertigstellen**.
   a. Wählen Sie den **Speicherdienst** aus der Drop-down-Liste aus.
   b. Wählen Sie den **Cloud-Speicher** aus der Drop-down-Liste aus.

      Hinweis: Wenn zuvor kein Cloud-Konto hinzugefügt wurde, klicken Sie auf **Hinzufügen**, um das Cloud-Konto hinzuzufügen.
   c. Wählen Sie den Komprimierungstyp aus der Drop-down-Liste aus.
   d. Wählen Sie die Art des **Verschlüsselungsalgorithmus** aus.
   e. Geben Sie zweimal das **Verschlüsselungskennwort** ein.

   Hinweis: Ein Bucket/Container wird mit der Namenskonvention *arcserve- {zufällig generierteid} - <BucketName>* erstellt. Allerdings erstellt jeder Job zum *Hochladen von Wiederherstellungspunkten in die Cloud* einen neuen Bucket/Container mit eindeutiger *{zufällig generierte id}* ID. Die genauen Bucket-/Containernamen finden Sie im Jobaktivitätsprotokoll.

   Der Wiederherstellungspunkt wird in die Cloud hochgeladen.

Kopieren von Wiederherstellungspunkten auf einen lokalen Datenträger oder eine Netzwerkfreigabe

Mithilfe dieser Funktion können Sie Wiederherstellungspunkte von Sicherungszielen wie RPS\lokalen Freigaben\Remote-Freigaben auf lokale oder Remote-Ziele kopieren.

Wichtig! Sie benötigen einen Knoten, für den ein Sicherungsplan konfiguriert und eine qualifizierte Sicherungssitzung verfügbar ist, um einen Kopiervorgang zu einer lokalen oder Remote-Freigabe vorzunehmen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite **Knoten: Alle Knoten** wird angezeigt.

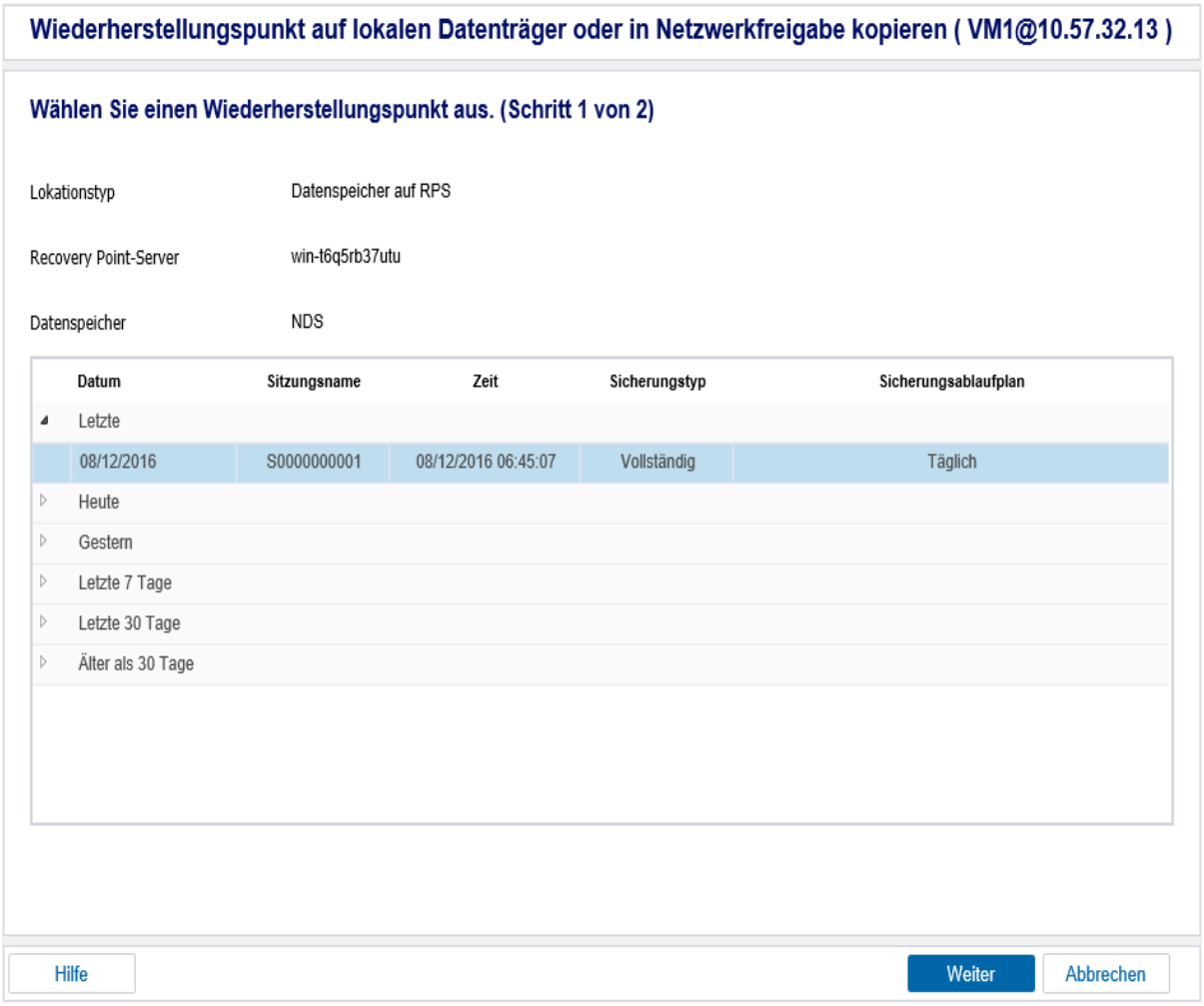
2. Führen Sie eine der folgenden Aktionen durch:

   - Klicken Sie mit der rechten Maustaste auf den Knotennamen.
   - Wählen Sie den Knotennamen aus, und klicken Sie im mittleren Fensterbereich auf das Drop-down-Menü **Aktionen**.

3. Klicken Sie auf **Kopieren von Wiederherstellungspunkten auf einen lokalen Datenträger oder eine Netzwerkfreigabe**.

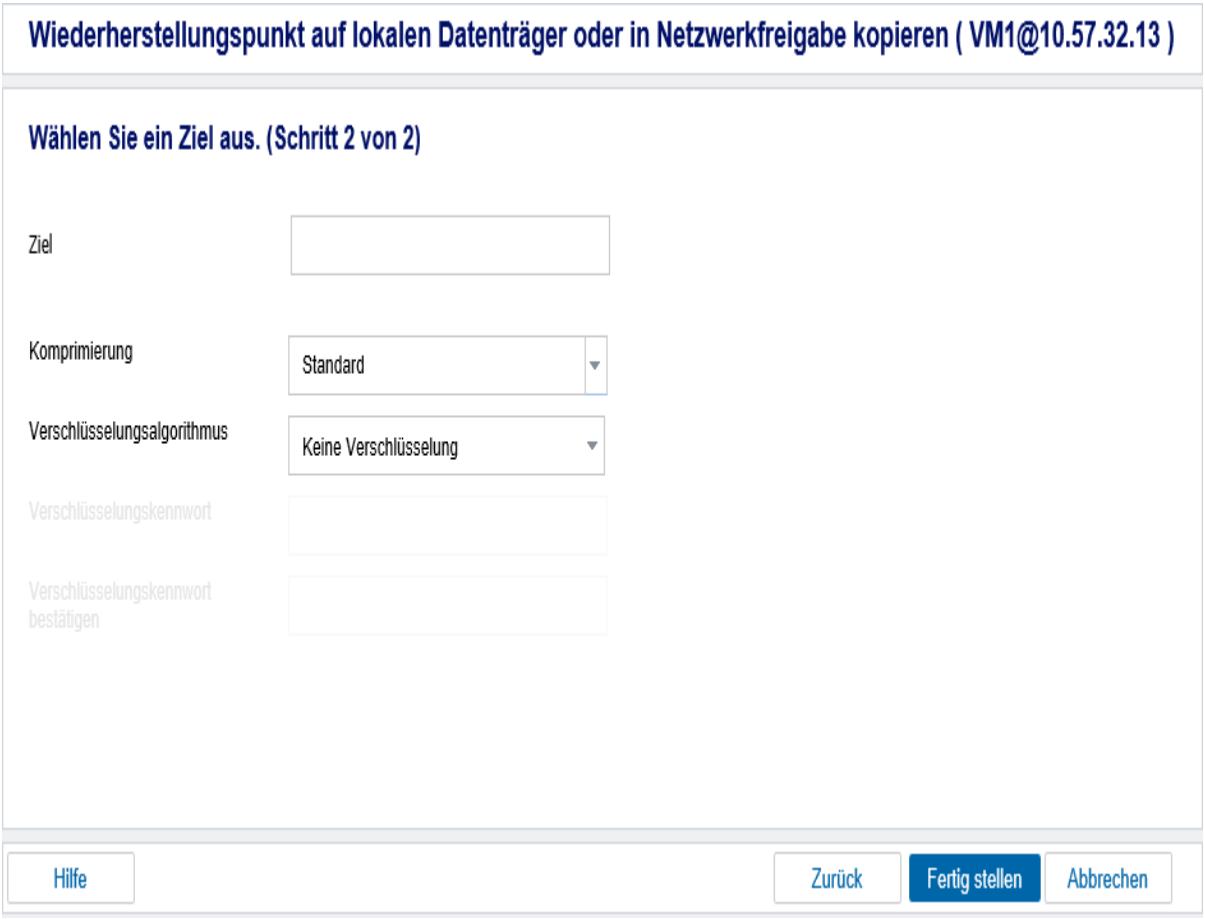
   Das Dialogfeld **Kopieren von Wiederherstellungspunkten auf einen lokalen Datenträger oder eine Netzwerkfreigabe** wird geöffnet.

   Sie können das Kopieren von Wiederherstellungspunkten auf einen lokalen Datenträger oder eine Netzwerkfreigabe in zwei Schritten vornehmen.



4. In Schritt 1 wählen Sie einen **Wiederherstellungspunkt** aus und klicken dann auf **Weiter**.

   Der nächste Bildschirm zum Kopieren von Wiederherstellungspunkten wird angezeigt.



5. Geben Sie in Schritt 2 die nachfolgenden Informationen an, und klicken Sie auf **Fertigstellen**.
   a. Geben Sie ein **Ziel** ein.

      Hinweis: Wenn Sie ein Remote-Ziel eingegeben haben, das validiert werden muss, wird nach Klicken auf **Fertig stellen** das Dialogfeld **Verbinden** angezeigt. Geben Sie Details ein, damit das Ziel validiert wird.

   b. Wählen Sie eine Art von **Komprimierung** aus.
   c. Wählen Sie die Art des **Verschlüsselungsalgorithmus** aus.
   d. Geben Sie zweimal das **Verschlüsselungskennwort** ein.

Der Wiederherstellungspunkt wird aus der Cloud kopiert.

Hinzufügen eines Speicher-Arrays

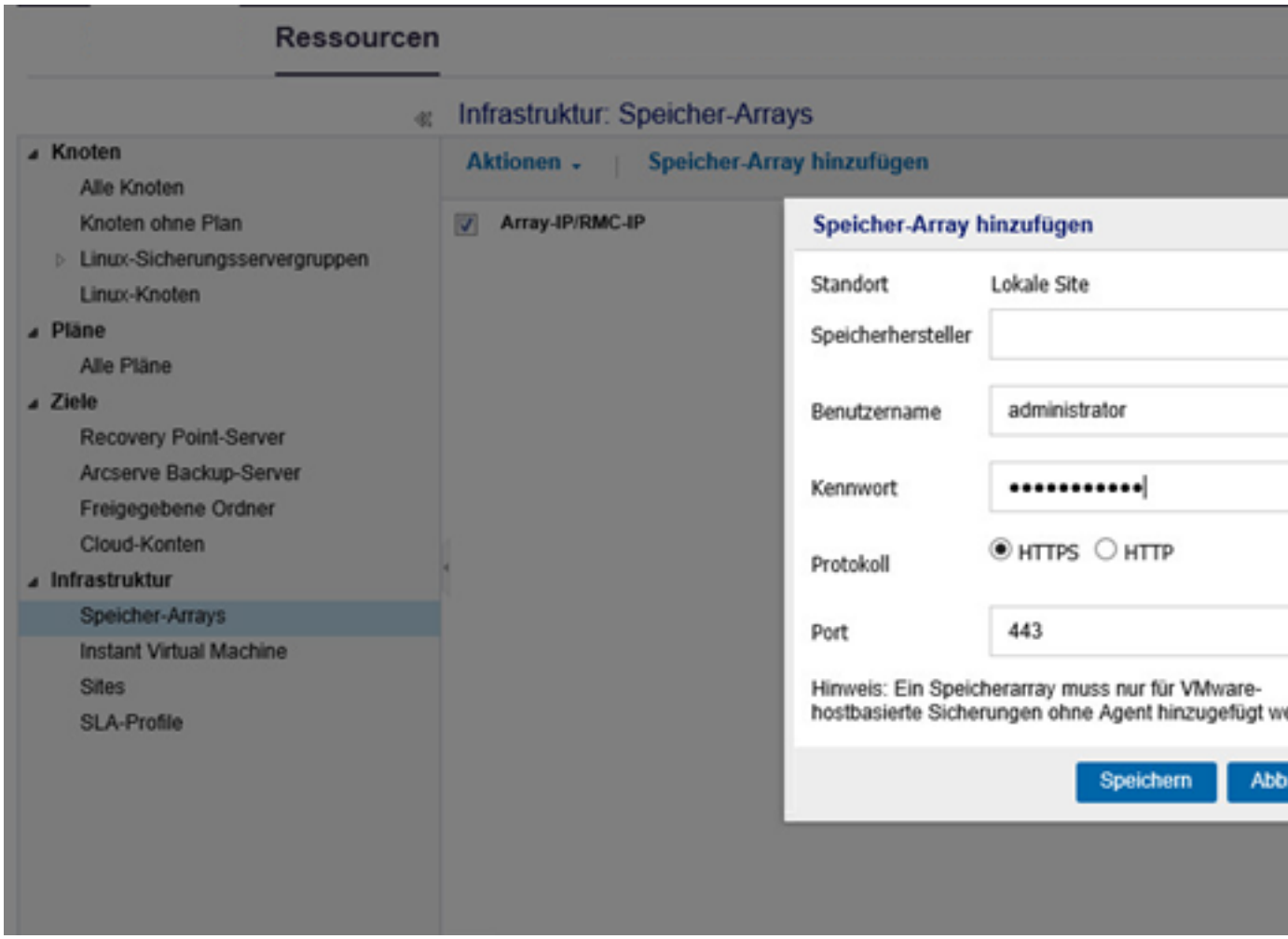
Wenn Sie Hardware-Snapshots verwenden, müssen Sie das Speicher-Array zur Konsole hinzufügen. Wenn Sie kein Speicher-Array hinzufügen und einen Sicherungsjob per Hardware-Snapshot übergeben, sucht der Sicherungsjob zuerst nach den Speicher-Array-Details in der Konsole. Wenn der Sicherungsjob die Details des Speicher-Arrays nicht finden kann, verwendet der Job einen Software-Snapshot, um Sicherungssitzungen zu erstellen.

Das Hinzufügen eines Speicher-Arrays ist nur bei hostbasierten agentenlosen VMware-Sicherungen erforderlich.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Rufen Sie **Infrastruktur** im linken Fensterbereich auf, und klicken Sie auf **Speicher-Arrays**.

   Das Dialogfeld **Speicher-Array hinzufügen** wird geöffnet.



Sie können Storage-Arrays der folgenden Hersteller hinzufügen:

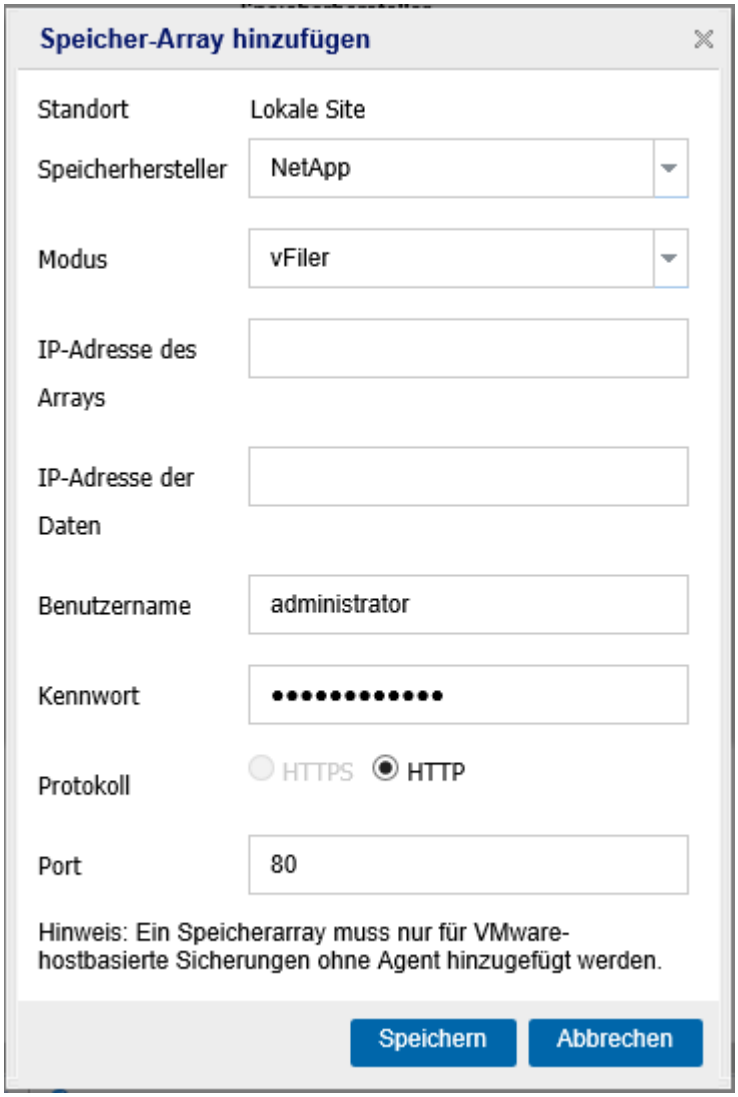
- NetApp
- HPE 3PAR
- Nimble

Hinzufügen eines NetApp-Speicher-Arrays

Sie können ein NetApp-Speicher-Array hinzufügen und dabei aus drei Optionen wählen.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Speicher-Array hinzufügen** im Drop-down-Menü **Speicherhersteller** die Option "NetApp" aus.



2. Wählen Sie unter "Mode" eine der folgenden Optionen für den Array-Typ aus:

Eigenständig

Gibt an, dass das Speicher-Array ein eigenständiges Gerät ist.

Cluster (SVM)

Gibt an, dass das Speicher-Array zu einem Cluster von Arrays gehört.

vFiler

Gibt an, dass das Speicher-Array ein vFiler ist.

3. Geben Sie folgende Details zum Array-Typ an:

Website

Gibt den Namen des Standorts an.

Array-IP

Gibt die IP-Adresse des Speicher-Arrays an. Geben Sie für den 7-Mode die IP-Adresse an, die auf die iSCSI-Schnittstelle und NFS zugreifen kann. VMware (ESXi) verwendet die IP-Adresse, um auf das Speicher-Array für Lese- und Schreibvorgänge zuzugreifen. Für Cluster und vFiler müssen Sie die Management-IP-Adresse des Speicher-Arrays oder die Management-IP-Adresse der Storage Virtual Machine (SVM) angeben.

Informationen zum Ermitteln der Array-IP-Adresse finden Sie im Thema Ermitteln der Array- und Daten-IP des SVM-Speicher-Arrays für die Arcserve UDP-Konsole.

Daten-IP

Geben Sie die Datenzugriffs-IP (logische Schnittstelle) der SVM an, über die die Zielrechner (ESXi) auf dieses Speicher-Array für Lese- und Schreibvorgänge zugreifen können. Diese Option steht nur für Cluster und vFiler zur Verfügung. Wenn die Speicher-VM nur das FC-Protokoll unterstützt, geben Sie "NA" ein.

Informationen zum Ermitteln der Daten-IP-Adresse finden Sie im Thema Ermitteln der Array- und Daten-IP des SVM-Speicher-Arrays für die Arcserve UDP-Konsole.

Benutzername

Gibt den Benutzernamen für Verbindungen mit dem Speicher-Array an.

Kennwort

Gibt das Kennwort für den Benutzernamen an.

Protokoll

Gibt das Protokoll für die Verbindung mit dem Array an.

Port

Gibt die Portnummer des Arrays an.

Standard: 443 (HTTPS), 80 (HTTP)

4. Klicken Sie auf **Speichern**.

Das Speicher-Array wird zur Konsole hinzugefügt.

Ermitteln der Array- und Daten-IP des SVM-Speicher-Arrays für die Arcserve UDP-Konsole

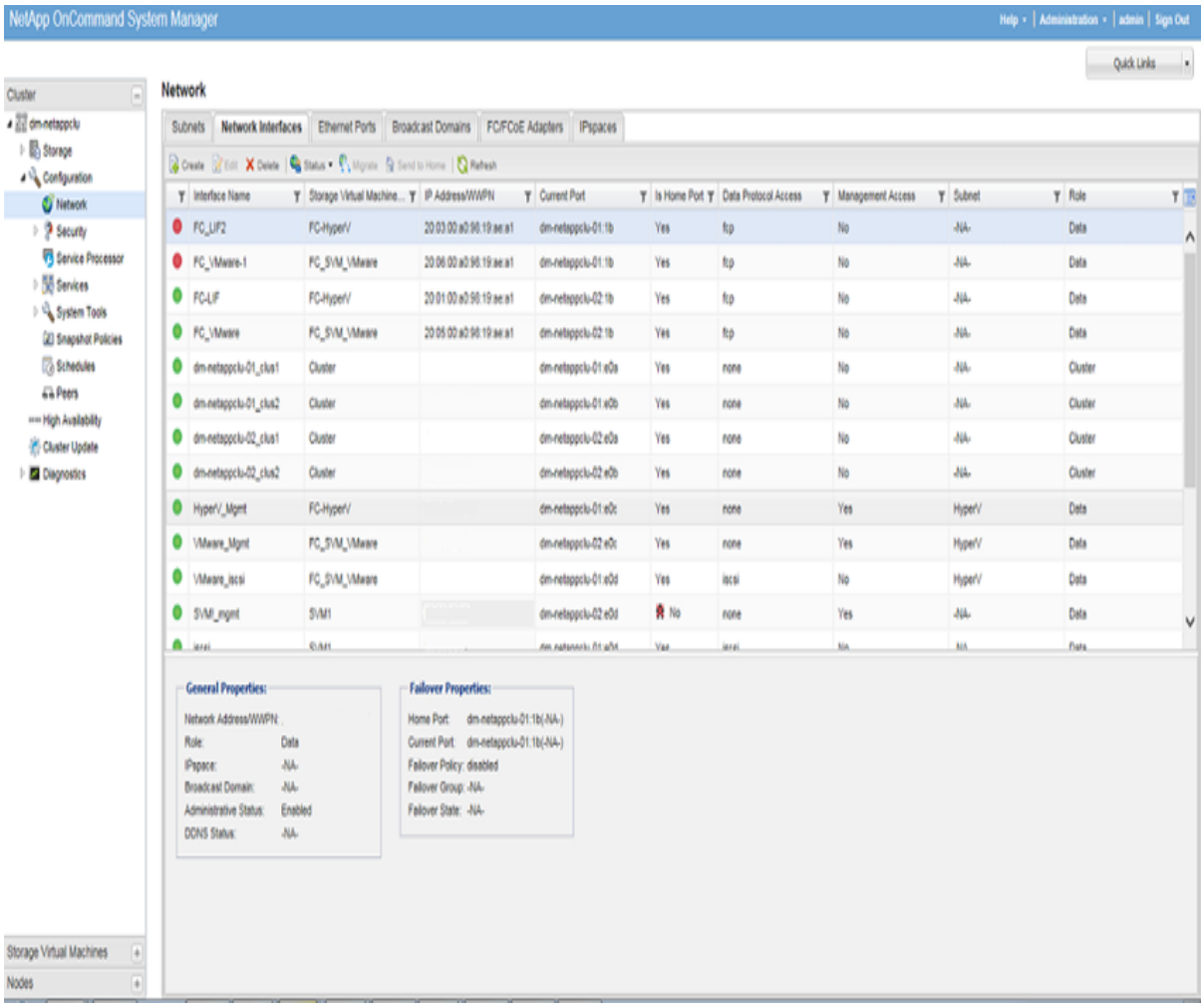
Dieser Abschnitt beschreibt, wie Sie die Array- und Daten-IP finden, wenn das NetApp-Speicher-Array im cDOT-Modus (geclusterter Modus) ausgeführt wird.

Hinweis: Nur für den Cluster (SVM) anwendbar.

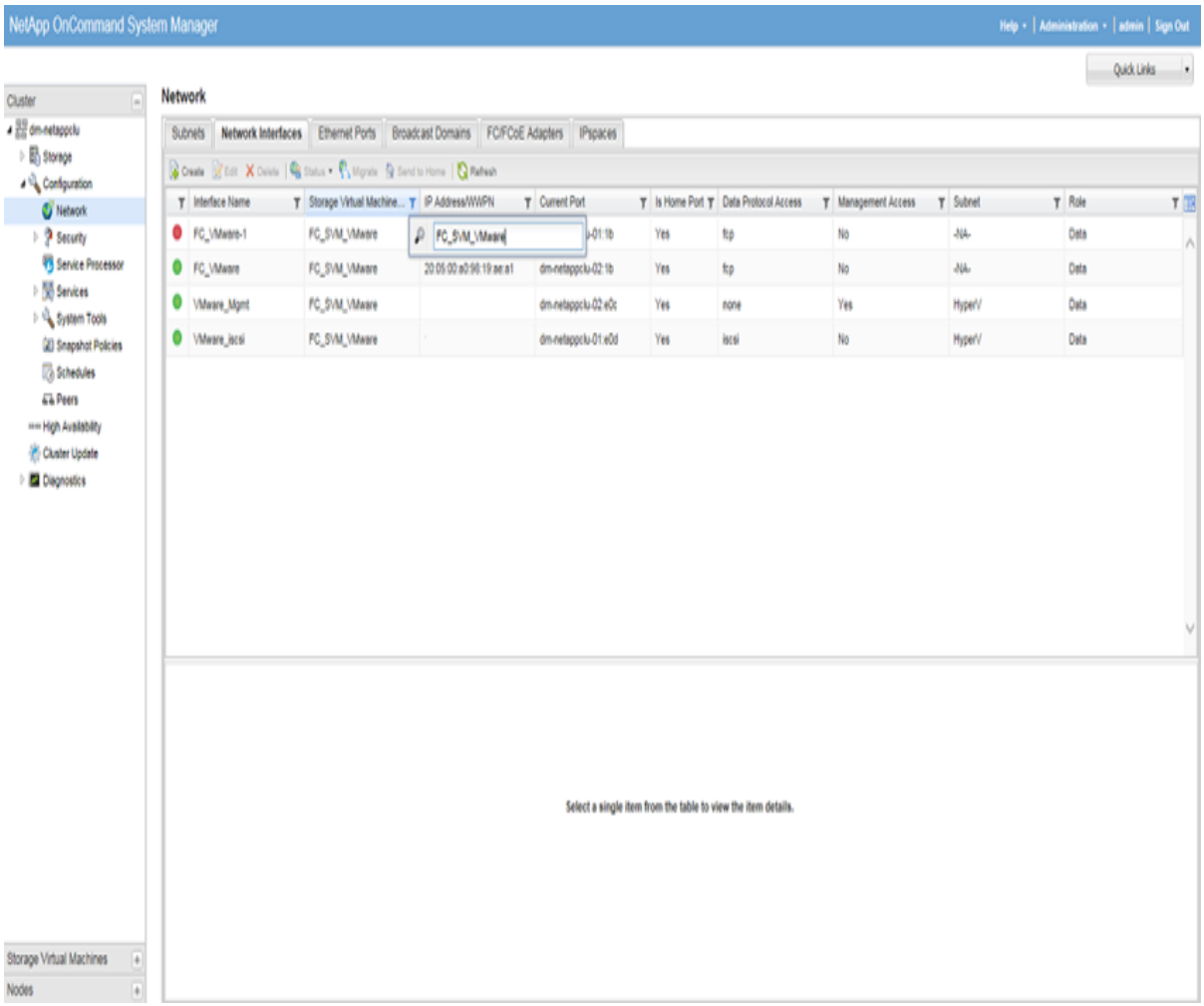
Gehen Sie wie folgt vor:

1. Loggen Sie sich in der NetApp Systemverwaltung ein und melden Sie sich mit gültigen Anmeldeinformationen im Cluster an.
2. Bestimmen Sie den SVM, der zur Arcserve UDP Konsole hinzugefügt werden kann.

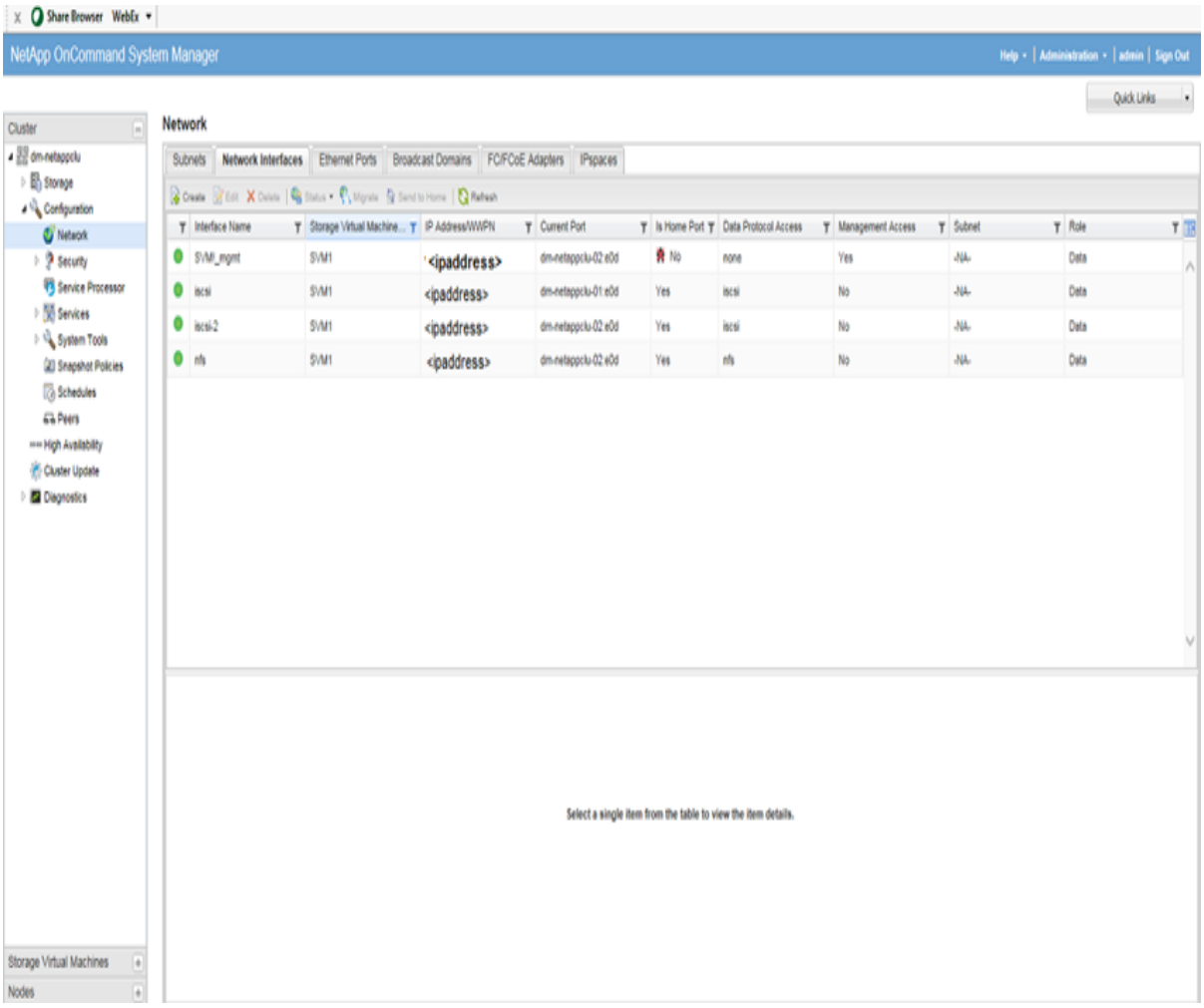
3. Ändern Sie die Ansicht zu "Cluster".
4. Klicken Sie unter Cluster > Konfiguration auf "Netzwerk" und öffnen Sie die Netzwerkschnittstellen.

5. 

6. Filtern Sie die SVM anhand der identifizierten SVM.

7. 

8. Stellen Sie fest, welche Schnittstelle die Management-Zugriffs-IP-Adresse und die Datenprotokollzugriffs-IP-Adresse besitzt, und geben Sie sie unter "Speicher-Array hinzufügen" in der UDP-Konsole ein.
   - Rufen Sie die Management-Zugriffs-IP-Adresse ab:
     - Suchen Sie die Schnittstelle, die die Option **Ja** in der Spalte **Management-Zugriff** enthält.
     - Wählen Sie in der Benutzeroberfläche die IP-Adresse aus, die unter **IP-Adresse/WWPN** verfügbar ist.
   - Rufen Sie die Datenprotokoll-Zugriffs-IP-Adresse ab:
     - Suchen Sie die Schnittstelle, die die Option **iSCSI** oder **NFS** in der Spalte **Datenprotokoll** enthält.
     - Wählen Sie für die ISCSI oder NFS-Schnittstelle die entsprechende IP-Adresse aus, die unter **IP-Adresse/WWPN** verfügbar ist.



Hinweis: Der ESXi Server muss dieselbe Datenprotokollzugang-IP-Adresse für das Lesen und Schreiben auf den NetApp Speicher-Array für iSCSI oder NFS verwenden.

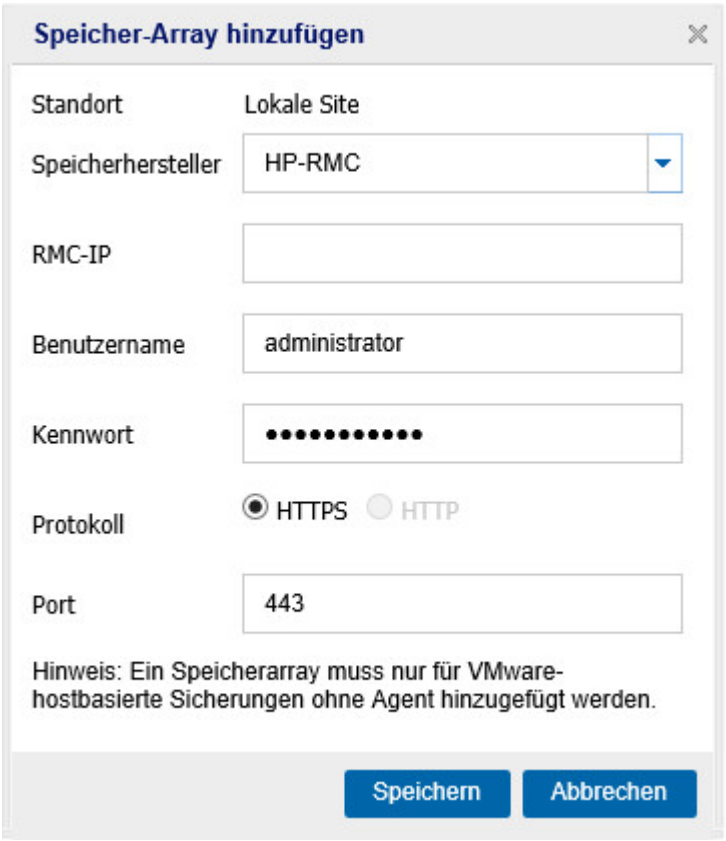
Details von HPE RMC hinzufügen, das ein HPE 3PAR Storeserv Speicher-Array verwaltet

Sie können Details von HPE RMC hinzufügen, das ein HPE 3PAR Storeserve Array verwaltet.

Wichtig! HPE 3PAR StoreServ muss von HP RMC verwaltet werden.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Speicher-Array hinzufügen** im Drop-down-Menü **Speicherhersteller** die Option "HP-RMC" aus.



2. Geben Sie folgende Details an:

RMC-IP

Gibt die HPE RMC-Management-IP-Adresse an.

Benutzername

Gibt den Benutzernamen für Verbindungen mit dem Speicher-Array an.

Kennwort

Gibt das Kennwort für den Benutzernamen an.

Protokoll

Gibt das Protokoll für die Verbindung mit dem Array an.

Hinweis: Es wird nur HTTPS unterstützt.

Port

Gibt die Portnummer des Arrays an.

Standard: 443

3. Klicken Sie auf **Speichern**.

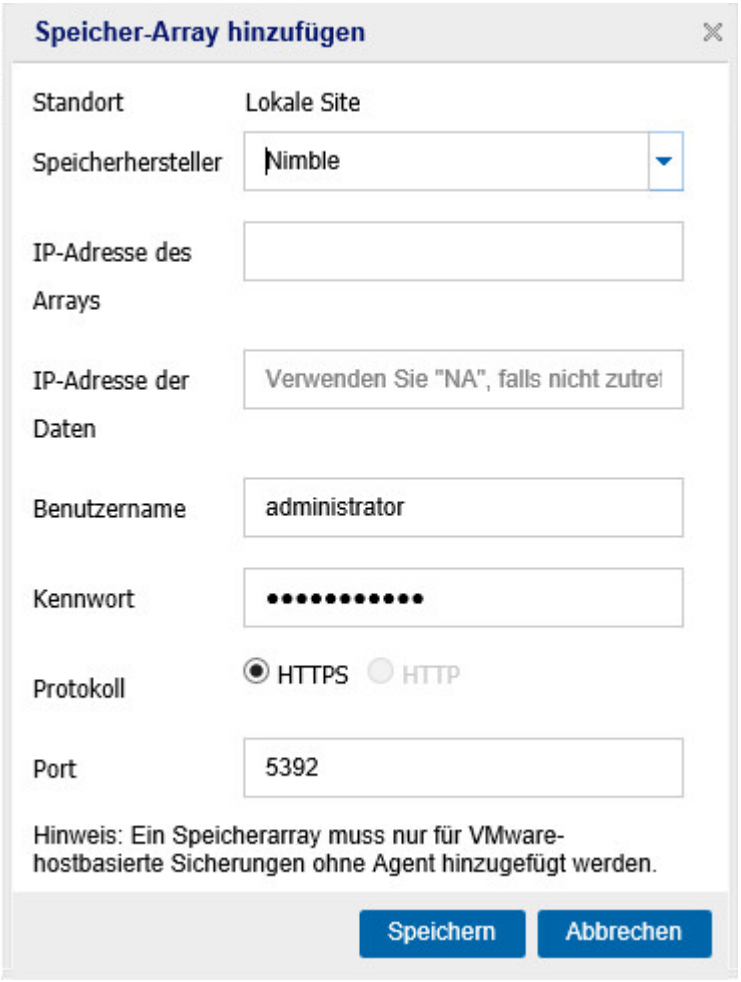
Das Speicher-Array wird zur Konsole hinzugefügt.

Hinzufügen eines Nimble-Speicher-Arrays

Sie können ein Nimble-Speicher-Array hinzufügen.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Speicher-Array hinzufügen** im Drop-down-Menü **Speicherhersteller** die Option "Nimble" aus.



2. Geben Sie folgende Details zum Array-Typ an:

Array-IP

Gibt die IP-Adresse des Speicher-Arrays an. Geben Sie die Management-IP-Adresse des Nimble-Speicher-Arrays ein.

Daten-IP

Gibt die Datenzugriffs-IP (logische Schnittstelle) des Nimble-Speicher-Arrays an, über die die Zielrechner (ESXi) auf dieses Speicher-Array für Lese- und Schreibvorgänge zugreifen können. Wenn das Nimble-Speicher-Array nur das FC-Protokoll unterstützt, geben Sie "NA" ein.

Benutzername

Gibt den Benutzernamen für Verbindungen mit dem Speicher-Array an.

Kennwort

Gibt das Kennwort für den Benutzernamen an.

Protokoll

Gibt das Protokoll für die Verbindung mit dem Array an.

Hinweis: Es wird nur HTTPS unterstützt.

Port

Gibt die Portnummer des Arrays an.

Standard: 5392

3. Klicken Sie auf **Speichern**.

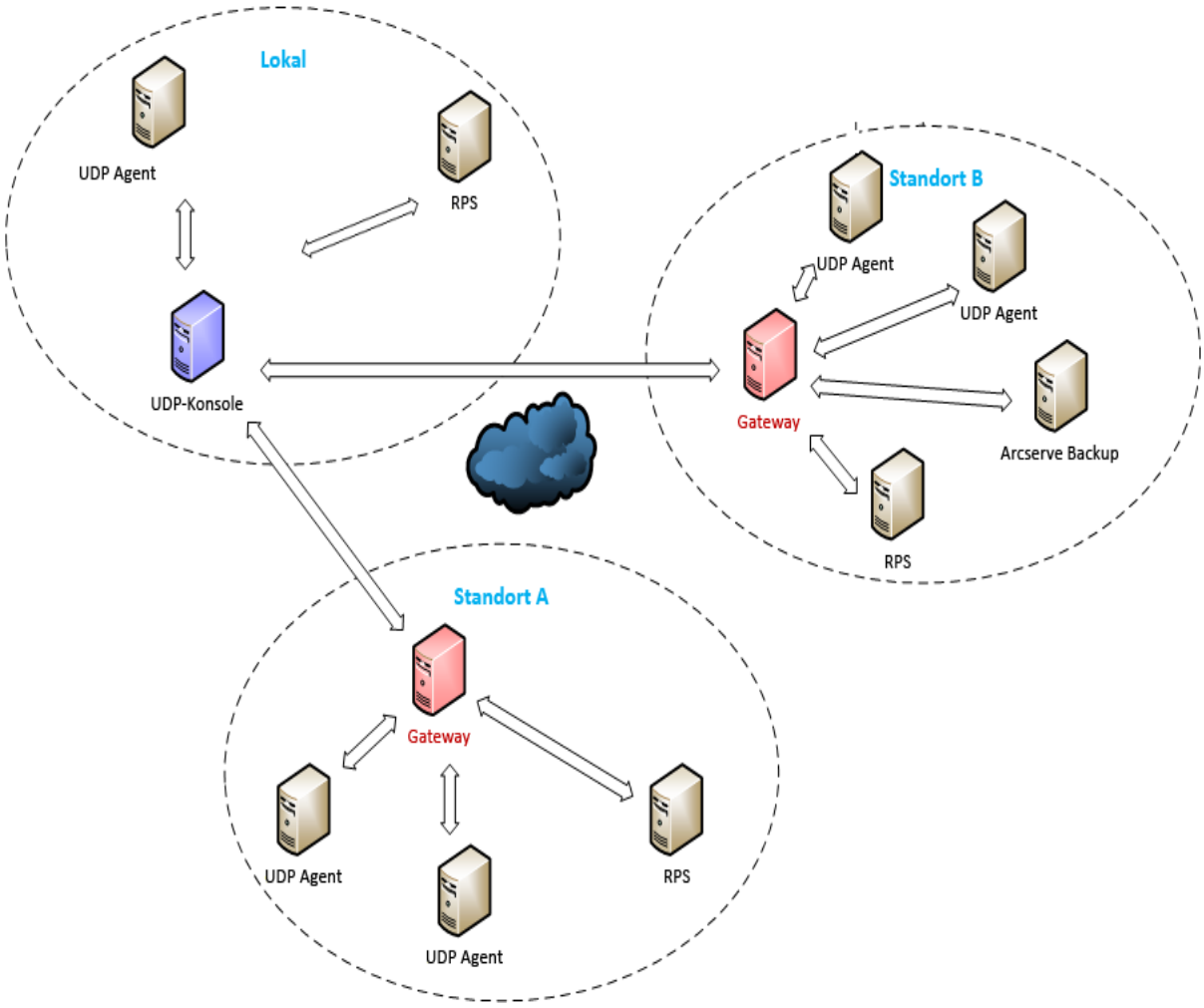
Das Speicher-Array wird zur Konsole hinzugefügt.

So fügen Sie einen Standort hinzu und verwalten ihn

Die Arcserve UDP-Konsole kann Remote-Knoten und -Recovery Point Server aus einem anderen Subnetz über ein WAN verwalten. Die Remote-Knoten und -Server an einem Standort interagieren mit der Konsole mithilfe eines Gateways. Das Gateway wird an Standorten installiert. Obwohl die Konsole keine direkte Verbindung mit den Remote-Knoten herstellen kann, verwendet Arcserve UDP das Gateway, um eine Verbindung zwischen der Konsole und den Knoten herzustellen.

Wichtig! Wenn die Wiederherstellungspunkte sich an einem Remote-Standort befinden, muss die Konsole über eine VPN-Verbindung mit dem Remote-Standort verbunden werden.

Das folgende Diagramm zeigt die Verbindung zwischen lokalen Rechnern und Standorten.



Nachdem Sie einen Standort hinzugefügt haben, können Sie Standorte ändern, aktualisieren oder aus der Konsole löschen. Außerdem können Sie die Remote-Knoten über die Konsole verwalten.

Angeben des Standortnamens

Auf der Seite "Standortname" können Sie einen Namen für den Standort angeben und ein Heartbeat-Intervall auswählen. Dieser Standortname wird auf der Konsole angezeigt.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Infrastrukturen**, und klicken Sie auf **Standorte**.

   Die Infrastruktur: Die Seite Remote-Sites wird im mittleren Bereich geöffnet.
3. Klicken Sie auf **Standort hinzufügen**.

   Der Assistent **Standort hinzufügen** wird geöffnet.
4. Geben Sie auf der Seite "Standort" folgende Details an.

   Standortname

   Geben Sie einen Namen für den Standort an.

   Heartbeat-Intervall

   Wählen Sie aus der Dropdown-Liste ein Zeitintervall für den Heartbeat aus. Der Heartbeat überprüft die Verbindung zwischen der Konsole und dem Standort im angegebenen Intervall.

   UDP-Konsolen-Verbindungs-URL

   Gibt die URL der UDP-Konsole an. Der Gateway-Server stellt eine Verbindung zu dieser URL her.

   UDP-Konsolen-Verbindungs-URL speichern

   Aktivieren Sie dieses Kontrollkästchen, damit die UDP-Konsolen-Verbindungs-URL gespeichert wird.
5. Klicken Sie auf **Weiter**.

   Die Seite "Arcserve Remote Management Gateway-Installationsanweisungen" wird geöffnet.

   Sie haben den Namen für den Remote-Standort angegeben.

Anweisung zur Freigabe der Registrierung

Die Anweisung zur Freigabe der Registrierung enthält Informationen zum Herunterladen und Installieren des Gateways. Die Download-Anweisungen werden an den Remote-Administrator gesendet. Der Remote-Administrator muss die Download-Informationen zum Herunterladen und Installieren das Gateway verwenden.

Gehen Sie wie folgt vor:

1. Kopieren Sie die Anweisungen, und speichern Sie sie als Referenz.

   Wenn Sie die Arcserve UDP-E-Mail nicht konfiguriert haben, senden Sie die kopierten Anweisungen mit einem anderen E-Mail-Server an den Remote-Administrator.

2. Wählen Sie **Senden Sie Anweisungen per Arcserve UDP-E-Mail**, und geben Sie die E-Mail-Adresse des Remote-Administrators an.

3. Klicken Sie auf **Weiter**.

   Die Seite **Konfiguration** wird geöffnet.

   Sie haben die Registrierungsanweisung erfolgreich freigegeben.

Überprüfen und Hinzufügen des Standorts

Überprüfen Sie die Details, bevor Sie den Standort hinzufügen. Klicken Sie auf **Zurück**, um die vorherigen Seiten aufzurufen.

Gehen Sie wie folgt vor:

1. Geben Sie folgende Details auf der Seite "Bestätigung" an.

   Sie können jegliche Informationen auf den vorherigen Seiten bearbeiten, falls erforderlich.

2. Klicken Sie auf **Fertig stellen**.

   Der Assistent wird geschlossen.

   Der Remote-Standort wird auf der Seite **Infrastruktur: Standorte** erstellt.

   Wenn der Remote-Administrator Arcserve Remote Management Gateway installiert und erfolgreich den Gateway-Autorisierungscode angibt, wird ein grünes Häkchen neben dem Standortnamen auf der Konsole angezeigt.

   Sie haben erfolgreich einen Standort hinzugefügt.

Ändern der Konsolen-URL

Wenn Sie die Konsolen URL ändern, muss das Gateway erneut registriert werden, um den Standort über die Konsole verwalten zu können. Die Registrierung des Gateways übernimmt der Remote-Administrator. Wenn Sie die Konsolen-URL aktualisieren, sendet Arcserve UDP eine E-Mail mit detaillierte Anweisungen zur Registrierung des Gateways in der Konsole an den Remote-Administrator.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Infrastruktur**, und klicken Sie auf **Standorte**.

   Die Seite **Infrastruktur: Standort** wird im mittleren Fensterbereich geöffnet.
3. Wählen Sie den Standort aus, und klicken Sie auf **Aktionen**, **Konsolen-URL aktualisieren**.

   Das Dialogfeld **Konsolen-URL aktualisieren** wird geöffnet.
4. Geben Sie die neue URL der Konsole an.
5. Klicken Sie auf **Senden**.

   Eine E-Mail wird an den Remote-Administrator gesendet. Wenn der Remote-Administrator die neue URL auf dem Gateway-Server aktualisiert, zeigt die Konsole ein grünes Häkchen neben dem aktualisierten Standort an.

   Sie haben die Konsolen-URL erfolgreich geändert.

Ändern des Standorts

Sie können den Standort bearbeiten, um Parameter des hinzugefügten Standorts zu ändern. Sie können den Standort z. B. umbenennen oder das Heartbeat-Intervall ändern.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Infrastruktur**, und klicken Sie auf **Standorte**.

   Die Seite **Infrastruktur: Standort** wird im mittleren Fensterbereich geöffnet.
3. Wählen Sie den Standort aus, und klicken Sie auf **Aktionen**, **Ändern**.

   Der Assistent **Standort ändern** wird geöffnet.
4. Verwenden Sie **Zurück** und **Weiter**, um die Seiten aufzurufen und Parameter zu ändern.
5. Klicken Sie auf **Fertig stellen**.

   Der Assistent **Standort ändern** wird geschlossen.

   Sie haben den Standort erfolgreich geändert.

Löschen eines Standorts

Sie können einen Standort löschen, der nicht verwaltet werden soll. Bevor Sie einen Standort löschen, müssen zuerst alle Knoten und Knotenerkennungsfilter im Zusammenhang mit diesem Standort gelöscht werden.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Infrastruktur**, und klicken Sie auf **Standorte**.

   Die Seite **Infrastruktur: Standort** wird im mittleren Fensterbereich geöffnet.
3. Wählen Sie den Standort aus, und klicken Sie auf **Aktionen**, "Löschen".

   Das Dialogfeld **Bestätigen** wird geöffnet.
4. Klicken Sie auf **Ja**.

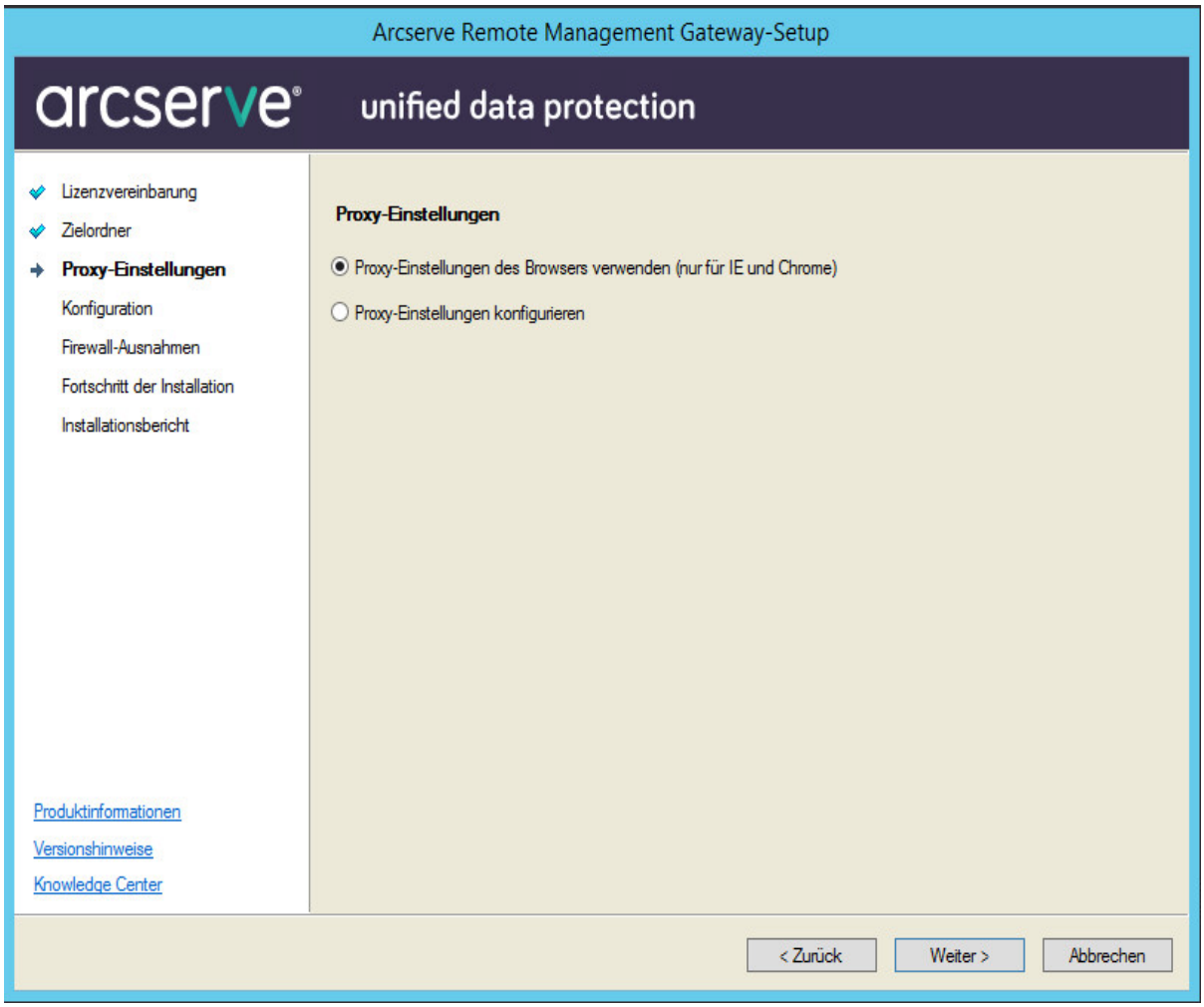
   Der Standort wird gelöscht.

Einrichten eines Proxy-Servers für das Gateway

Arcserve UDP unterstützt die Installation eines Proxy-Servers auf dem Gateway-Rechner. Das Gateway verwendet diese Proxy-Einstellung zur Kommunikation mit seiner registrierten Konsole.

Gehen Sie wie folgt vor:

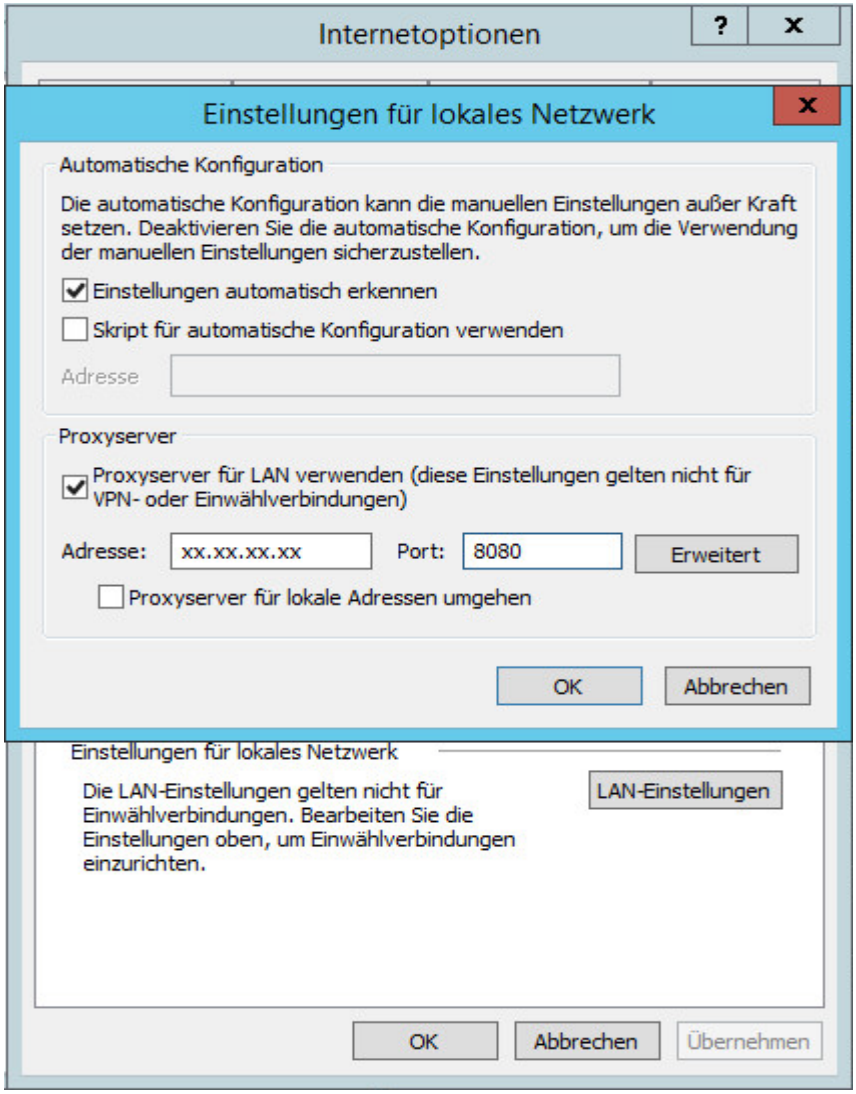
1. Öffnen Sie den Setup-Assistenten für Arcserve Remote Management Gateway.



2. Wählen Sie im Dialogfeld "Proxy-Einstellungen" eine der beiden folgenden Optionen aus:

   Proxy-Einstellungen des Browsers verwenden (nur für IE und Chrome)

Gibt an, dass die Proxy-Einstellungen des Browsers verwendet werden sollen. Sie müssen die Proxy-Einstellungen des Browsers aktualisieren. Öffnen Sie den Browser, und klicken Sie auf **Optionen**, **Verbindung**, **LAN-Einrichtung**.



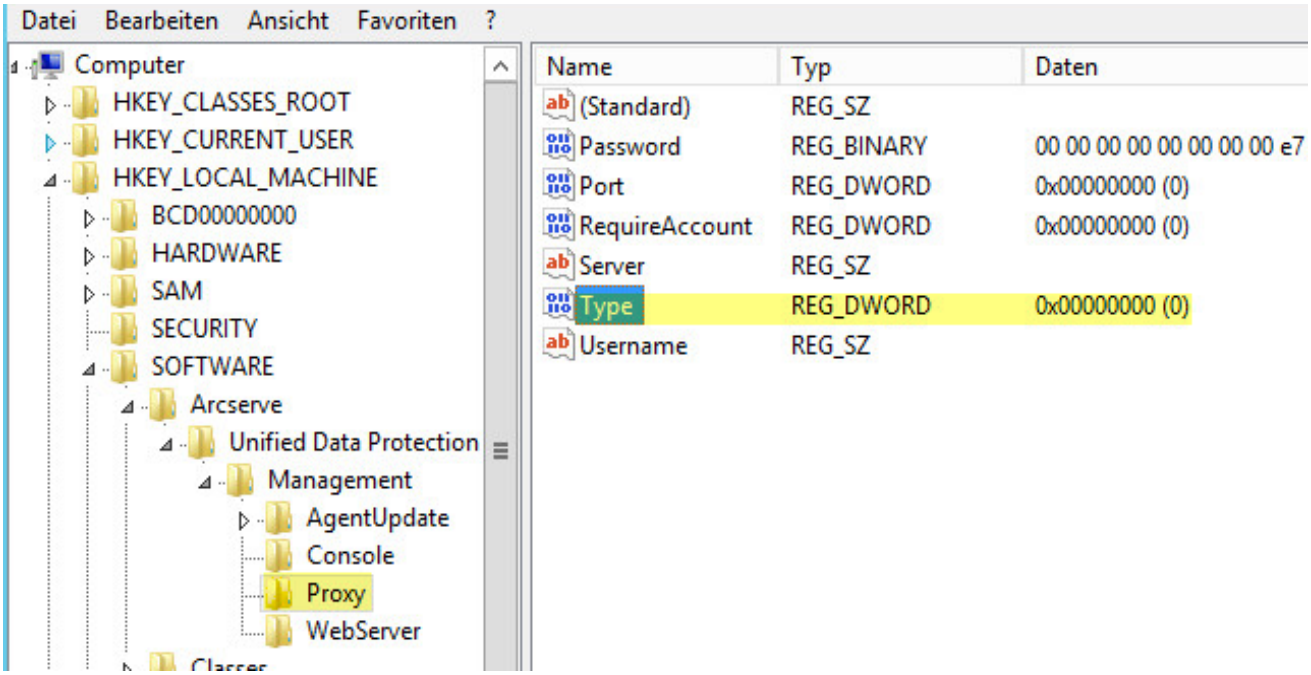
Proxy-Einstellungen konfigurieren

Gibt an, dass Sie die Details zum Proxy-Server auf der Seite des Assistenten angeben müssen.

3. Deaktivieren Sie das Kontrollkästchen "Authentifizierung", wenn der-Proxy keine Anmeldeinformationen unterstützt.

Der Proxy-Server wird für das Gateway eingerichtet.

4. Öffnen Sie Regedit und navigieren Sie zu Proxy, um die Proxy-Einstellung zu überprüfen.



Die 0 im Feld "Typ" gibt Browsereinstellungen an, während die 1 andere Einstellungen anzeigt.

Hinweis: Verwenden Sie Regedit, um jegliche Proxyeinstellungen wie Port, IP-Adresse oder Typ zu ändern.

So verwalten Sie Exchange Online-Knoten

Sie können die Exchange Online-Knoten nicht direkt zur Ansicht "Knoten" hinzufügen. Nach dem Hinzufügen zum Sicherungsplan wird der Exchange Online-Knoten direkt zur Ansicht "Knoten" hinzugefügt.

Sie können die folgenden Tasks durchführen:

1. Hinzufügen eines Exchange Online-Knotens
2. Aktualisieren eines Exchange Online-Knotens
3. Löschen eines Exchange Online-Knotens
4. Postfachunterstützung für öffentliche Ordner für Exchange Online-Schutz

Hinzufügen eines Exchange Online-Knotens

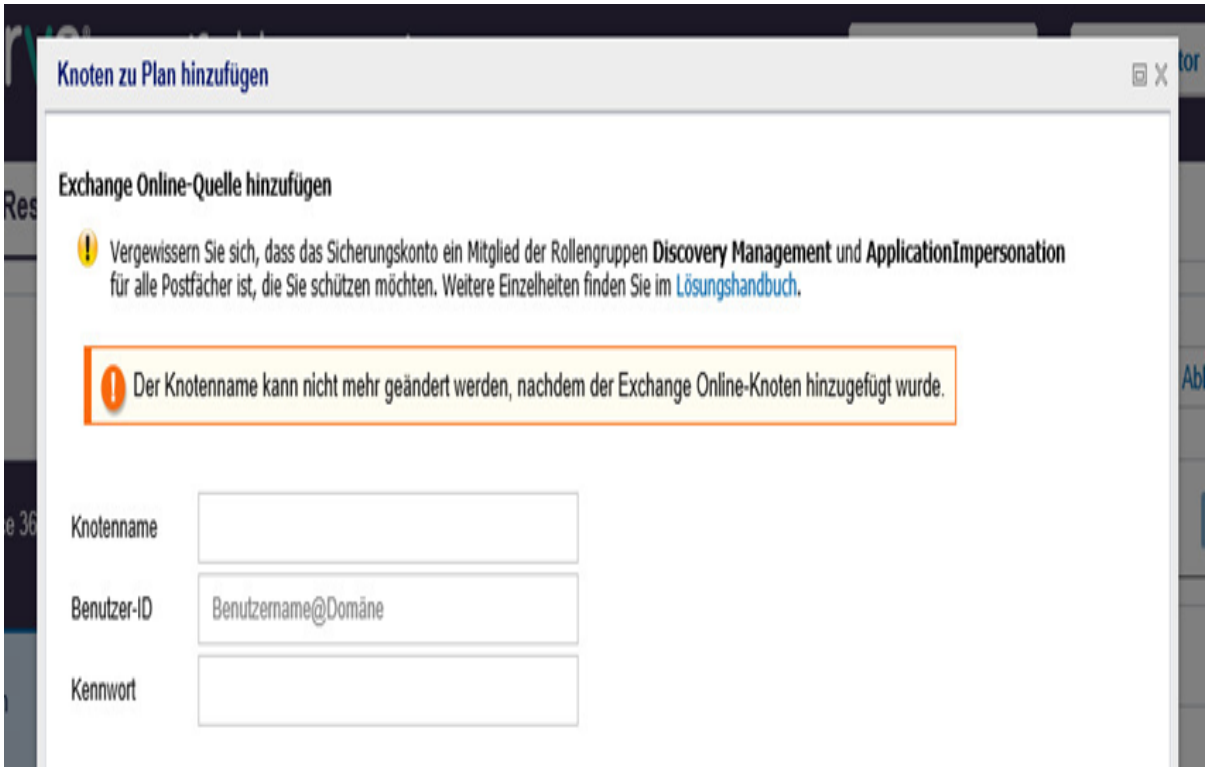
Hinweis: Anders als andere Knoten können Sie Exchange Online-Knoten nicht über die Seite Alle Knoten hinzufügen. Ein Exchange Online-Knoten wird nur in einem Plan oder während der Anpassung eines Plans hinzugefügt.

Informationen zum Erstellen eines Plans finden Sie unter So erstellen Sie einen Exchange Online-Plan.

Gehen Sie wie folgt vor:

1. Geben Sie im Feld "Benutzername" oder "Benutzerkonto" für den Exchange Online-Knoten den Benutzernamen des Exchange Online-Sicherungskontos ein, der die Voraussetzungen erfüllt.

   Mehrere Exchange Online-Knoten können dasselbe Benutzerkonto (Dienstkonto) von Exchange online verwenden. Um den Exchange Knoten nach Plan hinzuzufügen, müssen Sie den Knotennamen, Benutzernamen und das Kennwort angeben. Einmal erstellt, kann der Knotenname des Exchange Online-Knotens nicht geändert werden.



   Hinweis: Das Aktualisieren/Ändern des Benutzerkontos könnte die Anzahl geschützter Postfächer ändern. Stellen Sie sicher, dass das neue/aktualisierte Dienstkonto Identitätswechselrechte für zu schützende Postfächer besitzt.

2. Geben Sie das Kennwort ein, und klicken Sie auf **Verbinden**.

3. Wählen Sie die zu schützenden Exchange Online-Konten aus, und klicken Sie auf den Rechtspfeil (>), um sie zur geschützten Liste zu verschieben.

   Hinweis: Aktivieren Sie das Kontrollkästchen, um alle Office 365 Exchange-Quellen zu schützen, um wiederum alle Exchange Online-Konten auf allen Seiten zu schützen. Um alle auf der Seite aufgeführten Exchange Online-Konten zur geschützten Liste hinzuzufügen, klicken Sie auf den Rechtspfeil (>).

4. Klicken Sie auf **Speichern**.

   Sie können auf der Registerkarte "Quelle" über die Option "Wählen Sie aus der Sicherung auszuschließende Ordner aus" den/die Ordner auswählen, der/die nicht gesichert werden soll(en).

   Die ausgewählten Exchange Online-Konten werden hinzugefügt.

Aktualisieren eines Exchange Online-Knotens

Wenn Sie die Anmeldeinformationen eines Exchange Online-Knotens ändern, aktualisieren Sie den Exchange Online-Knoten über die Konsole.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Exchange Online-Knoten**.

   Die erstellten Exchange Online-Knoten werden im mittleren Fensterbereich angezeigt.
3. Wählen Sie den Exchange Online-Knoten aus, und klicken Sie auf **Aktionen**.
4. Klicken Sie auf **Aktualisieren**.

   Das Dialogfeld **Knoten aktualisieren** wird geöffnet.
5. Ändern Sie die Details nach Bedarf, und klicken Sie auf **OK**.

   Der Exchange Online-Knoten wird aktualisiert.

Löschen eines Exchange Online-Knotens

Sie können alle Exchange Online-Knoten löschen, die Sie nicht mehr benötigen.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie zu **Knoten**, und klicken Sie auf **Exchange Online-Knoten**.

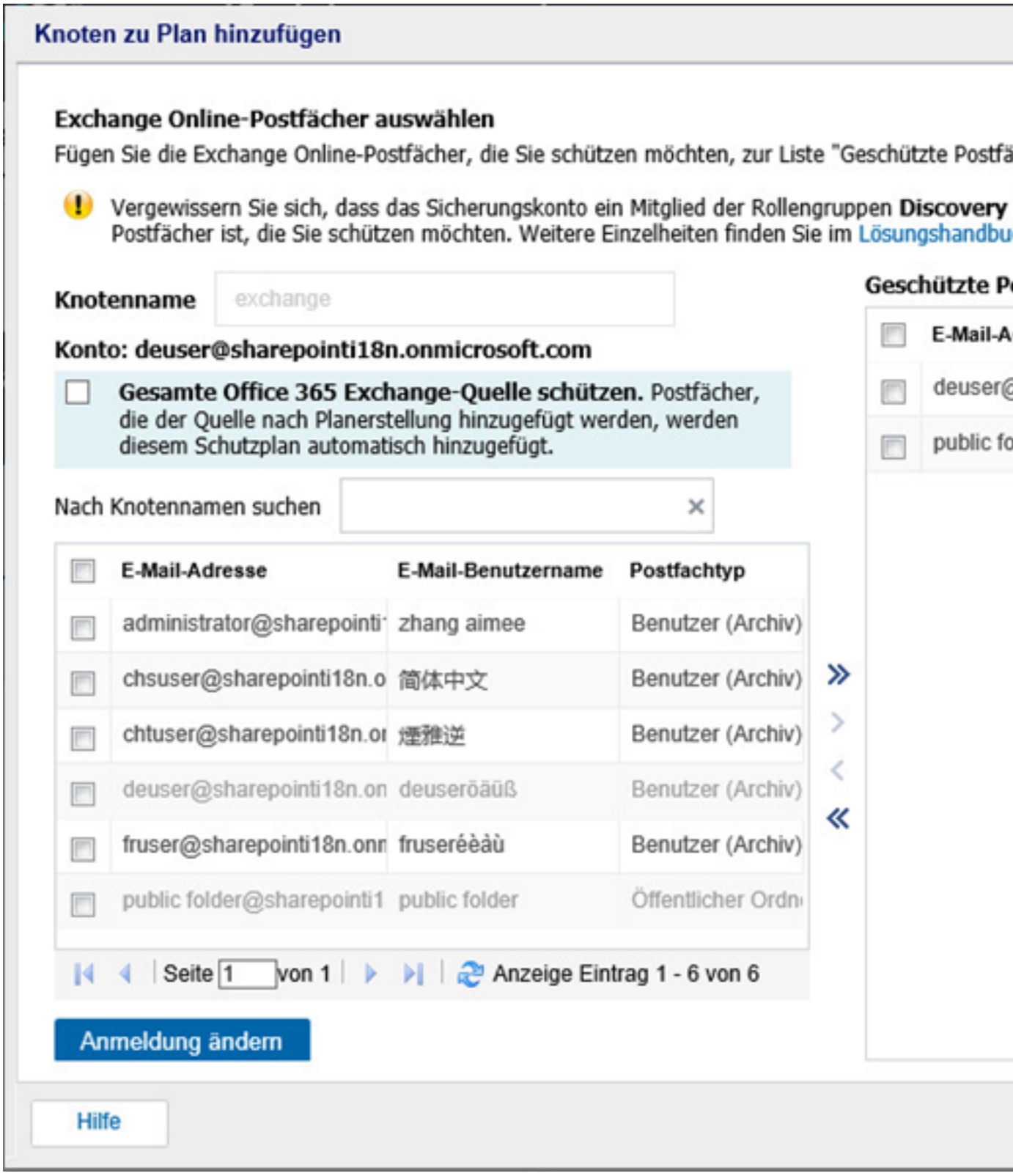
   Die erstellten Exchange Online-Knoten werden im mittleren Fensterbereich angezeigt.
3. Wählen Sie den Exchange Online-Knoten aus, und klicken Sie auf **Aktionen**.
4. Klicken Sie auf **Löschen**.

   Ein Bestätigungsdialogfeld wird angezeigt.
5. Klicken Sie auf **"OK**".

   Der Exchange Online-Knoten wird gelöscht.

Unterstützung für Postfach für öffentliche Ordner für Exchange Online-Schutz

Beim Hinzufügen des Exchange Online-Knotens wird die Spalte Postfachtyp im Fenster **Knoten zu Plan hinzufügen** angezeigt. In diesem Fenster wird Postfach für Öffentliche Ordner und in der Spalte als **Öffentliche Ordner** angezeigt. Um öffentliche Ordner zu schützen, fügen Sie das entsprechende öffentliche Postfach **Geschützte Postfächer** hinzu und speichern Sie den Plan.



Hinweis: Weitere Informationen zu Postfach für öffentliche Ordner in Exchange Online und Berechtigungen finden Sie unter Link 1 und Link 2.

So verwalten Sie SharePoint Online-Knoten

Sie können die SharePoint Online-Knoten nicht direkt zur Ansicht "Knoten" hinzufügen. Nach dem Hinzufügen zum Sicherungsplan wird der SharePoint Online-Knoten direkt zur Ansicht "Knoten" hinzugefügt.

Sie können die folgenden Tasks durchführen:

1. Hinzufügen eines SharePoint Online-Knotens
2. Aktualisieren eines SharePoint Online-Knotens
3. Löschen eines SharePoint Online-Knotens

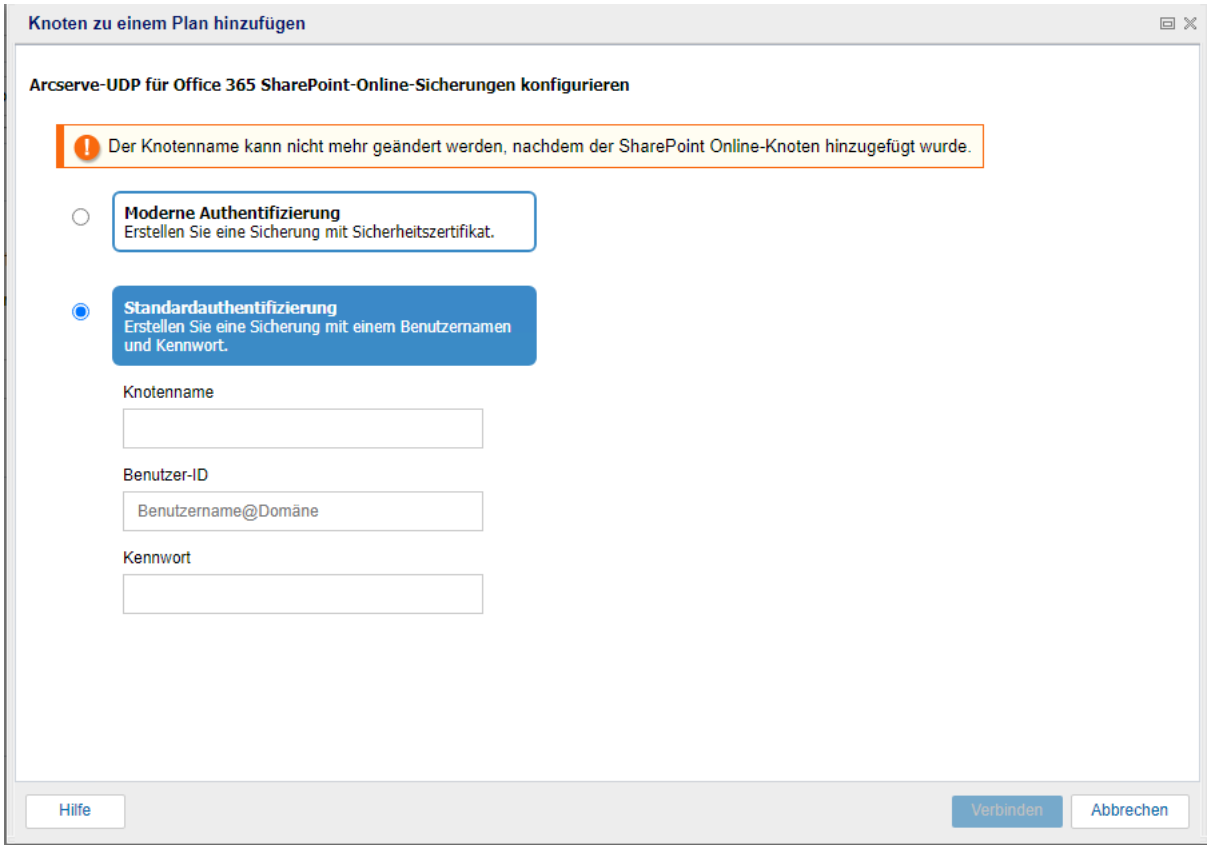
Hinzufügen eines SharePoint Online-Knotens

Hinweis: Anders als andere Knoten können Sie SharePoint Online-Knoten nicht über die Seite "Alle Knoten" hinzufügen. Ein SharePoint Online-Knoten wird nur beim Erstellen oder Ändern eines Plans in einem Plan hinzugefügt.

Informationen zum Erstellen eines Plans finden Sie unter So erstellen Sie einen Sharepoint Online-Plan.

Gehen Sie wie folgt vor:

1. Geben Sie den Benutzernamen des SharePoint-Knoten sowie Websitesammlungs-URL, Benutzername des Websitebesitzers und Kennwort ein.



2. Geben Sie das Kennwort ein, und klicken Sie auf **Verbinden**.
3. Wählen Sie eine SharePoint-Liste/-Bibliothek oder Listenelemente zum Schützen aus.
4. Klicken Sie auf **Speichern**.

   Die ausgewählten SharePoint Online-Konten werden hinzugefügt.

Aktualisieren eines SharePoint Online-Knotens

Wenn Sie die Anmeldeinformationen eines SharePoint Online-Knotens ändern, aktualisieren Sie den SharePoint Online-Knoten über die Konsole.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **SharePoint Online-Knoten**.

   Die erstellten SharePoint Online-Knoten werden im mittleren Fensterbereich angezeigt.
3. Wählen Sie den SharePoint Online-Knoten aus, und klicken Sie auf **Aktionen**.
4. Klicken Sie auf **Aktualisieren**.

   Das Dialogfeld **Knoten aktualisieren** wird geöffnet.
5. Ändern Sie die Details nach Bedarf, und klicken Sie auf **OK**.

   Der SharePoint Online-Knoten wird aktualisiert.

Löschen eines SharePoint Online-Knotens

Löschen Sie alle SharePoint Online-Knoten, die Sie nicht mehr benötigen.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie zu **Knoten**, und klicken Sie auf **SharePoint Online-Knoten**.

   Die erstellten SharePoint Online-Knoten werden im mittleren Fensterbereich angezeigt.
3. Wählen Sie den SharePoint Online-Knoten aus, und klicken Sie auf **Aktionen**.
4. Klicken Sie auf **Löschen**.

   Ein Bestätigungsdialogfeld wird angezeigt.
5. Klicken Sie auf **"OK**".

   Der SharePoint Online-Knoten wird gelöscht.

So verwalten Sie einen OneDrive-Knoten

Sie können die OneDrive Knoten nicht direkt zur Ansicht aller Knoten hinzufügen. Sobald Sie ihn dem Sicherungsplan hinzugefügt haben, wird der OneDrive Knoten direkt zur Ansicht aller Knoten hinzugefügt.

Sie können die folgenden Tasks durchführen:

1. Hinzufügen eines OneDrive-Knotens
2. **Löschen des Knotens:** Klicken Sie in der Option "Aktionen auf OneDrive Knoten" auf **Löschen**, und bestätigen Sie das Popup-Fenster, um den Knoten aus der Konsole zu löschen.
3. **Exportieren des Knotens:** Klicken Sie in der Option "Aktionen auf OneDrive Knoten" auf **Exportieren** und Sie erhalten den Knoten als Zip-Datei.
4. **Ändern eines Plans:** Klicken Sie in der Option "Aktionen auf OneDrive Knoten" auf **Plan ändern**, um den zugehörigen Plan zu öffnen und bei Bedarf zu aktualisieren.
5. **Anmelden bei Agent:** Klicken Sie in der Option "Aktionen auf OneDrive Knoten" auf **Bei Agent anmelden**, um agentenspezifische Aufgaben auszuführen, wie z.B. Wiederherstellen mit der Mount-Volume-Option.
6. **Sicherung jetzt:** Klicken Sie in der Option "Aktionen auf OneDrive Knoten" auf **Jetzt sichern** um die manuelle Sicherung auszuführen.
7. **Wiederherstellen:** Klicken Sie in der Option "Aktionen auf OneDrive Knoten" auf **Wiederherstellen** um sich anzumelden wiederherstellen auszuführen.

8. Herunterladen von Wiederherstellungspunkten aus der Cloud
9. Aktualisieren des Wiederherstellungspunkts in die Cloud
10. Kopieren von Wiederherstellungspunkten auf einen lokalen Datenträger oder eine Netzwerkfreigabe

Hinzufügen eines OneDrive-Knotens

Hinweis: Im Gegensatz zu anderen Knoten können Sie den OneDrive-Knoten nicht auf der Seite "Alle Knoten" hinzufügen. Ein OneDrive-Knoten wird nur in einem Plan hinzugefügt, wenn ein Plan erstellt oder geändert wird.

Informationen zum Hinzufügen des Knotens finden Sie unter "Angeben der Quelle" auf Seite 1078, wenn Sie einen OneDrive Sicherungsplan erstellen.

Löschen eines OneDrive Online-Knotens

Löschen Sie alle OneDrive Online-Knoten, die Sie nicht mehr benötigen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf **Löschen** aus der Option der **Aktionen** auf OneDrive Knoten.
2. Bestätigen Sie das Popup-Fenster, um den Knoten aus der Konsole zu löschen.

   Der OneDrive Online-Knoten wurde erfolgreich gelöscht.

So verwalten Sie Oracle-Datenbankgruppen-Knoten

Mit Arcserve UDP können Sie mehrere Aktionen ausführen, um Oracle-Datenbankknoten zu verwalten, z. B. Knoten aktualisieren, Knoten exportieren, Sicherungsjobs ausführen, Sicherungsjobs abbrechen und Knoten löschen.

In diesem Abschnitt werden die folgenden Themen behandelt:

Aktualisieren des Oracle-Datenbankknotens

Sie können Informationen aktualisieren, die sich auf die vorhandenen Knoten beziehen. Wenn Sie die Anmeldeinformationen der Oracle-Datenbankknoten ändern, müssen Sie die Oracle-Datenbankknoten auf der Konsole aktualisieren.

Befolgen Sie diese Schritte:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite Knoten: Alle Knoten wird angezeigt.
3. Wählen Sie eine der folgenden Vorgehensweisen:

- Navigieren Sie im linken Fensterbereich zu **Knoten**, **Oracle-Datenbankgruppe**, klicken Sie mit der rechten Maustaste auf den Knoten, den Sie aktualisieren möchten, und klicken Sie dann auf **Aktualisieren**.
- Wählen Sie im mittleren Fensterbereich den Knoten aus, der aktualisiert werden soll, klicken Sie auf die Drop-down-Liste **Aktionen** und anschließend auf **Aktualisieren**.

Das Dialogfeld Knoten aktualisieren wird geöffnet.

5. Ändern Sie im Dialogfeld "Knoten aktualisieren" die Details nach Bedarf, und klicken Sie dann auf **OK**.

   Der Knoten "Oracle-Datenbank" wird aktualisiert.

Exportieren von Knoten

Sie können die Knoten als ZIP (.zip)-Dateien exportieren. Bei Bedarf können Sie die ZIP-Datei importieren, um die Knoten aufzubewahren. Wenn Sie zum Beispiel die Knoten vor den Upgrades oder vor dem Neustart exportieren, ist dies für das Importieren des gleichen Satzes an Knoten hilfreich.

Sie können nur Knoten exportieren, die über gültige Anmeldeinformationen verfügen und unter Windows ausgeführt werden.

Befolgen Sie diese Schritte:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite Knoten: Alle Knoten wird angezeigt.
3. Wählen Sie eine der folgenden Vorgehensweisen:
   - Navigieren Sie im linken Fensterbereich zu **Knoten**, **Oracle-Datenbankgruppe**, klicken Sie mit der rechten Maustaste auf den Knoten, den Sie exportieren möchten, und klicken Sie dann auf **Exportieren**.
   - Wählen Sie im mittleren Fensterbereich den Knoten aus, der exportiert werden soll, klicken Sie auf die Drop-down-Liste **Aktionen** und anschließend auf **Exportieren**.

   Ein Dialogfeld wird geöffnet, in dem Sie dazu aufgefordert werden, eine Aktion für die Datei "list.zip" durchzuführen.
4. Klicken Sie auf **Öffnen** oder **Speichern**.

   Die Knotenliste wird exportiert.

Oracle-Datenbankknoten sichern

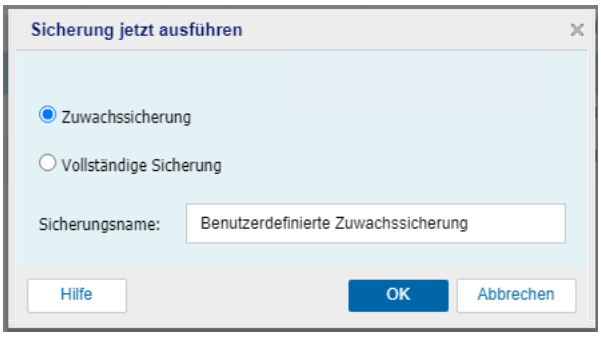
Normalerweise werden Ihre Sicherungen automatisch durchgeführt und von den Ablaufplan-Einstellungen gesteuert. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern.

Befolgen Sie diese Schritte:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite Knoten: Alle Knoten wird angezeigt.
3. Wählen Sie eine der folgenden Vorgehensweisen:
   - Navigieren Sie im linken Fensterbereich zu **Knoten**, **Oracle-Datenbankgruppe**, klicken Sie mit der rechten Maustaste auf den Knoten, den Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.
   - Wählen Sie im mittleren Fensterbereich den Knoten aus, der gesichert werden soll, klicken Sie auf die Drop-down-Liste **Aktionen** und anschließend auf **Jetzt sichern**.

   Das Dialogfeld Sicherung jetzt ausführen wird angezeigt.
4. Wählen Sie im Dialogfeld *Sicherung jetzt ausführen* den gewünschten Sicherungstyp aus, und geben Sie dann gegebenenfalls den Sicherungsnamen an.



   Es sind folgende Optionen verfügbar:

   Zuwachssicherung

   Startet eine Zuwachssicherung Ihres Rechners. Eine Zuwachssicherung sichert nur jene Blöcke, die seit der vorherigen Sicherung geändert wurden.

   Hinweis: Wenn Sie eine Sicherung zum ersten Mal ausführen, wird automatisch die vollständige Sicherung initiiert, auch wenn Sie die Option "Zuwachssicherung" ausgewählt haben.

Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

Vollständige Sicherung

Startet eine vollständige Sicherung Ihres gesamten Rechners oder der ausgewählten Volumes.

Hinweis: Wenn Sie keinen Sicherungsnamen angeben, wird automatisch der Name "Benutzerdefinierte vollständige Sicherung" oder "Benutzerdefinierte Zuwachssicherung" vergeben.

5. Klicken Sie auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.

6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.

   Der Sicherungsjob wurde erfolgreich ausgeführt.

Abbrechen des Sicherungsjobs von Oracle-Datenbankknoten

Nachdem der Sicherungsjob von Oracle-Datenbankknoten initiiert wurde, können Sie den Sicherungsjob jederzeit abbrechen. Wenn Sie den Sicherungsjob abbrechen, wird die Sicherung sofort angehalten.

Befolgen Sie diese Schritte:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite Knoten: Alle Knoten wird angezeigt.

3. Wählen Sie eine der folgenden Vorgehensweisen:

   - Navigieren Sie im linken Fensterbereich zu **Knoten**, **Oracle-Datenbankgruppe**, klicken Sie mit der rechten Maustaste auf den Knoten, für den Sie die Sicherung abbrechen möchten, und klicken Sie dann auf **Abbrechen**.
   - Wählen Sie im mittleren Fensterbereich den Knoten aus, für den Sie die Sicherung abbrechen möchten, klicken Sie auf die Drop-down-Liste **Aktionen** und anschließend auf **Abbrechen**.

   Eine Bestätigungsmeldung wird angezeigt.

5. Klicken Sie auf **Ja**, um zu bestätigen.

   Der Sicherungsjob wurde erfolgreich abgebrochen.

Löschen von Oracle-Datenbankknoten

Sie können alle Oracle-Datenbankknoten löschen, die Sie nicht mehr benötigen. Wenn Sie die Knoten löschen, werden auch die zugeordneten Protokolle und Jobübersichten gelöscht. Sie können gelöschte Knoten bei Bedarf zu einem späteren Zeitpunkt wieder hinzufügen.

Befolgen Sie diese Schritte:

1. Klicken Sie auf die Registerkarte **Ressourcen**.

   Die Seite Knoten: Alle Knoten wird angezeigt.

3. Wählen Sie eine der folgenden Vorgehensweisen:

   - Navigieren Sie im linken Fensterbereich zu **Knoten**, **Oracle-Datenbankgruppe**, klicken Sie mit der rechten Maustaste auf den Knoten, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
   - Wählen Sie im mittleren Fensterbereich den Knoten aus, den Sie löschen möchten, klicken Sie auf die Drop-down-Liste **Aktionen** und anschließend auf **Löschen**.

   Eine Bestätigungsmeldung wird angezeigt.

5. Klicken Sie auf **Ja**, um zu bestätigen.

   Der Knoten wurde erfolgreich aus der Konsole gelöscht.

Kapitel 9: Hinzufügen und Verwalten von Zielen

In diesem Abschnitt werden die folgenden Themen behandelt:

So fügen Sie ein Ziel hinzu

Ein Ziel ist ein Speicherort, an dem Sie Ihre Sicherungsdaten speichern. Mit Arcserve UDPkönnen Sie mehrere Ziele hinzufügen.

Der nächste Schritt:

1. Hinzufügen eines Zieles mit RPS
2. Hinzufügen von Arcserve Backup-Servern
3. Hinzufügen einer Remote-Konsole
4. Hinzufügen eines Cloud-Kontos
5. Hinzufügen eines Arcserve Cloud-Kontos

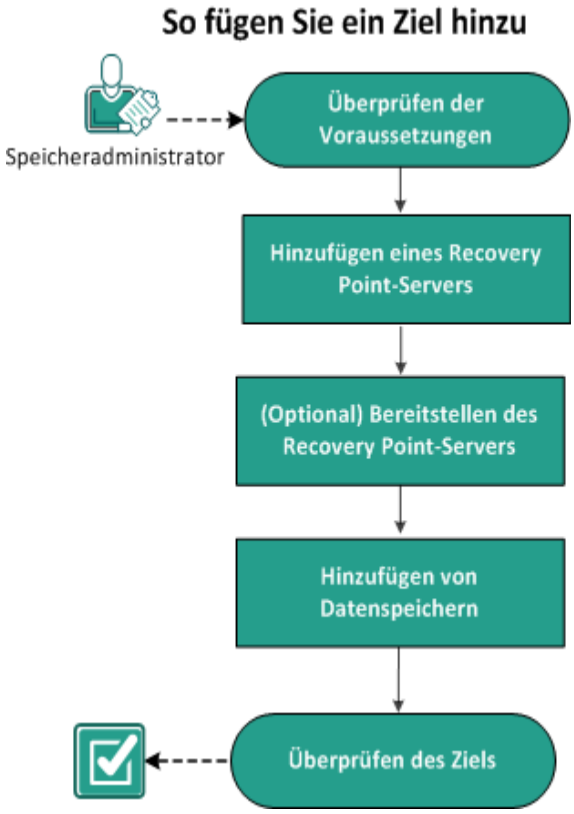
So fügen Sie ein Ziel hinzu

Für Arcserve UDP können Sie einen Recovery Point Server (RPS) als zentrales Ziel zuweisen. Sie können Daten von mehreren Knoten in einem Recovery Point Server speichern und die Daten später bei Bedarf wiederherstellen. Das Hinzufügen eines Ziels besteht aus zwei Hauptschritten:

a. Hinzufügen eines Recovery Point Server zur Konsole

b. Hinzufügen eines Datenspeichers zum Recovery Point Server

Folgendes Diagramm veranschaulicht, wie ein Ziel hinzugefügt wird:



Der nächste Schritt?

1. Überprüfen der Voraussetzungen
2. Hinzufügen eines Recovery Point Server
3. (Optional) Bereitstellen des Recovery Point Server
4. Hinzufügen von Datenspeichern
5. Überprüfen des Ziels

Überprüfen der Voraussetzungen

Erfüllen Sie folgende Voraussetzungen, bevor Sie einen Recovery Point Server einrichten:

- Lesen Sie in den Versionshinweisen die Beschreibungen der Systemanforderungen, die Liste der unterstützten Betriebssysteme und die Liste der bekannten Probleme in dieser Version von Arcserve Unified Data Protection.
- Stellen Sie sicher, dass Sie über Administratorrechte für die Installation von Arcserve Unified Data Protection verfügen.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Hinzufügen eines Recovery Point Servers

Der erste Schritt für das Hinzufügen eines Ziels besteht im Hinzufügen eines Recovery Point Servers zur Konsole. Später fügen Sie dem hinzugefügten RPS Datenspeicher hinzu.

Gehen Sie wie folgt vor:

1. Melden Sie sich auf Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Recovery Point Server hinzufügen**.

   Die Seite **Recovery Point Server hinzufügen** wird angezeigt.
4. Geben Sie die folgenden Details ein:

   Knotenname/IP-Adresse

   Definiert den Knotennamen des Recovery Point Server, den Sie zur Konsole hinzufügen möchten.

   Benutzername und Kennwort

   Definiert den Benutzernamen und das Kennwort für die Anmeldung beim Knoten.

   Hinweis: Verwenden Sie für den Benutzernamen eines der folgenden Formate: Computername, Domänenname/Benutzername oder Benutzername.

   Beschreibung

   (Optional) Definiert zusätzliche Informationen zum Knoten.
5. Füllen Sie folgende Felder für die **Installationseinstellungen** aus:

   Hinweis: Wenn auf dem Knoten bereits ein Recovery Point Server installiert ist, ignorieren Sie diese Installationseinstellungen.

   Installationsspeicherort

   Geben Sie den Speicherort an, an dem Sie den Recovery Point Server installieren möchten. Sie können den Standardpfad übernehmen oder einen anderen Pfad angeben.

   Port

   Gibt die Portnummer an, die eine Verbindung zur webbasierten Benutzeroberfläche herstellt.

Standard: 8014.

Protokoll

Geben Sie das Protokoll an, das Sie für die Kommunikation mit dem Zielserver verwenden möchten. Die verfügbare Auswahl ist "HTTP" und "HTTPS".

Hinweis: Wählen Sie für sichere Kommunikation das HTTPS-Protokoll aus.

Treiber für die Nachverfolgung von Änderungen

Legen Sie fest, ob Sie den **Treiber für die Nachverfolgung von Änderungen** installieren möchten.

6. Planen Sie die Installation oder das Upgrade, indem Sie eine der Optionen unter **Startzeit für Installation oder Upgrade** auswählen.

   Hinweis: Wenn auf dem Server bereits Recovery Point Server installiert ist, ignorieren Sie diese Einstellungen.

7. Klicken Sie auf **Speichern**.

   Der Bereitstellungsfortschritt wird im rechten Fensterbereich angezeigt. Der Recovery Point Server ist hinzugefügt.

   Jetzt ist der Recovery Point Server bereitgestellt. Nachdem der Recovery Point Server hinzugefügt wurde, können Sie Datenspeicher hinzufügen.

(Optional) Bereitstellen des Recovery Point Server

Mit Arcserve Unified Data Protection können Sie die aktuelle Version der RPS-Komponente erkennen und für Recovery Point Server bereitstellen. Nachdem Sie die RPS-Komponente bereitgestellt haben, kann der Knoten Sicherungssitzungen speichern und als Recovery Point Server agieren.

Hinweis: Die RPS-Komponenten werden im Zuge der Arcserve Unified Data Protection-Installation installiert.

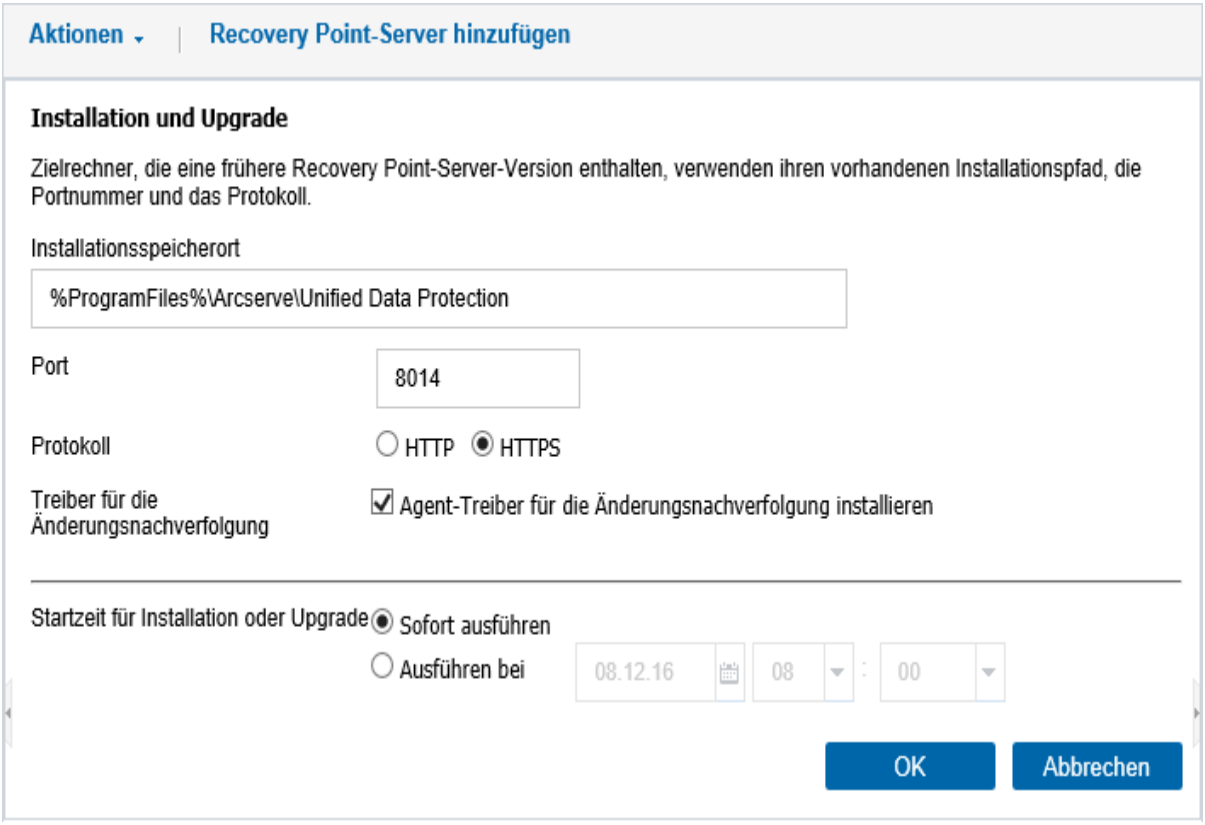
Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziel:** Recovery Point Server wird angezeigt.
3. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf einen Recovery Point Server.
   - Wählen Sie einen Recovery Point Server aus, und klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.
4. Klicken Sie auf **Recovery Point Server installieren/aktualisieren**.

   Die Seite **Installation und Upgrade** wird angezeigt.



5. Ändern Sie die Bereitstellungseinstellungen, und klicken Sie auf **OK**, um den Recovery Point Server auf dem ausgewählten Knoten bereitzustellen.

   Die Bereitstellung des Recovery Point Servers startet. Der Fortschritt der Bereitstellung wird im rechten Fensterbereich angezeigt.

Hinzufügen von Datenspeichern

Damit das Ziel erstellt werden kann, benötigt der Recovery Point Server Datenspeicher. Der Datenspeicher gibt an, wo die Sicherungsdaten gespeichert werden. Sie können mehrere Datenspeicher zu einem RPS hinzufügen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird angezeigt.
3. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf einen Recovery Point Server.
   - Wählen Sie einen Recovery Point Server aus, und klicken Sie im mittleren Fensterbereich auf die Drop-down-Liste **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.
4. Klicken Sie auf **Einen Datenspeicher hinzufügen**.

   Die Seite **Einen Datenspeicher erstellen** wird angezeigt. Sie enthält den Namen des angegebenen Recovery Point Server.
5. Füllen Sie die folgenden Felder aus, und klicken Sie auf **Speichern**:

   Recovery Point Server

   Definiert den Recovery Point Server, in dem der Datenspeicher erstellt wird. Der Recovery Point Server wurde bereits standardmäßig hinzugefügt.

   Name des Datenspeichers

   Definiert den Namen des Datenspeichers.

   Datenspeicherordner

   Definiert den Speicherort des Ordners, in dem der Datenspeicher erstellt wird. Klicken Sie auf "Durchsuchen", um den Zielordner auszuwählen.

   Hinweise:

   - Sie können versteckte Volumes jetzt aktivieren und anzeigen. Weitere Informationen finden Sie unter Aktivieren und Anzeigen versteckter Volumes beim Erstellen eines Datenspeichers.
   - Für Datenspeicher mit und ohne Deduplizierung sollte der Zielpfad auf einen leeren Ordner verweisen.

   Beschränkung der gleichzeitig aktiven Knoten auf

Gibt die Höchstanzahl an gleichzeitigen Jobs für den Datenspeicher an.

Standardwert: 4

Bezieht sich auf einen Wert von 1 bis 9999. Der Wert steht für die Anzahl von Jobs, die gleichzeitig ausgeführt werden können. Wenn die Anzahl der ausgeführten Jobs die festgelegte Anzahl erreicht, wird ein weiterer Job in die Warteschlange gereiht und kann nur gestartet werden, wenn ein ausgeführter Job abgeschlossen wird. Fertiggestellte, abgebrochene oder fehlgeschlagene Jobs werden als abgeschlossene Jobs betrachtet.

Die Zahl bezieht sich auf die Jobtypen, nicht auf die Serverknoten. Zum Beispiel zeigt die Zahl 5 an, dass fünf Sicherungsjobs ausgeführt werden. Alle Jobs, die nach diesen fünf Sicherungsjobs geplant sind, werden in die Warteschlange gestellt. Andere Jobs wie z. B. Dateisystem-Katalogjobs können jedoch übermittelt werden.

Wenn der Wert größer als 16 oder 32 ist, werden Meldungen angezeigt, um Sie zu warnen, dass die Hardware stärker ausgelastet wird.

Hinweis: Eine Beschränkung der Anzahl wirkt sich nur auf den ausgehenden, nicht auf den eingehenden Replikationsjob aus. Eine Beschränkung der Anzahl wirkt sich nicht auf Wiederherstellungs- oder BMR-Jobs aus. Solche Jobs werden nicht in Warteschlangen gereiht.

Deduplizierung aktivieren

Gibt an, dass die Deduplizierung für diesen Datenspeicher aktiviert ist. Arcserve UDP unterstützt beide Arten der Deduplizierung: Deduplizierung an der Quelle und globale Deduplizierung. Deduplizierung an der Quelle vermeidet, dass Datenblöcke von spezifischen Agenten mehrfach über das Netzwerk übertragen werden. Globale Deduplizierung beseitigt doppelte Daten auf allen Client-Rechnern basierend auf der Ebene von Volume-Clustern.

Blockgröße der Deduplizierung

Definiert die Größe der Deduplizierungsblöcke. Die Optionen sind 4 KB, 8 KB, 16 KB, 32 KB und 64 KB. Die Größe der Deduplizierungsblöcke wirkt sich auch auf die geschätzte Deduplizierungskapazität aus. Wenn Sie beispielsweise den Standardwert von 16 KB in 32 KB umändern, wird die geschätzte Deduplizierungskapazität verdoppelt. Eine Vergrößerung der Deduplizierungsblockgröße kann den Deduplizierungsprozentsatz verringern.

Hash-Arbeitsspeicherzuordnung

Gibt den physischen Arbeitsspeicher an, den Sie zuordnen, um Hash-Werte beizubehalten. Dieses Feld ist vorab mit einem Standardwert ausgefüllt. Der Standardwert basiert auf der folgenden Formel:

Wenn der physische Arbeitsspeicher des RPS kleiner als 4 GB ist (oder gleich 4 GB ist), ist der Standardwert der **Hash-Arbeitsspeicherzuordnung** identisch mit dem physischen Arbeitsspeicher des RPS.

Wenn der physische Arbeitsspeicher des RPS größer als 4 GB ist, berechnet Arcserve UDP den derzeit verfügbaren freien Speicherplatz. Nehmen wir an, dass der verfügbare freie Speicherplatz derzeit X GB beträgt. Arcserve UDP überprüft folgende Bedingungen:

- Wenn (X * 80 %) > = 4 GB, lautet der Standardwert der **Hash-Arbeitsspeicherzuordnung** (X * 80 %).
- Wenn (X * 80 %) < 4 GB, lautet der Standardwert der **Hash-Arbeitsspeicherzuordnung** 4 GB.

Beispiel: Wir gehen davon aus, dass der RPS über 32 GB freien physischen Speicherplatz verfügt. Außerdem nehmen wir beim Erstellen des Datenspeichers an, dass das Betriebssystem und andere Anwendungen 4 GB Arbeitsspeicher verwenden. Der verfügbare freie Arbeitsspeicher zu diesem Zeitpunkt beträgt also 28 GB. Der Standardwert der **Hash-Arbeitsspeicherzuordnung** liegt also bei 22,4 GB (22,4 GB = 28 GB * 80 %).

Hash-Ziel ist auf einem Solid State Drive (SSD)

Gibt an, ob sich der Hash-Ordner auf einem Solid State Drive (SSD) befindet.

Hinweis: Konfigurieren Sie das Hash-Ziel auf dem lokalen SSD, wenn die Option "Hash-Ziel ist auf einem Solid State Drive (SSD)" aktiviert ist.

Datenziel

Definiert den Datenzielordner, in dem die eindeutigen Datenblöcke gespeichert werden sollen. Speichern Sie die Daten, die die ursprünglichen Datenblöcke der Quelle enthalten, auf dem größten Datenträger.

Hinweis: Der Pfad für **Datenziel** sollte auf einen leeren Ordner verweisen.

Indexziel

Definiert den Indexzielordner, in dem die Indexdateien gespeichert werden sollen. Wählen Sie einen anderen Datenträger aus, um die Deduplizierungsverarbeitung zu verbessern.

Hinweis: Der Pfad für **Indexziel** sollte auf einen leeren Ordner verweisen.

Hash-Ziel

Definiert den Pfad, in dem die Hash-Datenbank gespeichert werden soll. Arcserve UDP verwendet den SHA1-Algorithmus, um den Hash für Quelldaten zu generieren. Die Hash-Werte werden von der Hash-Datenbank verwaltet. Durch die Auswahl eines Hochgeschwindigkeits-Solid-State-Drive (SSD) kann

die Deduplizierungskapazität gesteigert und der Bedarf an Arbeitsspeicher gesenkt werden. Für eine bessere Hash-Leistung empfehlen wir, das SSD-Volume als NTFS-Dateisystem mit einer Volume-Cluster-Größe von 4 KB zu formatieren.

Hinweis: Der Pfad für **Hash-Ziel** sollte auf einen leeren Ordner verweisen.

Hinweis: Sie können für folgende vier Ordner nicht denselben Pfad angeben: **Datenspeicher, Datenziel, Indexziel** und **Hash-Ziel**.

Komprimierung aktivieren

Gibt an, dass die Einstellungen für die Datenkomprimierung aktiviert sind.

Komprimierungstyp

Gibt an, ob der standardmäßige oder der maximale Komprimierungstyp verwendet werden soll.

Eine Komprimierung wird oft ausgewählt, um den verwendeten Speicherplatz zu verringern, hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit der Sicherung. Sie können eine der drei verfügbaren Optionen aktivieren.

Hinweis: Weitere Informationen finden Sie unter Komprimierungstyp.

Verschlüsselung aktivieren

Gibt an, dass die Verschlüsselungseinstellungen aktiviert sind. Wenn Sie diese Option auswählen, müssen Sie das Verschlüsselungskennwort angeben und bestätigen.

Bei der Datenverschlüsselung werden Daten in ein Format umgewandelt, das ohne den entsprechenden Entschlüsselungsmechanismus nicht verständlich ist. Die Arcserve Unified Data Protection-Lösung verwendet sichere AES-Verschlüsselungsalgorithmen (Advanced Encryption Standard) für größtmögliche Sicherheit und Datenschutz für Ihre Daten. Für Datenspeicher wird "Verschlüsselung" oder "Keine Verschlüsselung" unterstützt. Für "Verschlüsselung" ist nur AES-256 verfügbar.

Ein Kennwort ist nicht erforderlich, wenn Sie versuchen, die Wiederherstellung auf dem gleichen Rechner durchzuführen, auf dem die Sicherung ausgeführt wurde. Wenn Sie jedoch versuchen, die Wiederherstellung auf einem anderen Rechner durchzuführen, ist ein Kennwort erforderlich. Standardmäßig ist nur für die erste Anmeldung ein Kennwort erforderlich. Um das Kennwort auch nach der ersten Anmeldung einzugeben, muss der Administrator Arcserve den Erweiterungsdienst des UDP Agent-Explorers manuell anhalten.

Warnung per E-Mail senden, wenn ein Ziel die Kapazitätsgrenze erreicht

Durch Wahl dieser Option sendet der Datenspeicher eine Warnung per E-Mail. Der RPS sendet eine Warnung per E-Mail an den Empfänger, wenn der Zielordner des Datenspeichers fast voll ist.

E-Mail konfigurieren

Diese Schaltfläche wird nur angezeigt, wenn Sie die Option *Warnung per E-Mail senden, wenn ein Ziel die Kapazitätsgrenze erreicht* aktivieren. Mit der Schaltfläche können Sie eine E-Mail-Benachrichtigungen-ID angeben, um Warnungen zu empfangen. Klicken Sie auf die Schaltfläche **E-Mail konfigurieren**, um globale E-Mail-Einstellungen von "Konsole>Einstellungen>Konfiguration von E-Mail und Warnung" zu laden. Wenn keine globalen E-Mail-Einstellungen verfügbar sind, wird durch Klicken auf die Schaltfläche **E-Mail konfigurieren** das Dialogfeld **E-Mail-Einstellungen** geöffnet, um die E-Mail-Details zu definieren.

Der Datenspeicher ist erstellt und wird im mittleren Fensterbereich angezeigt. Klicken Sie auf den Datenspeicher, um die Details im rechten Fensterbereich anzuzeigen.

Verschiedene Status des Datenspeichers

Der Datenspeicher hat je nach durchgeführter Aufgabe einen anderen Status. Wenn Sie einen Datenspeicher auf der Registerkarte **Ressourcen** auswählen, wird der Datenspeicherstatus rechts angezeigt.

- **Angehalten:** Der Datenspeicher ist inaktiv. Sie können keine Jobs in diesem Status übermitteln.
- **Starten:** Der Datenspeicher wird gestartet. Wenn der Datenspeicher gestartet wird, wird der Fortschritt in der Konsole angezeigt.
- **Wird ausgeführt:** Der Datenspeicher ist aktiv. Sie können Jobs in diesem Status übermitteln.
- **Stoppen:** Der Datenspeicher wird gestoppt. Wenn der Datenspeicher gestoppt wird, wird der Fortschritt in der Konsole angezeigt.
- **Ändern:** Der Datenspeicher wird mit neuen Daten aktualisiert. Wenn der Datenspeicher geändert wird, wird der Fortschritt in der Konsole angezeigt.
- **Löschen:** Der Datenspeicher wird gelöscht. Wenn der Datenspeicher gelöscht wird, wird der Fortschritt in der Konsole angezeigt.
- **Außer Betrieb:** Der Datenspeicher funktioniert nicht ordnungsgemäß. Sie können keine Jobs in diesem Status übergeben. Stoppen Sie den Datenspeicher, und überprüfen Sie den Grund für dieses Verhalten. Die folgenden Szenarios können zum Status "Außer Betrieb" eines Datenspeichers führen:
  - Auf das Sicherungsziel des Datenspeichers kann nicht zugegriffen werden.
  - Die Konfigurationen in der Registrierung oder Datei sind beschädigt.
  - Der GDD-Index oder die Datenrolle weist interne Fehler auf.
  - Der Prozess für den GDD-Index oder die Datenrolle wurde manuell abgebrochen.
- **Nur Wiederherstellung:** Im Status "Nur Wiederherstellung" werden keine Jobs ausgeführt, bei denen Daten in den Datenspeicher geschrieben werden müssen. Dazu gehören Jobs wie Sicherung, Replikation (eingehend), Jumpstart (eingehend) und Datenmigration. Alle anderen Jobs, bei denen Daten aus dem Datenspeicher gelesen werden müssen, werden ausgeführt. Der Datenspeicherstatus ändert sich unter den folgenden Bedingungen in "Nur Wiederherstellen":

- Der Hash-Rollenprozess wird manuell abgebrochen.
- Wenn die Sicherungsziel/Daten/Index/Hash-Pfad Volume-Kapazität/der zugeordnete Hash-Speicher seinen zulässigen Höchstwert erreicht.

Wichtig! Wenn der Status des Datenspeichers "Nur Wiederherstellen (Heruntergestufter Status)" oder "Außer Betrieb (Ungültiger Status)" ist, funktioniert der Datenspeicher nicht mehr ordnungsgemäß. Sie müssen den Datenspeicher stoppen und die Ursache für den Status überprüfen. Zum Beispiel kann das Problem sein, dass das Datendeduplizierungs-Volume seine Obergrenze erreicht hat. Starten Sie nach der Behebung des Problems den Datenspeicher, und übergeben Sie den Sicherungsjob erneut.

Überprüfen des Ziels

Nachdem Sie alle Vorgänge zum Hinzufügen des Recovery Point-Servers abgeschlossen haben, überprüfen Sie, ob er erfolgreich hinzugefügt wurde.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird angezeigt.
3. Überprüfen Sie folgende Details:
   - Der von Ihnen erstellte RPS wird angezeigt.
   - Die Datenspeicher werden unter dem RPS angezeigt.

Hinzufügen von Arcserve Backup-Servern

Fügen Sie einen Arcserve Backup-Server zum Archivieren von Daten auf Band hinzu. Wenn Sie einen Plan zum Archivieren der Daten auf einem Bandgerät erstellen, können Sie dieses Ziel verwenden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an, und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Arcserve Backup-Server**.

   Die Seite **Ziele: Arcserve Backup Server** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Einen Arcserve Backup-Server hinzufügen**.

   Die Seite **Einen Arcserve Backup-Server hinzufügen** wird angezeigt.
4. Geben Sie die folgenden Details ein:

   Knotenname/IP-Adresse

   Definiert den Knotennamen oder die IP-Adresse des Arcserve Backup-Servers.

   Authentifizierungstyp

   Gibt den Authentifizierungstyp an, der für die Anmeldung beim Arcserve Backup-Server erforderlich ist. Die beiden folgenden Optionen stehen zur Verfügung:

   Windows-Authentifizierung

   Gibt an, dass die Windows-Authentifizierung für die Anmeldung beim Arcserve Backup-Server verwendet wird.

   Hinweis: Windows-Benutzer müssen sich zuerst mithilfe von Arcserve Backup User Profile Manager bei Arcserve Backup registrieren.

   Arcserve Backup-Authentifizierung

   Gibt an, dass die Windows-Authentifizierung für die Anmeldung beim Arcserve Backup-Server verwendet wird.

   Benutzername und Kennwort

   Legt den Benutzernamen und das dazugehörige Kennwort für die Anmeldung beim Knoten fest.

   Hinweis: Verwenden Sie für den Benutzernamen eines der folgenden Formate: Computername, Domänenname/Benutzername oder Benutzername.

Port

Gibt die Portnummer für die Verbindung mit dem Arcserve Backup-Server an.

Hinweis: Arcserve UDP verwendet für die Verbindung mit beiden Servern die Portnummer, also sowohl für die Verbindung mit dem Arcserve Backup-Primärserver als auch mit dem Mitgliedsserver in der Arcserve Backup-Domäne.

5. Klicken Sie auf **Speichern**.

   Der Arcserve Backup-Server wird zur Konsole hinzugefügt.

   Nachdem der Arcserve Backup-Server zur Konsole hinzugefügt wurde, können Sie zu **Ressourcen, Ziel, Arcserve Backup-Server** navigieren und sich detaillierte Informationen zu den Bandmedien ansehen.

Remote-Konsole hinzufügen

Fügen Sie eine Remotekonsole hinzu, um einen Wiederherstellungspunkt zu einem remote verwalteten Recovery Point Server zu replizieren.. Sie können die Remotekonsole verwenden, um einen Replikationsplan zum Senden von Daten an die Zielkonsole zu erstellen. Sie können die hinzugefügte Remotekonsole auch verwalten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an, und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Bereich auf **Ziele**, und klicken Sie auf **Remotekonsole**.

   Die **Ziele: Die Seite "Remotekonsole"** wird in der Mitte angezeigt..
3. Klicken Sie auf **Remotekonsole hinzufügen**.

   Die Seite zum **Hinzufügen einer Remotekonsole** wird angezeigt.
4. Geben Sie die folgenden Details ein:

   Remote-Konsole

   Verweist auf den URL der Remotekonsole, den Sie der Konsole hinzufügenmöchten.

   Benutzername

   Bezieht sich auf den Benutzernamen mit dem Sie sichbei der der Remotekonsole anmelden können.

   Hinweis: Verwenden Sie für den Benutzernamen eines der folgenden Formate: Computername, Domänenname/Benutzername oder Benutzername.

   Kennwort

   Bezieht sich auf das Kennwort für den Benutzernamen.

   Port

   Bezieht sich auf die Portnummer, die mit der webbasierten Benutzeroberfläche verbunden ist.

   Standard: 8015.

   Protokoll

   Geben Sie das Protokoll an, das Sie für die Kommunikation mit dem Zielserver verwenden möchten. Die verfügbare Auswahl ist "HTTP" und "HTTPS".

   Hinweis: Wählen Sie für sichere Kommunikation das HTTPS-Protokoll aus.

   Proxy-Einstellungen

Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

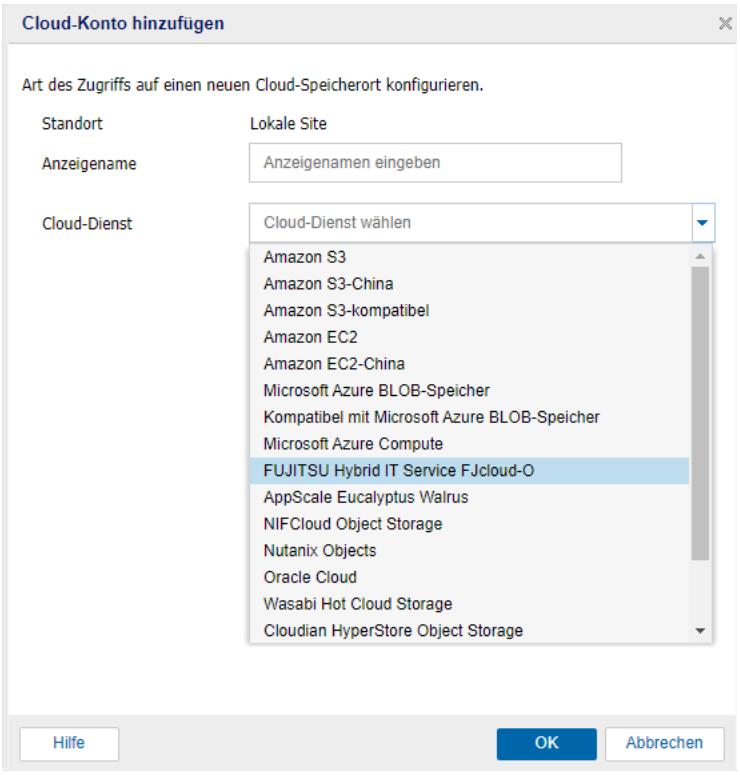
5. Klicken Sie auf **"OK"**.

   Die Remotekonsole wird nun hinzugefügt.

Hinzufügen eines Cloud-Kontos

Fügen Sie ein Cloud-Konto hinzu, um Dateien oder Wiederherstellungspunkte in einen Cloud-Speicher zu kopieren. Sie können verwandte Konten beim Erstellen von Tasks oder einem oder mehrerer Pläne auf Wiederherstellungspunkt kopieren/Dateikopie/Dateiarchiv/Virtual Standby to Cloud/Instant Virtual Machine auf Amazon EC2 verwenden. Geben Sie einen eindeutigen Speichernamen an und wählen Sie den erforderlichen Speicherdienst aus den in der Drop-down-Liste angezeigten Optionen aus.

Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.



Die Konfigurationsoptionen für jeden Cloud-Anbieter sind ähnlich (mit etwas unterschiedlicher Terminologie), und alle Unterschiede werden beschrieben. Ein Cloud-Konto Ihrer Wahl hinzufügen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Geben Sie für **Display Name** einen eindeutigen Namen an.

   Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.
5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

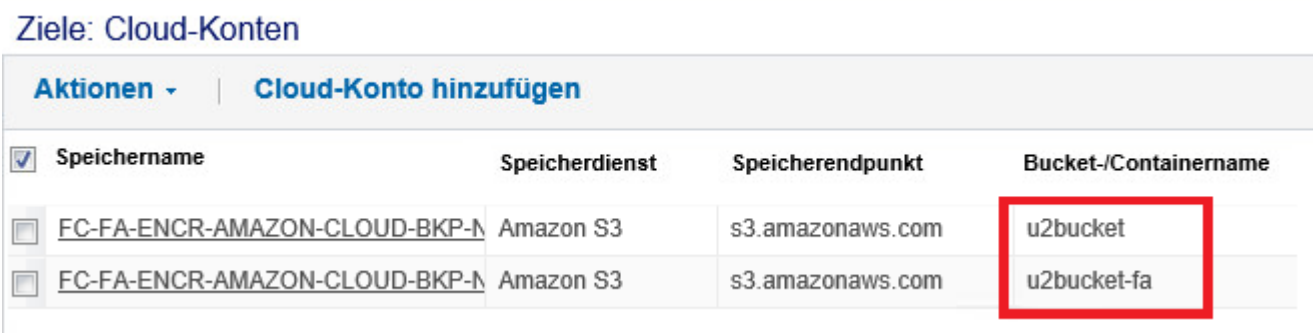
   Mehrere Felder erscheinen für die Konfiguration.
6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Folgende Speicherdienstoptionen sind verfügbar: Amazon S3, Amazon S3-kompatibel, Microsoft Azure BLOB-Speicher, Kompatibel mit Microsoft Azure BLOB-Speicher, FUJITSU Hybrid IT Service FJcloud-O, AppScale Eucalyptus Walrus, Amazon EC2, Amazon EC2-China, Microsoft Azure Compute, Nutanix Objects, Wasabi Hot Cloud Storage und Oracle Cloud.

   Hinweis: Klicken Sie auf Speicherdienstnamen, um zu sehen, wie Sie ein Cloud-Konto für diesen Speicherdienst hinzufügen.

   Die Konfigurationsoption variiert je nach ausgewähltem Speicherdienst.

   Die ausgewählte Speicherdienst-Cloud wird derArcserve UDPKonsole hinzugefügt und auf dem Bildschirm**Ziele: Cloud-Konten** angezeigt. Zum Beispiel werden Amazon S3 Konten unten angezeigt.



Der nächste Schritt?

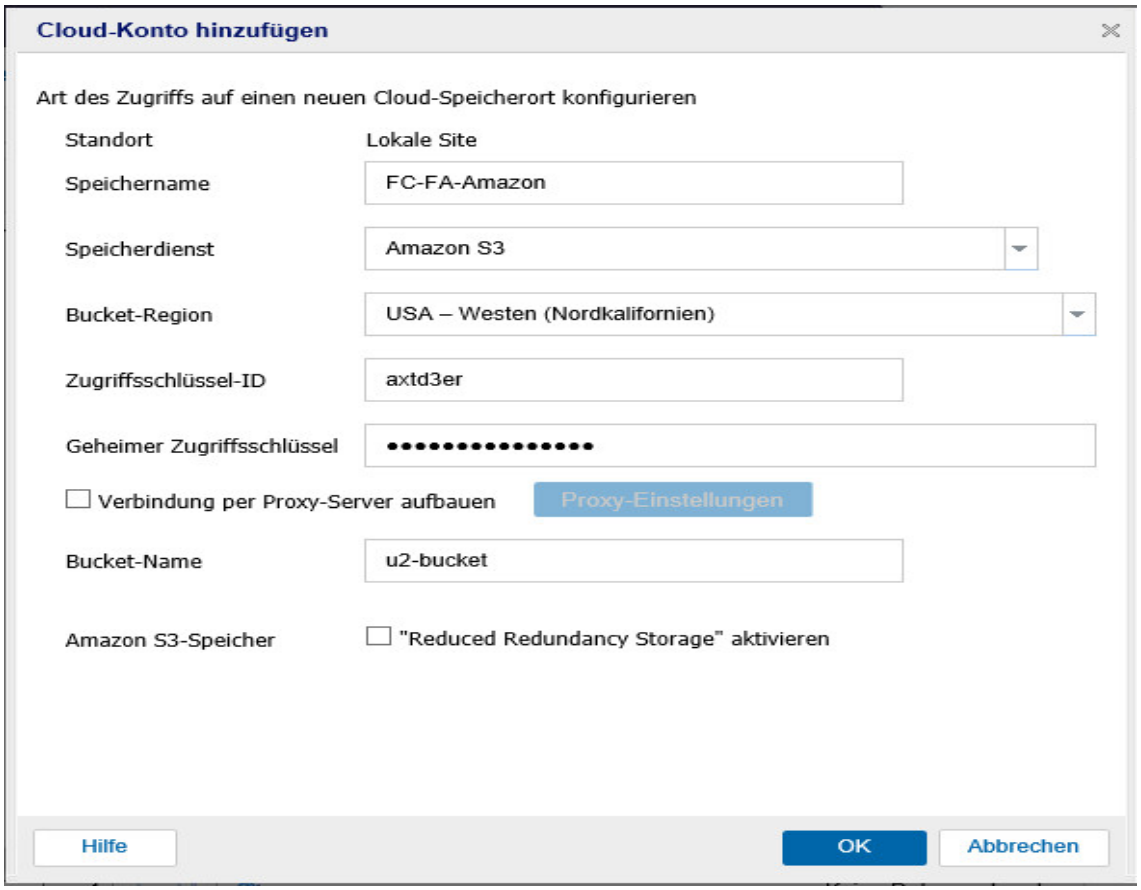
Hinzufügen eines Cloud-Kontos für:

- Amazon S3
- Amazon S3-kompatibel
- Microsoft Azure BLOB-Speicher
- Kompatibel mit Microsoft Azure BLOB-Speicher
- FUJITSU Hybrid IT Service FJcloud-O
- AppScale Eucalyptus Walrus
- Für Amazon EC2
- Amazon EC2-China
- Microsoft Azure Compute
- Nutanix Objects
- Wasabi Hot Cloud-Speicher
- Oracle Cloud

Hinzufügen eines Cloud-Kontos für Amazon S3

Fügen Sie ein Cloud-Konto für Amazon S3 zum Kopieren von Dateien oder Wiederherstellungspunkte in Cloud-Speicher hinzu.

Sie können dieses Konto verwenden, während Sie den Wiederherstellungspunkt / den Dateikopie-oder /oder den Dateiarchivierungs-Task erstellen..



Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Geben Sie für **Display Name** einen eindeutigen Namen an.

Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.

5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Bucket-Region

   Verweist auf die Bucket-Region in Amazon.

   Zugriffsschlüssel-ID

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Geheimer Zugriffsschlüssel

   Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Bewahren Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

   Proxy-Einstellungen

   Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

   Bucket-Name

   Alle in den Cloud-Anbieter verschobenen oder kopierten Dateien und Ordner werden gespeichert und in den Buckets verwaltet. Buckets sind wie Container für Ihre Dateien und werden verwendet, um Objekte zu gruppieren und gemein-

sam zu verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

"Reduced Redundancy Storage" aktivieren

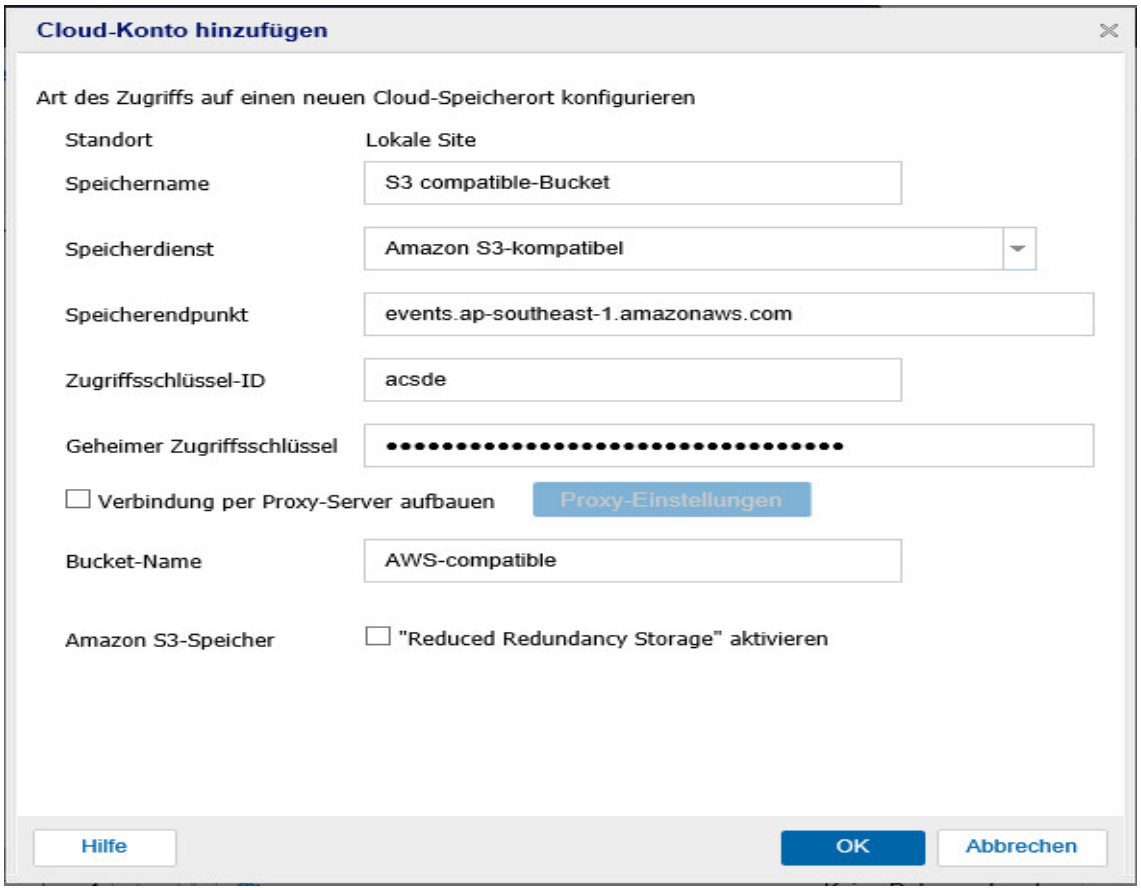
Nur bei Amazon S3 können Sie mit dieser Option "Reduced Redundancy Storage" (RRS) aktivieren. RRS ist eine Speicherungsoption von Amazon S3, mit der Sie Kosten reduzieren können, indem Sie nicht kritische, reproduzierbare Daten auf geringeren Redundanz-Ebenen als dem Standardspeicher von Amazon S3 speichern. Sowohl die Standardoption als auch die RRS-Option speichern Daten in mehreren Einrichtungen und auf mehreren Geräten. Allerdings werden die Daten mit RRS weniger oft repliziert, sodass die Kosten geringer sind. Sie sollten die gleiche Latenz und den gleichen Durchsatz erhalten, indem Sie entweder den Standardspeicher von Amazon S3 oder RRS verwenden. Standardmäßig ist diese Option nicht aktiviert (Amazon S3 verwendet die standardmäßige Speicheroption).

Das Cloud-Konto wird zur Konsole hinzugefügt.

Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Hinzufügen eines Cloud-Kontos für Amazon S3-kompatibel

Hinzufügen eines Cloud-Kontos für Amazon S3-kompatibel für Kopien von Dateien oder Wiederherstellungspunkten in Cloud-Speicher. Sie können dieses Konto verwenden, während Sie den Wiederherstellungspunkt / den Dateikopie-oder /oder den Dateiarchivierungs-Task erstellen..



Hinweise:

- Für S3-kompatible bzw. S3-Unteranbieter, die den Authentifizierungstyp V3/V2 verwenden, um für Arcserve CCI zertifiziert zu werden, funktioniert das, da das Standard-Übersteuerungskennzeichen für den Signierertyp auf **True** festgelegt ist. Unteranbieter, die die V4-Authentifizierung verwenden, müssen jedoch das Kennzeichen in der Datei "AmazonPlugin.properties" auf **False** festlegen und die Dienste neu starten.

  SIGNER_OVERRIDE=false

- Zur Unterstützung von HGST Cloud für Amazon S3-kompatibel müssen Sie die folgende AmazonPlugin.property ändern:

  SET_STORAGECLASS_HEADER=false

Anhand dieser Eigenschaft kann der Speicher-Header übersprungen werden. Wenn Sie daher diese Eigenschaft beim Hinzufügen einer Dateikopie- oder Dateiarchivaufgabe mit Amazon als Cloud-Ziel verwenden, wird der Speicher-Header standardmäßig übersprungen.

Die AmazonPlugin.properties-Datei befindet sich an folgendem Speicherort:

C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\CCI\Config

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Geben Sie für **Display Name** einen eindeutigen Namen an.

   Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.
5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.
6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Speicherendpunkt

   Gibt die Dienst-URL des Anbieters an. (Beispiel: *http:///[Servername]:Portnummer*)

   Zugriffsschlüssel-ID

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Geheimer Zugriffsschlüssel

   Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Bewahren Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen

öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

Proxy-Einstellungen

Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

Bucket-Name

Alle in den Cloud-Anbieter verschobenen oder kopierten Dateien und Ordner werden gespeichert und in den Buckets verwaltet. Buckets sind wie Container für Ihre Dateien und werden verwendet, um Objekte zu gruppieren und gemeinsam zu verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

"Reduced Redundancy Storage" aktivieren

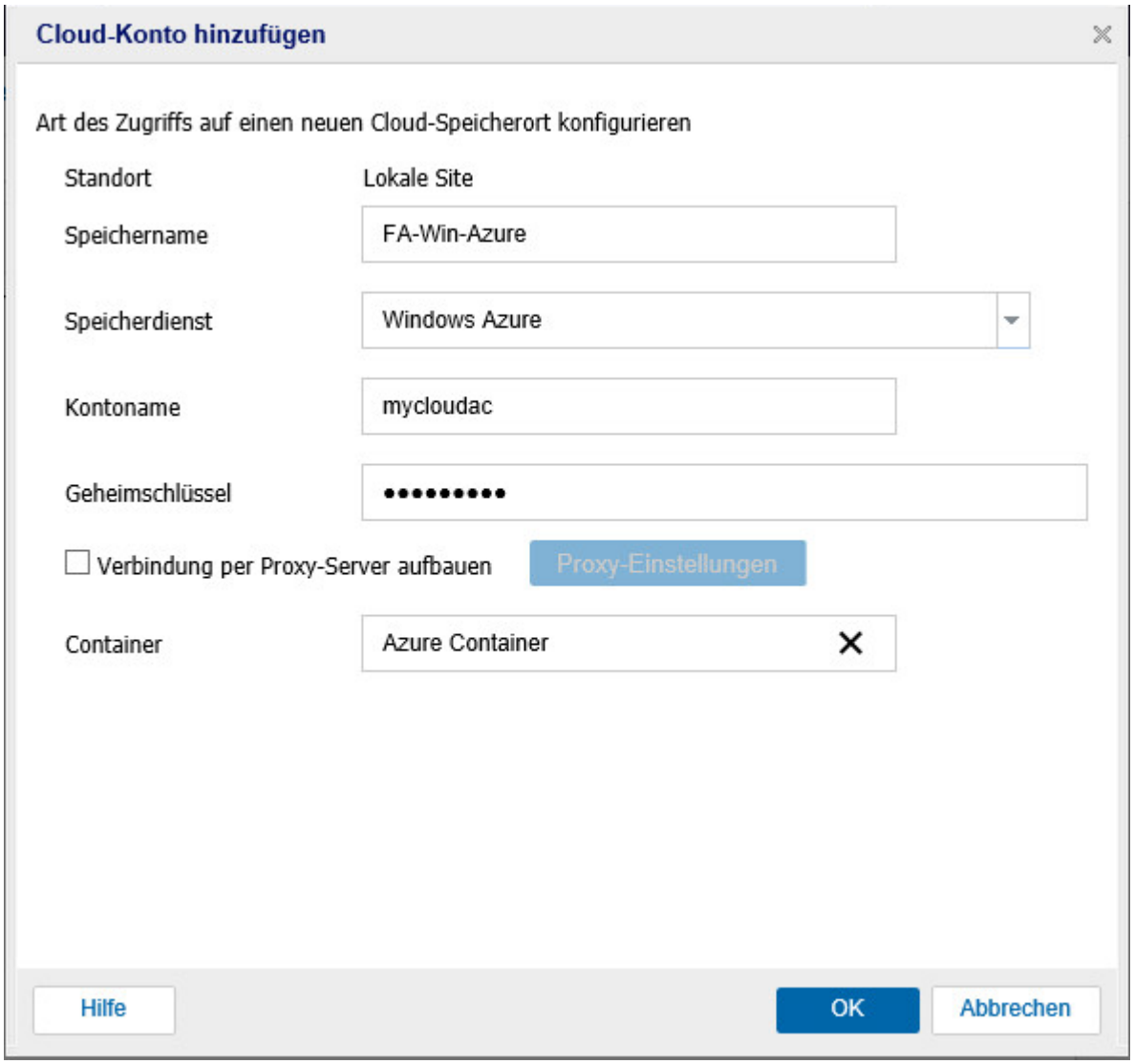
Nur bei Amazon S3 können Sie mit dieser Option "Reduced Redundancy Storage" (RRS) aktivieren. RRS ist eine Speicherungsoption von Amazon S3, mit der Sie Kosten reduzieren können, indem Sie nicht kritische, reproduzierbare Daten auf geringeren Redundanz-Ebenen als dem Standardspeicher von Amazon S3 speichern. Sowohl die Standardoption als auch die RRS-Option speichern Daten in mehreren Einrichtungen und auf mehreren Geräten. Allerdings werden die Daten mit RRS weniger oft repliziert, sodass die Kosten geringer sind. Sie sollten die gleiche Latenz und den gleichen Durchsatz erhalten, indem Sie entweder den Standardspeicher von Amazon S3 oder RRS verwenden. Standardmäßig ist diese Option nicht aktiviert (Amazon S3 verwendet die standardmäßige Speicheroption).

Das Cloud-Konto wird zur Konsole hinzugefügt.

Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Hinzufügen eines Cloud-Kontos für Microsoft Azure Blob-Speicher

Fügen Sie ein Cloud-Konto für Microsoft Azure Blob-Speicher zum Kopieren von Dateien oder Wiederherstellungspunkten zu Cloud-Speichern hinzu. Sie können dieses Konto verwenden, während Sie den Wiederherstellungspunkt / den Dateikopie- oder /oder den Dateiarchivierungs-Task erstellen..



Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.

4. Geben Sie für **Display Name** einen eindeutigen Namen an.

   Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.

5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Kontoname

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Geheimschlüssel

   Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Speicherort aufbewahren. Betten Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

   Proxy-Einstellungen

   Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

   Container

   Alle in den Cloud-Anbieter verschobenen oder kopierten Dateien und Ordner werden gespeichert und in Ihren Containern verwaltet. Mit Hilfe von Containern können Sie Objekte gruppieren und gemeinsam verwalten. Jedes

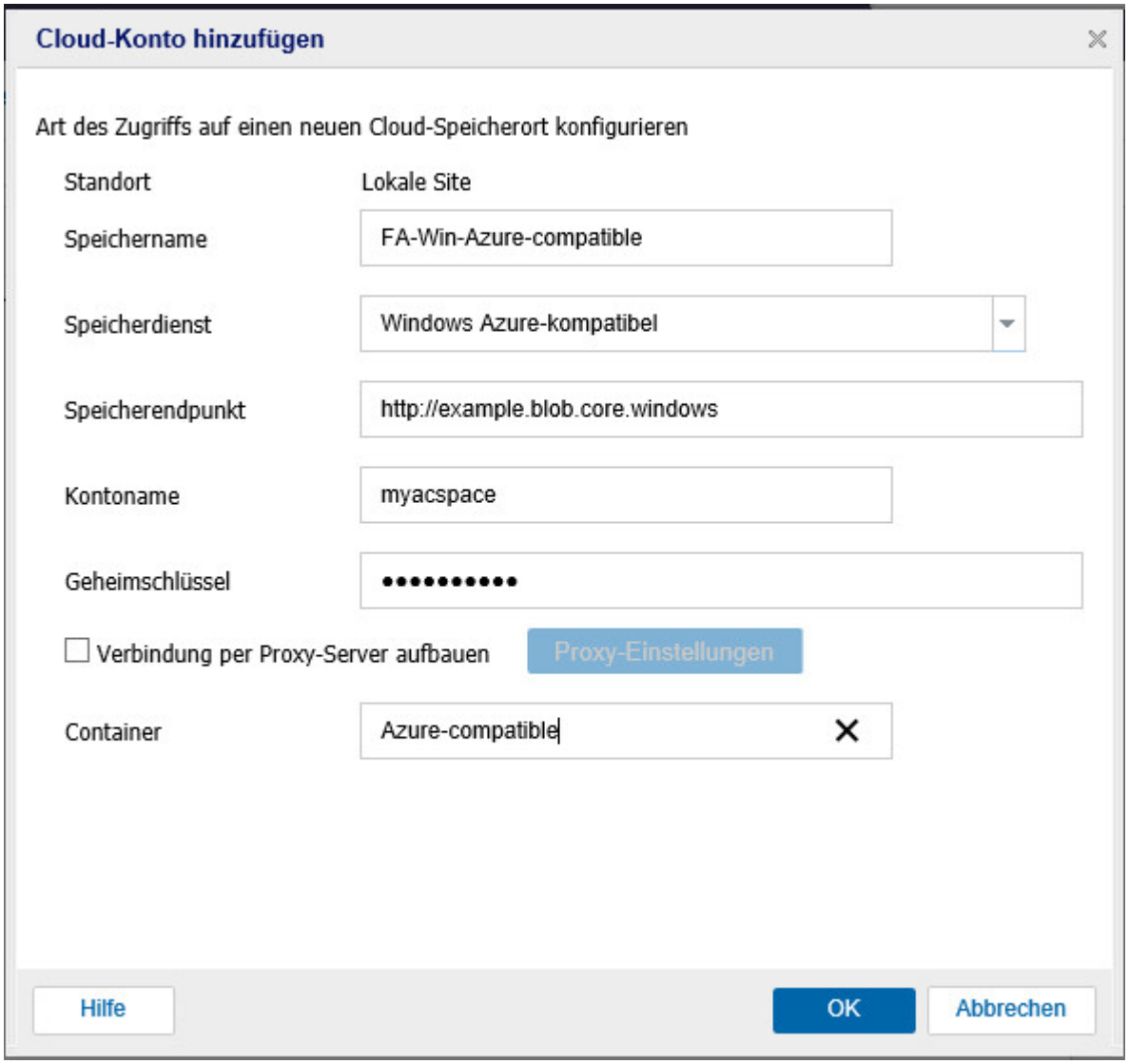
Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

Das Cloud-Konto wird zur Konsole hinzugefügt.

Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Hinzufügen eines Cloud-Kontos, das mit Microsoft Azure Blob-Speicher kompatibel ist

Fügen Sie ein Cloud-Konto, das mit Microsoft Azure Blob-Speicher kompatibel ist, zum Kopieren von Dateien oder Wiederherstellungspunkten zu Cloud-Speichern hinzu. Sie können dieses Konto verwenden, während Sie den Wiederherstellungspunkt / den Dateikopie-oder /oder den Dateiarchivierungs-Task erstellen..



Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.

3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.

4. Geben Sie für **Display Name** einen eindeutigen Namen an.

   Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.

5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Speicherendpunkt

   Gibt die Dienst-URL des Anbieters an. (Beispiel: *http://[Servername]:Portnummer*)

   Kontoname

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Geheimschlüssel

   Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Speicherort aufbewahren. Betten Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

   Proxy-Einstellungen

   Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

   Container

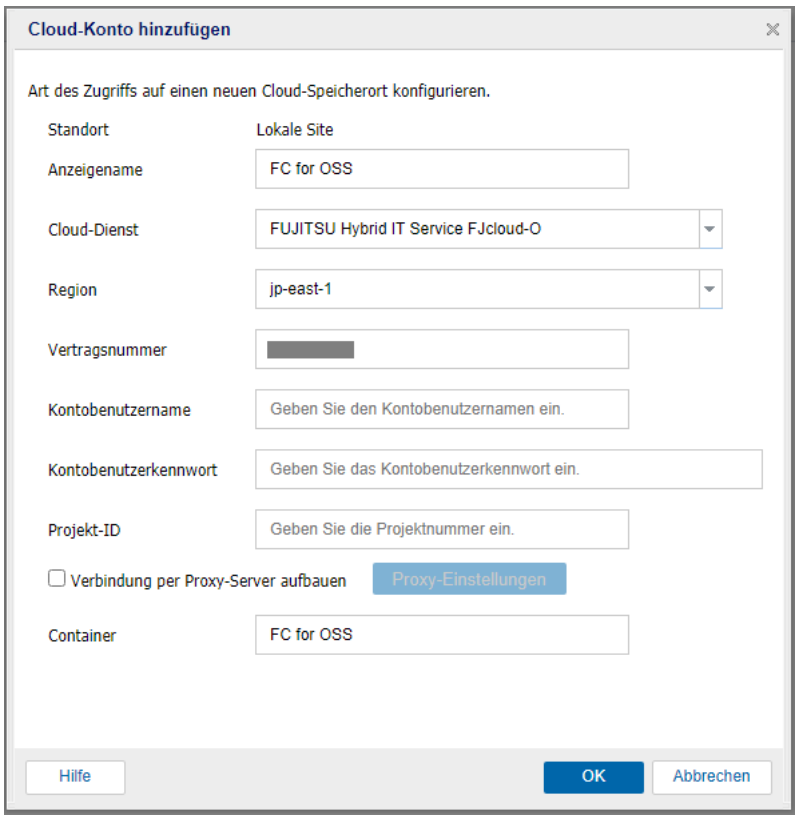
Alle in den Cloud-Anbieter verschobenen oder kopierten Dateien und Ordner werden gespeichert und in Ihren Containern verwaltet. Mit Hilfe von Containern können Sie Objekte gruppieren und gemeinsam verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

Das Cloud-Konto wird zur Konsole hinzugefügt.

Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Hinzufügen eines Cloud-Kontos für FUJITSU Hybrid IT Service FJcloud-O

Fügen Sie ein Cloud-Konto für FUJITSU Hybrid IT Service FJcloud-O hinzu, um Dateien oder Wiederherstellungspunkten in Cloud-Speicher zu kopieren. Sie können dieses Konto beim Erstellen eines Tasks vom Typ Dateikopie/Dateiarchivierung verwenden.



Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Geben Sie für **Display Name** einen eindeutigen Namen an.

Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.

5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Bucket-Region

   Bezieht sich auf die Region des Buckets in FUJITSU Hybrid IT Service FJcloud-O.

   Benutzername

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Benutzerkennwort

   Bezieht sich auf ein Kennwort, das verwendet wird, um die Echtheit der Anforderung auf diesen Speicherort zu überprüfen, weil das Kennwort nicht verschlüsselt ist.

   Wichtig!Dieses Kennwort ist entscheidend für die Sicherheit Ihrer Konten. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Speichern Sie Ihr Kennwort nicht auf einer Webseite oder einem anderen öffentlich zugänglichen Quellcode und übertragen Sie es nicht über unsichere Kanäle.

   Proxy-Einstellungen

   Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

   Vertragsnummer

   Bezieht sich auf die Nummer Ihres Vertrages für FUJITSU Hybrid IT Service FJcloud-O.

   Projekt-ID

Bezieht sich auf die von FUJITSU Hybrid IT Service FJcloud-O generierte ID des Projekts.

Container

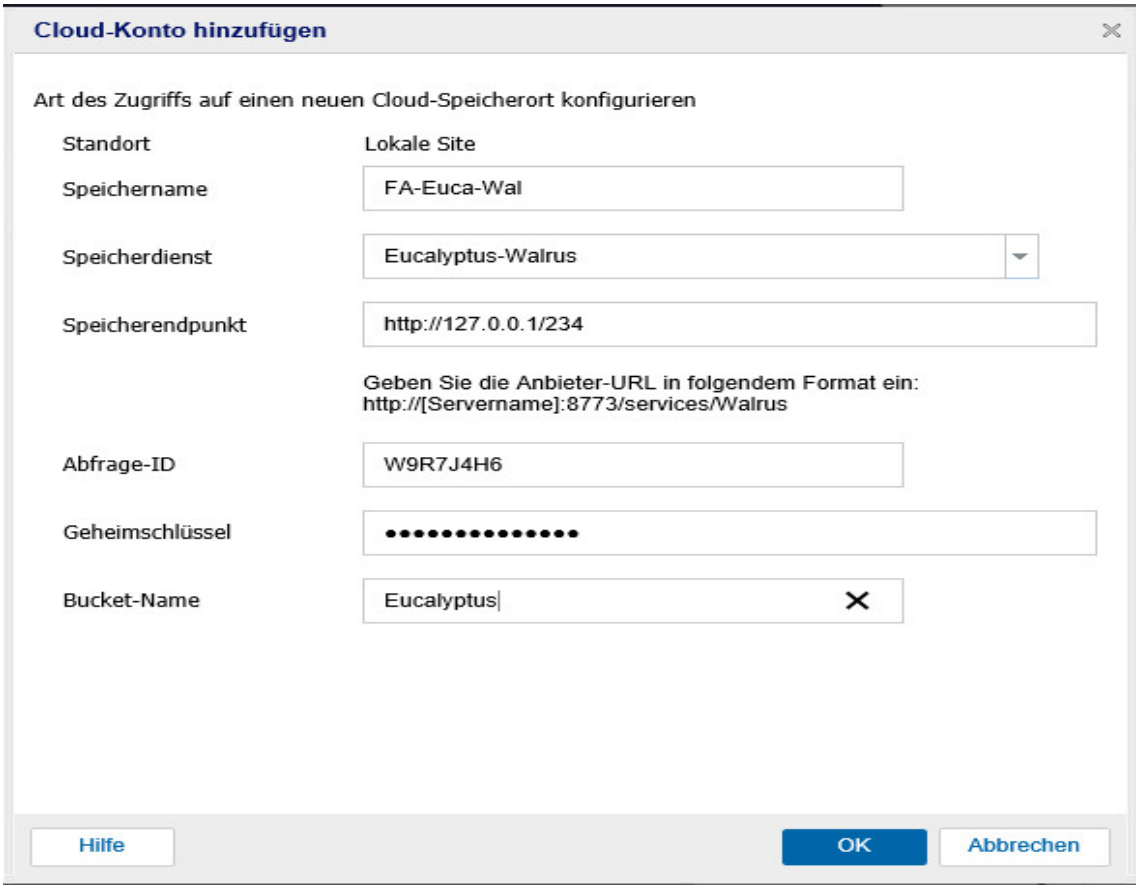
Alle in den Cloud-Anbieter verschobenen oder kopierten Dateien und Ordner werden gespeichert und in Ihren Containern verwaltet. Mit Hilfe von Containern können Sie Objekte gruppieren und gemeinsam verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

Das Cloud-Konto wird zur Konsole hinzugefügt.

Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Hinzufügen eines Cloud-Kontos für AppScale Eucalyptus Walrus

Fügen Sie ein AppScale Eucalyptus Walrus-Cloud-Konto zum Kopieren von Dateien oder Wiederherstellungspunkten in Cloud-Speicher hinzu. Sie können dieses Konto verwenden, während Sie den Wiederherstellungspunkt / den Dateikopie-oder /oder den Dateiarchivierungs-Task erstellen..



Hinweis: Mit AppScale Eucalyptus Walrus als Ihrem Cloud-Anbieter für Dateikopien können Sie keine Dateien kopieren, deren Pfad mehr als 170 Zeichen lang ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Geben Sie für **Display Name** einen eindeutigen Namen an.

Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.

5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Speicherendpunkt

   Gibt die Dienst-URL des Anbieters an. (Beispiel: *http:///[Servername]:Portnummer*)

   Abfrage ID

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Geheimschlüssel

   Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Speicherort aufbewahren. Betten Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

   Bucket-Name

   Alle in den Cloud-Anbieter verschobenen oder kopierten Dateien und Ordner werden gespeichert und in den Buckets verwaltet. Buckets sind wie Container für Ihre Dateien und werden verwendet, um Objekte zu gruppieren und gemeinsam zu verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

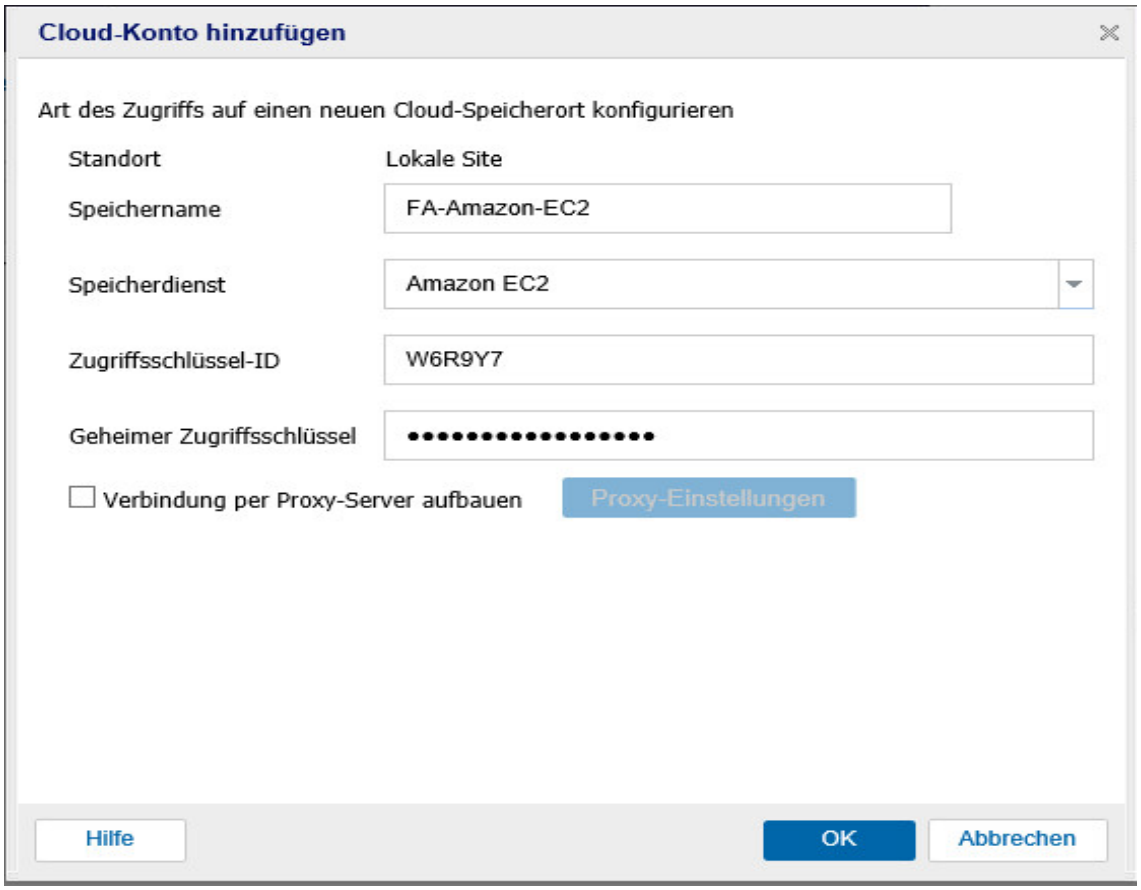
   Das Cloud-Konto wird zur Konsole hinzugefügt.

   Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Ein Cloud-Konto für Amazon EC2 hinzufügen

Hinzufügen eines Cloud-Kontos für Amazon EC2 für das Kopieren von Dateien oder Wiederherstellungspunkten in Cloud-Speicher,

Sie können dieses Konto verwenden, wenn Sie Tasks für einen Plan für Virtual Standby to Cloud oder Instant Virtual Machine auf Amazon EC2 erstellen.



Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Geben Sie für **Display Name** einen eindeutigen Namen an.

Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.

5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Zugriffsschlüssel-ID

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Geheimer Zugriffsschlüssel

   Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Bewahren Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

   Proxy-Einstellungen

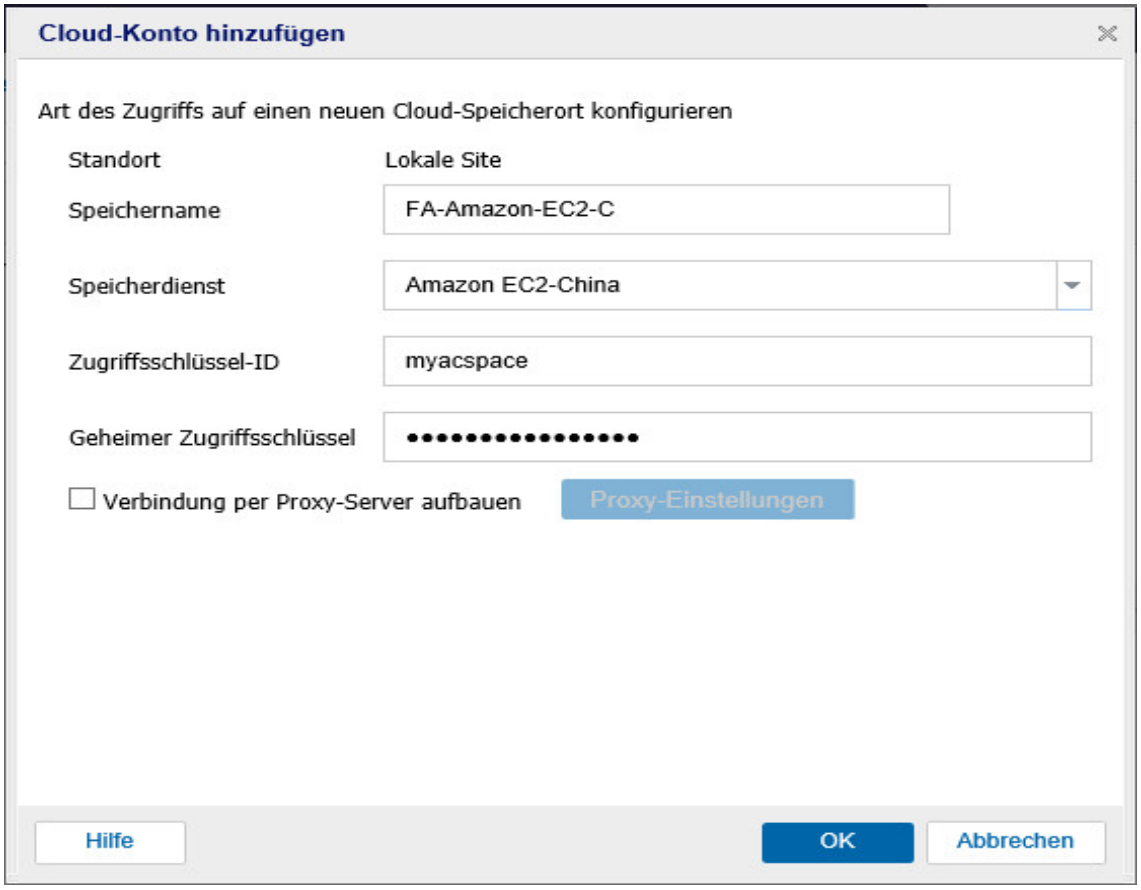
   Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

   Das Cloud-Konto wird zur Konsole hinzugefügt.

   Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Hinzufügen eines Cloud-Kontos für Amazon EC2-China

Fügen Sie ein Cloud-Konto für Amazon EC2-China zum Kopieren von Dateien oder Wiederherstellungspunkten in Cloud-Speicher hinzu. Sie können dieses Konto verwenden, wenn Sie Tasks für einen Plan für Virtual Standby to Cloud oder Instant Virtual Machine auf Amazon EC2 erstellen.



Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Geben Sie für **Display Name** einen eindeutigen Namen an.

   Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.

5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Zugriffsschlüssel-ID

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Geheimer Zugriffsschlüssel

   Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Bewahren Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

   Proxy-Einstellungen

   Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

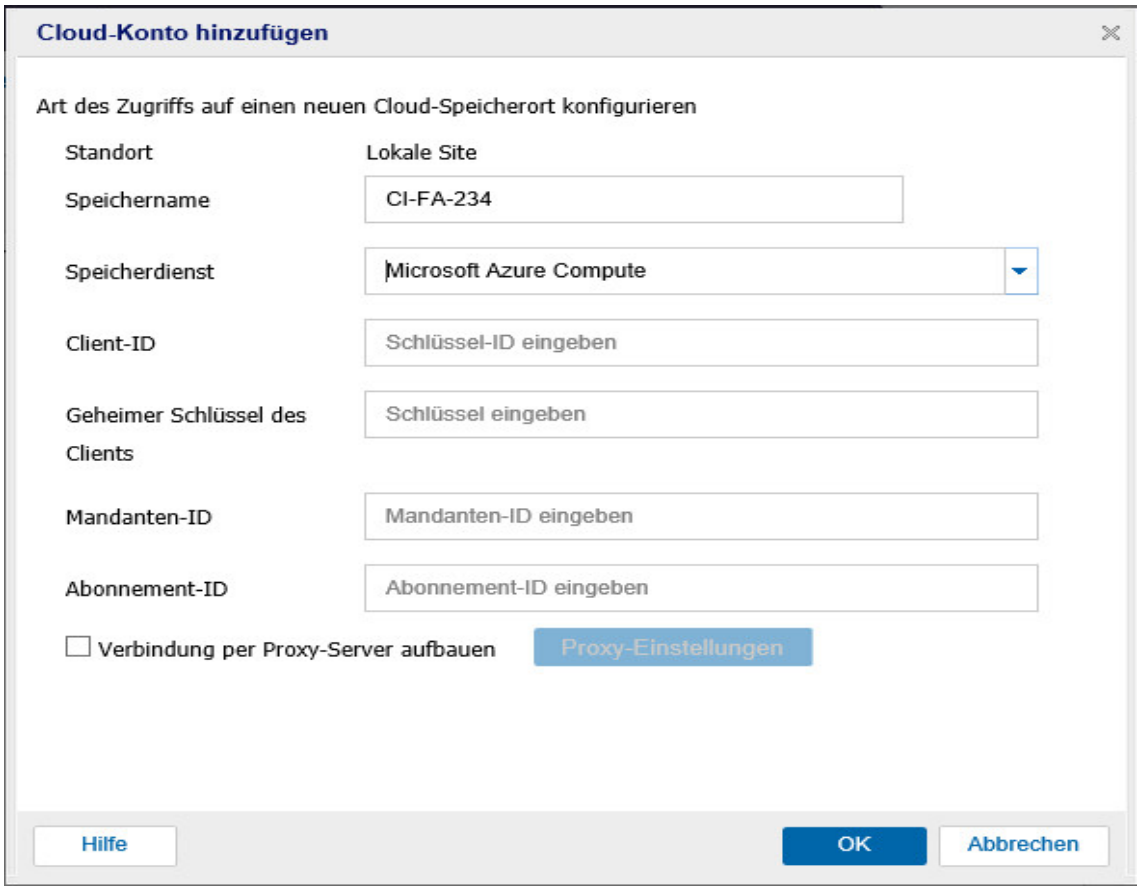
   Das Cloud-Konto wird zur Konsole hinzugefügt.

   Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Hinzufügen eines Cloud-Kontos für Microsoft Azure Compute

Fügen Sie ein Cloud-Konto für Windows Azure zum Kopieren von Dateien oder Wiederherstellungspunkten zu Cloud-Speichern hinzu. Sie können dieses Konto verwenden, wenn Sie Tasks für die Pläne Virtual Standby zu Cloud oder Instant Virtual Machine auf Microsoft Azure erstellen.

Hinweis: Um ein Cloud-Konto für Microsoft Azure hinzuzufügen, müssen Sie die erforderlichen Voraussetzungen erfüllen. Informationen finden Sie unter Komponenten.



Gehen Sie wie folgt vor:

1. Melden Sie sich an auf Arcserve Unified Data Protection und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.

4. Als **Kontonamen** geben Sie einen eindeutigen Namen an.

   Kontoname gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Speichernamen haben.

5. Wählen Sie die Option aus der Dropdownliste **Konten**.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Client-ID

   Bezieht sich auf die Anwendungs-ID der Anwendung Azure Active Directory. Kopieren Sie Ihre Client-ID im Text-Editor.

   Client-Geheimschlüssel

   Bezieht sich auf den Authentifizierungsschlüssel, der für die Active Directory Azure-Anwendung generiert wurde, die Sie als Client-ID eingeben. Kopieren Sie Ihren Client-Geheimschlüssel in den Texteditor.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Speicherort aufbewahren. Bewahren Sie Ihren geheimen Schlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode auf und übertragen Sie ihn nicht über unsichere Kanäle.

   Mandanten-ID

   Verweist auf die ID des Azure Active Directory, wo Sie die Active Directory Azure-Anwendung erstellt haben. Kopieren Sie die Mandanten-ID im Texteditor.

   Abonnement-ID

   Verweist auf einen Globally Unique Identifier (GUID), der Ihr Abonnement eindeutig für die Nutzung von Azure Services identifiziert. Kopieren Sie Ihre Abonnement-ID im Texteditor.

   Proxy-Einstellungen

   Legt die Proxy-Server-Einstellungen fest. Wählen Sie **Über einen Proxy-Server verbinden**, um diese Option zu aktivieren. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Sie müssen die

entsprechenden Authentifizierungsinformationen angeben, die für die Verwendung des Proxyservers erforderlich sind.

Das Cloud-Konto wird zur Konsole hinzugefügt.

Voraussetzungen für das Hinzufügen eines Cloud-Kontos für Microsoft Azure

Bevor Sie ein Cloud-Konto für Microsoft Azure erstellen können, müssen Sie die folgenden obligatorischen Aufgaben in der angegebenen Reihenfolge durchführen:

1. Bereiten Sie Server auf die Bereitstellung als Arcserve UDP-Konsole und Recovery Point Server vor. Diese Server müssen die Systemanforderungen für die einzelnen Komponenten erfüllen.
2. Stellen Sie sicher, dass Sie die erforderlichen Berechtigungen zum Erstellen einer Anwendung in Azure Active Directory verfügen.

   Eine Anleitung hierzu finden Sie unter Azure Active Directory-Berechtigungen überprpüfen in der Microsoft-Dokumentation.
3. Erstellen einer Active Directory Azure-Anwendung. Kopieren Sie in einem Texteditor (z.B. Notepad) die Anwendungs-ID der Anwendung und bezeichnen Sie diese als Client-ID.

   Eine Anleitung hierzu finden Sie unter Azure Active Directory-Berechtigungen überprpüfen in der Microsoft-Dokumentation.
4. Nach Abrufen der Anwendungs-ID erzeugen Sie einen Authentifizierungsschlüssel für diese Anwendung. Kopieren Sie Authentifizierungsschlüsselzeichenfolge in den Texteditor (z.B. Notepad) und bezeichnen Sie die Zeichenfolge als Client-Geheimschlüssel.

   Eine Anleitung hierzu finden Sie unter Anwendungs-ID und Anwendungsschlüssel abrufen in der Microsoft-Dokumentation.
5. Erhalten Sie die Tenant-ID, die der ID des Azure Active Directory entspricht, in dem Sie die Anwendung erstellt haben. Kopieren Sie die ID in einem Texteditor (z.B. Notepad) und bezeichnen Sie sie als Mandanten-ID.

   Eine Anleitung hierzu finden Sie unter Mandanten-ID abrufen in der Microsoft-Dokumentation.
6. Führen Sie die folgenden Schritte aus, um der Anwendung eine Teilnehmerrolle zuzuweisen.
   a. Wählen Sie im linken Bereich des Microsoft Azure Portal Menüs **Abonnements**aus.
   b. Wählen Sie Ihr Abonnement.
   c. Wählen Sie die Registerkarte Access Control (IAM).

d. Fügen Sie Ihre Anwendung hinzu.

e. Weisen Sie der Anwendung die Teilnehmerrolle hinzu.

Weitere Informationen finden Sie unter Der Anwendung eine Rolle zuweisen in der Microsoft-Dokumentation.

7. Rufen Sie Ihre Azure-Abonnement-ID ab.

Hinweis: Die Abonnement-ID ist eine GUID, die Ihr Abonnement eindeutig für die Nutzung von Azure Services identifiziert.

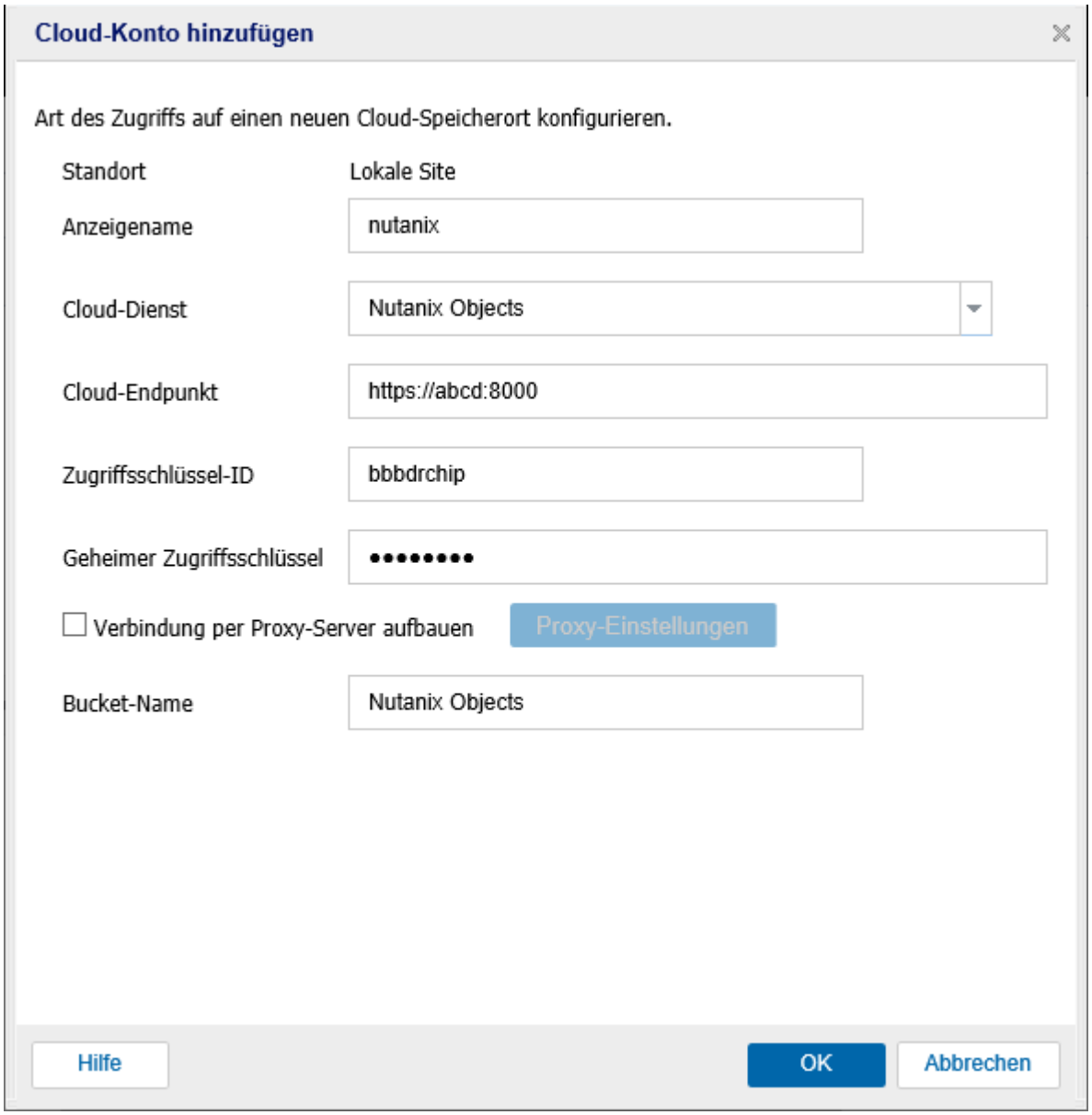
a. Melden Sie sich auf dem Microsoft Azure-Portal an.

b. Klicken Sie im linken Navigationsbereich auf Abonnements.

Die Liste der Abonnements wird zusammen mit der Abonnement-ID angezeigt.

Hinzufügen eines Cloud-Kontos für Nutanix Objects

Fügen Sie ein Nutanix Objects-Cloud-Konto für das Kopieren von Dateien oder Wiederherstellungspunkten in Cloud-Speicher hinzu. Sie können dieses Konto verwenden, während Sie den Wiederherstellungspunkt / den Dateikopie-oder /oder den Dateiarchivierungs-Task erstellen..



Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Geben Sie für **Display Name** einen eindeutigen Namen an.

Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.

5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Speicherendpunkt

   Gibt die Dienst-URL des Anbieters an. (Beispiel: *http:///[Servername]:Portnummer*)

   Zugriffsschlüssel-ID

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Geheimer Zugriffsschlüssel

   Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Bewahren Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

   Proxy-Einstellungen

   Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

   Bucket-Name

   Alle in den Cloud-Anbieter verschobenen oder kopierten Dateien und Ordner werden gespeichert und in den Buckets verwaltet. Buckets sind wie Container für Ihre Dateien und werden verwendet, um Objekte zu gruppieren und

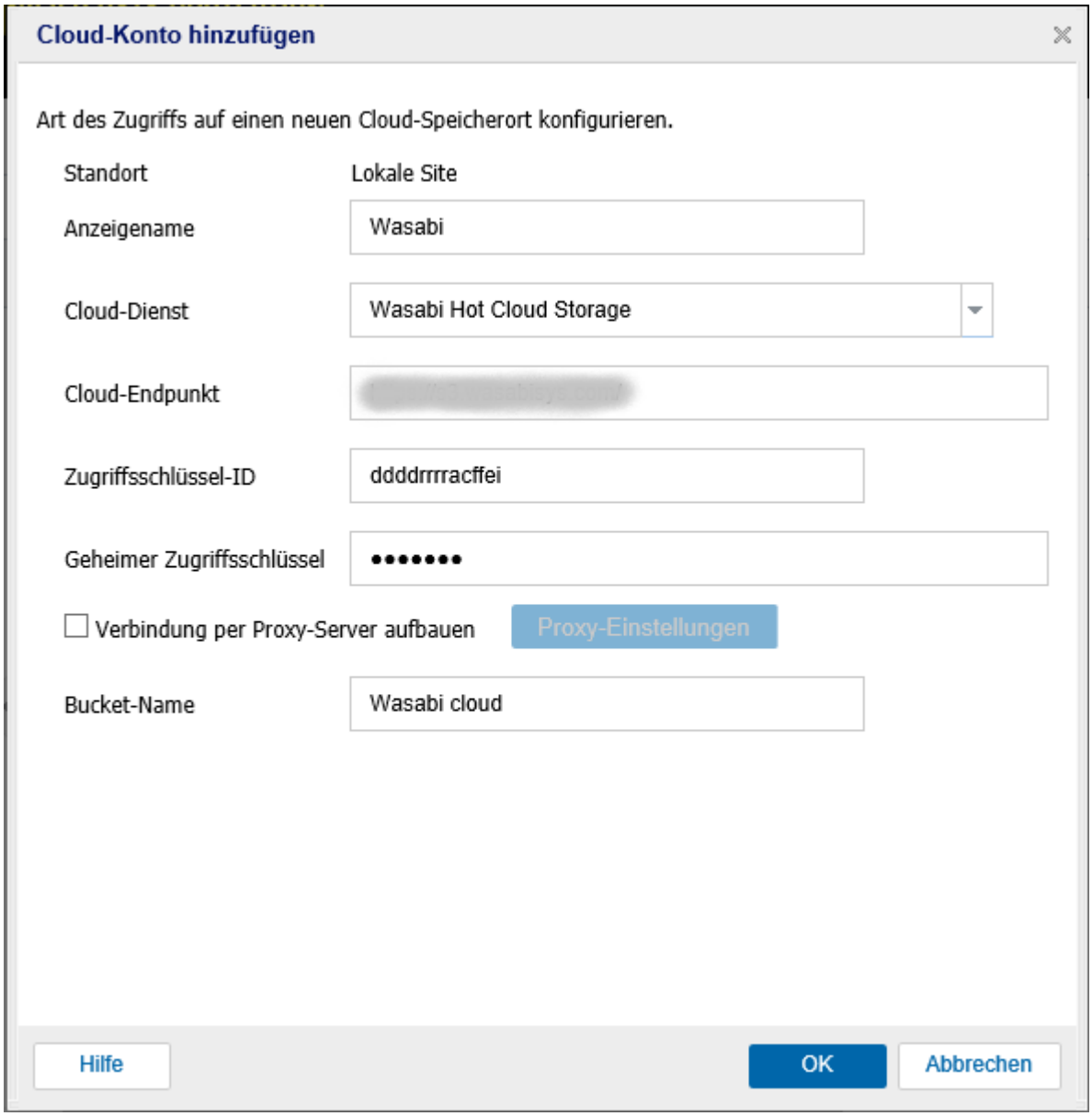
gemeinsam zu verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

Das Cloud-Konto wird zur Konsole hinzugefügt.

Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Hinzufügen eines Cloud-Kontos für Wasabi Hot Cloud Storage

Fügen Sie ein Wasabi Hot Cloud Storage-Cloud-Konto zum Kopieren von Dateien oder Wiederherstellungspunkten in Cloud-Speicher hinzu. Sie können dieses Konto verwenden, während Sie den Wiederherstellungspunkt / den Dateikopie-oder /oder den Dateiarchivierungs-Task erstellen..



Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Geben Sie für **Display Name** einen eindeutigen Namen an.

   Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.

5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Speicherendpunkt

   Wasabi Hot Cloud Storage unterstützt die folgenden drei Regionen:

   - Für die Region Osten der USA ist der Endpunkt s3.wasabisys.com.
   - Für die Region Westen der USA ist der Endpunkt s3.us-west-1.wasabisys.com.
   - Für Region Zentraleuropa ist der Endpunkt s3.eu-central-1.wasabisys.com.

   Zugriffsschlüssel-ID

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Geheimer Zugriffsschlüssel

   Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Bewahren Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

   Proxy-Einstellungen

   Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

   Bucket-Name

   Alle in den Cloud-Anbieter verschobenen oder kopierten Dateien und Ordner werden gespeichert und in den Buckets verwaltet. Buckets sind wie Container für Ihre Dateien und werden verwendet, um Objekte zu gruppieren und

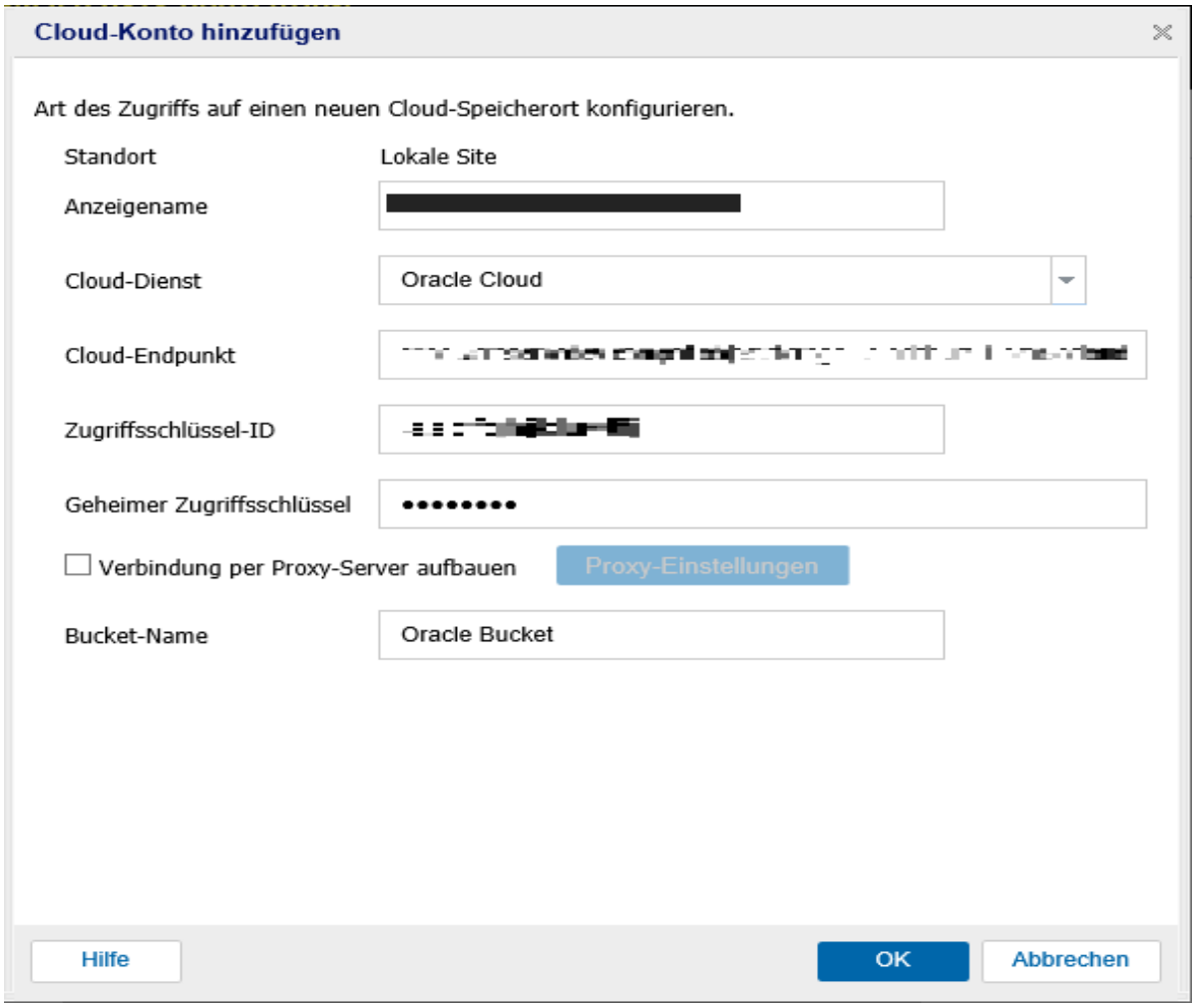
gemeinsam zu verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

Das Cloud-Konto wird zur Konsole hinzugefügt.

Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Hinzufügen eines Cloud-Kontos für Oracle Cloud

Fügen Sie ein Oracle-Cloud-Konto zum Kopieren von Dateien oder Wiederherstellungspunkten in Cloud-Speicher hinzu. Sie können dieses Konto verwenden, während Sie den Wiederherstellungspunkt / den Dateikopie-oder /oder den Dateiarchivierungs-Task erstellen..



Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Geben Sie für **Display Name** einen eindeutigen Namen an.

Anzeigename gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Anzeigenamen haben.

5. Wählen Sie die Option aus der Dropdown-Liste **Cloud Service** aus.

   Mehrere Felder erscheinen für die Konfiguration.

6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Cloud-Endpunkt

   Gibt die Dienst-URL des Anbieters an. Beispiel: *https://namespace.compat.objectstorage.region.oraclecloud.com*

   Bucket-Region

   Bezieht sich auf die Bucket-Region des Anbieters.

   Zugriffsschlüssel-ID

   Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

   Geheimer Zugriffsschlüssel

   Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Bewahren Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

   Proxy-Einstellungen

   Legt die Proxy-Server-Einstellungen fest. Aktivieren Sie das Kontrollkästchen **Verbindung über Proxy-Server herstellen**, wenn Sie diese Option aktivieren möchten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Anschließend müssen Sie die entsprechenden Authentifizierungsinformationen angeben (Domain-Name\Benutzername und Kennwort), die für die Verwendung des Proxyservers erforderlich sind.

   Bucket-Name

Alle in den Cloud-Anbieter verschobenen oder kopierten Dateien und Ordner werden gespeichert und in den Buckets verwaltet. Buckets sind wie Container für Ihre Dateien und werden verwendet, um Objekte zu gruppieren und gemeinsam zu verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

Das Cloud-Konto wird zur Konsole hinzugefügt.

Hinweis: Wenn Sie Dateikopie und Dateiarchiv in der Version Arcserve UDP 6.0 oder einer früheren Version konfiguriert haben und jetzt auf die neueste Version von Arcserve UDP aktualisieren, erstellt Arcserve UDP für Dateiarchiv einen neuen Cloud-Bucket mit dem Suffix **-fa**. Dateikopie verwendet den gleichen Bucket, der in der vorherigen Version verwendet wurde.

Hinzufügen eines Arcserve-Cloud-Kontos

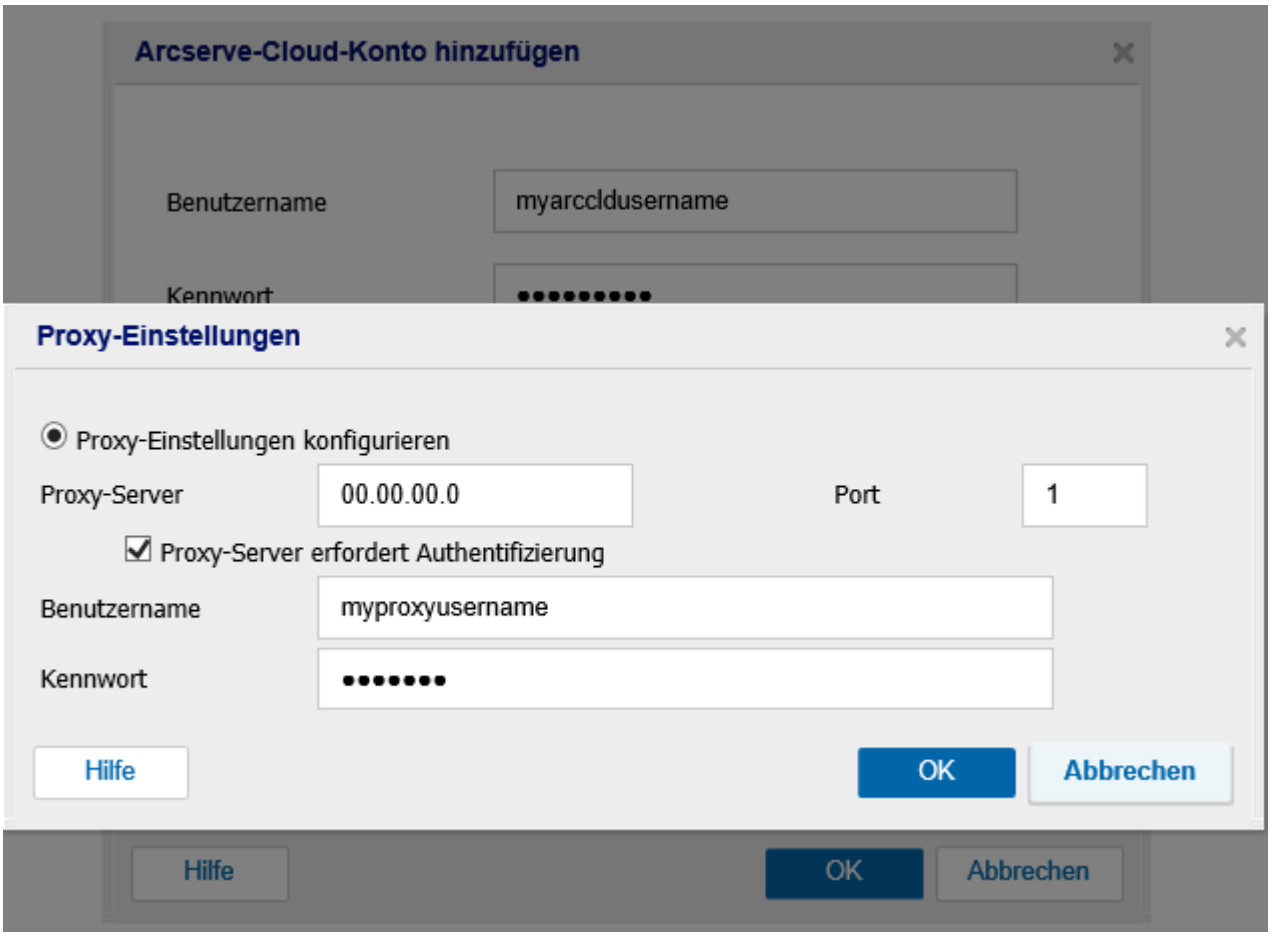
Fügen Sie ein Arcserve-Cloud-Konto hinzu, um Dateien oder Wiederherstellungspunkte in den Arcserve-Cloud-Speicher zu kopieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve UDP an und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich auf **Ziele** und klicken Sie auf **Arcserve Cloud**.

   Der Bildschirm "Ziele: Arcserve Cloud" wird angezeigt.
3. Klicken Sie auf **Arcserve-Cloud-Konto hinzufügen**.

   Der Bildschirm "Arcserve-Cloud-Konto hinzufügen" wird angezeigt.



4. Geben Sie die folgenden Details ein:

   Benutzername

   Gibt den Benutzernamen für das Arcserve-Cloud-Konto an, der bei Arcserve registriert ist.

   Kennwort

   Gibt das Kennwort für das Arcserve-Cloud-Konto des entsprechenden Benutzers an, das bei Arcserve registriert ist.

   Verbindung mit einem Proxy-Server herstellen

   Aktivieren Sie diese Option, um die Verbindung der Arcserve-Cloud über einen Proxyserver herzustellen, der mit dem Internet verbunden ist.

   Proxy-Einstellungen

   Klicken Sie auf "Proxy-Einstellungen", wenn "Verbindung mit einem Proxy-Server herstellen" aktiviert ist.

   Das Fenster "Proxy-Einstellungen" wird angezeigt. Geben Sie die folgenden Details ein und klicken Sie auf **OK**.

Proxy-Server

Gibt die IP-Adresse des Proxy-Servers an.

Port

Gibt die Nummer des Ports an, der auf dem Proxy-Server geöffnet ist.

Proxy-Server erfordert Authentifizierung

Aktivieren Sie diese Option, wenn für den Zugriff auf den Proxy-Server eine Authentifizierung erforderlich sein muss.

Benutzername

Gibt den Namen des Benutzers an, der über Zugriff auf den Proxy-Server verfügt.

Kennwort

Gibt das Kennwort für das Konto des entsprechenden Benutzers an, der über Zugriff auf den Proxy-Server verfügt.

5. Klicken Sie auf **OK**.

   Das Arcserve-Cloud-Konto wird erfolgreich hinzugefügt.

Verwalten von Datenspeichern

Nachdem Sie einen Datenspeicher erstellt haben, müssen Sie möglicherweise verschiedene Vorgänge wie Ändern, Löschen, Anhalten und Starten eines Datenspeichers ausführen.

Sie können auch On-Demand-Zusammenführungsjobs für mehrere Knoten ausführen, um mehr Speicherplatz in einen Datenspeicher zu schaffen.

Der nächste Schritt?

- Überprüfen der Voraussetzungen
- Ändern von Datenspeichern
- Löschen eines Datenspeichers aus der Konsole
- Anhalten von Datenspeichern
- Starten von Datenspeichern
- Überwachen der Datenspeicher-Speicherplatzkapazität
- Durchsuchen von Wiederherstellungspunkten in einem Datenspeicher
- Löschen von Knotendaten aus einem Datenspeicher
- Ändern von gleichzeitig aktivem Knotengrenzwert für manuelle Sicherung
- Ausführen eines manuellen oder On-Demand-Zusammenführungsjobs
- Fehlerbehebung: So verwenden Sie einen Datenspeicher, wenn der Sicherungszielordner voll ist

Überprüfen der Voraussetzungen

Um einen Datenspeicher zu verwalten, müssen Sie folgende Voraussetzungen erfüllen:

- Sie haben bereits einen Datenspeicher hinzugefügt.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Ändern von Datenspeichern

Sie können einen bereits vorhandenen Datenspeicher ändern. Dabei gelten jedoch gewisse Einschränkungen, und Sie können folgende Details eines Datenspeichers nicht ändern:

- Komprimierungsdetails
- Datenspeicher ohne Deduplizierung auf Datenspeicher mit Deduplizierung oder Datenspeicher mit Deduplizierung auf Datenspeicher ohne Deduplizierung.
- Deduplizierungsoptionen: "Daten deduplizieren" und "Blockgröße der Deduplizierung".

Hinweise, bevor Sie einen Datenspeicher ändern:

- Wenn Sie den Pfad oder das Verschlüsselungskennwort des Datenspeichers ändern, werden alle Jobs, die in diesem Datenspeicher ausgeführt werden, abgebrochen, auch solche, die sich in der Warteschlange befinden. Änderungen an Datenspeichernamen, Hash-Speichergröße oder der Anzahl gleichzeitig aktiver Knoten haben keine Auswirkungen auf die laufenden Jobs.
- Für Datenspeicher ohne Deduplizierung: Wenn Sie den Datenspeicherpfad ändern, lassen Sie den Ordner des Sicherungsziels leer.
- Für Datenspeicher mit Deduplizierung: Wenn Sie den Datenspeicherpfad ändern, lassen Sie folgende Ordner leer:
  - Ordner des Sicherungsziels
  - Datenziel
  - Indexziel
  - Hash-Ziel
- Die Optionen für **Verschlüsselungskennwort** können nur bearbeitet werden, wenn Sie beim Erstellen des Datenspeichers die Option **Datenverschlüsselung** aktiviert haben.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird mit einer Liste von verfügbaren Recovery Point Servern angezeigt.
3. Erweitern Sie einen Recovery Point Server.

Die Liste der Datenspeicher, die mit dem Recovery Point Server verknüpft sind, wird angezeigt.

4. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf den Namen des Datenspeichers.
   - Wählen Sie den Datenspeicher aus, und klicken Sie im mittleren Fensterbereich auf das Drop-down-Menü **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.
5. Klicken Sie auf "**Ändern**".

   Die Seite "**Datenspeicher ändern**" wird angezeigt.
6. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf "**Speichern**":

   Recovery Point Server

   Definiert den Recovery Point Server, in dem der Datenspeicher erstellt wird. Der Recovery Point Server wurde bereits standardmäßig hinzugefügt.

   Name des Datenspeichers

   Definiert den Namen des Datenspeichers.

   Datenspeicherordner

   Definiert den Speicherort des Ordners, in dem der Datenspeicher erstellt wird. Klicken Sie auf "Durchsuchen", um den Zielordner auszuwählen.

   Hinweise:

   - Sie können versteckte Volumes jetzt aktivieren und anzeigen. Weitere Informationen finden Sie unter Aktivieren und Anzeigen versteckter Volumes beim Erstellen eines Datenspeichers.
   - Für Datenspeicher mit und ohne Deduplizierung sollte der Zielpfad auf einen leeren Ordner verweisen.

   Beschränkung der gleichzeitig aktiven Knoten auf

   Gibt die Höchstanzahl an gleichzeitigen Jobs für den Datenspeicher an.

   Standardwert: 4

   Bezieht sich auf einen Wert von 1 bis 9999. Der Wert steht für die Anzahl von Jobs, die gleichzeitig ausgeführt werden können. Wenn die Anzahl der ausgeführten Jobs die festgelegte Anzahl erreicht, wird ein weiterer Job in die Warteschlange gereiht und kann nur gestartet werden, wenn ein ausgeführter Job abgeschlossen wird. Fertiggestellte, abgebrochene oder fehlgeschlagene Jobs werden als abgeschlossene Jobs betrachtet.

Die Zahl bezieht sich auf die Jobtypen, nicht auf die Serverknoten. Zum Beispiel zeigt die Zahl 5 an, dass fünf Sicherungsjobs ausgeführt werden. Alle Jobs, die nach diesen fünf Sicherungsjobs geplant sind, werden in die Warteschlange gestellt. Andere Jobs wie z. B. Dateisystem-Katalogjobs können jedoch übermittelt werden.

Wenn der Wert größer als 16 oder 32 ist, werden Meldungen angezeigt, um Sie zu warnen, dass die Hardware stärker ausgelastet wird.

Hinweis: Eine Beschränkung der Anzahl wirkt sich nur auf den ausgehenden, nicht auf den eingehenden Replikationsjob aus. Eine Beschränkung der Anzahl wirkt sich nicht auf Wiederherstellungs- oder BMR-Jobs aus. Solche Jobs werden nicht in Warteschlangen gereiht.

Deduplizierung aktivieren

Gibt an, dass die Deduplizierung für diesen Datenspeicher aktiviert ist. Arcserve UDP unterstützt beide Arten der Deduplizierung: Deduplizierung an der Quelle und globale Deduplizierung. Deduplizierung an der Quelle vermeidet, dass Datenblöcke von spezifischen Agenten mehrfach über das Netzwerk übertragen werden. Globale Deduplizierung beseitigt doppelte Daten auf allen Client-Rechnern basierend auf der Ebene von Volume-Clustern.

Blockgröße der Deduplizierung

Definiert die Größe der Deduplizierungsblöcke. Die Optionen sind 4 KB, 8 KB, 16 KB, 32 KB und 64 KB. Die Größe der Deduplizierungsblöcke wirkt sich auch auf die geschätzte Deduplizierungskapazität aus. Wenn Sie beispielsweise den Standardwert von 16 KB in 32 KB umändern, wird die geschätzte Deduplizierungskapazität verdoppelt. Eine Vergrößerung der Deduplizierungsblockgröße kann den Deduplizierungsprozentsatz verringern.

Hash-Arbeitsspeicherzuordnung

Gibt den physischen Arbeitsspeicher an, den Sie zuordnen, um Hash-Werte beizubehalten. Dieses Feld ist vorab mit einem Standardwert ausgefüllt. Der Standardwert basiert auf der folgenden Formel:

Wenn der physische Arbeitsspeicher des RPS kleiner als 4 GB ist (oder gleich 4 GB ist), ist der Standardwert der **Hash-Arbeitsspeicherzuordnung** identisch mit dem physischen Arbeitsspeicher des RPS.

Wenn der physische Arbeitsspeicher des RPS größer als 4 GB ist, berechnet Arcserve UDP den derzeit verfügbaren freien Speicherplatz. Nehmen wir an, dass der verfügbare freie Speicherplatz derzeit X GB beträgt. Arcserve UDP überprüft folgende Bedingungen:

- Wenn (X * 80 %) > = 4 GB, lautet der Standardwert der **Hash-Arbeitsspeicherzuordnung** (X * 80 %).
- Wenn (X * 80 %) < 4 GB, lautet der Standardwert der **Hash-Arbeitsspeicherzuordnung** 4 GB.

  Beispiel: Wir gehen davon aus, dass der RPS über 32 GB freien physischen Speicherplatz verfügt. Außerdem nehmen wir beim Erstellen des Datenspeichers an, dass das Betriebssystem und andere Anwendungen 4 GB Arbeitsspeicher verwenden. Der verfügbare freie Arbeitsspeicher zu diesem Zeitpunkt beträgt also 28 GB. Der Standardwert der **Hash-Arbeitsspeicherzuordnung** liegt also bei 22,4 GB (22,4 GB = 28 GB * 80 %).

Hash-Ziel ist auf einem Solid State Drive (SSD)

Gibt an, ob sich der Hash-Ordner auf einem Solid State Drive (SSD) befindet.

Hinweis: Konfigurieren Sie das Hash-Ziel auf dem lokalen SSD, wenn die Option "Hash-Ziel ist auf einem Solid State Drive (SSD)" aktiviert ist.

Datenziel

Definiert den Datenzielordner, in dem die eindeutigen Datenblöcke gespeichert werden sollen. Speichern Sie die Daten, die die ursprünglichen Datenblöcke der Quelle enthalten, auf dem größten Datenträger.

Hinweis: Der Pfad für **Datenziel** sollte auf einen leeren Ordner verweisen.

Indexziel

Definiert den Indexzielordner, in dem die Indexdateien gespeichert werden sollen. Wählen Sie einen anderen Datenträger aus, um die Deduplizierungsverarbeitung zu verbessern.

Hinweis: Der Pfad für **Indexziel** sollte auf einen leeren Ordner verweisen.

Hash-Ziel

Definiert den Pfad, in dem die Hash-Datenbank gespeichert werden soll. Arcserve UDP verwendet den SHA1-Algorithmus, um den Hash für Quelldaten zu generieren. Die Hash-Werte werden von der Hash-Datenbank verwaltet. Durch die Auswahl eines Hochgeschwindigkeits-Solid-State-Drive (SSD) kann die Deduplizierungskapazität gesteigert und der Bedarf an Arbeitsspeicher gesenkt werden. Für eine bessere Hash-Leistung empfehlen wir, das SSD-Volume als NTFS-Dateisystem mit einer Volume-Cluster-Größe von 4 KB zu formatieren.

Hinweis: Der Pfad für **Hash-Ziel** sollte auf einen leeren Ordner verweisen.

Hinweis: Sie können für folgende vier Ordner nicht denselben Pfad angeben: **Datenspeicher, Datenziel, Indexziel** und **Hash-Ziel**.

Komprimierung aktivieren

Gibt an, dass die Einstellungen für die Datenkomprimierung aktiviert sind.

Komprimierungstyp

Gibt an, ob der standardmäßige oder der maximale Komprimierungstyp verwendet werden soll.

Eine Komprimierung wird oft ausgewählt, um den verwendeten Speicherplatz zu verringern, hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit der Sicherung. Sie können eine der drei verfügbaren Optionen aktivieren.

Hinweis: Weitere Informationen finden Sie unter Komprimierungstyp.

Verschlüsselung aktivieren

Gibt an, dass die Verschlüsselungseinstellungen aktiviert sind. Wenn Sie diese Option auswählen, müssen Sie das Verschlüsselungskennwort angeben und bestätigen.

Bei der Datenverschlüsselung werden Daten in ein Format umgewandelt, das ohne den entsprechenden Entschlüsselungsmechanismus nicht verständlich ist. Die Arcserve Unified Data Protection-Lösung verwendet sichere AES-Verschlüsselungsalgorithmen (Advanced Encryption Standard) für größtmögliche Sicherheit und Datenschutz für Ihre Daten. Für Datenspeicher wird "Verschlüsselung" oder "Keine Verschlüsselung" unterstützt. Für "Verschlüsselung" ist nur AES-256 verfügbar.

Ein Kennwort ist nicht erforderlich, wenn Sie versuchen, die Wiederherstellung auf dem gleichen Rechner durchzuführen, auf dem die Sicherung ausgeführt wurde. Wenn Sie jedoch versuchen, die Wiederherstellung auf einem anderen Rechner durchzuführen, ist ein Kennwort erforderlich. Standardmäßig ist nur für die erste Anmeldung ein Kennwort erforderlich. Um das Kennwort auch nach der ersten Anmeldung einzugeben, muss der Administrator Arcserve den Erweiterungsdienst des UDP Agent-Explorers manuell anhalten.

Warnung per E-Mail senden, wenn ein Ziel die Kapazitätsgrenze erreicht

Durch Wahl dieser Option sendet der Datenspeicher eine Warnung per E-Mail. Der RPS sendet eine Warnung per E-Mail an den Empfänger, wenn der Zielordner des Datenspeichers fast voll ist.

E-Mail konfigurieren

Diese Schaltfläche wird nur angezeigt, wenn Sie die Option *Warnung per E-Mail senden, wenn ein Ziel die Kapazitätsgrenze erreicht* aktivieren. Mit der Schaltfläche können Sie eine E-Mail-Benachrichtigungen-ID angeben, um Warnungen zu empfangen. Klicken Sie auf die Schaltfläche **E-Mail konfigurieren**,

um globale E-Mail-Einstellungen von "Konsole>Einstellungen>Konfiguration von E-Mail und Warnung" zu laden. Wenn keine globalen E-Mail-Einstellungen verfügbar sind, wird durch Klicken auf die Schaltfläche **E-Mail konfigurieren** das Dialogfeld **E-Mail-Einstellungen** geöffnet, um die E-Mail-Details zu definieren.

Der Datenspeicher wurde aktualisiert.

Ändern des Datenspeicher-Schwellenwerts

Dieses Thema bietet Informationen zu den Speicherorten der Schwellenwertregistrierung, zum Schwellenwert-Schlüsselnamen und zu den Standardwerten, wann eine Schwellenwert-Fehler- oder Warnmeldung angezeigt wird und wie Sie den Datenspeicher-Schwellenwert ändern können.

Ein Datenspeicher weist eine Schwellenwertkonfiguration für die Speicherplatzkapazität auf, mit der Sie Informationen zur Nutzung des freien Speicherplatzes des Datenspeicherziels überwachen können. In Datenspeichern mit Deduplizierung überwacht der Schwellenwert den zugeordneten Speicher für das Hash-Ziel und den zugeordneten Speicherplatz für Sicherungszielordner, Indexziel und Datenziel. In Datenspeichern ohne Deduplizierung überwacht der Schwellenwert nur den Speicherplatz für den Ordner des Sicherungsziels. Für alle fünf Elemente, die vom Schwellenwert überwacht werden, gibt es zwei Arten von Werten:

- Fehlerschwellenwert
- Warnungsschwellenwert

Der Schwellenwert wird in der Systemregistrierung gespeichert. Sie können den Standardwert manuell ändern.

Schwellenwert-Registrierungsspeicherorte

1. Datenspeicher-Ordner: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\CommStore]
2. Datenziel für Deduplizierung: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\DataRole]
3. Hash-Ziel und -Speicher für Deduplizierung: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Daten Protection\Engine\DataStore\XXXXXXX\GDD\HashRole]

   Hinweis: Die Hash-Rolle überwacht sowohl Speicher- als auch Datenträgerauslastung. "Path" steht für die Auslastung des Datenträgers, "Mem" für die des Speichers.
4. Indexziel für Deduplizierung: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\DataRole]

Schwellenwert-Schlüsselnamen und Standardwerte

Pfadtyp	Schwellenwerttyp	Name des Registrierungsschlüssels	Standardwert	Standardwert (Vor v6.5 Update 1)

Daten-speicherordner	Warnung	WarnPathThreshold	0,05	0,03
	Fehler	ErrorPathThreshold	2048	100
Indexpfad für Deduplizierung	Warnung	WarnPathThreshold	0,05	0,03
	Fehler	ErrorPathThreshold	2048	100
Hash-Pfad für Deduplizierung	Warnung	WarnPathThreshold	0,05	0,03
	Fehler	ErrorPathThreshold	2048	100
Datenrollenpfad für Deduplizierung	Warnung	WarnPathThreshold	0,05	0,03
	Fehler	ErrorPathThreshold	2048	100
Arbeitsspeicher	Warnung	WarnMemThreshold	0,05	0,03
	Fehler	ErrorMemThreshold	30	10

- Ein Wert kleiner als 1 gibt freien Speicherplatz in Prozent an, z. B. 0,05 bedeutet 5 %. Wenn der freie Speicherplatz geringer als 5 % des gesamten Speicherplatzes ist, ist der Warnungsschwellenwert erreicht.
- Ein Wert größer oder gleich 1 gibt tatsächlichen freien Speicherplatz an. Die Einheit ist MB. Beispielsweise bedeutet der Standard 2048 2048 MB. Wenn der freie Speicherplatz kleiner als 2048 MB ist, ist der Fehlerschwellenwert erreicht.

Der Standardschwellenwert soll die Leistung des Datenspeichers steigern. Sie können die Schwellenwerte ändern. Wir empfehlen das Ändern dieser Werte nicht, es sei denn, zusätzlicher Speicherplatz wird benötigt.

Führen Sie diese Schritte aus, um den Schwellenwert zu konfigurieren:

1. Navigieren Sie zum jeweiligen Registrierungsspeicherort.
2. Ändern Sie den Standardwert für den Schwellenwert manuell.

Nur das Hash-Ziel ändern

Wenn ein Datenspeicher mit Deduplizierung geändert wird, kann nur das Hash-Pfad-Ziel in einen leeren Ordner geändert werden. Arcserve UDP regeneriert den Hash-Pfad für den neuen Datenspeicher. Dieses Verfahren ist nützlich, wenn der Hash-Ordner nicht genügend Speicherplatz besitzt und alle Jobs abgebrochen werden. Sie können den Datenspeicher modifizieren und einen neuen Hash-Zielordner angeben.

Wechseln der Hash-Ziel-Modi

Wenn Sie einen Deduplizierungsdatenspeicher erstellen, geben Sie an, ob sich das Hash-Ziel auf einem Solid State Drive (SSD-Modus) oder auf dem Festplattenlaufwerk (RAM-Modus) befindet. Wenn Sie die Festplatte als Hash-Ziel konfiguriert haben, benötigen Sie mehr Speicher, um den Hash-Schlüssel zu bearbeiten. Wenn Ihre Sicherungsgröße wächst, dann wird dadurch möglicherweise Ihr gesamter Speicher ausgelastet. In diesem Fall können Sie ein SSD hinzufügen, um mehr Daten zu sichern. Wenn Sie ein SSD als Hash-Ziel konfiguriert haben, dann benötigen Sie weniger Speicher, um Hash-Schlüssel zu verarbeiten. Wenn Sie zu einem Rechner mit mehr Speicher wechseln, dann sollten Sie für eine schnellere Hash-Verarbeitung in den RAM-Modus wechseln.

Um das Hash-Ziel von RAM auf SSD oder von SSD auf RAM zu wechseln, ermöglicht es Ihnen Arcserve UDP, einen vorhandenen Datenspeicher und den Modus nach Bedarf zu ändern.

Sie können einen vorhandenen Datenspeicher sogar dann ändern, wenn er ausgeführt wird. Allerdings wird der Datenspeicher neu gestartet, nachdem Sie die Änderung gespeichert haben.

Ändern vom RAM-Modus in den SSD-Modus

Wenn Sie vom RAM-Modus in den SSD-Modus wechseln, dann würden Sie weniger Speicher benötigen. Arcserve UDP vermindert automatisch den Mindestwert für "Hash-Arbeitsspeicherzuordnung". Allerdings können Sie die Hash-Arbeitsspeicherzuordnung manuell ändern. In diesem Fall ändern Sie die Hash-Zielordner auf SSD. Wenn Sie das Hash-Ziel ändern, kopiert Arcserve UDP automatisch die Hash-Dateien in einen neuen Speicherort auf SSD.

Ändern vom SSD-Modus in den RAM-Modus

Wenn Sie vom SSD-Modus in den RAM-Modus wechseln, sollte der RAM groß genug sein, um die aktuelle Hash-Datenbank unterzubringen. Vor der Änderung hat der Datenspeicher zum Beispiel 30 GB an Hash-Dateien auf SSD erstellt. Nun sollten Sie nach der Änderung mindestens 30 GB Arbeitsspeicher für Hash-Dateien zuordnen. Wenn der RAM nicht ausreichend ist, dann schlägt der Wechsel fehl. In diesem Fall vergrößert Arcserve UDP automatisch die folgenden zwei Parameter:

- Mindestwert der Hash-Arbeitsspeicherzuordnung
- Hash-Arbeitsspeicherzuordnung

Dadurch wird sichergestellt, dass der Datenspeicher nach der Änderung startet.

In diesem Fall ändern Sie die Hash-Zielordner auf das Festplattenlaufwerk. Wenn Sie das Hash-Ziel ändern, kopiert Arcserve UDP automatisch die Hash-Dateien an einen neuen Speicherort auf dem Festplattenlaufwerk.

Starten von Datenspeichern

Wenn Sie einen laufenden Datenspeicher für eine routinemäßige Wartungsprüfung angehalten haben, können Sie den Datenspeicher nach Abschluss der Wartungsprüfung erneut starten. Wenn Sie den Datenspeicher starten, werden die ausstehenden Jobs ab dem Punkt, an dem sie unterbrochen wurden, gestartet.

Hinweis: Beim Starten eines Deduplizierungsdatenspeichers nimmt das Laden der Hash-Daten von der Festplatte in den Speicher je nach Hash-Größe eine gewisse Zeit in Anspruch. Der Fortschritt des Datenspeichers wird im rechten Fensterbereich als Prozentsatz angezeigt.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird mit einer Liste von verfügbaren Recovery Point Servern angezeigt.
3. Erweitern Sie einen Recovery Point Server.

   Die Liste der Datenspeicher, die mit dem Recovery Point Server verknüpft sind, wird angezeigt.
4. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf den Namen des Datenspeichers.
   - Wählen Sie den Datenspeicher aus, und klicken Sie im mittleren Fensterbereich auf das Drop-down-Menü **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.
5. Klicken Sie auf **Starten**.

   Im rechten Fensterbereich wird die Information angezeigt, dass der Datenspeicher startet. Das Statussymbol für den ausgewählten Datenspeicher ändert sich von **Angehalten** in **Wird ausgeführt**.

Anhalten von Datenspeichern

Wenn ein Datenspeicher nicht ausgeführt werden soll, verwenden Sie die Option "Anhalten". Beim Anhalten eines Datenspeichers wird sichergestellt, dass kein Job darauf ausgeführt wird.

Hinweise:

- Wenn Sie einen Datenspeicher anhalten, werden alle auf diesem Datenspeicher ausgeführten Jobs, auch Jobs in der Warteschlange, abgebrochen.
- Wenn Sie einen Datenspeicher anhalten, während ein Replikationsjob ausgeführt wird, startet der Replikationsjob nach dem Neustart des Datenspeichers ab derselben Position, an der Sie den Datenspeicher angehalten haben.
- Wenn Sie den Datenspeicher zu einem Zeitpunkt anhalten, zu dem ein Replikationsjob (zum Beispiel Job-10) ausgeführt wird und zwei weitere Sicherungsjobs (zum Beispiel Job-11, Job-12) abgeschlossen sind, werden die Replikationsjobs nach einem Neustart des Datenspeichers nacheinander abgeschlossen (Job-10, Job-11, Job-12).

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird mit einer Liste von verfügbaren Recovery Point Servern angezeigt.
3. Erweitern Sie einen Recovery Point Server.

   Die Liste der Datenspeicher, die mit dem Recovery Point Server verknüpft sind, wird angezeigt.
4. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf den Namen des Datenspeichers.
   - Wählen Sie den Datenspeicher aus, und klicken Sie im mittleren Fensterbereich auf das Drop-down-Menü **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.
5. Klicken Sie auf "**Anhalten**".

   Das Dialogfeld "**Bestätigen**" wird geöffnet.
6. Wählen Sie "**Ja**" aus, um den Datenspeicher anzuhalten.

Im rechten Fensterbereich wird die Information angezeigt, dass der Datenspeicher angehalten wird.

Der Datenspeicher wird angehalten, und das Statussymbol für den ausgewählten Datenspeicher ändert sich von **Wird ausgeführt** in **Angehalten**.

Löschen eines Datenspeichers aus der Konsole

Wenn Sie einen Datenspeicher nicht mehr verwenden möchten, können Sie ihn löschen. Durch die Löschung wird der Datenspeicher aus der Konsole entfernt. Im Recovery Point Server ist der gelöschte Datenspeicher allerdings weiterhin vorhanden.

Hinweise:

- Sie können den gelöschten Datenspeicher bei Bedarf importieren.
- Um einen Datenspeicher zu löschen, der mit Plänen verknüpft ist, müssen Sie zunächst den Plan löschen, der mit dem Datenspeicher verknüpft ist.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird mit einer Liste von verfügbaren Recovery Point Servern angezeigt.
3. Erweitern Sie einen Recovery Point Server.

   Die Liste der Datenspeicher, die mit dem Recovery Point Server verknüpft sind, wird angezeigt.
4. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf den Namen des Datenspeichers.
   - Wählen Sie den Datenspeicher aus, und klicken Sie im mittleren Fensterbereich auf das Drop-down-Menü **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.
5. Klicken Sie auf **Löschen**.

   Ein **Bestätigungsdialogfeld** wird geöffnet.

   Hinweis: Wenn der Datenspeicher mit einem Plan verknüpft ist, wird anstelle des Bestätigungsdialogfelds ein **Warnungsdialogfeld** angezeigt.
6. Klicken Sie auf **Ja**.

   Der Datenspeicher wurde entfernt.

Löschen von Knotendaten aus einem Datenspeicher

Als Speicheradministrator möchten Sie möglicherweise gesicherte Knotendaten von einem Datenspeicher löschen, um Speicherplatz freizugeben und Ihren Speicherplatz effizient zu verwalten. Mit Arcserve UDP können Sie die Knotendaten in einem Datenspeicher auswählen und löschen. Sie können mehrere Knoten in einem Datenspeicher auswählen. Sie können alle Typen von Knotendaten, einschließlich der verschlüsselten Daten und der deduplizierten Daten, löschen. Der Datenspeicher sollte sich im ausgeführten Status befinden, wenn Sie diesen Job starten. Dieser Job wird als Bereinigungsjob bezeichnet.

Hinweis: Sie können nur löschen, wenn der Knoten keinen Job ausführt (beispielsweise Sicherungs-/Wiederherstellungs-/Zusammenführungsjob).

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Klicken Sie auf den Datenspeicher, der die Knotendaten enthält, die Sie löschen möchten.
3. Die **Übersichtsseite der Wiederherstellungspunkte** wird angezeigt.
4. Wählen Sie den Knoten aus, der gelöscht werden soll.

   Warnung! Wählen Sie nur aus, und klicken Sie nicht auf den Knotennamen. Wenn Sie auf den Knotennamen klicken, wird eine andere Seite geöffnet, auf der Sie die Löschen-Aktion nicht ausführen können.
5. Klicken Sie auf **Aktionen**, **Löschen**.

   Hinweis: Wenn Sie einen Deduplizierungsdatenspeicher verwenden, wird der Speicherplatz auf der Festplatte nach dem Löschen der Wiederherstellungspunkte eines Knotens eventuell nicht sofort freigegeben. Die Verzögerung entsteht, weil für Deduplizierungsdatenspeicher Folgendes gilt:

   - Der Prozess für die Backend-Bereinigung und -Wiedergewinnung wird für einen Zeitpunkt angesetzt, zu dem sich der Datenspeicher im Leerlauf befindet.
   - Teile der Datenblöcke der gelöschten Wiederherstellungspunkte des betreffenden Knotens werden eventuell noch von Wiederherstellungspunkten anderer Knoten verwendet.

     Wie viel Festplattenplatz zurückgewonnen werden kann, hängt vom Deduplizierungsverhältnis des Knotens ab, den Sie löschen möchten.
6. Bestätigen Sie, dass Sie die Knotendaten löschen möchten.

Der Bereinigungsjob wird initiiert, und die Knotendaten werden aus der Datenquelle gelöscht. Der Status des Bereinigungsjobs wird unter **Letzte Ereignisse** und in den Protokollen angezeigt.

Überwachen der Datenspeicher-Speicherplatzkapazität

ARCserve UDP-Datenspeicher werden auf RPS-Volumes oder freigegebenen Remote-Datenträgern erstellt. Der Mechanismus zur Überwachung der Datenspeicher-Speicherplatzkapazität unterstützt Sie bei der Überwachung der Verwendung des Zielordners, wenn das Ziel die Kapazitätsgrenze erreicht. Der freie Speicherplatz im Zielordner reicht nicht für die Ausführung des Datenspeichers aus. Eine E-Mail-Warnung kann gesendet werden, wenn der Datenspeicher die E-Mail-Warnmeldungskonfigurationaktiviert hat. Das Aktivitätsprotokoll stellt die Ausgabe bereit. Inzwischen wird der Status der ausgeführten Datenspeicher in "Nur wiederherstellen" geändert. Infolgedessen wird verhindert, dass neue Sicherungs-/Replikationsjobs neue Sicherungsdaten sichern.

Die Überwachung umfasst folgende Optionen:

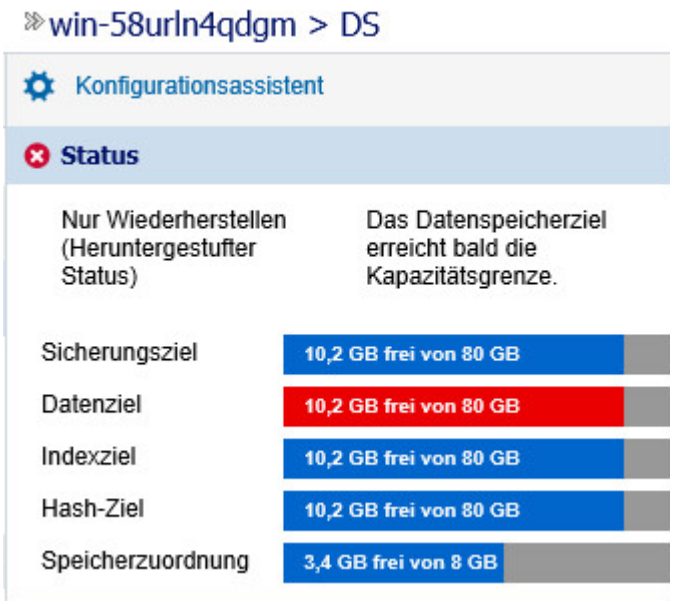
- Ändern des Datenspeicher-Schwellenwerts
- Verwendung des Fehlerschwellenwerts
- Verwendung des Warnungsschwellenwerts
- Aktivieren von E-Mail-Warnungen und Verstehen des E-Mail-Formats

Verwendung des Fehlerschwellenwerts

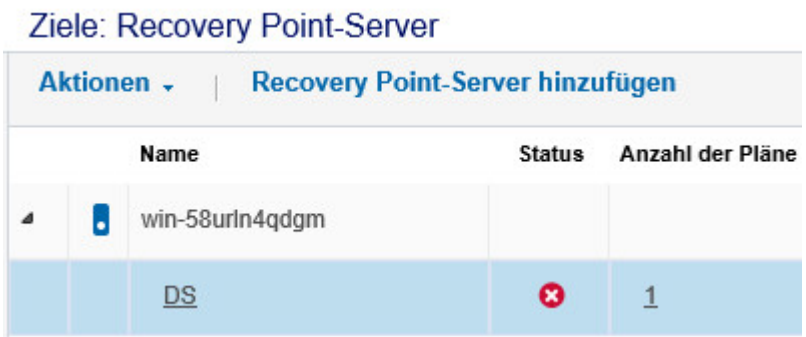
Der Fehlerschwellenwert gibt das Fehlen von erforderlichem freien Speicherplatz für den ausgeführten Datenspeicher an. Außerdem funktionieren einige Kernelkomponenten nicht ordnungsgemäß. In diesem Fall stellt der Datenspeicher den Status nur automatisch wieder her, wenn der Datenspeicher nicht manuell angehalten wird.

Wenn der freie Speicherplatz des Datenspeichers den Fehlerschwellenwert erreicht, gilt Folgendes:

- Der Datenspeicherstatus wird automatisch in "Nur wiederherstellen" (heruntergestufter Status) geändert. Inzwischen können keine neuen Sicherungs-/Replikationsjobs zu diesem Datenspeicher ausgelöst werden. Andere Jobtypen, die keine neuen Daten generieren, können noch ausgelöst werden. Beispielweise Wiederherstellungsjobs und Zusammenführungsjobs.
- Die Datenspeicher-Speicherplatzleiste ist rot markiert.

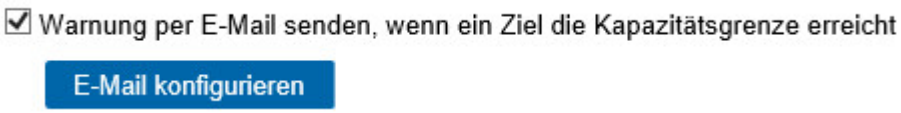


- Der Datenspeicherstatus ist mit einem roten Symbol markiert.



- Aktivitätsprotokolle informieren Sie darüber, dass der Datenspeicher-Zielordner nicht über genügend freien Speicherplatz verfügt, möglicherweise keine neuen Sicherungsdaten speichern kann und die Fehlerstufe erreicht.

- Wenn der Datenspeicher E-Mail-Warnungen sendet, wenn der Zielordner sich der maximalen Kapazität nähert, sendet RPS E-Mail-Warnungen an die Empfänger.

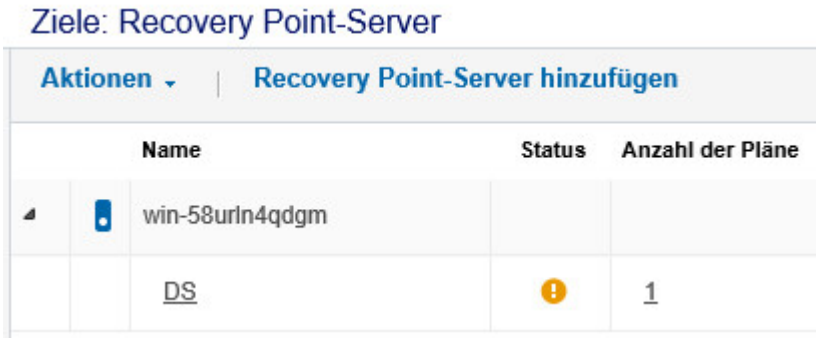


Verwendung des Warnungsschwellenwerts

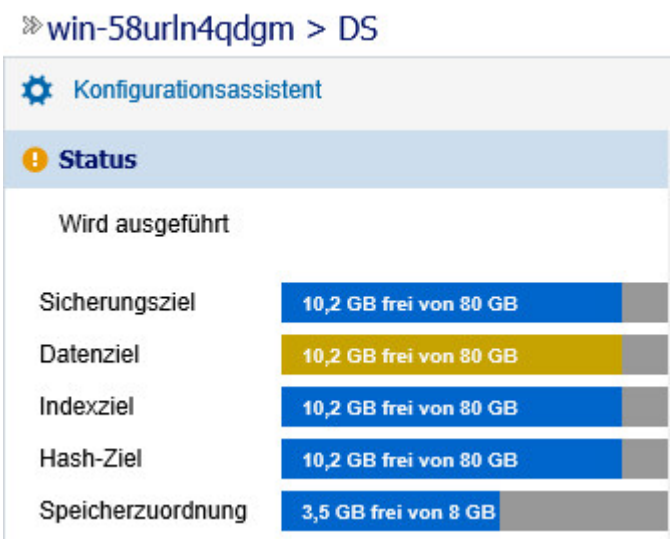
Der Warnungsschwellenwert gibt an, dass noch etwas freier Speicherplatz am Ziel vorhanden ist. Aber der Speicherplatz kann schnell erschöpft sein, wenn neue Sicherungs-/Replikationsjobs weiterhin ausgeführt werden.

Wenn der freie Speicherplatz des Datenspeichers den Warnungsschwellenwert erreicht, gilt Folgendes:

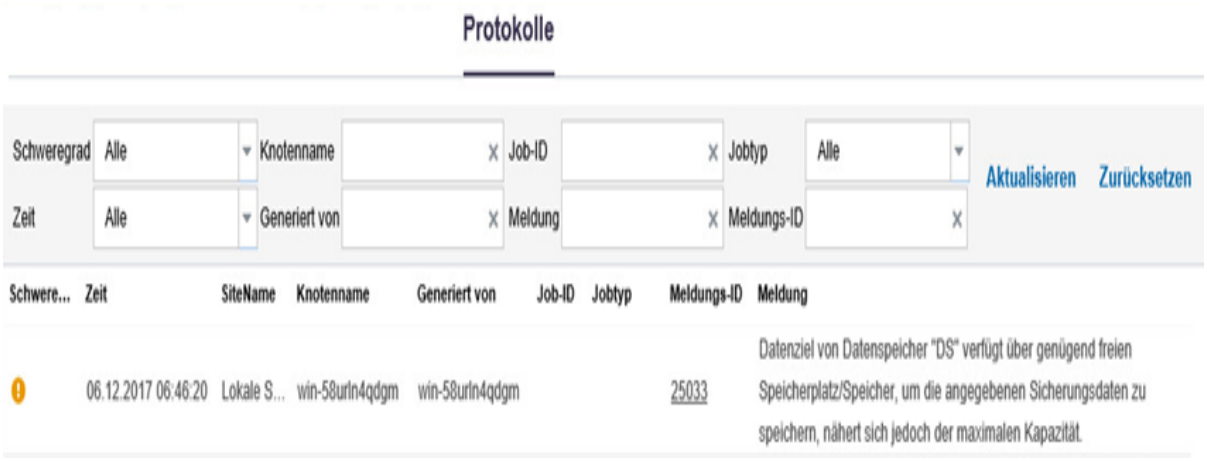
- Der Datenspeicherstatus wird nicht beeinträchtigt, und es wird weiterhin der ursprüngliche Status beibehalten. Z. B. der Status "Wird ausgeführt".
- Der Jobzeitplan wird nicht beeinträchtigt.
- Der Datenspeicherstatus ist mit einem gelben Ausrufezeichen markiert.



- Die Datenspeicher-Speicherplatzleiste ist gelb markiert.



- Ein Aktivitätsprotokoll informiert Sie darüber, dass der Zielordner des Datenspeichers sich der maximalen Kapazität nähert und die Warnstufe erreicht hat.



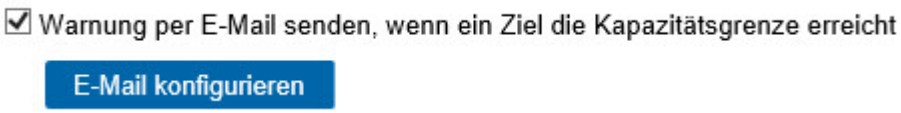
- Wenn der Datenspeicher E-Mail-Warnungen sendet, wenn der Zielordner sich der maximalen Kapazität nähert, sendet RPS E-Mail-Warnungen an die Empfänger.

Aktivieren von E-Mail-Warnungen und Verstehen des E-Mail-Formats

Wenn die Kapazität des Datenspeicher-Ziels nahezu erreicht ist oder der freie Speicherplatz des Zielordners den Warnungs- oder Fehlerschwellenwert erreicht, wird eine E-Mail-Warnung an spezielle Empfänger gesendet, um sie über die Situation zu informieren. Um eine E-Mail-Warnung zu erhalten, müssen Sie die E-Mail-Einstellungen konfigurieren und die Option zum Empfangen von E-Mail-Warnungen aktivieren.

Gehen Sie folgendermaßen vor, um die Konfiguration zu aktivieren:

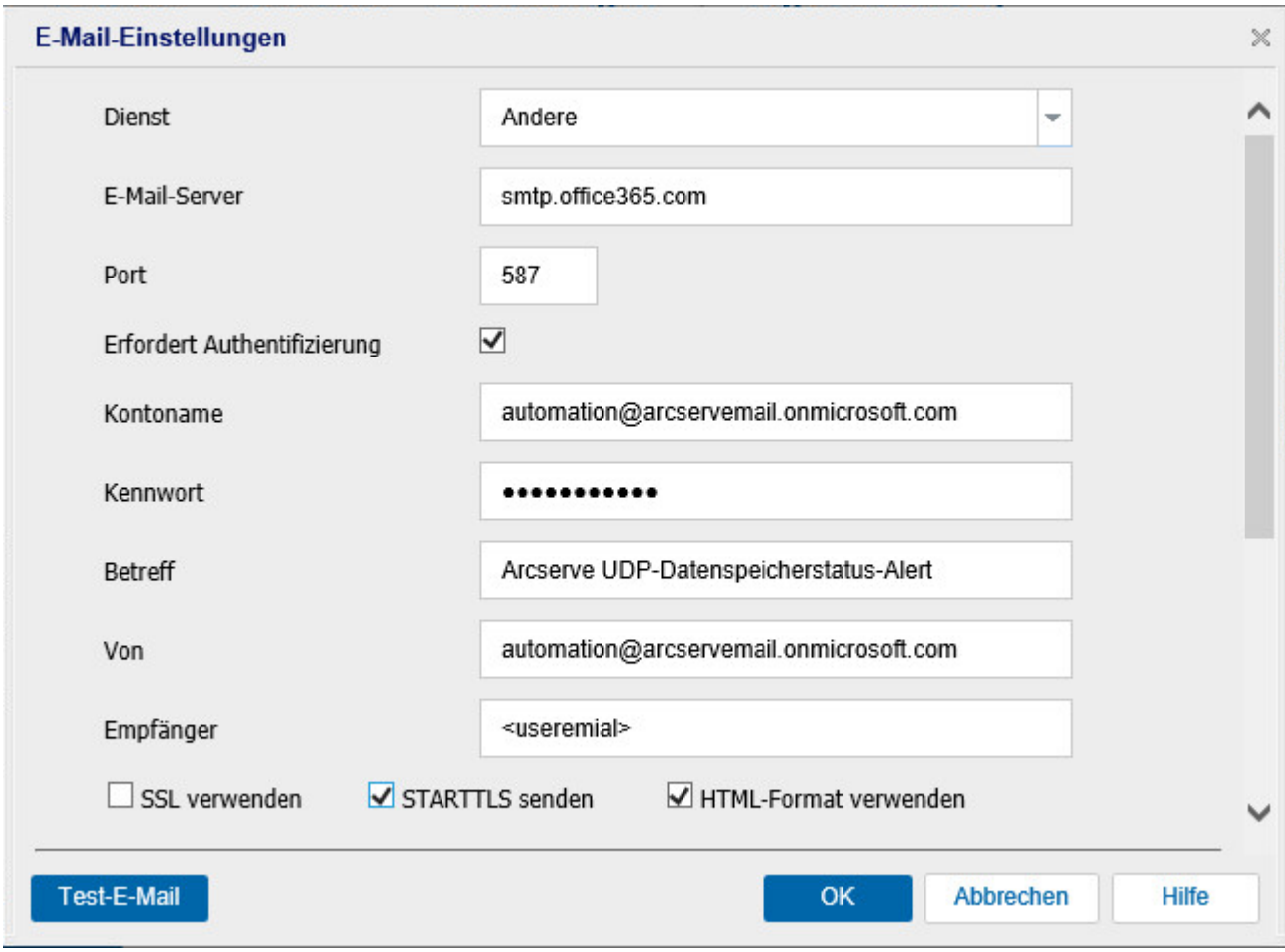
1. Aktivieren Sie das Kontrollkästchen **Warnung per E-Mail senden, wenn ein Ziel die Kapazitätsgrenze erreicht**, wenn Sie den Datenspeicher hinzufügen/ändern/importieren.

   Die Schaltfläche "E-Mail konfigurieren" wird angezeigt.

2. Klicken Sie auf **E-Mail konfigurieren**.

   Das Dialogfeld "E-Mail-Einstellungen" wird angezeigt.



3. Geben Sie die entsprechenden Informationen ein, und klicken Sie auf **OK**.

   Alle Warnungen für den Datenspeicher werden per E-Mail empfangen.

   Hinweis: Mit **Test-E-Mail** können Sie überprüfen, ob die Empfänger-E-Mail-ID die E-Mail empfängt. Wir empfehlen, darauf zu klicken und dies zu testen, bevor Sie dieses Dialogfeld schließen.

Die E-Mail-Warnung wird an die konfigurierten Empfänger gesendet, wenn:

- sich die Datenspeicher-Pfadkapazität von "Fehlerfrei" in "Warnung" ändert (Warnungsschwellenwert erreicht).
- sich die Datenspeicher-Pfadkapazität von "Warnung" in "Fehler" ändert (Fehlerschwellenwert erreicht).
- Der Datenspeicher-Zielordner gibt Speicherplatz frei (wie nach einer Datenspeicherzusammenführung oder einer Vergrößerung des Speicherplatzes des Ziel-Volume). Der Warnungs-/Fehlerschwellenwert ist dann "OK".

Format der Warnung per E-Mail

Warnung Arcserve UDP-Datenspeicherkapazität Fehler

Arcserve UDP-Wiederherstellungspunktserver	WIN-58URLN4QDGM	
Name des Datenspeichers:	DS	
Pfad des Datenspeichers:	E:\Files	
Ebene:	Fehler	
Sicherungsziel:	Gesamt:	81916 MB
	Verfügbar:	10454 MB (12,76%)
Datenziel:	Gesamt:	81916 MB
	Verfügbar:	10454 MB (12,76%)
Indexziel:	Gesamt:	81916 MB
	Verfügbar:	10454 MB (12,76%)
Hash-Ziel:	Gesamt:	81916 MB
	Verfügbar:	10454 MB (12,76%)
Speicherzuordnung:	Gesamt:	8191 MB
	Verfügbar:	3522 MB (43,00%)
Vorkommniszeit:	06.12.2017 06:38:27	

Um die aktuelle Datenspeicherkapazität anzuzeigen, greifen Sie auf folgende Adresse zu: https://win-58urln4qdgm:8015/management/

Wenn Sie weitere Informationen zur Konfiguration der Datenspeicherkapazität benötigen, klicken Sie hier.

Durchsuchen von Wiederherstellungspunkten in einem Datenspeicher

Sie können die Option **Nach Wiederherstellungspunkten suchen** verwenden, um Details zu Wiederherstellungspunkten und Plänen des Datenspeichers anzuzeigen. Sie können beispielsweise die Details zu Datenspeichereinstellungen und aktuellen Ereignissen anzeigen.

Sie können auch in der Ansicht "Freigegebene Ordner" nach Wiederherstellungspunkten suchen.

Um einen Knoten aus einem Datenspeicher zu löschen, lesen Sie den Abschnitt Löschen von Knotendaten aus einem Datenspeicher.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird mit einer Liste von verfügbaren Recovery Point Servern angezeigt.
3. Erweitern Sie einen Recovery Point Server.

   Die Liste der Datenspeicher, die mit dem Recovery Point Server verknüpft sind, wird angezeigt.
4. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf den Namen des Datenspeichers.
   - Wählen Sie den Datenspeicher aus, und klicken Sie im mittleren Fensterbereich auf das Drop-down-Menü **Aktionen**.

   Eine Liste mit Optionen wird angezeigt.

   Hinweis: Sie können auch auf den Namen eines Datenspeichers klicken, um den Datenspeicher zu durchsuchen.
5. Klicken Sie in den Optionen, die nach der Auswahl eines Datenspeichers angezeigt werden, auf **Nach Wiederherstellungspunkten** suchen.

   Die Seite für den ausgewählten Datenspeicher wird mit Informationen zu **Wiederherstellungspunkten** in der Übersicht angezeigt. Beispiele sind Details mit Bezug zu **Datenspeichereinstellungen** und **Letzte Ereignisse**.
6. Um Informationen zum Plan oder zum Datenspeicher zu aktualisieren, wählen Sie den Plan oder den Datenspeicher aus, und klicken Sie auf **Aktionen**, **Aktualisieren**.

7. Wählen Sie zum Wiederherstellen den Knoten "Agent" aus, und klicken Sie auf **Aktionen**, **Wiederherstellen**.

   Das Dialogfeld **Wiederherstellen** wird angezeigt. Darin können Sie die Wiederherstellungsoption festlegen, die Sie für den Datenspeicher verwenden möchten.

FQDN-Support für Datenspeicher

Beim Erstellen eines Datenspeichers auf einem lokalen Datenträger erstellt Arcserve UDP einen freigegebenen Ordner für den Datenspeicher, sodass die Jobs, die auf anderen Servern ausgeführt werden, auf die Daten zugreifen können.

In Arcserve UDP Version 5.0 wurde der Ordner mit dem Hostnamen (z. B. <hostname>\sharename) freigegeben. Wenn der Remote-Server nur auf den RPS mit vollständig qualifiziertem Domänennamen (Fully qualified domain name, FQDN) zugreifen konnte, hatte er dadurch keinen Zugriff auf den RPS mit Hostnamen, und die Jobs schlugen fehl.

Nun kann der Datenspeicherordner mit FQDN oder IP-Adresse freigegeben werden. Dies ermöglicht es dem Remote-Server, auf den Datenspeicher zuzugreifen.

Um dies umzusetzen, aktualisieren Sie den Recovery Point Server auf der Konsole auf FQDN oder IP-Adresse, und erstellen Sie einen neuen Datenspeicher.

Hinweis: Halten Sie bei einer vorhandenen Datenbank den Datenspeicher an, und importieren Sie ihn erneut. Sie können den Datenspeicher überschreiben, anstatt ihn zu löschen. Stellen Sie anschließend die Pläne, die den Datenspeicher verwenden, erneut bereit.

Ausführen eines manuellen oder On-Demand-Zusammenführungsjobs

Als Speicheradministrator können Sie On-Demand-Zusammenführungsjobs ausführen und die Anzahl von beizubehaltenden Wiederherstellungspunkten angeben. Die Werte können sich von den Planeinstellungen unterscheiden. Der Zusammenführungsjob löscht die ausgewählten Sicherungssitzungen aus einem Datenspeicher, um Speicherplatz freizugeben, und sorgt so für eine effiziente Verwaltung Ihres Speicherplatzes. Sie können mehrere Knoten auswählen, und den On-Demand-Zusammenführungsjob ausführen.

Hinweis: Wenn ein Replikationstask bei einem Zusammenführungsjob konfiguriert ist und Sie einen On-Demand-Zusammenführungsjob über den Quelldatenspeicher ausführen, überprüft der Job nicht, ob die Sitzungen repliziert werden oder nicht. Als Folge können die zusammengeführten Sitzungen nicht auf den Zieldatenspeicher repliziert werden, und Sie replizieren am Ende mehr Daten. Angenommen es gibt fünf Sitzungen, s1, s2, s3, s4 und s5, und s1 und s2 werden repliziert. Nun führen Sie einen On-Demand-Zusammenführungsjob auf der Quellseite aus und behalten zwei Sitzungen bei. s4 und s5 werden beibehalten. s4 ist eine vollständige Sitzung. Wenn also der nächste Replikationsjob gestartet wird, muss der Job eine vollständige Sitzung replizieren.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.
3. Klicken Sie im mittleren Fensterbereich auf den Datenspeicher, der die Knotendaten enthält, die Sie zusammenführen möchten.

   Die **Übersichtsseite der Wiederherstellungspunkte** wird angezeigt.
4. Wählen Sie den Knoten aus, der zusammengeführt werden soll.
5. Klicken Sie auf **Aktionen**, **Jetzt zusammenführen**.

   Hinweis: Um mehrere Knoten aus einem Datenspeicher zusammenzuführen, drücken Sie die Strg- oder Umschalt-Taste, wählen Sie die Knoten aus, und klicken Sie dann auf **Aktion**, **Jetzt zusammenführen**.

   Das Dialogfeld **Eine Zusammenführung jetzt durchführen** wird geöffnet.
6. Geben Sie die Anzahl der Wiederherstellungspunkte an, die Sie beibehalten möchten, und klicken Sie auf **OK**.

Der On-Demand-Zusammenführungsjob wird initiiert, und die Knotendaten werden aus der Datenquelle gelöscht. Der Status des Zusammenführungsjobs wird unter "Letzte Ereignisse" und "Protokolle" angezeigt.

Ändern von Schwellenwert gleichzeitig aktiver Knoten für manuelle Sicherung

Um manuelle Backups gleichzeitig für mehrere Knoten zu übermitteln, nicht kontrolliert durch die Option *Schwellenwert gleichzeitig aktiver Knoten* , fügen Sie einen Registrierungsschlüssel auf Recovery Point Server hinzu. Schwellenwerte für gleichzeitig aktive Knoten im Datenspeicher werden auf der Benutzeroberflächedes Datenspeichers konfiguriert.

Gehen Sie wie folgt vor:

1. Der Registrierungs-Editor von Windows wird geöffnet. Zum Öffnen klicken Sie **Start**, geben *Regedit* im Feld "Programme/Dateien durchsuchen" ein und drücken **Enter**.

   Hinweis: Möglicherweise müssen Sie Admin-Anmeldeinformationen angeben, um den Windows-Registrierungs-Editor zu öffnen.

2. Suchen Sie den folgenden Registrierungsschlüssel, und klicken Sie darauf:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

3. Klicken Sie im Menü Bearbeiten auf **Neu** und anschließend auf **DWORD-Wert (32-Bit)**.

   Die Liste der Datenspeicher, die mit dem Recovery Point Server verknüpft sind, wird angezeigt.

4. Wählen Sie "ManualJobsIgnoreConcurrentJobLimit" als Namen für den neuen Eintrag und drücken Sie **Enter**.

5. Klicken Sie mit der rechten Maustaste auf "ManualJobsIgnoreConcurrentJobLimit" und klicken Sie auf **Ändern**.

6. Geben Sie im Datenfeld **Wert** 1 ein und klicken Sie auf **OK**.

7. Verlassen Sie den Registrierungseditor.

   Hinweis: Nach der Aktivierung mit 1 funktioniert der Registrierungsschlüssel "ManualJobsIgnoreConcurrentJobLimit" für alle Datenspeicher auf dem RPS-Server.

Fehlerbehebung: So verwenden Sie einen Datenspeicher, wenn der Sicherungszielordner voll ist

Problem:

So können Sie den Datenspeicher weiterhin verwenden, wenn einer der folgenden Ordner voll belegt ist:

- Sicherungsziel des Datenspeichers
- Deduplizierungsindex
- Hash
- Data

Lösung:

Sicherungszielpfad ändern

1. Datenspeicherung stoppen.
2. Ändern Sie die Pläne, die für diesen Datenspeicher verwendet werden. Richten Sie in der Registerkarte "Ziel" das Ziel auf einen anderen Datenspeicher oder einen freigegebenen Ordner, aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen** und **Speichern** den Plan.
3. Löschen des Datenspeichers.
4. Kopieren Sie die entsprechenden Ordner des Sicherungsziels in ein großes Volume. Vergewissern Sie sich, dass Größe und Anzahl der Dateien im Quell- und Zielordner identisch sind.

   Hinweis: Stellen Sie sicher, dass Sie den Datenspeicher anhalten, bevor Sie den Ordner kopieren. Stellen Sie beim Kopieren sicher, dass alle Dateien in den Zielordner kopiert werden, ohne dass Dateien übersprungen werden.

   Warnung! Das Überspringen von Dateien kann zu Datenbeschädigungen führen. Wenn die Anzahl der Dateien oder Größe zwischen Quell-und Zielordner nicht übereinstimmt, fahren Sie nicht zum nächsten Schritt fort.
5. Datenspeicher importieren. Geben Sie beim Import des Datenspeichers den neuen Daten-/Indexpfad an.
6. Navigieren Sie von der UDP-Konsole aus zu Ressourcen, Zielen und Wiederherstellungspunkt-Servern.
7. Wählen Sie den Datenspeicher unter dem Wiederherstellungspunkt-Server aus.

8. Stellen Sie im rechten Fensterbereich unter Einstellungen sicher, dass der Pfad für das Daten-/Indexziel auf den richtigen Speicherort verweist.

   Wichtig! Während Sie die oben genannten Schritte ausführen, starten Sie den Datenspeicher NICHT, bis Schritt 8 abgeschlossen ist.

9. Starten des Datenspeichers.
10. Ändern Sie die Pläne, die Sie angehalten haben, und konfigurieren Sie sie neu, um den importierten Datenspeicher zu verwenden (gemäß der Anforderung). Klare Auswahl der Option **Diesen Plan unterbrechen** und den Plan **Speichern**.

    Hinweis: Nachdem Sie den Datenspeicher importiert haben, um mit dem neuen Standort zu verlinken, und den Datenspeicher gestartet haben, **wechseln Sie NICHT** in den ursprünglichen Pfad. Solche Maßnahmen können zu Datenbeschädigungen führen.

Daten- oder Indexzielpfad ändern

1. Datenspeicherung stoppen.
2. Kopieren Sie den entsprechenden Ordner (Daten-/Index entsprechend der Anforderung), in ein großes Volume. Vergewissern Sie sich, dass die Größe und Anzahl der Dateien im Quell- und Zielordner gleich sind.

   Hinweis: Stellen Sie sicher, dass Sie den Datenspeicher anhalten, bevor Sie den Ordner kopieren. Stellen Sie beim Kopieren sicher, dass alle Dateien in den Zielordner kopiert werden, ohne dass Dateien übersprungen werden.

   Warnung! Das Überspringen von Dateien kann zu Datenbeschädigungen führen. Wenn die Anzahl der Dateien oder Größe zwischen Quell-und Zielordner nicht übereinstimmt, fahren Sie nicht zum nächsten Schritt fort.

3. Datenspeicher importieren. Geben Sie beim Import des Datenspeichers den neuen Daten-/Indexpfad an.
4. Navigieren Sie von der UDP-Konsole aus zu Ressourcen, Zielen und Wiederherstellungspunkt-Servern.
5. Wählen Sie den Datenspeicher unter dem Wiederherstellungspunkt-Server aus.
6. Stellen Sie im rechten Fensterbereich unter Einstellungen sicher, dass der Daten/Index-Zielpfad auf den richtigen Speicherort verweist.

   Wichtig! Während Sie die oben genannten Schritte ausführen, starten Sie den Datenspeicher NICHT, bis Schritt 6 abgeschlossen ist.

7. Starten des Datenspeichers.

Hinweis: Nachdem Sie den Datenspeicher importiert haben, um mit dem neuen Standort zu verlinken, und den Datenspeicher gestartet haben, **wechseln Sie NICHT** in den ursprünglichen Pfad. Solche Maßnahmen können zu Datenbeschädigungen führen.

Hash-Zielpfad ändern

Weitere Informationen finden Sie in Hash-Pfad ändern.

Verwalten eines Recovery Point Server

Mit Arcserve UDP können Sie verschiedene Vorgänge wie Aktualisierungen, Löschungen, Imports und Upgrades für vorhandene Recovery Point Server durchführen.

Der Recovery Point Server wird auf der Seite **Ziele: Recovery Point Server** unter **Name** angezeigt. Klicken Sie auf der Seite **Ziele: Recovery Point Server** auf die Registerkarte **Aktionen** oder auf den Namen des Recovery Point-Servers, um alle Optionen für die Verwaltung Ihres Recovery Point-Servers abzurufen.

Der nächste Schritt?

- Überprüfen der Voraussetzungen
- Aktualisieren eines Recovery Point Server
- Löschen eines Recovery Point Server aus der Konsole
- Importieren von Datenspeichern
- Installieren/Aktualisieren von Recovery Point-Servern

Überprüfen der Voraussetzungen

Um einen Recovery Point Server zu verwalten, müssen Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich bei der Konsole an.
- Fügen Sie einen Wiederherstellungspunktspeicher hinzu.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Aktualisieren eines Recovery Point Server

Wenn die Anmeldeinformationen oder das Protokoll für den Recovery Point Server geändert wurden, müssen Sie den Recovery Point Server aktualisieren. Anderenfalls funktioniert der Recovery Point Server nicht ordnungsgemäß.

Hinweis: Wenn ein Knoten sowohl als Recovery Point Server als auch als Agent eingesetzt wird und Sie die Anmeldeinformationen oder das Protokoll dieses Knotens ändern, aktualisieren Sie den Knoten über die Seite **Ziele: Recovery Point Server**. Nachdem Sie den Recovery Point Server aktualisiert haben, wird der Plan automatisch für den Agent bereitgestellt. Wenn Sie den Knoten von der Seite **Knoten: Alle Knoten** aktualisieren, werden die Pläne, welche diese Knoten umfassen, nicht erfolgreich bereitgestellt. Um den Plan bereitzustellen, aktualisieren Sie den Knoten erneut über die Seite **Ziele: Recovery Point Server**.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird angezeigt.
3. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf einen Recovery Point Server.
   - Wählen Sie einen Recovery Point Server aus, und klicken Sie im mittleren Menü auf die Drop-down-Liste **Aktionen**.
4. Klicken Sie auf **Aktualisieren**.

   Das Dialogfeld "**Knoten aktualisieren**" wird geöffnet.
5. Ändern Sie die Details nach Bedarf, und klicken Sie auf "**OK**".

   Der Recovery Point Server ist nun aktualisiert.

Löschen eines Recovery Point Server aus der Konsole

Um einen Recovery Point Server aus der Konsole zu entfernen, verwenden Sie die Option **Löschen**.

Hinweis: Wenn Sie einen Recovery Point Server entfernen, werden die zugeordneten Datenspeicher nicht gelöscht. Ein Recovery Point Server, der im Plan verwendet wird, kann nicht gelöscht werden.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird angezeigt.
3. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf einen Recovery Point Server.
   - Wählen Sie einen Recovery Point Server aus, und klicken Sie im mittleren Menü auf die Drop-down-Liste **Aktionen**.
4. Klicken Sie auf **Löschen**.

   Das Dialogfeld **Bestätigen** wird geöffnet.
5. Klicken Sie auf **Ja**.

   Der Recovery Point Server wurde gelöscht.

Importieren von Datenspeichern

Mit der Funktion **Datenspeicher importieren** können Sie einen Datenspeicher zum Recovery Point Server hinzufügen. Sie können alle vorhandenen Datenspeicher zu einem Recovery Point Server importieren. Datenspeicher, die Sie zu einem früheren Zeitpunkt aus einem Recovery Point Server gelöscht haben, stehen für den Import zur Verfügung.

Hinweis: Wenn die Hashdaten eines Deduplizierungsdatenspeichers fehlen oder beschädigt sind, können Sie den Datenspeicher trotzdem importieren. Geben Sie einen leeren Ordner als Hash-Ordner an. Der Datenspeicher startet im **Wiederherstellungsstatus** und eine Fehlermeldung zeigt an, dass die Hash-Rolle des Datenspeichers für den leeren Hash-Ordner nicht in Betrieb ist. Mit dieser Methode können Sie den Datenspeicher nur für Wiederherstellungsaufträge verwenden. Erstellen Sie den Hashwert erneut, falls Sie denSicherungsauftrag ausführen wollen.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird angezeigt.
3. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf einen Recovery Point Server.
   - Wählen Sie einen Recovery Point Server aus, und klicken Sie im mittleren Menü auf die Drop-down-Liste **Aktionen**.
   - Um E-Mail-Alerts zu erhalten, aktivieren Sie das Kontrollkästchen *Warnung per E-Mail senden, wenn ein Ziel die Kapazitätsgrenze erreicht*.

     Hinweis: Wenn zuvor keine Konfiguration erfolgt ist, klicken Sie auf **E-Mail konfigurieren**, um Ihre E-Mail-Einstellungen bereitzustellen.
4. Klicken Sie auf **Datenspeicher importieren**.

   Die Seite **Datenspeicher importieren** wird angezeigt.
5. Führen Sie folgende Aktionen durch, und klicken Sie auf **Weiter**:
   - **Durchsuchen** Sie Ihr System, um den **Ordner des Sicherungsziels** auszuwählen, aus dem Sie den Datenspeicher importieren möchten.
   - Geben Sie das **Verschlüsselungskennwort** ein.

   Hinweis: Lassen Sie das Feld leer, wenn der Datenspeicher nicht verschlüsselt ist.

Nach der Authentifizierung des **Ordners des Sicherungsziels** wird die Seite **Datenspeicher importieren** angezeigt. Sie enthält die Details zum Datenspeicher.

6. Ändern Sie die Details bei Bedarf, und klicken Sie auf **Speichern**.

   Wenn Sie Ordner für Datenziel, Index-Ziel und Hash-Ziel für Deduplizierungs-Datenspeicher kopiert haben, ändern Sie den Ordnerpfad.

   Hinweis: Sie können die Verschlüsselungsoption für vorhandene Datenspeicher nicht aktivieren oder deaktivieren.

   Der Datenspeicher wird zum Recovery Point Server hinzugefügt und im Dialogfeld **Ziele: Recovery Point Server** angezeigt.

Installieren/Aktualisieren von Recovery Point-Servern

Verwenden Sie die Option **Recovery Point Server installieren/aktualisieren** in den folgenden Situationen:

- Wenn die Installation fehlschlägt.
- Wenn Sie ein Upgrade des Produkts durchführen möchten.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird angezeigt.
3. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf einen Recovery Point Server.
   - Wählen Sie einen Recovery Point Server aus, und klicken Sie im mittleren Menü auf die Drop-down-Liste **Aktionen**.
4. Klicken Sie auf **Recovery Point Server installieren/aktualisieren**.

   Die Details zum Installationspfad werden auf derselben Seite über der Liste des hinzugefügten Recovery Point Servers angezeigt.
5. Aktualisieren Sie die Details nach Bedarf.
6. Geben Sie den **Ablaufplan** für die Installation bzw. für das Upgrade an, und klicken Sie auf "OK".

   Die Installation oder das Upgrade wird nach Ablaufplan durchgeführt. Der Fortschritt der Installation bzw. des Upgrade wird im rechten Fensterbereich angezeigt.

   Hinweis: Sie können eine Bereitstellung des Recovery Point-Servers abbrechen, wenn sie für einen späteren Zeitpunkt geplant ist. Um eine Bereitstellung des Recovery Point-Servers abzubrechen, wählen Sie den Agenten aus, und klicken Sie auf "Aktionen", "Agentbereitstellung abbrechen".

So verwalten Sie Arcserve Backup-Server

Sie können Arcserve Backup-Server über die Arcserve UDP-Konsole verwalten. Über die Konsole können Sie Arcserve Backup-Server auch aktualisieren und löschen.

Aktualisieren von Arcserve Backup-Servern

Wenn die Anmeldeinformationen oder der Arcserve Webservice-Port des Arcserve Backup-Servers geändert werden, müssen Sie die entsprechenden Informationen auf der Konsole aktualisieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Konsole an, und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Arcserve Backup-Server**.

   Die Seite **Ziele:** Die Seite **Arcserve Backup-Server** wird im mittleren Fensterbereich angezeigt.
3. Wählen Sie einen Arcserve Backup-Server aus, klicken Sie mit der rechten Maustaste auf den Server, und wählen Sie **Aktualisieren**.

   Die Seite "**Arcserve Backup-Server aktualisieren**" wird angezeigt.
4. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf "**Speichern**":

   Die Seite "**Arcserve Backup-Server aktualisieren**" wird geschlossen.

   Der Arcserve Backup-Server wurde erfolgreich aktualisiert.

Löschen von Arcserve Backup-Servern

Wenn Sie einen Arcserve Backup-Server nicht mehr benötigen, können Sie den Server aus der Konsole löschen. Stellen Sie vor dem Löschen einen Arcserve Backup-Servers sicher, dass der Arcserve Backup-Server in keinem Task eines Plans enthalten ist. Wenn der Server in einem Task enthalten ist, löschen Sie den Task, oder ändern Sie das Sicherungsziel.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Konsole an, und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Arcserve Backup-Server**.

   Die Seite **Ziele: Arcserve Backup-Server** wird im mittleren Fensterbereich angezeigt.
3. Wählen Sie einen Arcserve Backup-Server aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Löschen**.

   Das Bestätigungsdialogfeld wird geöffnet.
4. Klicken Sie auf **Ja**.

   Sie haben den Arcserve Backup-Server erfolgreich aus der Konsole gelöscht.

So verwalten Sie freigegebene Ordner

Sie können freigegebene Ordner über die Arcserve UDP-Konsole verwalten. Sie können den freigegebenen Ordner auch über die Konsole ändern und löschen.

Freigegebenen Ordner ändern

Arcserve UDP ermöglicht Ihnen Details eines hinzugefügten freigegebenen Ordners zu ändern. Falls Informationen zu freigegebenen Ordnern geändert wurden, müssen Sie den in Arcserve UDP hinzugefügten freigegebenen Ordner ändern, damit die Pläne funktionieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an, und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Freigegebene Ordner**.

   Die **Ziele: Die Seite "freigegebene Ordner"** zeigt hinzugefügte freigegebene Ordner in der Mitte an.
3. Klicken Sie zum Verwalten mit der rechten Maustaste auf einen der hinzugefügten freigegebenen Ordner oder markieren Sie einen freigegebenen Ordner und klicken Sie auf **Aktionen**.
4. Klicken Sie in den angezeigten Optionen auf **Update**.

   Das Dialogfeld **Update** wird angezeigt.
5. Ändern Sie die Informationen und klicken Sie auf **OK**.

   Der freigegebene Ordner ist jetzt aktualisiert.

Freigegebenen Ordner löschen

Arcserve UDP ermöglicht Ihnen einen hinzugefügten freigegebenen Ordner zu löschen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an, und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Freigegebene Ordner**.

   Die **Ziele: Die Seite "freigegebene Ordner"** zeigt hinzugefügte freigegebene Ordner in der Mitte an.
3. Klicken Sie zum Verwalten mit der rechten Maustaste auf einen der hinzugefügten freigegebenen Ordneroder markieren Sie einen freigegebenen Ordner und klicken Sie auf **Aktionen**.
4. Klicken Sie in den angezeigten Optionen auf **öschen**.

   Es wird eine **Bestätigung** oder ein **Fehler** eingeblendet.
5. Bestätigungsdialog: klicken Sie zum Löschen auf **OK**.
6. (Optional) Fehlermeldung: beheben Sie den Fehler, und versuchen Sie erneut zu löschen.

   Der freigegebene Ordner ist jetzt aktualisiert.

Eine Remotekonsole verwalten

Nach dem erstellen einer Remotekonsole müssen Sie möglicherweise verschiedene Operationen ausführen, wie z. B.Verbindungen ändern, löschen oder testen.

Der nächste Schritt?

- Ändern einer Remotekonsole
- Löschen einer Remotekonsole
- Remoteverbindung einer Konsole testen

Ändern einer Remote-Konsole

Arcserve UDP ermöglicht Ihnen, die Details einer hinzugefügten Remotekonsole zu ändern. Falls Sie die Verbindungsinformationen für die Remotekonsole geändert haben, müssen Sie das in Arcserve UDP hinzugefügte Konto der Remotekonsole ändern.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an, und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Bereich auf **Ziele**, und klicken Sie auf **Remotekonsole**.

   Die **Ziele: Die Seite "Remotekonsole"** zeigt die hinzugefügten Remotekonsolen in der Mitte an.
3. Klicken Sie zum Verwalten mit der rechten Maustaste auf eine der hinzugefügten Remotekonsolen oder markieren Sie eine Remotekonsole und klicken Sie auf **Aktionen**.

   Die Seite zum **Ändern einer Remotekonsole** wird angezeigt.
4. Ändern Sie die Informationen und klicken Sie auf **OK**.

   Die Remotekonsole wird jetzt aktualisiert.

Löschen einer Remote-Konsole

Arcserve UDP ermöglicht Ihnen , eine Remotekonsole bei Bedarf zu entfernen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an, und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Bereich auf **Ziele**, und klicken Sie auf **Remotekonsole**.

   Die **Ziele: Die Seite "Remotekonsole"** zeigt die hinzugefügten Remotekonsolen in der Mitte an.
3. Klicken Sie zum Verwalten mit der rechten Maustaste auf eine der hinzugefügten Remotekonsolen oder markieren Sie eine Remotekonsoleund klicken Sie auf **Aktionen**.

   Es wird eine **Bestätigung** oder eine **Fehler**meldung angezeigt.

   Bestätigung:

   Wird angezeigt, wenn die Remotekonsole keinem Plan hinzugefügt ist.

   Fehlermeldung:

   Wird angezeigt, wenn die Remotekonsole zu einem vorhandenen Plan gehört.
4. (Optional) Wenn die Fehlermeldung angezeigt wird:
   a. Klicken Sie auf **OK**, um die Fehlermeldung zu schließen.
   b. Öffnen Sie den Plan, dem die Remotekonsole zugeordnet ist.
   c. Löschen Sie den zugehörigen Plan oder ändern Sie den Plan, um die Remotekonsole in der Registerkarte "Ziel" der **Replikation auf einen remote verwalteten RPS** Plan zu ändern.

   Nach dem Entfernen der Remotekonsole aus dem Plan, kehren Sie zur Seite "Remotekonsole" zurück und versuchen Sie, die Remotekonsole erneut zu löschen.
5. Klicken Sie im Bestätigungsdialog auf **Ja**.

   Die Remotekonsole wird jetzt entfernt.

Verbindung zur Remote-Konsole testen

Arcserve UDP ermöglicht Ihnen die Verbindung einer zusätzlichen Remotekonsole zu testen. Die Verbindung zur Remotekonsole ist für die Funktion des Replikationsplanserforderlich, da dasKonto der Remotekonsole dem Plan zugeordnet ist.

Die Verbindung zur Remotekonsole kann aus mehreren Gründen fehlschlagen:

- Wenn die Zieldaten der Remotekonsole falsch sind.
- Wenn Anmeldeinformationen, Port, Protokoll oder Proxy der Remotekonsole geändert, aber nicht in der Arcserve UDP Konsole aktualisiert wurden.
- Wenn die Netzwerkverbindung zwischen Konsole und Remotekonsole unterbrochen wird..
- Wenn der Arcserve UDP-Verwaltungsdienst in der Remotekonsolebeendet wird.

Aus der Option zum Prüfen der Remoteverbindung ist ersichtlich, ob eine Remotekonsole verbunden ist und die richtigen Kontoinformationen hinzugefürt wurden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an, und klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Bereich auf **Ziele**, und klicken Sie auf **Remotekonsole**.

   Die **Ziele: Die Seite "Remotekonsole"** zeigt die hinzugefügten Remotekonsolen in der Mitte an.
3. Klicken Sie zum Verwalten mit der rechten Maustaste auf die hinzugefügten Remotekonsolen oder markieren Sie eine Remotekonsole und klicken Sie auf **Aktionen**.

   Es werden mehrere Optionen angezeigt.
4. Klicken Sie in den angezeigten Optionenauf **Verbindung zur Remotekonsole testen**.

   Eine Meldung mit **Informationen** wird angezeigt, falls die Details der Remotekonsole richtig sind.

   Eine **Fehler**meldung wird angezeigt, wenn die Details der Remotekonsole falsch sind. Korrigieren Sie die Angaben und testen Sie die Verbindung erneut.
5. (Optional) falls eine Fehlermeldung angezeigt wird, beheben Sie den Verbindungsfehler, indem Sie eine oder alle der folgenden Ursachen überprüfen:
   - Sind die Kontoinformationen korrekt?

- Ist die Verbindung zum Netzwerk hergestellt?
- Funktioniert der Arcserve UDP-Verwaltungsdienst in der Remotekonsole?

Die Verbindung zur Remotekonsole ist nunerfolgreich überprüft worden.

Kapitel 10: Erstellen von Plänen zum Schützen von Daten

In diesem Abschnitt werden die folgenden Themen behandelt:

Funktionsweise von Plan und Tasks

Um einen Knoten zu schützen, müssen Sie einen Plan mit einem Sicherungstask erstellen. Ein Plan ist eine Gruppe von Tasks zum Verwalten der Sicherung, Replikation, und Erstellung von Virtual Standby-Knoten. Ein Plan besteht aus einem einzelnen oder mehreren Tasks. Tasks sind eine Reihe von Aktivitäten zum Definieren von Quelle, Ziel, Ablaufplan und erweiterten Parametern.

Sie können die folgenden Tasks erstellen:

Sicherungstasks

Ermöglicht es Ihnen, einen Sicherungstask zum Schützen von Windows-Knoten, Linux-Knoten und hostbasierten virtuellen Rechnerknoten zu erstellen. Verwenden Sie je nach der Art der Knoten, die Sie schützen möchten, eine der folgenden Sicherungstasks:

Agentenbasierte Windows-Sicherung

Definiert einen Sicherungstask zum Schutz von Windows-Knoten. Bei einer agentenbasierten Sicherungsmethode wird eine Agentenkomponente verwendet, um Daten zu sichern. Der Agent wird auf dem Quellknoten installiert.

Hostbasierte agentenlose Sicherung

Definiert einen Sicherungstask zum Schutz von hostbasierten virtuellen Rechnern auf VMware vCenter/ESX- oder Microsoft Hyper-V-Servern. Bei einer agentenlosen Sicherungsmethode müssen Sie keine Agentenkomponenten auf dem Server oder virtuellen Rechner installieren. Sie müssen den Agenten jedoch auf einem Proxy-Server installieren.

Agentenbasiert, Linux

Definiert einen Sicherungstask zum Schutz von Linux-Knoten. Der Agent wird auf einem Linux-Sicherungsserver und nicht auf den Quellknoten, die Sie schützen möchten, installiert.

Von einem Remote-RPS-Task replizieren

Ermöglicht es Ihnen, einen Task zum Empfangen von Daten von einem Remote-Recovery Point Server zu erstellen.

Replikationstask

Ermöglicht es Ihnen, einen Task erstellen, um Sicherungsdaten von einem Recovery Point Server auf einem anderen Recovery Point Server zu replizieren.

Virtual Standby-Task

Ermöglicht es Ihnen, einen Task zu Erstellen eines Virtual Standby-Knotens zu erstellen.

Dateikopie-Task

Ermöglicht es Ihnen, ausgewählte Dateien vom Quellknoten zu kopieren und die kopierten Dateien in einem lokalen oder freigegebenen Ordner zu speichern. Sie können die Dateien auch in einem Cloud-Speicher speichern.

Task für das Kopieren von Wiederherstellungspunkten

Ermöglicht es Ihnen, die Wiederherstellungspunkte in einen lokalen oder freigegebenen Ordner sowie in eine Cloud zu kopieren.

Auf einem remote verwalteten RPS replizieren

Ermöglicht es Ihnen, einen Task zum Replizieren oder Senden von Daten zu einem Remote-Recovery Point Server zu erstellen.

Dateiarchivierungs-Task

Ermöglicht es Ihnen, die Wiederherstellungspunkte in einen freigegebenen Ordner im Netzwerk, Cloud-Speicher oder Volume auf einen geschützten Knoten zu kopieren. Wenn die Wiederherstellungspunkte in das Ziel kopiert werden, werden die Quelldateien gelöscht.

Task "Auf Band kopieren"

Ermöglicht es Ihnen, die Wiederherstellungspunkte auf ein Band zu kopieren (mit detaillierter Wiederherstellungsfunktion direkt vom Band).

Assured Recovery-Task

Ermöglicht es Ihnen zu überprüfen, ob auf die Daten zugegriffen werden kann und sie auf jeden Fall wiederhergestellt werden können.

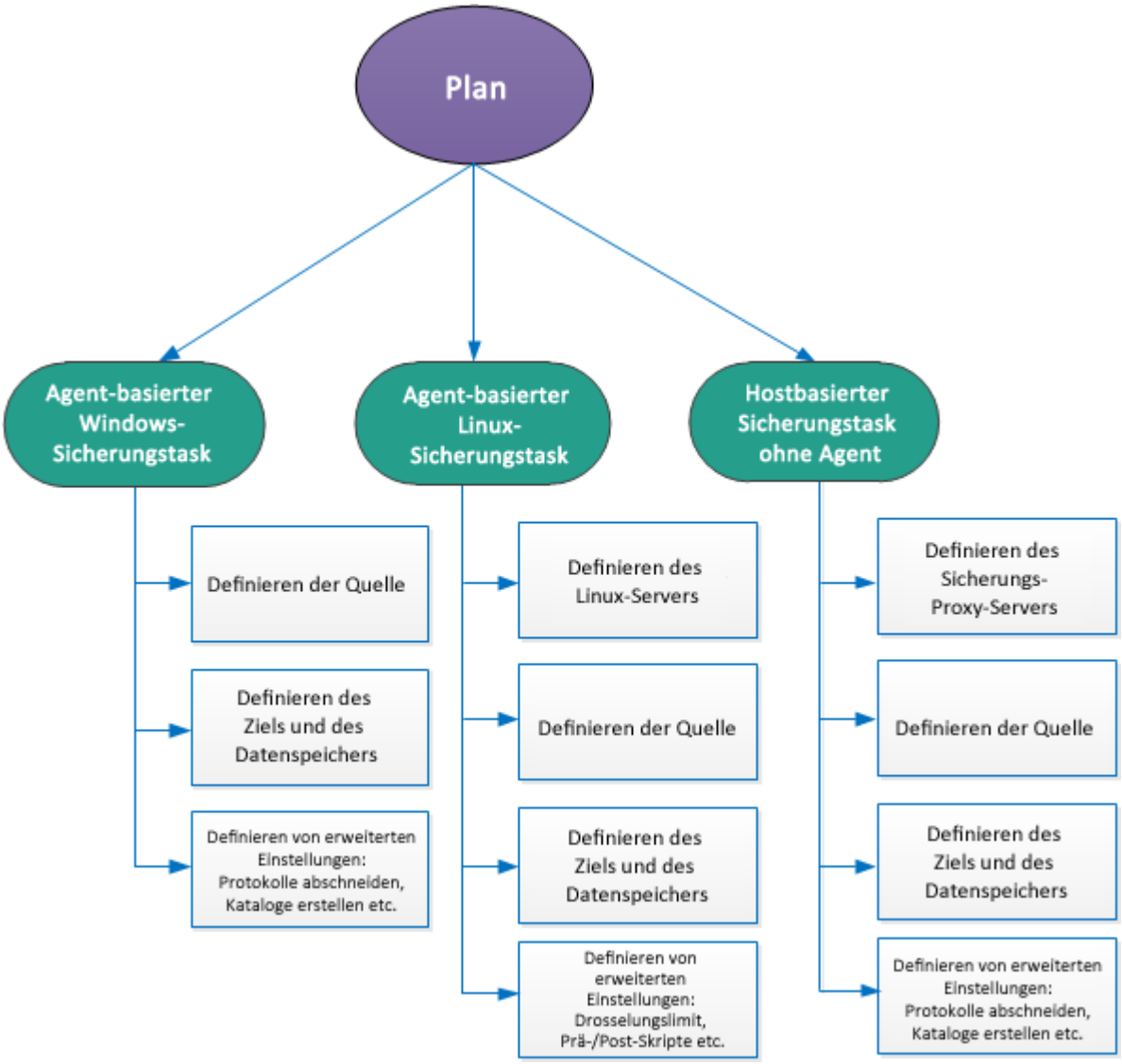
Die folgende Tabelle zeigt die Liste der weiteren Aufgaben an, die Sie nach Aufgabe 1 hinzufügen können:

Aufgabe 1	Folgetask
Sicherung: agentenbasiert, Windows	■ Replizieren ■ Virtual Standby ■ Kopieren von Wiederherstellungspunkten ■ Dateikopie ■ Zu einem remote verwalteten RPS replizieren ■ Dateiarchiv ■ Auf Band kopieren ■ Assured Recovery-Test
Sicherung: Hostbasiert	■ Replizieren

und ohne Agent	■ Virtual Standby ■ Kopieren von Wiederherstellungspunkten ■ Zu einem remote verwalteten RPS replizieren ■ Auf Band kopieren ■ Assured Recovery-Test
Sicherung: agentenbasiert, Linux	■ Replizieren ■ Zu einem remote verwalteten RPS replizieren ■ Auf Band kopieren ■ Assured Recovery-Test
Von einem Remote-RPS replizieren	■ Virtual Standby ■ Replizieren ■ Assured Recovery-Test
Sicherung: Office 365 Exchange Online	■ Replizieren ■ Kopieren von Wiederherstellungspunkten ■ Zu einem remote verwalteten RPS replizieren ■ Auf Band kopieren ■ Assured Recovery-Test
Sicherung: Office 365 OneDrive	■ Replizieren ■ Kopieren von Wiederherstellungspunkten ■ Zu einem remote verwalteten RPS replizieren ■ Auf Band kopieren ■ Assured Recovery-Test
Sicherung: Office 365 SharePoint Online	■ Replizieren ■ Kopieren von Wiederherstellungspunkten ■ Zu einem remote verwalteten RPS replizieren ■ Auf Band kopieren ■ Assured Recovery-Test
Sicherung: Dateien unter dem UNC- oder NFS-Pfad	■ Replizieren ■ Kopieren von Wiederherstellungspunkten ■ Zu einem remote verwalteten RPS replizieren ■ Auf Band kopieren

	■ Assured Recovery-Test

Das folgende Diagramm veranschaulicht die verschiedenen Tasks, aus denen sich ein Sicherungsplan zusammensetzt. Die Abbildung enthält auch Parameter, die Sie in den einzelnen Tasks definieren können.



Erstellen eines Sicherungsplans für Windows

Um Ihre Windows-Knoten oder geclusterte Knoten zu schützen, müssen Sie einen Plan erstellen. Der Plan für Windows-Knoten besteht aus einem Sicherungstask. In diesem Sicherungstask können Sie die Knoten, die Sie schützen möchten, das Sicherungsziel und den Ablaufplan für die Sicherung angeben. Beim Sicherungsziel handelt es sich um einen Recovery Point Server, auf dem Sie Ihre Sicherungsdaten speichern möchten. Das Sicherungsziel kann ein lokales Ziel oder ein freigegebener Remote-Ordner sein.

Sie können auch eine Oracle-Datenbank sichern. Bevor Sie einen Plan zur Sicherung einer Oracle-Datenbank erstellen, überprüfen Sie folgende Voraussetzungen:

- Voraussetzung zur Sicherung einer Oracle-Datenbank

Um geclusterte Microsoft-Knoten und freigegebene Datenträger zu sichern, überprüfen Sie folgende Voraussetzungen:

- Überprüfen der Voraussetzungen zum Sichern von geclusterten Microsoft-Knoten und freigegebenen Datenträgern

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen eines Sicherungsplans
3. (Optional) Ausführen einer manuellen Sicherung
4. Überprüfen der Sicherung

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie die folgenden erforderlichen Aufgaben durchgeführt haben:

- Die neueste Version von Arcserve UDP Agent (Windows) ist installiert.
- Melden Sie sich bei der Konsole an.
- (Optional) Erstellen Sie Datenspeicher zum Speichern Ihrer Sicherungsdaten.
- Überprüfen der Voraussetzungen für Oracle-Datenbank mit UDP Windows-Agent.
- Überprüfen der Voraussetzungen zum Sichern von geclusterten Microsoft-Knoten und freigegebenen Datenträgern.
- (Für die Sicherung einer SQL-Datenbank im vollständigen Modus) Lesen Sie Aktivieren von Protokollkürzungen, wenn die SQL-Datenbank sich im vollständigen Wiederherstellungsmodus befindet.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Für Hardwaresnapshots müssen folgende Voraussetzungen gegeben sein:

- Installieren Sie einen VSS-Hardwareanbieter, der Hardware-Snapshots auf den Arcserve UDP-Agenten unterstützt. Die typische Konfiguration eines VSS-Hardwareanbieters umfasst:
  - Angeben eines Servers, der die LUN steuert.
  - Angeben der Anmeldeinformationen des Datenträger-Arrays für den Zugriff auf das Datenträger-Array.

  Hinweis: Weitere Informationen zur Konfiguration des VSS-Hardwareanbieters erhalten Sie bei Ihrem Hardwareanbieter.

Die folgenden Voraussetzungen sind spezifisch für Netzwerksicherungen:

- Windows-Agent und RPS müssen sich im selben Netzwerk befinden.
- Der Windows-Schutzknoten ist geplant.
- Lokaler RPS mit mehreren NICs ist verbunden.

Überprüfen der Voraussetzungen für Oracle-Datenbank mit UDP Windows-Agent

Um eine Oracle-Datenbank mit konsistenten Daten zu sichern, stellen Sie sicher, dass der ARCHIVELOG-Modus aktiviert ist, damit die Redo-Protokolle archiviert werden.

Hinweis: Das Daten-Volume muss Oracle-Datendateien, Kontrolldateien, Server-Parameterdateien und Online-Redo-Protokolle enthalten. Die archivierten Redo-Protokolle müssen sich physisch auf einem separaten Volume befinden.

Befolgen Sie diese Schritte, um zu überprüfen, ob der ARCHIVELOG-Modus aktiviert ist:

a. Auf dem Oracle Server als Oracle-Benutzer mit SYSDBA-Berechtigungen anmelden.

b. Geben Sie folgenden Befehl ein, wenn die SQL*Plus-Eingabeaufforderung angezeigt wird:

   ARCHIVE LOG LIST;

   Einstellungen des Archivprotokolls für die aktuelle Instanz werden angezeigt.

c. Konfigurieren Sie folgende Einstellungen:

   Datenbankprotokollierungsmodus: Archivierungsmodus

   Automatische Archivierung: aktiviert

d. Starten Sie den ARCHIVELOG-Modus.

   Hinweis: Wenn der ARCHIVELOG-Modus nicht aktiviert ist, starten Sie den ARCHIVELOG-Modus, um die Datenbank zu sichern.

Befolgen Sie diese Schritte, um den ARCHIVELOG-Modus zu starten:

a. Fahren Sie den Oracle-Server herunter.

b. Führen Sie die folgenden Anweisungen in Oracle aus:

   CONNECT SYS/SYS_PASSWORD AS SYSDBA

   STARTUP MOUNT;

   ALTER DATABASE ARCHIVELOG;

   ALTER DATABASE OPEN;

   Standardmäßig werden Protokolle im Flash-Wiederherstellungsbereich gespeichert. Wenn Archivprotokolle nicht im Flash-Wiederherstellungsbereich gespeichert werden sollen, stellen Sie das LOG_ARCHIVE_DEST_n-Parameter auf den Speicherort ein, in dem die Archivprotokolle gespeichert werden sollen.

```
SQL>ALTER SYSTEM SET LOG_ARCHIVE_DEST_
1='LOCATION=e:\app\administrator\oradata\<Name_der_Oracle-Datenbank>\arch'
SCOPE= BOTH;

System geändert.

SQL> ARCHIVE LOG LIST;
```

Einstellungen des Archivprotokolls für die aktuelle Instanz werden angezeigt.

c. Konfigurieren Sie folgende Einstellungen:

Datenbankprotokollierungsmodus: Archivierungsmodus

Automatische Archivierung: aktiviert

Archivziel: E:\app\oracle\oradata\<Name_der_Oracle-Datenbank>\arch

Älteste Online-Protokollsequenz: 21

Aktuelle Protokollsequenz: 23

Der Oracle VSS Writer Service wurde gestartet und funktioniert ordnungsgemäß.

Hinweis: Wenn der Oracle VSS Writer-Dienst nicht ausgeführt wird, dann startet Arcserve UDP Agent (Windows) den Service automatisch, bevor ein Snapshot erfasst wird.

- Arcserve UDP Agent (Windows) ist installiert und ein Plan ist festgelegt.

  Stellen Sie sicher, dass Sie die Volumes ausgewählt haben, die alle Oracle-Datendateien enthalten: Server-Parameterdatei, Kontrolldateien, archivierte Redo-Protokolle und Online-Redo-Protokolle für die Sicherung.

- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Wenn Sie eine BMR für eine Disaster Recovery ausführen möchten, dann stellen Sie sicher, dass Sie die System-Volumes und die Volumes ausgewählt haben, die alle Oracle-Installationsdateien enthalten.

Überprüfen der Voraussetzungen zum Sichern von geclusterten Microsoft-Knoten und freigegebenen Datenträgern

Überprüfen Sie folgende erforderliche Schritte, wenn Sie Microsoft-Clusterknoten und freigegebene Datenträger sichern:

- Installieren Sie Arcserve UDP Agent auf allen Clusterknoten.
- Fügen Sie alle Agenten bzw. Knoten zum selben Sicherungsplan hinzu.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Hinweis: Die freigegebenen Datenträger werden gemeinsam mit dem Agenten gesichert, der die freigegebenen Datenträger besitzt. Wenn ein freigegebener Datenträger während eines Failover von Knoten A auf Knoten B verschoben wird, wird er auch dann vollständig gesichert, wenn es sich beim Job um eine Zuwachssicherung handelt. Wenn der freigegebene Datenträger nach einem weiteren Failover wieder zurück auf Knoten A verschoben wird, wird er auch dann vollständig gesichert, wenn es sich beim Job um eine Zuwachssicherung handelt.

Aktivieren von Protokollkürzungen, wenn die SQL-Datenbank sich im vollständigen Wiederherstellungsmodus befindet

Problem

Wenn sich die Datenbank im vollständigen Modus befindet und eine vollständige Datenbanksicherung durchgeführt wird, kann das SQL-Kürzungsprotokoll nicht gekürzt werden.

Lösung

Um dieses Problem zu beheben, fügen Sie zwei Registrierungswerte hinzu, damit Arcserve UDP den Befehl BACKUP LOG ausführen kann, um das Transaktionsprotokoll zu sichern. Mit diesem Befehl wird der Speicherplatz, der in der Datenbankdatei bereits beschrieben ist, als wiederverwendbar markiert.

Führen Sie diese Schritte aus, um den Registrierungswert hinzuzufügen:

1. Öffnen Sie den Registrierungstabellen-Editor auf dem Agentenrechner mit dem folgenden Befehl:

   ```
   regedit
   ```

2. Rufen Sie folgende Schlüssel ab, je nachdem, ob eine agentenbasierte oder agentenlose Sicherung erfolgt:

   Navigieren Sie für die agentenbasierte Sicherung für 32-Bit und 64-Bit-Betriebssysteme auf dem Agentenrechner zu folgendem Schlüssel:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Wenn Sie eine Version unter Arcserve UDP v6.5 Update 2 verwenden, navigieren Sie für agentlose Sicherungen zum untenstehenden Schlüssel. Erstellen Sie den Registrierungstabellenwert auf dem virtuellen Rechner, den Sie auf dem Proxy-Server sichern möchten. Wenn der Schlüssel der Registry-Tabelle nicht verfügbar ist, erstellen Sie den vollständigen Schlüsselpfad.

   - **32-Bit-BS:**

     HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   - **64-Bit-BS:**

     HKEY_LOCAL_MACHINE\SOFTWARE\WoW6432Node\Arcserve\Unified Data Protection\Engine\AFBackupDll

3. Erstellen Sie die folgenden beiden Registrierungswerte, und legen Sie für beide den Wert auf 1 fest:
   - dword-Wert mit dem Namen "BackupSQLLog4Purge"
   - dword-Wert mit dem Namen "ForceShrinkSQLLog"

     Der Registrierungswert wird hinzugefügt.

   Die Lösung tritt in Kraft, wenn der nächste Bereinigungsjob durchgeführt wird.

Erstellen eines Sicherungsplans mit einem Sicherungstask

Ein Sicherungsplan enthält einen Sicherungstask, der eine Sicherung eines physischen Knotens ausführt und die Daten an einem angegebenen Ziel speichert. Jeder Task besteht aus Parametern, die Quelle, Ziel, Ablaufplan und weitere Sicherungsdetails definieren.

Gehen Sie wie folgt vor:

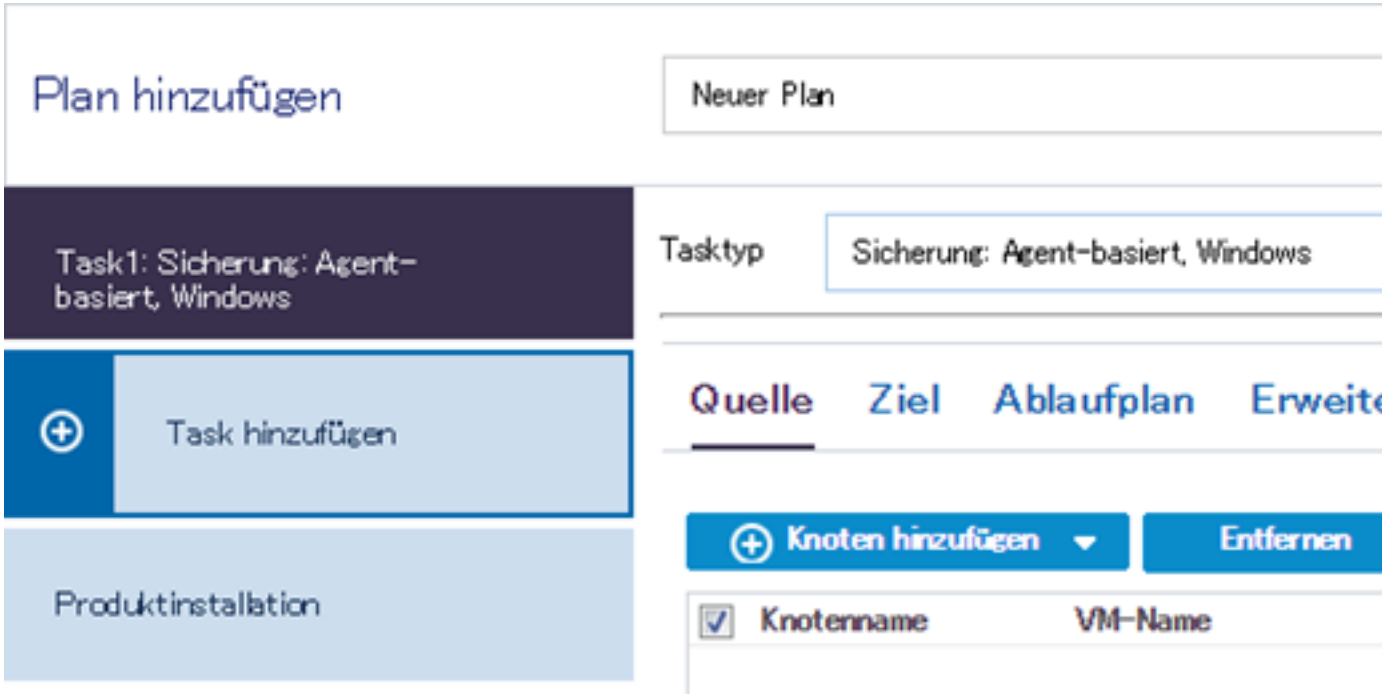
1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Navigieren Sie zu **Ressourcen** > **Pläne** > **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Die Seite Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Drop-down-Liste Tasktyp die Option **Sicherung: agentenbasiert, Windows** aus.



Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die Quellknoten angeben, die Sie schützen möchten. Sie können mehrere Knoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Knoten hinzufügen, wenn Sie einen Plan auf der Quellenseite erstellen oder ändern. Sie können einen Plan auch speichern, ohne Quellknoten hinzuzufügen. Der Plan wird erst bereitgestellt, wenn Sie Quellknoten hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Quelle" auf **Hinzufügen**.
2. Wählen Sie eine der folgenden Optionen:

   Wählen Sie zu sichernden Knoten in Arcserve UDP aus

   Öffnet das Dialogfeld "Wählen Sie zu sichernden Knoten in Arcserve UDP aus". Wählen Sie die Knoten in der angezeigten Liste aus. Wählen Sie diese Option aus, wenn Sie die Knoten bereits zu der Konsole hinzugefügt haben.

   Windows-Knoten hinzufügen

   Öffnet das Dialogfeld "Knoten zu Plan hinzufügen". Wählen Sie diese Option aus, wenn Sie die Knoten nicht hinzugefügt haben und Sie die zu schützenden Knoten manuell hinzufügen möchten.

   Knoten aus Active Directory erkennen

   Öffnet das Dialogfeld Knoten zu Arcserve UDP-Konsole hinzufügen. Wählen Sie diese Option, wenn Sie Knoten aus Active Directory erkennen und hinzufügen möchten.

3. Wenn Sie die Option **Wählen Sie zu sichernden Knoten in Arcserve UDP aus** ausgewählt haben, gehen Sie im Dialogfeld "Zu schützende Knoten auswählen" folgendermaßen vor:

   a. (Optional) Wählen Sie einen Filter aus der Dropdown-Liste "Gruppen" aus, um nach Knoten zu filtern. Sie können Schlüsselwörter eingeben, um den Knotenfilter weiter einzuschränken.

      Die Knoten werden in der Spalte "Verfügbare Knoten" angezeigt.

   b. Wählen Sie die Knoten aus der Spalte "Verfügbare Knoten" aus, und klicken Sie dann auf den einfachen Nach-rechts-Pfeil (>) oder den doppelten Nach-rechts-Pfeil (>>), um die ausgewählten Knoten bzw. alle Knoten in die Spalte "Ausgewählte Knoten" zu verschieben.

Die Knoten werden in der Spalte "Ausgewählte Knoten" angezeigt.

c. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

4. Wählen Sie zum Festlegen des Schutztyps eine der folgenden Optionen aus:

Alle Volumes sichern

Bereitet einen Sicherungs-Snapshot aller Volumes vor.

Ausgewählte Volumes sichern

Bereitet einen Sicherungs-Snapshot des ausgewählten Volumes vor.

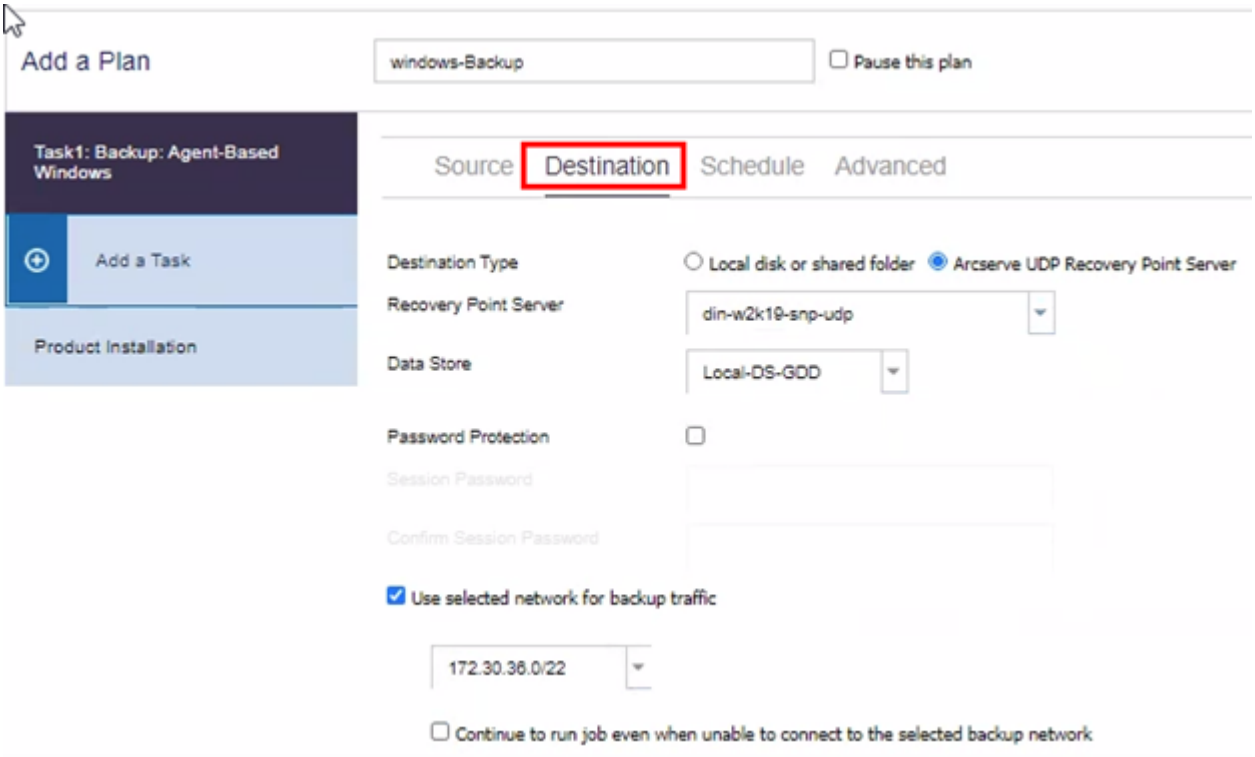
Die Sicherungsquelle ist nun angegeben.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ziel**.



2. Wählen Sie einen der folgenden Zieltypen aus:

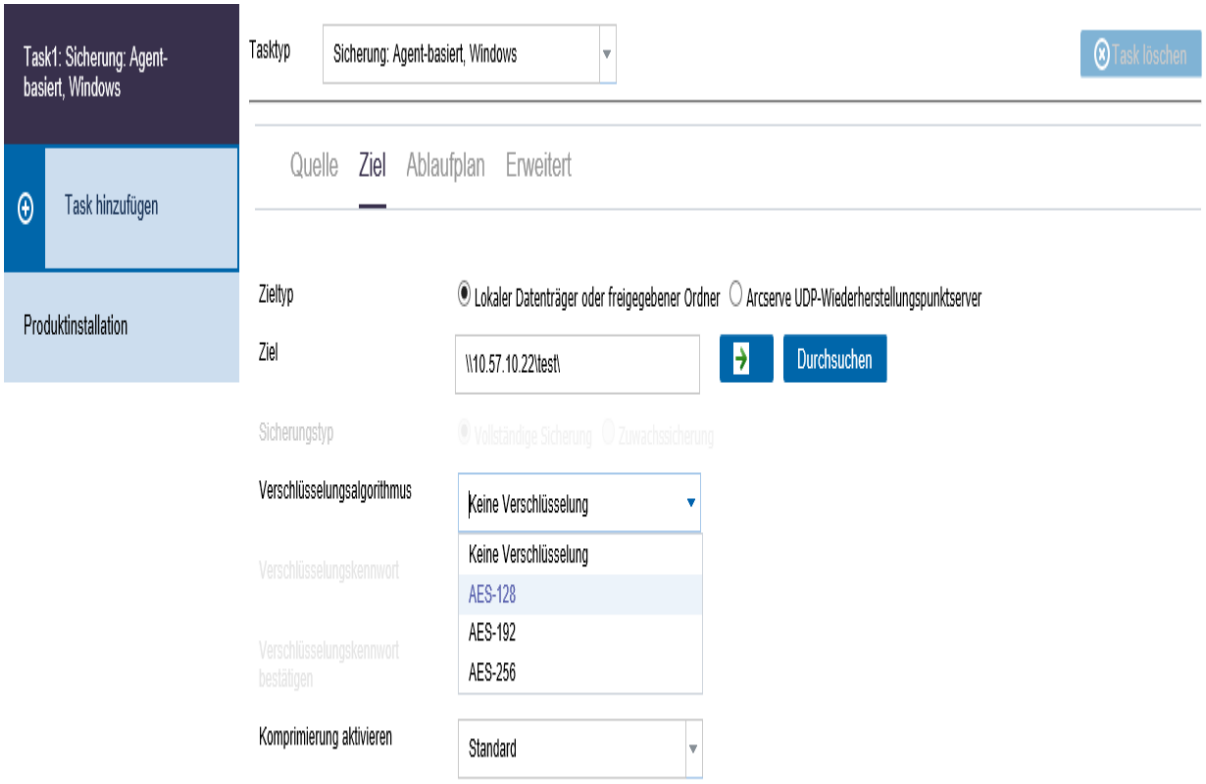
   Lokaler Datenträger oder freigegebener Ordner

   Gibt an, dass das Sicherungsziel ein lokales Ziel oder ein freigegebener Ordner ist. Wenn Sie diese Option auswählen, können Sie Daten als Wiederherstellungspunkte oder Wiederherstellungssätze speichern. Die Optionen für Wiederherstellungspunkte und Wiederherstellungssätze sind auf der Registerkarte Ablaufplan verfügbar.

   Arcserve UDP-Recovery Point Server

   Gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.

3. Wenn Sie **Lokaler Datenträger oder freigegebener Ordner** als Zieltyp auswählen, geben Sie die folgenden Details an:



- Ziel: Geben Sie den vollständigen Pfad des lokalen Ziels oder Netzwerkziels an. Geben Sie für das Netzwerkziel Anmeldeinformationen für ein Konto mit Schreibzugriff an. Klicken Sie auf **Durchsuchen**, um das Ziel zu suchen, oder auf das Pfeilsymbol, um die Verbindung zu testen und die Anmeldeinformationen für den Zielordner anzugeben.
- Verschlüsselungsalgorithmus: Wählen Sie den Verschlüsselungsalgorithmus in der Drop-down-Liste aus. Weitere Informationen finden Sie unter Verschlüsselungseinstellungen.
- (Optional) Verschlüsselungskennwort: Geben Sie ein Verschlüsselungskennwort an.
- Verschlüsselungskennwort bestätigen: Geben Sie das Verschlüsselungskennwort zur Bestätigung erneut ein.
- Komprimierung aktivieren: Wählen Sie einen Komprimierungstyp in der Drop-down-Liste aus. Weitere Informationen finden Sie unter "Komprimierungstyp".

Hinweis: Wenn Sie die Daten auf einem lokalen Datenträger oder in einem freigegebenen Ordner speichern, können Sie die Daten nicht auf einem anderen Recovery Point Server replizieren. Die Replikation wird nur unterstützt, wenn Sie die Daten auf einem Recovery Point Server speichern.

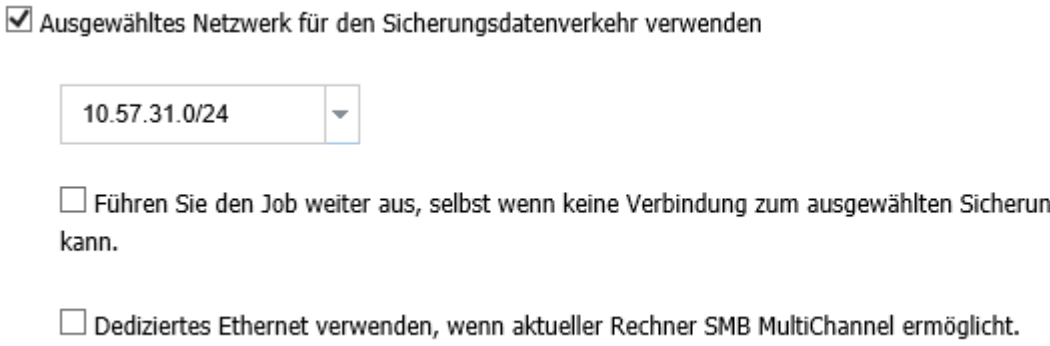
4. Wenn Sie **Arcserve UDP-Recovery Point Server** als Zieltyp auswählen, gehen Sie folgendermaßen vor:

   - Recovery Point Server: Wählen Sie den Ziel-Recovery Point Server (RPS) in der Drop-down-Liste aus.
   - Datenspeicher: Wählen Sie den Zieldatenspeicher in der Drop-down-Liste aus.
   - Kennwortschutz: Aktivieren Sie das Kontrollkästchen **Kennwortschutz**, geben Sie das Sitzungskennwort ein, und geben Sie es zur Bestätigung erneut ein.

     Hinweis: Das Sitzungskennwort ist optional, wenn das Sicherungsziel ein unverschlüsselter RPS-Datenspeicher ist..

   - (Optional) Aktivieren Sie das Kontrollkästchen **Ausgewähltes Netzwerk für den Sicherungsdatenverkehr verwenden**, und führen Sie die folgenden Schritte aus:

     a. Um die Kommunikation zwischen Windows-Agent und Recovery Point Server zu ermöglichen, wählen Sie in der Drop-down-Liste das CIDR-Netzwerk aus.



Hinweis: Um den Job mit dem verfügbaren Netzwerk oder dem Standardnetzwerk fortzusetzen, falls das ausgewählte Sicherungsnetzwerk nicht zugänglich ist, aktivieren Sie das Kontrollkästchen **Führen Sie den Job weiter aus, selbst wenn keine Verbindung zum ausgewählten Sicherungsnetzwerk hergestellt werden kann**.

b. Um den SMB-Multichannel zu deaktivieren, sodass Daten nur über das ausgewählte Netzwerk übertragen wird, aktivieren Sie das Kontrollkästchen **Dediziertes Ethernet verwenden, wenn aktueller Rechner SMB MultiChannel ermöglicht**.

Hinweise:

- Diese Option ist nicht standardmäßig verfügbar. Um diese Option zu aktivieren, wechseln Sie zu dem folgenden Ordnerspeicherort: C:\Program Files\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. Ändern Sie dann den Wert für *useDedicatedEthernet* zu "True".

```
- <SpecifyNetwork>
    <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

  Die Funktion "Netzwerk angeben" wird im Falle eines Remotedatenspeichers deaktiviert, der den freigegebenen Netzwerkordner als Ziel verwendet hat.

- Wenn die Arcserve UDP-Verwaltungsdienste neu gestartet werden, wird die SMB-Multichannel-Funktion aktiviert.
- Die SMB-Multichannel-Funktion ist standardmäßig in Windows aktiviert.

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

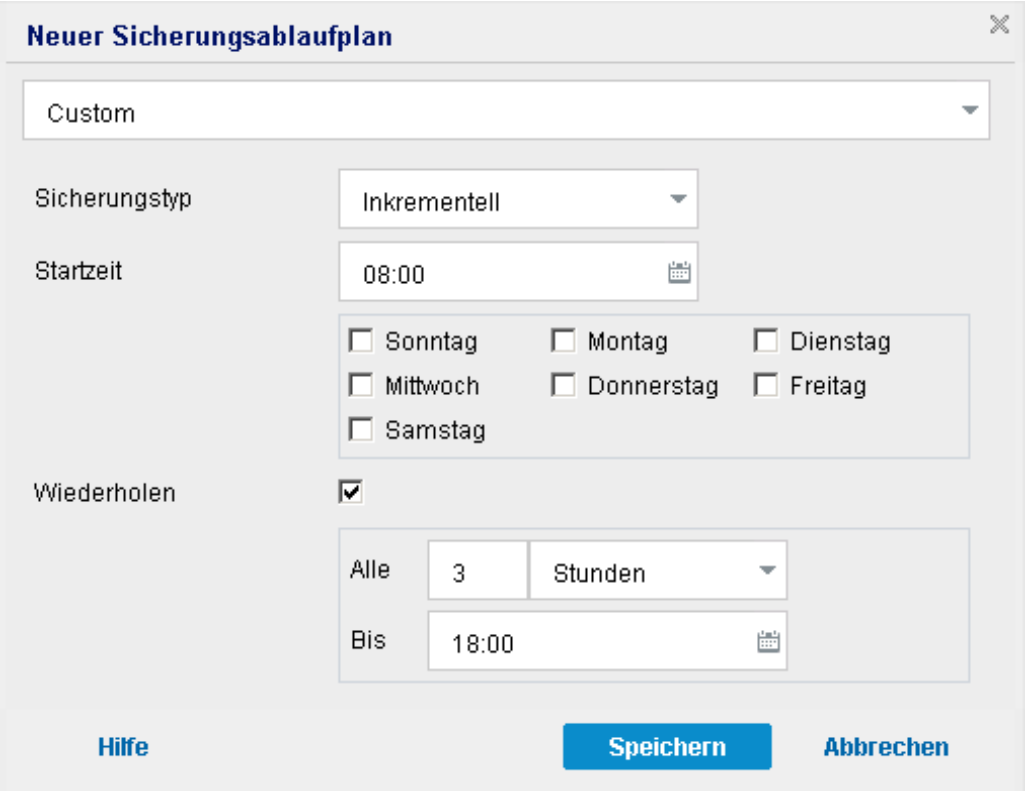
Gehen Sie wie folgt vor:

1. Hinzufügen von Backup, Zusammenführen, Drosselung für Datenträger-Lesevorgang und Ablaufpläne für die Netzwerkdrosselung.

Hinzufügen eines Sicherungsablaufplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

   Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke

des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Überprüfen

Legt den Ablaufplan für Überprüfungssicherungen fest.

Arcserve UDP überprüft die Gültigkeit und Vollständigkeit der geschützten Daten durch einen Vergleich des gespeicherten Sicherungs-Images mit der Sicherungsquelle. Im Bedarfsfall wird das Image neu synchronisiert. Bei einer Überprüfungssicherung wird die letzte Sicherung jedes einzelnen Blocks mit den Inhalten und Informationen der Quelle verglichen. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht (zumeist aufgrund von Änderungen seit der letzten Sicherung), aktualisiert Arcserve UDP die Sicherung dieses Blocks (Neusynchronisierung). In seltenen Fällen kann eine Überprüfungssicherung auch durchgeführt werden, um eine vollständige Sicherung zu erhalten, ohne den erforderlichen Speicherplatz einer vollständigen Sicherung zu verwenden.

Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteile: Die Sicherung benötigt viel Zeit, da alle Quellenblöcke mit den Blöcken der letzten Sicherung verglichen werden.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

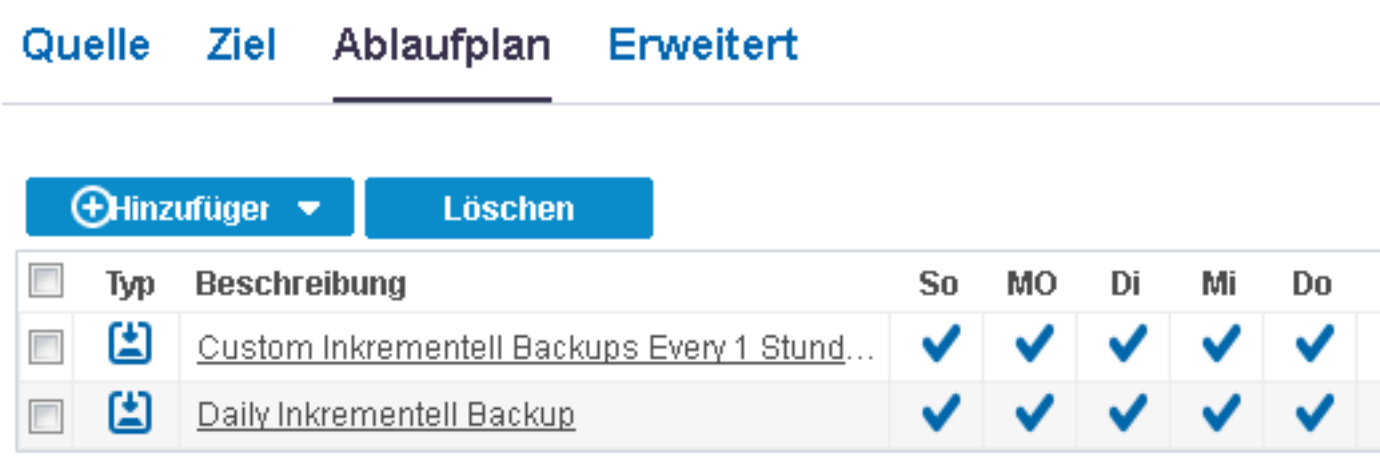
Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die nach der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Diese ist der optimale Weg, um eine Sicherung durchzuführen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

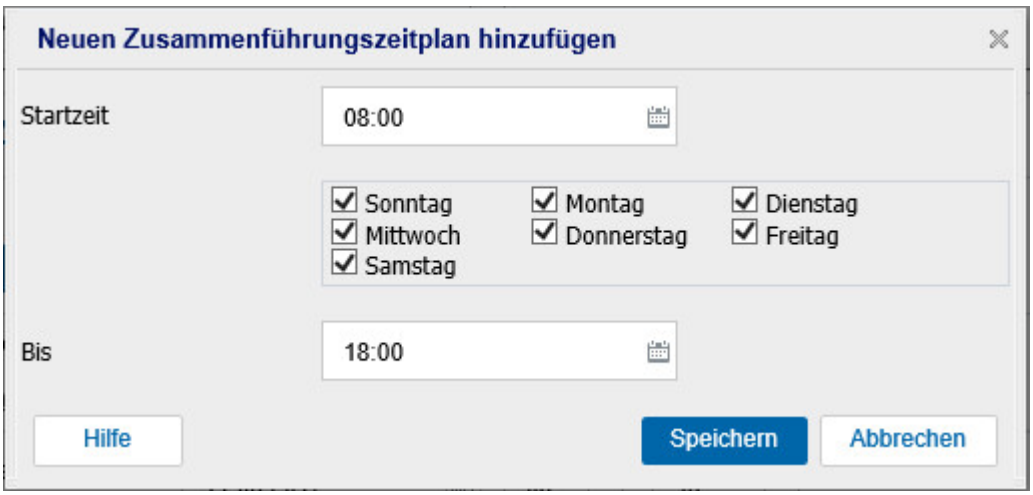
Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.



Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zusammenführungsplan hinzufügen** aus.

   Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.



b. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

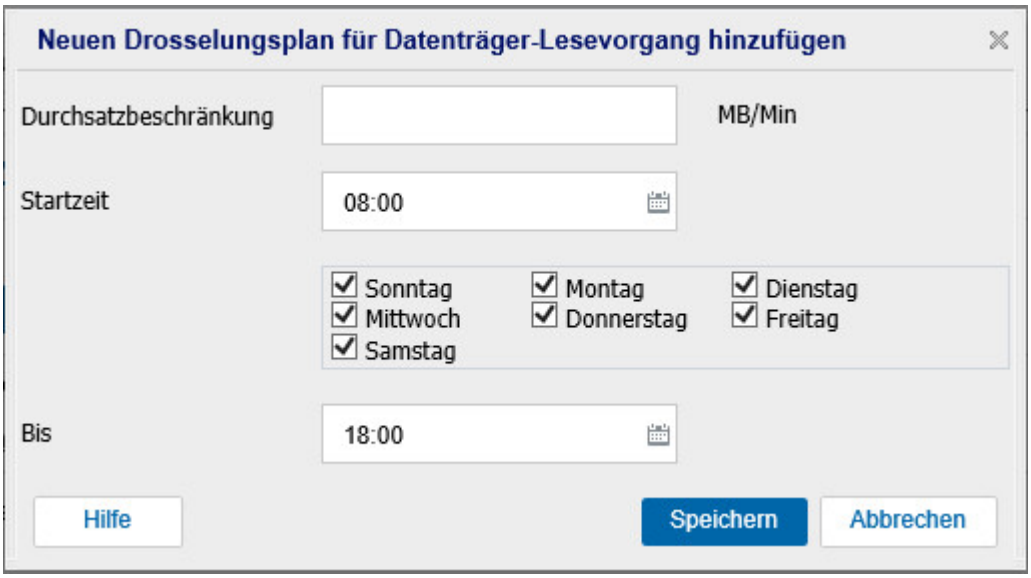
d. Klicken Sie auf **Speichern**.

Der Zusammenführungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Drosselungsplans für Datenträger-Lesevorgänge

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan für Datenträger-Lesevorgang hinzufügen** aus.

   Das Dialogfeld **Neuen Drosselungsplan für Datenträger-Lesevorgang hinzufügen** wird geöffnet.



b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

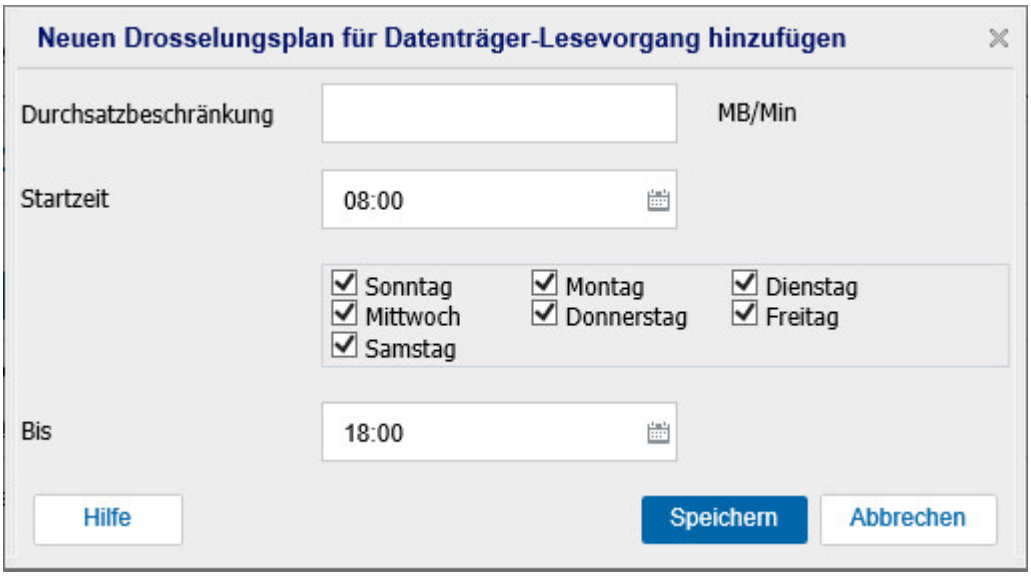
Der Drosselungsplan für Datenträger-Lesevorgänge ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Netzwerkdrosselungsplans

Hinweis: Die Option für Netzwerkdrosselungspläne wird für Sicherungen mit Windows-Agenten nur dann angezeigt, wenn Sie einen Datenspeicher mit Deduplizierung als Ziel für den Plan angeben.

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Netzwerk-Drosselungsplan hinzufügen** aus.

   Das Dialogfeld **Neuen Netzwerk-Drosselungsplan hinzufügen** wird geöffnet.



b. Definiert die Durchsatzbeschränkung in Mbps oder kbps.

Hinweis: Standard-Minimalwert: 500 kbps. Um den Standardwert zu ändern, führen Sie folgende Schritte aus:

i. Vom Registrierungspfad SOFTWARE\Arcserve\Unified Data Protection\Management\Console fügen Sie den Schlüssel MinNetworkThrottleValueInKpbs hinzu, der Typ ist REG_SZ, und legen Sie den Wert fest.

ii. Starten Sie den Arcserve UDP Verwaltungsdienst neu.

iii. Ändern Sie den Plan oder erstellen Sie einen neuen Plan.

Der benutzerdefinierte Wert wird wirksam.

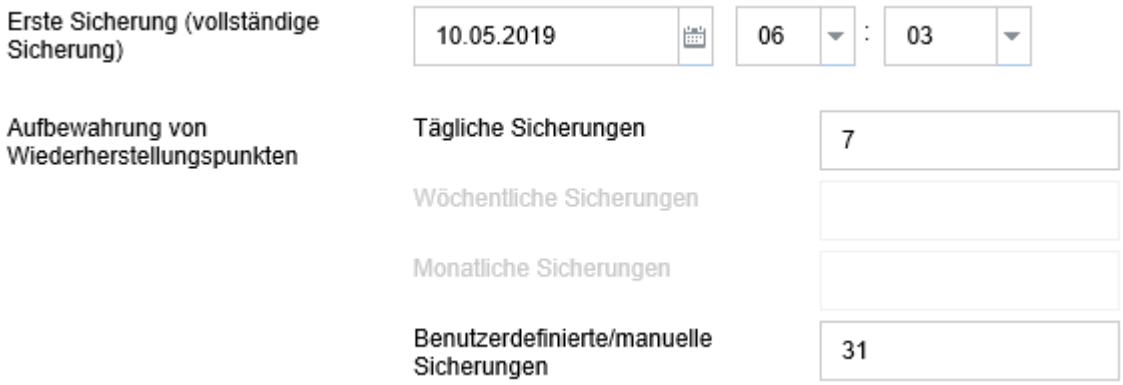
c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Netzwerkdrosselungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

2. Geben Sie die Startzeit für die geplante Sicherung an.



3. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld "Sicherungsablaufplan" übernommen.

   Der Ablaufplan ist nun angegeben.

Funktionsweise der erweiterten Planung und Aufbewahrung

Mit der Ablaufplanoption können Sie einen benutzerdefinierten Ablaufplan, einen Ablaufplan für tägliche/wöchentliche/monatliche Sicherungen oder beides festlegen. Im benutzerdefinierten Ablaufplan können Sie den Sicherungsablaufplan für jeden Tag der Woche konfigurieren und bis zu vier Sicherungsablaufpläne für jeden Tag hinzufügen. Sie können einen bestimmten Wochentag auswählen und ein Zeitfenster erstellen, um anzugeben, wann und wie oft die Sicherung durchgeführt werden soll.

Ablaufplan	Unterstützter Job	Kommentare
Sichern	Sicherungsjob	Gibt Zeitfenster für die Ausführung von Sicherungsjobs an.
Sicherungsdrosselung	Sicherungsjob	Gibt die Zeitfenster an, um die Sicherungsgeschwindigkeit zu steuern.
Zusammenführen	Zusammenführungsjob	Gibt an, wann Zusammenführungsjobs ausgeführt werden sollen.
Täglicher Ablaufplan	Sicherungsjob	Gibt an, wann tägliche Sicherungsjobs ausgeführt werden sollen.
Wöchentlicher Ablaufplan	Sicherungsjob	Gibt an, wann wöchentliche Sicherungsjobs ausgeführt werden sollen.
Monatlicher Ablaufplan	Sicherungsjob	Gibt an, wann monatliche Sicherungsjobs ausgeführt werden sollen.

Sie können auch die Aufbewahrungseinstellungen für die Wiederherstellungspunkte angeben.

Hinweis: Legen Sie innerhalb der einzelnen Pläne Einstellungen für die Aufbewahrungszeit fest, um zu steuern, wie die Daten für die Knoten des entsprechenden Plans im Zieldatenspeicher aufbewahrt werden.

Ablaufpläne für tägliche/wöchentliche/monatliche Sicherungen sind vom benutzerdefinierten Ablaufplan und voneinander unabhängig. Sie können die Ausführung einer täglichen, wöchentlichen oder monatlichen Sicherung konfigurieren, ohne einen benutzerdefinierten Ablaufplan zu konfigurieren.

Jobplan der Sicherung

Sie können vier Zeitfenster pro Tag in Ihrem Sicherungsablaufplan hinzufügen. Ein gültiges Zeitfenster liegt im Bereich 12:00 Uhr bis 23:59 Uhr. Sie können kein Zeitfenster wie z. B. 18:00 Uhr bis 06:00 Uhr angeben. In solchen Fällen müssen Sie manuell zwei verschiedene Zeitfenster angeben.

Für jedes Zeitfenster wird die Startzeit einbezogen, und die Endzeit wird nicht einbezogen. Zum Beispiel haben Sie das Ausführen einer Zuwachssicherung konfiguriert, die stündlich zwischen 06:00 Uhr und 09:00 Uhr stattfinden soll, und die Sicherung wird um 06:00 Uhr gestartet. Das bedeutet, dass die Sicherung um 06:00 Uhr, 07:00 Uhr und 08:00 Uhr ausgeführt wird, NICHT aber um 09:00 Uhr.

Hinweis: Wenn Sie die Sicherung bis zum Ende des Tages wiederholt ausführen möchten, legen Sie den Ablaufplan bis 12:00 Uhr fest. Um den Sicherungsjob beispielsweise alle 15 Minuten während des gesamten Tages auszuführen, legen Sie den Ablaufplan von 00:00 Uhr bis 00:00 Uhr alle 15 Minuten fest.

Drosselungsplan der Sicherung

Mit dem Drosselungsplan der Sicherung können Sie die Geschwindigkeit des Sicherungsdurchsatzes steuern, die wiederum die Ressourcenverwendung (Datenträger-E/A, CPU, Netzwerkbandbreite) des Servers, der gesichert wird, steuert. Dies ist hilfreich, wenn die Serverleistung während der Geschäftszeiten nicht beeinträchtigt werden soll. Sie können vier Zeitfenster pro Tag in Ihrem Drosselungsplan der Sicherung hinzufügen. Für jedes Zeitfenster können Sie einen Wert in MB pro Minute angeben. Dieser Wert wird verwendet, um den Sicherungsdurchsatz zu steuern. Gültige Werte liegen im Bereich zwischen 1 MB/Minute bis 99.999 MB/Minute.

Wenn ein Sicherungsjob die angegebene Zeit überschreitet, dann wird das Drosselungslimit entsprechend dem angegebenen Zeitfenster angepasst. Zum Beispiel haben Sie als Drosselungslimit der Sicherung den Wert 500 MB/Minute von 08:00 Uhr bis 20:00 Uhr und 2500 MB/Minute von 20:00 Uhr bis 22:00 Uhr angegeben. Wenn ein Sicherungsjob um 19:00 Uhr startet und drei Stunden ausgeführt wird, dann hat das Drosselungslimit von 19:00 Uhr bis 20:00 Uhr den Wert 500 MB/Minute. Von 20:00 Uhr bis 22:00 Uhr hat das Drosselungslimit den Wert 2.500 MB/Minute.

Wenn Sie keinen Sicherungsablaufplan und keinen Ablaufplan für den Sicherungsdurchsatz angeben, dann wird die Sicherung so schnell wie möglich ausgeführt.

Ablaufplan für Zusammenführung

Ermöglicht es Ihnen, Wiederherstellungspunkte basierend auf dem angegebenen Ablaufplan zusammenzuführen.

Beachten Sie folgende Punkte für den Zusammenführungsjob:

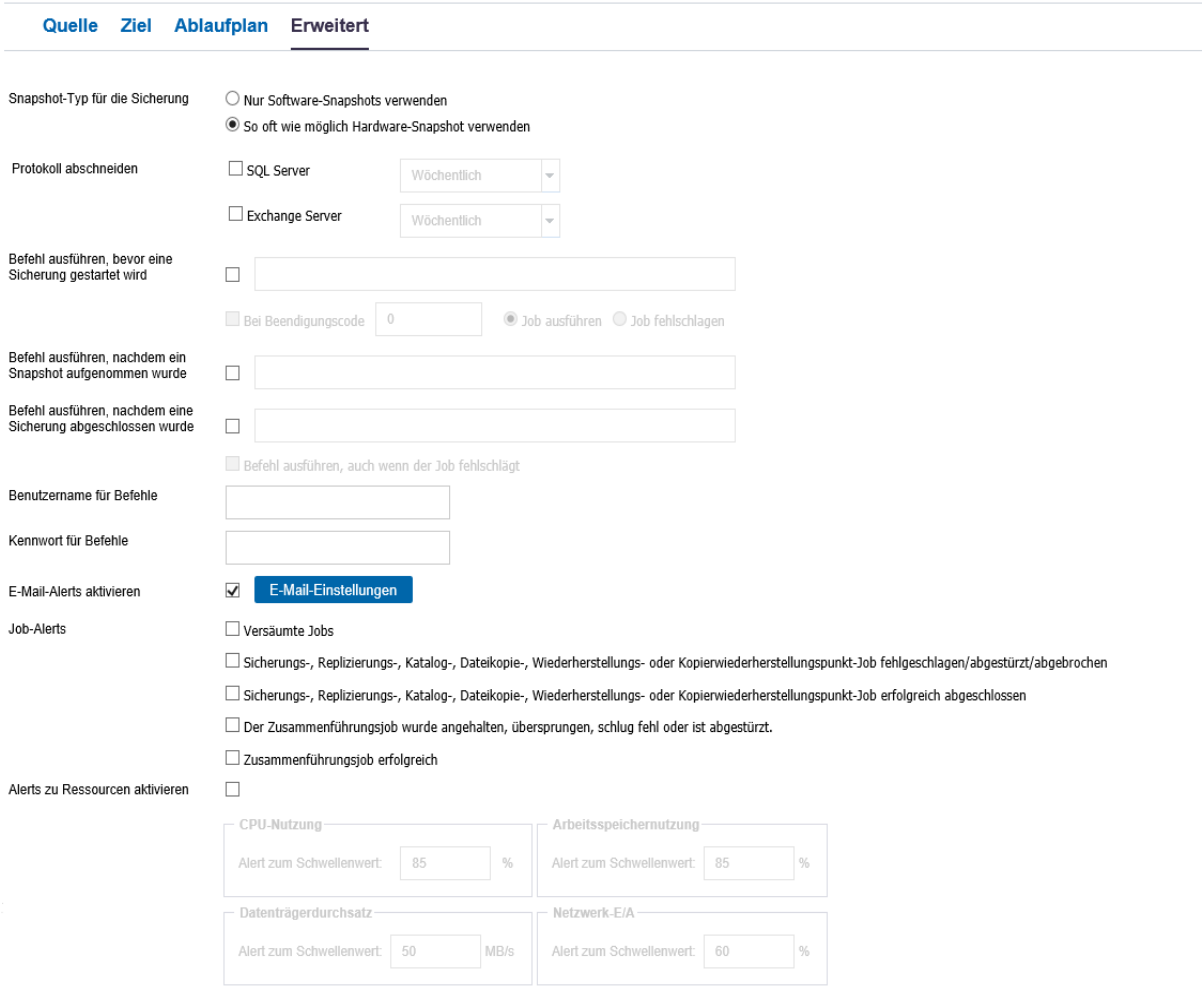
- Es kann immer nur ein Zusammenführungsjob für einen Knoten ausgeführt werden.

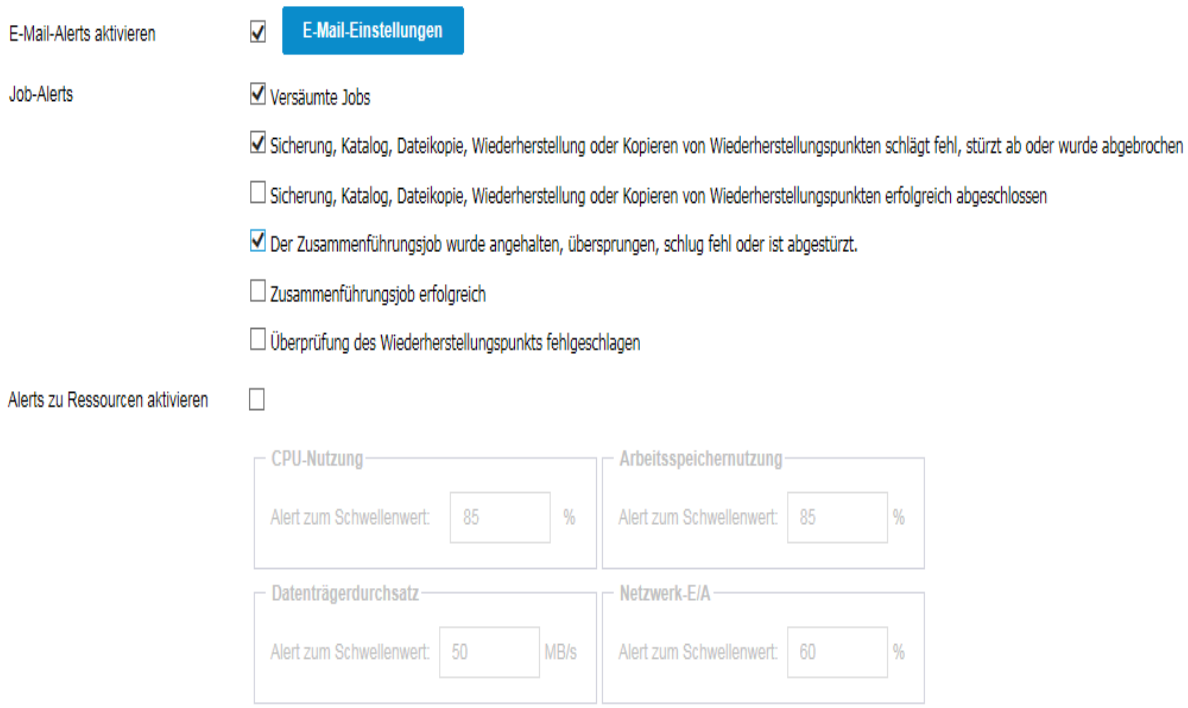
- Wenn ein Zusammenführungsjob gestartet wird, muss er abgeschlossen werden, bevor der nächste Zusammenführungsjob gestartet werden kann. Das bedeutet: Wenn ein oder mehrere Sätze an Wiederherstellungspunkten zusammengeführt werden, dann kann der neue Wiederherstellungspunkt nicht zu diesem Zusammenführungsprozess hinzugefügt werden, bis der Zusammenführungsprozess für den aktuellen Satz an Wiederherstellungspunkten abgeschlossen ist.
- Wenn ein Zusammenführungsjob mehr als einen Satz an Wiederherstellungspunkten bearbeitet (zum Beispiel Satz [1~4], Satz [5~11] und Satz [12~14], also drei Sätze), dann werden diese Sätze nacheinander vom Recovery Point Server bearbeitet.
- Wenn ein Zusammenführungsjob nach einer Pause fortgesetzt wird, erkennt der Job an welchem Punkt er unterbrochen wurde, und die Zusammenführung wird ab der Abbruchstelle fortgesetzt.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen die Einstellungen zum Abschneiden von Protokollen, das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte Erweitert:


Quelle
Ziel
Ablaufplan
Erweitert
Snapshot-Typ für die Sicherung
Nur Software-Snapshots verwenden
So oft wie möglich Hardware-Snapshot verwenden
Protokoll abschneiden
SQL Server
Wöchentlich
Exchange Server
Wöchentlich
Befehl ausführen, bevor eine Sicherung gestartet wird
Bei Beendigungscode
0
Job ausführen
Job fehlschlagen
Befehl ausführen, nachdem ein Snapshot aufgenommen wurde
Befehl ausführen, nachdem eine Sicherung abgeschlossen wurde
Befehl ausführen, auch wenn der Job fehlschlägt
Benutzername für Befehle
Kennwort für Befehle
E-Mail-Alerts aktivieren
E-Mail-Einstellungen
Job-Alerts
Versäumte Jobs
Sicherungs-, Replizierungs-, Katalog-, Dateikopie-, Wiederherstellungs- oder Kopierwiederherstellungspunkt-Job fehlgeschlagen/abgestürzt/abgebrochen
Sicherungs-, Replizierungs-, Katalog-, Dateikopie-, Wiederherstellungs- oder Kopierwiederherstellungspunkt-Job erfolgreich abgeschlossen
Der Zusammenführungsjob wurde angehalten, übersprungen, schlug fehl oder ist abgestürzt.
Zusammenführungsjob erfolgreich
Alerts zu Ressourcen aktivieren
CPU-Nutzung
Alert zum Schwellenwert:
85
%
Arbeitsspeichernutzung
Alert zum Schwellenwert:
85
%
Datenträgerdurchsatz
Alert zum Schwellenwert:
50
MB/s
Netzwerk-E/A
Alert zum Schwellenwert:
60
%



Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

Art des Snapshots für die Sicherung

Wählen Sie eine der folgenden Optionen für den Sicherungs-Snapshot aus.

Nur Software-Snapshot verwenden

Gibt an, dass der Sicherungstyp nur den Software-Snapshot verwendet. Der Hardware-Snapshot wird von UDP nicht überprüft. Der Software-Snapshot nutzt weniger Ressourcen auf den virtuellen Rechnern. Diese Option eignet sich für Server mit niedrigeren Konfigurationen und Verarbeitungsgeschwindigkeiten.

So oft wie möglich Hardware-Snapshot verwenden

Gibt an, dass beim Sicherungstyp erst auf einen Hardware-Snapshot geprüft wird. Wenn alle Kriterien erfüllt sind, verwendet der Sicherungstyp den Hardware-Snapshot.

Hinweis: Weitere Informationen zu den Hardware-Snapshot-Kriterien finden Sie in den Voraussetzungen.

Protokoll abschneiden

Ermöglicht es Ihnen, den Ablaufplan anzugeben, um Protokolle für SQL Server und Exchange Server zu kürzen. Sie können den Ablaufplan als **Täglich**, **Wöchentlich** oder **Monatlich** angeben.

Aktivieren Sie die Bereinigung von Protokollen im Stundentakt für SQL über einen Registrierungsschalter.

- Konfigurieren Sie die Planeinstellungen. Aktivieren Sie die Option "SQL Server" im Abschnitt "Protokoll verkürzen" unter der Registerkarte "Erweitert" und wählen Sie dann "Täglich".
- Legen Sie den Registrierungsschlüssel auf dem SQL-Server-Rechner fest, auf dem sich der UDP-Agent befindet. "PurgeSqlLogPerHour" ist das Intervall in Stunden für die Bereinigung des SQL-Protokolls.

  Pfad: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

  Wertname: PurgeSqlLogPerHour (gibt das Intervall in Stunden für die Bereinigung des SQL-Protokolls an.)

  Werttyp: REG_DWORD

Benutzername

Ermöglicht es Ihnen, den Benutzer anzugeben, der zur Ausführung eines Skripts autorisiert ist.

Kennwort

Ermöglicht es Ihnen, das Kennwort des Benutzers anzugeben, der zur Ausführung des Skripts autorisiert ist.

Befehl ausführen, bevor eine Sicherung gestartet wird

Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem ein Snapshot aufgenommen wurde

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungs-Snapshot aufgenommen wurde. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist.

Um das Skript nach dem Snapshot auch während eines Snapshot-Fehlers auszuführen, wählen Sie **Befehl ausführen, auch wenn der Snapshot fehlschlägt** aus.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Arten der Alerts angeben, die Sie in Form von E-Mails empfangen möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers. Weitere Informationen zur Konfiguration von E-Mail-Einstellungen finden Sie unter Konfigurieren von E-Mails und Alerts.

Job-Alerts

Ermöglicht es Ihnen, die Typen der Job-E-Mails auszuwählen, die Sie erhalten möchten.

Warnmeldungen zu Ressourcen aktivieren

Ermöglicht es Ihnen, einen Schwellenwert für CPU-Auslastung, Speicherverwendung, Datenträgerdurchsatz, Netzwerk-E/A anzugeben. Sie können den Wert in Prozent angeben. Sie erhalten eine E-Mail, wenn der Wert "Warnmeldung zum Schwellenwert" überschritten ist.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Knoten installiert ist und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agenten oder kein Agent installiert ist. Um den Agent auf diesen Knoten zu installieren bzw. um ein Upgrade der Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus und klicken auf Speichern.

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie eine andere Task hinzufügen müssen, müssen Sie den Plan aus der Registerkarte **Ressourcen** auswählen und den Plan ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern.

Der Sicherungsplan wird erstellt und automatisch für den Quellknoten bereitgestellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

(Optional) Ausführen einer manuellen Sicherung

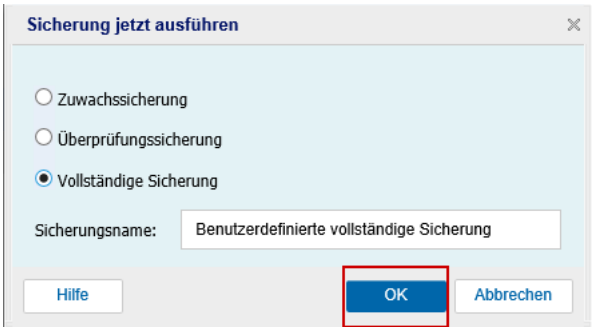
Normalerweise werden Ihre Sicherungen automatisch durchgeführt und von den Ablaufplan-Einstellungen gesteuert. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern. Wenn Sie z. B. einen Wiederholungsplan für vollständige Sicherungen, Zuwachssicherungen und Überprüfungssicherungen festgelegt haben und größere Veränderungen an Ihrem Rechner vornehmen möchten, müssen Sie sofort eine manuelle Sicherung durchführen, ohne auf die nächste geplante Sicherung zu warten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Navigieren Sie zu **Ressourcen** > **Plan** > **Alle Pläne**.

   Die Liste aller Pläne wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Plan, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
4. Wählen Sie im Dialogfeld "Sicherung jetzt ausführen" den gewünschten Sicherungstyp aus, und geben Sie dann gegebenenfalls den Sicherungsnamen an.



Es sind folgende Optionen verfügbar:

Zuwachssicherung

Startet eine Zuwachssicherung Ihres Rechners. Eine Zuwachssicherung sichert nur jene Blöcke, die seit der vorherigen Sicherung geändert wurden.

Hinweis: Wenn Sie eine Sicherung zum ersten Mal ausführen, wird automatisch die vollständige Sicherung initiiert, auch wenn Sie die Option "Zuwachssicherung" ausgewählt haben.

Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

Überprüfungssicherung

Startet eine Überprüfungssicherung Ihres Rechners, indem die aktuellste Sicherung von jedem einzelnen Block überprüft und der Inhalt und die Informationen mit der ursprünglichen Quelle verglichen wird. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht, aktualisiert Arcserve UDP Agent (Windows) die Sicherung dieses Blocks (Neusynchronisierung).

Vorteil: Im Vergleich zu einer vollständigen Sicherung wird nur ein sehr kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteil: Die Sicherung benötigt viel Zeit, da alle Blöcke des Quelldatenträgers mit den Blöcken der letzten Sicherung verglichen werden.

Vollständige Sicherung

Startet eine vollständige Sicherung Ihres gesamten Rechners oder der ausgewählten Volumes.

Hinweise:

- Wenn Sie der Sicherungsquelle ein neues Volume hinzufügen, wird das neue Volume vollständig gesichert, unabhängig davon, welche allgemeine Sicherungsmethode ausgewählt wurde.
- Wenn Sie keinen Sicherungsnamen angeben, wird automatisch der Name "Benutzerdefinierte vollständige Sicherung/Zuwachssicherung/Überprüfungssicherung" vergeben.

5. Klicken Sie auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.

6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.

7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Hinweis: Nur ein Job kann gleichzeitig ausgeführt werden. Wenn Sie versuchen, einen Sicherungsjob manuell zu starten, während gerade ein anderer Job ausgeführt wird, werden Sie in einer Warnmeldung darüber informiert, dass ein anderer Job ausgeführt wird, und aufgefordert, es später erneut zu versuchen.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Überprüfen der Sicherung

Zur Überprüfung Ihres Sicherungsjobs bestätigen Sie, dass Sie den Sicherungsplan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Sie können den Status von Sicherungsjobs auf der Registerkarte **Jobs** überprüfen.

Gehen Sie wie folgt vor, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Wenden Sie zur Überprüfung von Sicherungsjobs eine der folgenden Methoden an:

Methode 1

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs vollständig**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Methode 2

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Jobs erfolgreich abgeschlossen**.

   Die Liste der abgeschlossenen Sicherungsjobs wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf den Job, den Sie überprüfen möchten.

   Der rechte Fensterbereich wird aktualisiert.
4. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
5. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

So erstellen Sie einen Nutanix Sicherungsplan

Um Ihre Nutanix-Knoten zu schützen, müssen Sie einen Plan erstellen. Der Plankn-oten besteht aus einem Sicherungsauftrag. In diesem Sicherungstask können Sie die Knoten, die Sie schützen möchten, das Sicherungsziel und den Ablaufplan für die Sicherung angeben. Beim Sicherungsziel handelt es sich um einen Recovery Point Server, auf dem Sie Ihre Sicherungsdaten speichern möchten. Das Sicherungsziel kann ein lokales Ziel oder ein freigegebener Remote-Ordner sein.

Um die Funktionen zu erkunden, die für das Nutanix-Feature in Arcserve UDP verfügbar sind, lesen Sie bitteSo arbeiten Sie mit Nutanix mithilfe von Arcserve UDP.

So erstellen Sie einen virtuellen Standby für Nutanix AHV

Zum Schutz von Virtual Standby auf Nutanix AHV siehe Virtual Standby auf Nutanix AHV schützen.

Erstellen einer Instant VM auf Nutanix AHV

Informationen zum Erstellen einer Instant VM auf Nutanix AHV finden Sie unter Erstellen einer Instant VM auf Nutanix AHV.

Erstellen eines Assured Recovery-Plans zum Schützen von Nutanix AHV für Linux-Knoten

Informationen zum Erstellen eines Assured Recovery-Plans zum Schützen von Nutanix AHV für Linux-Knoten finden Sie unter Erstellen eines Assured Recovery-Plans zum Schützen von Nutanix AHV für Linux-Knoten.

So führen Sie eine Sicherung des Cluster Shared Volume durch

Arcserve UDP unterstützt die Sicherung von Cluster Shared Volume (CSV) aus v6.5 Update 4. Die CSV-Volumes werden bei Speicherplatz erstellt und sind für Arcserve UDPAgent (Windows) transparent. CSV wird immer bei einer vollständigen Sicherung auf Volume-Ebene berücksichtigt, unabhängig von dem Sicherungsjobtyp (vollständig oder inkrementell). Die CSV-Sicherung schützt die Daten aller gängigen Dateisysteme wie NTFS, NTFS-Deduplizierung, ReFS und CSVFS.

Über die Arcserve UDP-Konsole können Sie einen agentenbasierten Plan erstellen oder einen vorhandenen agentenbasierten Plan aktualisieren, um die Sicherung einer angegebenen CSV durchzuführen.

Gehen Sie wie folgt vor:

1. Wählen Sie auf dem Agent-Rechner das Cluster Shared Volume aus. Weitere Informationen finden Sie unter Ändern der Agentenrechnereinstellungen für die Sicherung des CSV-Volume.

   Hinweis: Sie können den Sicherungsjob auch über den Windows-Agent-Rechner ausführen. Weitere Informationen finden Sie unter So führen Sie eine Sicherung über den Windows-Agent-Rechner durch.

2. Um die Sicherung über die Arcserve UDP-Konsole durchzuführen, navigieren Sie zu der Registerkarte **Ressourcen**.
3. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.
4. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**, und geben Sie einen Plannamen ein.
5. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Sicherung: agentenbasiert, Windows** aus.
6. Aktivieren Sie auf der Registerkarte **Quelle** des Plans das Kontrollkästchen **Alle Volumes sichern** unter **Schutztyp**.
7. Geben Sie nun Details unter Ziel, Ablaufplan und Erweitert an. Weitere Informationen finden Sie unter Erstellen eines Sicherungsplans für Windows.

   Nachdem der Plan gespeichert wurde, wird beim Ausführen des Sicherungsjobs das angegebene CSV-Volume für Windows-Agent gesichert.
8. Überprüfen Sie den Status der gesicherten Jobs. Weitere Informationen finden Sie unter Überprüfen der Sicherung.

   Hinweise:

   - Das Aktivitätsprotokoll des Eigentümerknotens zeigt den Fortschritt des Sicherungsauftrags an und protokolliert die Erfolgsmeldung nach Abschluss der Sicherung. Das Aktivitätsprotokoll des Mitgliedsknotens (der nicht der Eigentümer ist) zeigt eine Warnmeldung wie folgt an, aber der Sicherungsstatus wird als erfolgreich angezeigt.

     Warnung: Der physische Speicherort des Cluster Shared Volume konnte nicht ermittelt werden[C:\ClusterStorage\Volume1]. Dieses Volume wird von der Sicherung ausgeschlossen.
   - Wenn Sie das CSV-Volume während der Sicherung ausschließen möchten, führen Sie die folgenden Schritte aus:
     a. Öffnen Sie auf dem Knoten UDP Agent die Registry mit dem folgenden Pfad:

        HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll
     b. Erstellen Sie einen DWORD als 'BackupCSV'.
     c. Legen Sie den Wert auf 0 fest.

Das CSV Volume wird nun während der Sicherung ausgeschlossen.

Ändern der Agentenrechnereinstellungen für die Sicherung des CSV-Volume

Bevor Sie Ihre erste Sicherung ausführen, müssen Sie die Sicherungseinstellungen angeben, die für die Sicherungsjobs verwendet werden sollen. Diese Einstellungen können für künftige Sicherungen beibehalten und jederzeit auf der Startseite von Arcserve UDP Agent (Windows) geändert werden.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite von Arcserve UDP Agent (Windows) (oder Arcserve UDP Agent (Windows) Monitor) auf **Einstellungen**.

   Das Fenster "Einstellungen" wird geöffnet.

2. Klicken Sie auf die Registerkarte **Sicherungseinstellungen**.

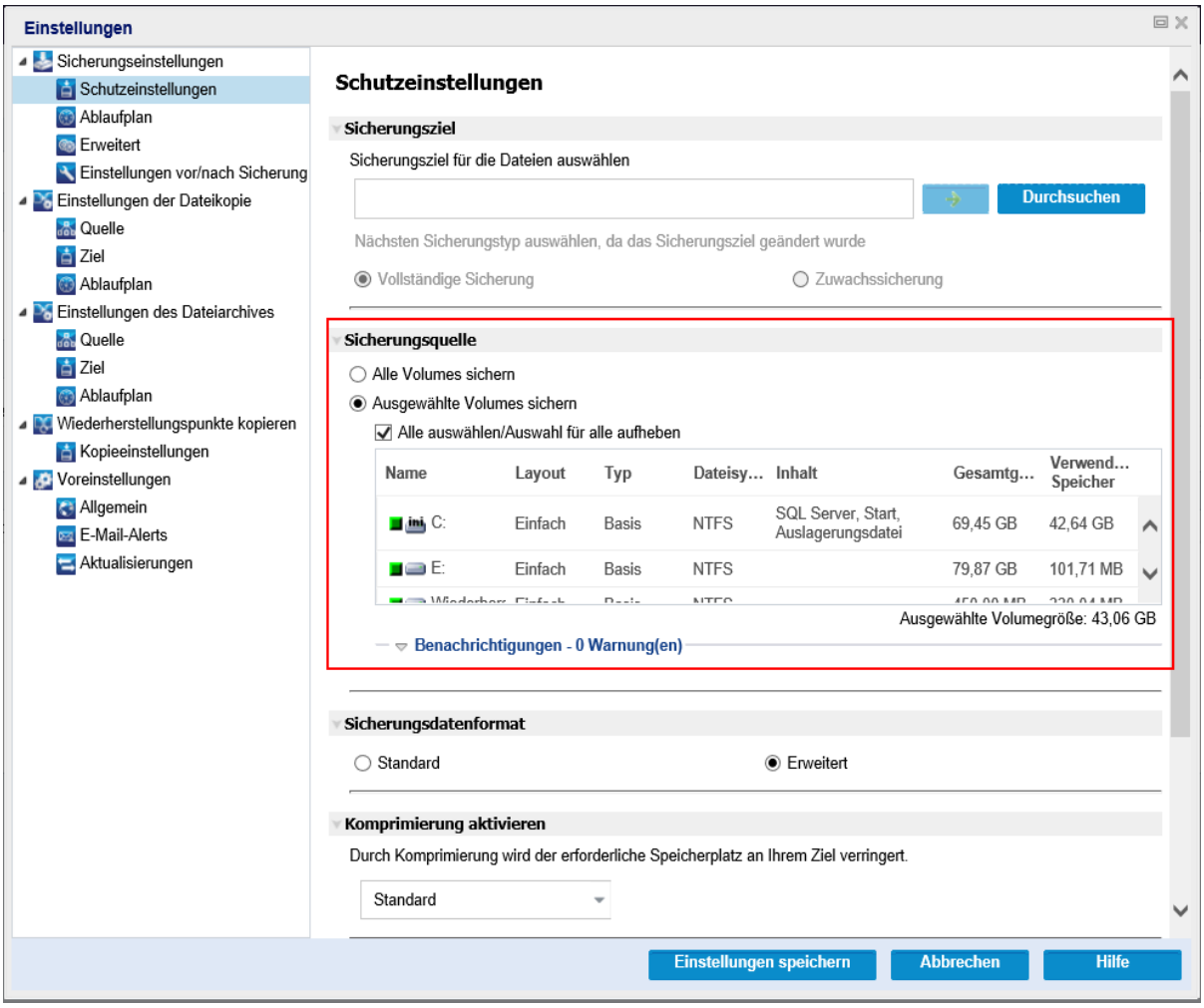
   Das Fenster "Sicherungseinstellungen" wird geöffnet.

3. Klicken Sie auf "Schutzeinstellungen".

4. Das Fenster "Schutzeinstellungen" wird geöffnet.

   Hinweise:

   - Wenn Arcserve UDP Agent (Windows) per Konsole verwaltet wird, sind nicht alle Einstellungen verfügbar und werden schreibgeschützt angezeigt.
   - Wenn der Agent von der Konsole verwaltet wird und nicht in einem Plan geschützt ist, stehen alle Einstellungen weiterhin zur Verfügung, mit Ausnahme des Fensterbereichs "Voreinstellungen" > "Aktualisierungen".



5. Wählen Sie in der Gruppe **Sicherungsquelle** die Option **Ausgewählte Volumes sichern** aus.

   Die Liste der verfügbaren Volumes auf dem Agent-Rechner wird angezeigt.

6. Wählen Sie das CSV-Volume aus, das gesichert werden soll, und klicken Sie auf **Einstellungen speichern**.

   Ihre Einstellungen für den Sicherungsschutz wurden gespeichert.

So führen Sie die Sicherung von Volumes ohne Laufwerksbuchstaben aus

In Arcserve UDP v6.5 Update 4 können Sie die Volumes ohne Laufwerksbuchstaben mithilfe der Option **In NTFS-Ordner-Volumes geladen** unter **Ausgewählte Volumes sichern** schützen. Bevor Sie die Option auswählen **In NTFS-Ordner-Volumes geladen** über die Arcserve UDP-Konsole auswählen, müssen Sie das NTFS-Ordner-Volume laden. Sie können auch weitere Anpassungen vornehmen und die Sicherung nur für einige Volumes ohne Laufwerksbuchstaben, statt für alle, durchführen.

Weitere Informationen finden Sie in den folgenden Themen:

- Überprüfen der Voraussetzungen
- Laden des Volume ohne Laufwerksbuchstaben in NTFS-Ordner
- Angeben des Volume ohne Laufwerksbuchstaben in der Registrierung

Überprüfen der Voraussetzungen

Überprüfen Sie Folgendes:

- Damit der Datenspeicher zwischen RPS-Neustarts den Status "Wird ausgeführt" behält, aktivieren Sie das automatische Laden auf dem RPS-Server. Sie können das automatische Laden mit dem Befehl "diskpart - automount" aktivieren.

  Gehen Sie wie folgt vor:

  1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
  2. Gehen Sie in die Eingabeaufforderung mit erhöhten Rechten wie folgt vor:
  3. Geben Sie *diskpart* ein, und drücken Sie die **Eingabetaste**.
  4. Geben Sie *automount enable* ein, und drücken Sie die **Eingabetaste**.
  5. Schließen Sie die Eingabeaufforderung mit erhöhten Rechten.
  6. Starten Sie den Computer neu, um die Änderungen anzuwenden.

Laden des Volume ohne Laufwerksbuchstaben in NTFS-Ordner

Sie müssen das Volume ohne Laufwerksbuchstaben in den NTFS-Ordner laden, um das Volume und die Inhalte des Bereitstellungspunkts zu sichern.

Gehen Sie wie folgt vor:

1. Wählen Sie unter **Windows Disk Manager**den neuen Datenträger aus, dem kein Laufwerksbuchstabe zugewiesen ist.
2. Klicken Sie mit der rechten Maustaste darauf, und klicken Sie in den verfügbaren Optionen auf **Laufwerksbuchstaben und Pfade ändern**.

   Das Dialogfeld "Laufwerksbuchstaben und Pfade hinzufügen" wird geöffnet.
3. Klicken Sie auf **Ändern**.

   Das Dialogfeld "Laufwerksbuchstaben oder Pfad ändern" wird geöffnet.

4. Wählen Sie **In folgenden leeren NTFS-Ordner laden**, geben Sie den folgenden Pfad ein, und klicken Sie auf **OK**.

   C:\MountPoint

   Der Bereitstellungspunkt wird im Windows-Explorer angezeigt. Das Volume ohne Laufwerksbuchstaben wurde erfolgreich geladen.

Angeben des Volume ohne Laufwerksbuchstaben in der Registrierung

Sie müssen das Volume ohne Laufwerksbuchstaben in der Registrierung angeben, um das Volume und die Inhalte des Bereitstellungspunkts zu schützen.

Gehen Sie wie folgt vor:

1. Wählen Sie unter **Windows Disk Manager**den neuen Datenträger aus, dem kein Laufwerksbuchstabe zugewiesen ist.
2. Klicken Sie mit der rechten Maustaste darauf, und klicken Sie auf **Eigenschaften**.

   Das Fenster "Datenträgereigenschaften" wird geöffnet.
3. Kopieren Sie auf der Registerkarte **Sicherheit** den **Objektnamen**.
4. Navigieren Sie auf dem **Windows-Agent**-Rechner zum entsprechenden **Agentenknoten**, und öffnen Sie **Registrierung**.

   Das Fenster "Registrierung" wird geöffnet.
5. Navigieren Sie zu dem folgenden Pfad, und klicken Sie auf **BackupVolumesWIthMountedVolumes**.

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Das Dialogfeld "Mehrteilige Zeichenfolge bearbeiten" wird angezeigt.
6. Fügen Sie in das Feld **Wertdaten** den Objektnamen ein, den Sie kopiert haben.
7. Klicken Sie auf **OK**.

   Das Volume ohne Laufwerksbuchstaben ist in der Registrierung festgelegt.

   Wenn Sie die Sicherung über die Arcserve UDP-Konsole durchführen, werden für die Sicherung nur die in der Registrierung angegebenen Volumes berücksichtigt.

So führen Sie eine Sicherung des ausgewählten Volume durch

Dieses Thema beschreibt die Sicherung einiger ausgewählter Volumes. Um ein bestimmtes Volume zu sichern, müssen Sie unter der Option "Quelle" beim Erstellen eines Plans das Kontrollkästchen **Ausgewählte Volumes sichern** aktivieren.

Gehen Sie wie folgt vor:

1. Wählen Sie beim Erstellen oder Ändern eines Plans die Registerkarte "Quelle" aus.
2. Aktivieren Sie unter "Schutztyp" das Kontrollkästchen "Ausgewähltes Volume sichern".

   Es werden mehrere Felder angezeigt, in denen Sie die Laufwerks- sowie andere Optionen für das Volume auswählen können.
3. Wählen Sie ein oder mehrere Laufwerke aus der Liste der Laufwerke aus.
4. Wählen Sie eine oder mehrere Optionen aus der folgenden Liste von Volumes aus:

   Für das System reserviertes Volume

   Bezieht sich auf das Volume, das beim Starten des Betriebssystems benötigt wird. Wählen Sie die Option aus, wenn Sie BMR für den Sicherungsknoten ausführen oder die Sicherung für ein bestimmtes Laufwerk ausführen möchten.

   Wiederherstellungs-Volume

   Bezieht sich auf das Volume, das für die Windows-Wiederherstellungsumgebung erforderlich ist. Wählen Sie die Option aus, wenn Sie das Wiederherstellungs-Volume sichern möchten.

   Startvolume

   Bezieht sich auf das Volume, das beim Starten des Windows-Betriebssystem erforderlich ist. Wählen Sie die Option aus, wenn Sie BMR für den Sicherungsknoten ausführen oder die Sicherung für ein bestimmtes Laufwerk ausführen möchten.

   In NTFS-Ordner-Volumes geladen

   Bezieht sich auf die Option "In NTFS-Ordner-Volumes geladen". Wählen Sie diese Option aus, wenn Sie eine Sicherung der Volumes ohne Laufwerksbuchstaben durchführen können. Bevor Sie die Option für einen Plan auswählen, müssen Sie das NTFS-Ordner-Volume laden. Sie können

auch weitere Anpassungen vornehmen und die Sicherung nur für einige Volumes ohne Laufwerksbuchstaben, statt für alle, durchführen. Weitere Informationen finden Sie unter So führen Sie eine Sicherung von Volumes ohne Laufwerksbuchstaben durch.

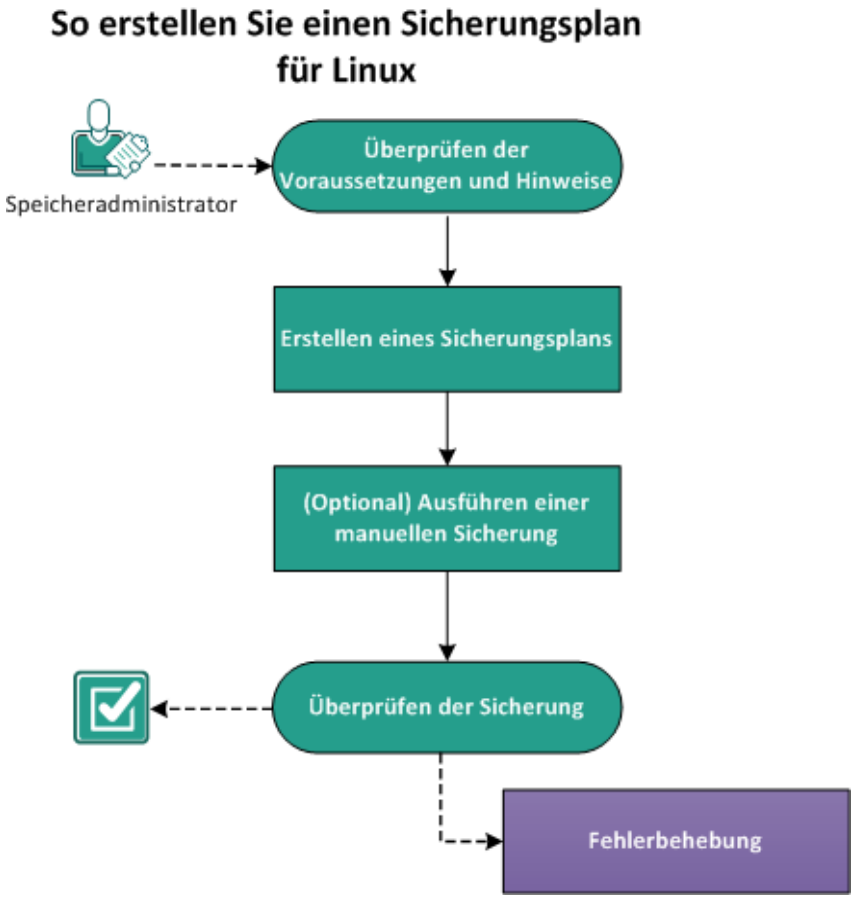
5. Geben Sie auf den restlichen Registerkarten des Plans die entsprechenden Informationen ein, und speichern Sie den Plan.

   Sie haben das Laufwerk oder Volume festgelegt. Die Sicherung erfolgt nur für das ausgewählte Volume oder Laufwerk, wenn der Sicherungsjob ausgeführt wird.

Erstellen eines Sicherungsplans für Linux

Um Ihre Linux-Knoten zu schützen, müssen Sie einen Plan erstellen. Ein Sicherungsplan für Linux-Knoten besteht aus einem Sicherungstask. In diesem Sicherungstask können Sie die Knoten, die Sie schützen möchten, das Sicherungsziel und den Ablaufplan für die Sicherung angeben. Das Sicherungsziel kann ein lokales Ziel, ein Remote-Ordner oder ein Datenspeicher auf einem Recovery Point Server sein.

Folgende Abbildung beschreibt, wie Linux-Knoten geschützt werden:



Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen eines Sicherungsplans
3. (Optional) Ausführen einer manuellen Sicherung
4. Überprüfen der Sicherung
5. Fehlerbehebung

Überprüfen der Voraussetzungen und Hinweise

Erfüllen Sie folgende Voraussetzungen:

- Melden Sie sich bei der Konsole an.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Erstellen eines Sicherungsplans

Ein Sicherungsplan besteht aus einem Sicherungstask, der eine Sicherung des physischen oder virtuellen Knotens ausführt und die Daten am angegebenen Ziel speichert.

Gehen Sie wie folgt vor:

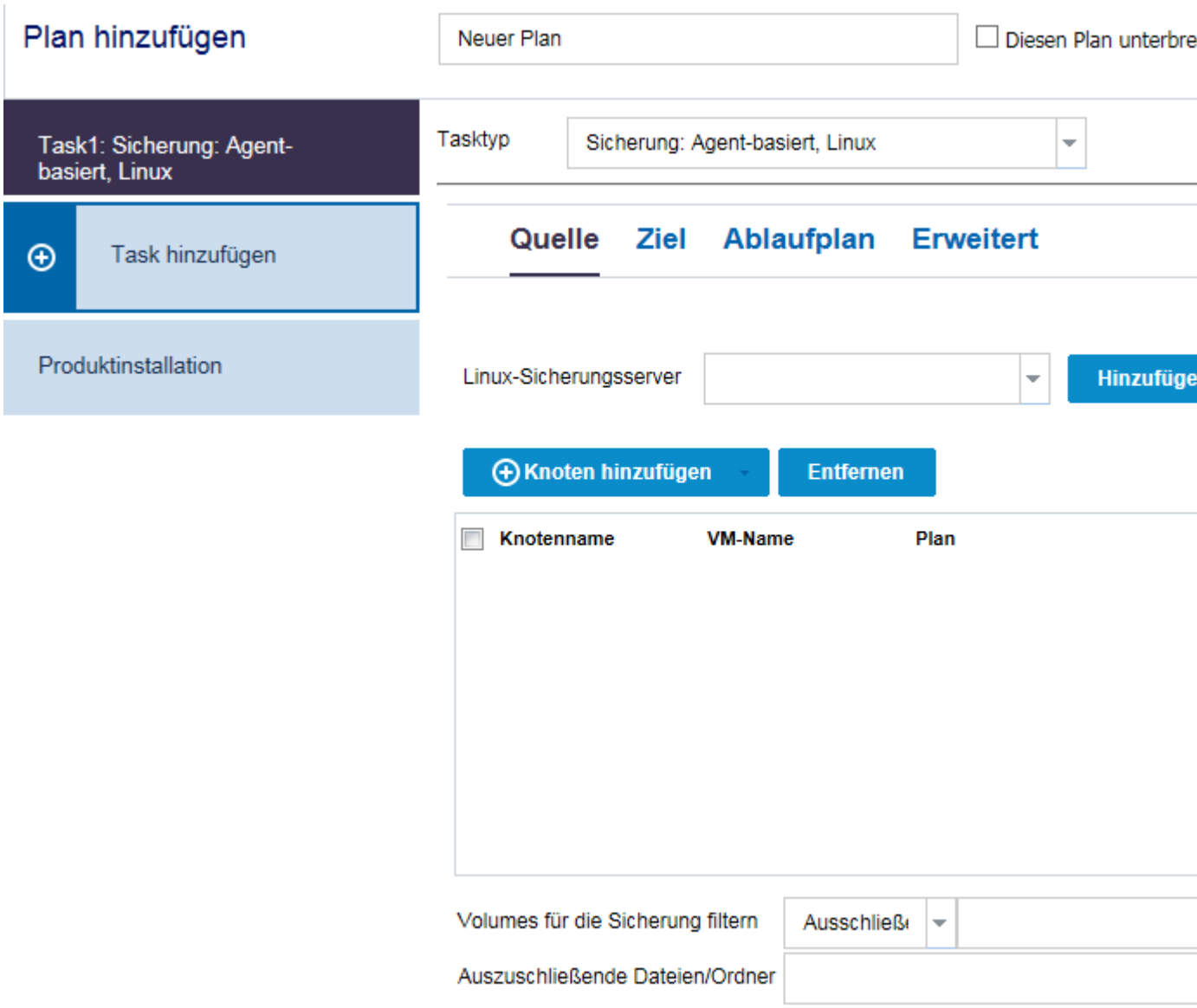
1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Navigieren Sie zur Registerkarte **Ressourcen** > **Plan** > **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Die Seite Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Drop-down-Liste "Tasktyp" die Option **Sicherung: agentenbasiert, Linux** aus.



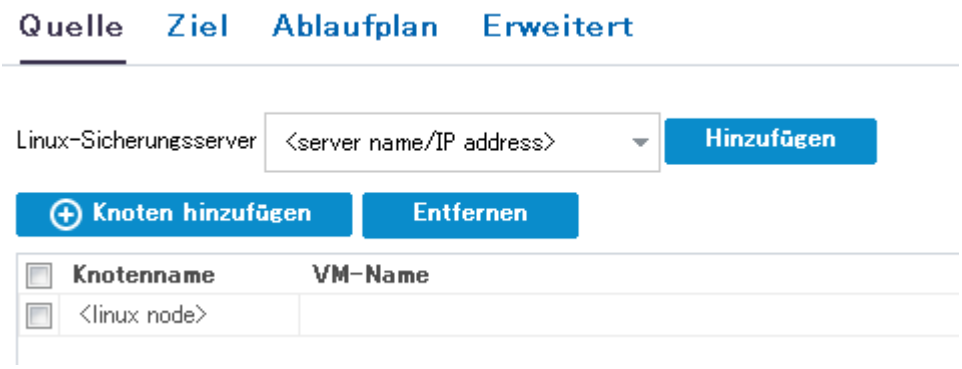
Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die Quellknoten angeben, die Sie schützen möchten. Sie können mehrere Knoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Knoten von der Quellseite hinzufügen. Sie können einen Plan speichern, ohne Quellknoten hinzuzufügen. Der Plan wird jedoch nur bereitgestellt, wenn Sie mindestens einen Knoten hinzufügen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte Quelle.
2. Wählen Sie in der Drop-down-Liste "Linux-Sicherungsserver" den Linux-Sicherungsserver aus.



3. (Optional) Klicken Sie auf **Hinzufügen**, um einen neuen Linux-Sicherungsserver zur Liste hinzuzufügen.
4. Klicken Sie auf **+Hinzufügen**, und wählen Sie dann eine der folgenden Optionen aus:

Wählen Sie zu sichernden Knoten in Arcserve UDP aus

Das Dialogfeld "Zu schützende Knoten auswählen" wird geöffnet. Wählen Sie die Knoten in der angezeigten Liste aus. Wählen Sie diese Option aus, wenn Sie die Knoten bereits zu der Konsole hinzugefügt haben.

Linux-Knoten hinzufügen

Das Dialogfeld "Knoten zu Arcserve UDP-Konsole hinzufügen" wird geöffnet. Wählen Sie diese Option aus, wenn Sie die Knoten nicht hinzugefügt haben und Sie die zu schützenden Knoten manuell hinzufügen möchten.

Wenn ausgewählt, wird UDP Archiving Node von dem auf diesem Knoten installierten Linux Backup-Server gesichert, selbst wenn Sie manuell einen anderen Linux Backup-Server auswählen. Um den Knoten über einen anderen Linux Backup-Server zu sichern, können Sie diesen Knoten als Linux Knoten hin-

zufügen statt als UDP Archiving Knoten. Weitere Informationen finden Sie unter Knoten hinzufügen.

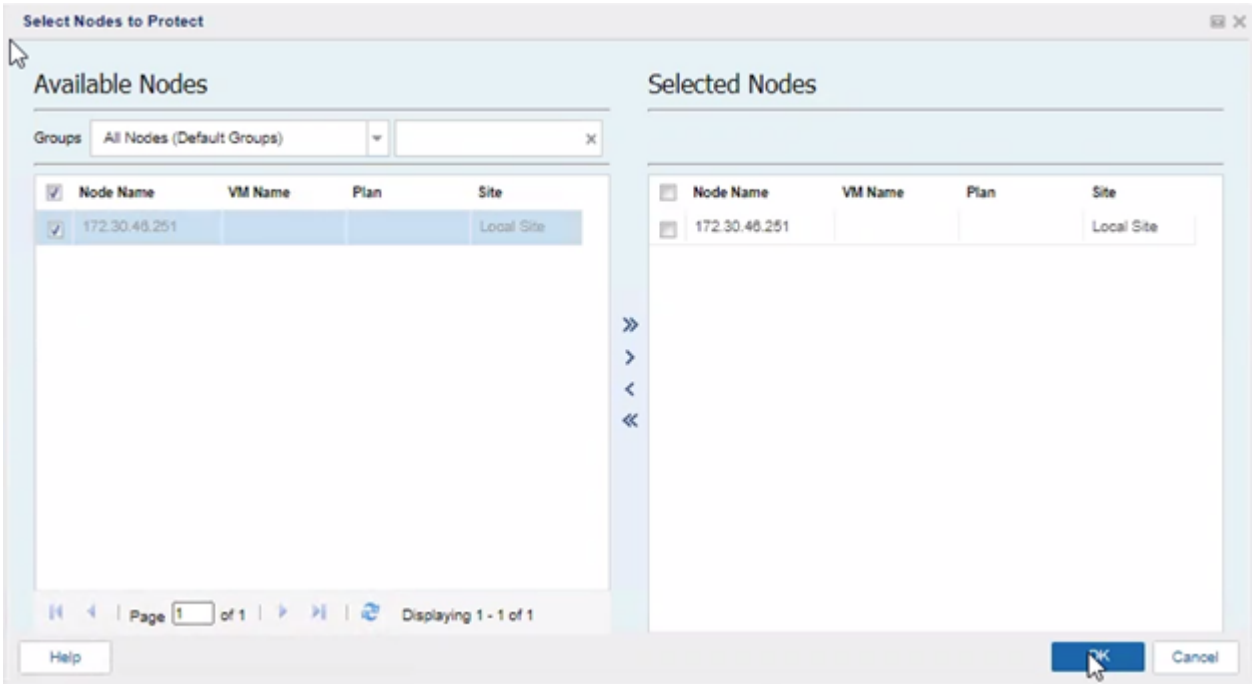
5. Gehen Sie im Dialogfeld "Zu schützende Knoten auswählen" wie folgt vor:

   a. (Optional) Wählen Sie einen Filter aus der Dropdown-Liste "Gruppen" aus, um nach Knoten zu filtern. Sie können Schlüsselwörter eingeben, um den Knotenfilter weiter einzuschränken.

      Die Knoten werden in der Spalte "Verfügbare Knoten" angezeigt.

   b. Wählen Sie die Knoten in der Spalte "Verfügbare Knoten" aus, klicken Sie auf den Nach-rechts-Pfeil und dann auf **OK**.

      Die ausgewählten Knoten werden in der Spalte "Ausgewählte Knoten" angezeigt.



6. (Optional) Stellen Sie die Details für folgende Optionen bereit:

   Filtern von Volumes für die Sicherung

   Wählen Sie **Einschließen** oder **Ausschließen** in der Dropdown-Liste aus. "Einschließen" gibt an, dass nur die angegebenen Volumes in die Sicherung miteinbezogen werden. Nicht angegebene Volumes werden nicht gesichert. "Ausschließen" gibt an, dass die Volumes aus der Sicherung ausgeschlossen werden.

   Dateien/Ordner, die ausgeschlossen werden sollen

   Geben Sie für alle aufgelisteten Knoten die Dateien und Ordner an, die Sie nicht sichern möchten. Wenn Sie nicht mehrere Dateien und Ordner sichern

möchten, trennen Sie alle Dateien und Ordner durch einen Doppelpunkt (:). Geben Sie den vollständigen Pfad der Datei und des Ordners an, den Sie ausschließen möchten.

7. Um bei Festlegung des Sicherungsnetzwerks das Netzwerk zwischen Linux-Sicherungsserver und Linux-Knoten auszuwählen, aktivieren Sie das Kontrollkästchen **Ausgewähltes Netzwerk für den Sicherungsdatenverkehr verwenden**, und wählen Sie dann das Netzwerk in der Drop-down-Liste aus.

   Hinweis: Um den Job mit dem verfügbaren Netzwerk oder dem Standardnetzwerk fortzusetzen, falls das ausgewählte Sicherungsnetzwerk nicht zugänglich ist, aktivieren Sie das Kontrollkästchen **Führen Sie den Job weiter aus, selbst wenn keine Verbindung zum ausgewählten Sicherungsnetzwerk hergestellt werden kann**.

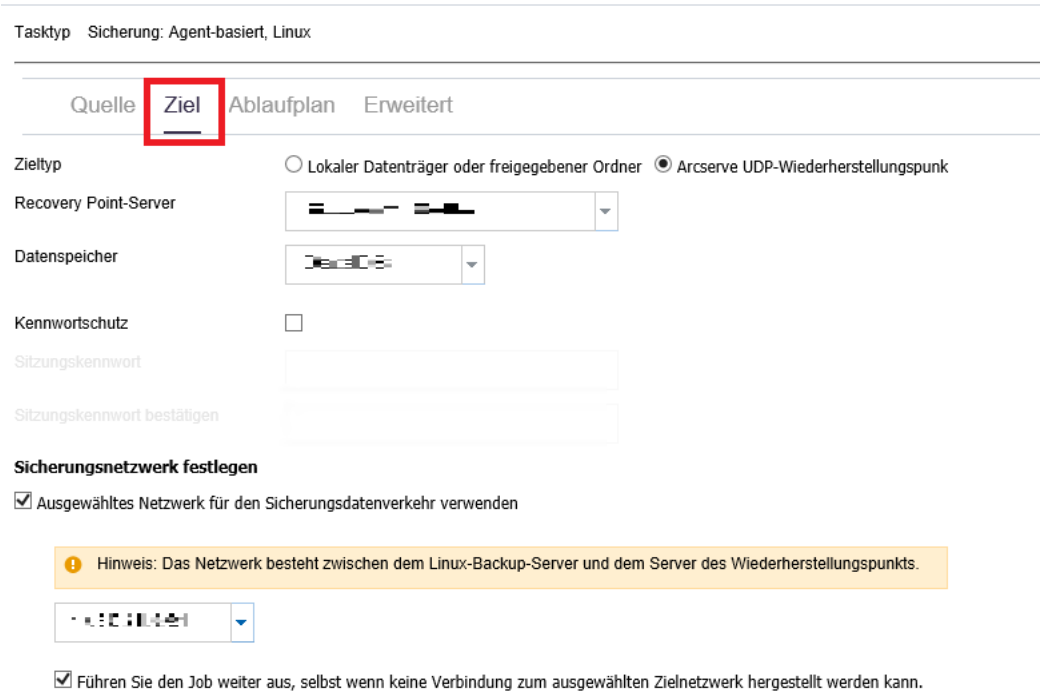
   Die Sicherungsquelle ist nun angegeben.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ziel**.



2. Wählen Sie einen der folgenden Zieltypen aus:

   Lokaler Datenträger oder freigegebener Ordner

   Gibt an, dass die Sicherungsdaten auf einem lokalen Datenträger oder einem freigegebenen Ordner gespeichert werden.

   Arcserve UDP-Recovery Point Server

   Gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.

3. Wenn Sie **Lokaler Datenträger oder freigegebener Ordner** als Zieltyp auswählen, geben Sie die folgenden Details an:

   - Wenn Sie **NFS-Freigabe** ausgewählt haben, geben Sie die Details des Sicherungsziels in folgendem Format ein:

     IP-Adresse der NFS-Freigabe:/vollständiger Pfad des Speicherorts

- Klicken Sie auf die Pfeilschaltfläche, um die Sicherungsziel-Informationen zu validieren.

  Wenn das Sicherungsziel ungültig ist, wird eine Fehlermeldung angezeigt.

Hinweis: Einige Versionen des Data Domain-NAS unterstützen den Mechanismus der Dateisperre von NFS nicht. Dadurch können solche NFS-Freigaben nicht als Sicherungsziel verwendet werden. Weitere Informationen zu diesem Problem finden Sie unter Kompatibilitätsprobleme mit Arcserve Unified Data Protection Agent for Linux.

- Wenn Sie **CIFS-Freigabe** ausgewählt haben, geben Sie die Details des Sicherungsziels in folgendem Format ein:

  //Hostname/Freigabeordner

  - Klicken Sie auf die Pfeilschaltfläche, um die Sicherungsziel-Informationen zu validieren.

    Wenn das Sicherungsziel ungültig ist, wird eine Fehlermeldung angezeigt.

  Hinweis: Stellen Sie sicher, dass der Name des freigegebenen Ordners keine Leerzeichen enthält.

- Wenn Sie **Quelle - lokal** ausgewählt haben, gehen Sie folgendermaßen vor:

  a. Geben Sie den Pfad des lokalen Ziels an.

     Beispiel: /root

  b. Wählen Sie eine Komprimierungsebene aus der Drop-down-Liste Komprimierung, um den für die Sicherung verwendeten Komprimierungstyp anzugeben.

     Die verfügbaren Optionen für Komprimierung sind:

     Standard-Komprimierung

     Gibt eine Komprimierungsebene aus der Drop-down-Liste "Komprimierung" an, um den für die Sicherung verwendeten Komprimierungstyp festzulegen.

     Maximale Komprimierung

     Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigste Speicherplatzverwendung für Ihr Sicherungs-Image.

c. Wählen Sie einen Algorithmus aus der Drop-down-Liste Verschlüsselungsalgorithmus aus, und geben Sie bei Bedarf das Verschlüsselungskennwort ein.

d. Wählen Sie den Verschlüsselungsalgorithmus aus, den Sie für Sicherungen verwenden möchten.

   Bei der Datenverschlüsselung werden Daten in ein Format umgewandelt, das ohne den entsprechenden Entschlüsselungsmechanismus nicht verständlich ist. Die Datensicherheitslösung Arcserve UDP Agent (Linux) verwendet sichere AES-Verschlüsselungsalgorithmen (Advanced Encryption Standard), um größtmögliche Sicherheit und Datenschutz für Ihre Daten zu erzielen.

   Verfügbare Formatoptionen der Verschlüsselung finden Sie unter Verschlüsselungseinstellungen.

   - Eine vollständige Sicherung und alle verknüpften Zuwachssicherungen müssen den gleichen Verschlüsselungsalgorithmus verwenden.
   - Wenn sich der Verschlüsselungsalgorithmus für eine Zuwachssicherung geändert hat, müssen Sie eine vollständige Sicherung ausführen.

   Wenn Sie zum Beispiel das Algorithmusformat ändern und dann eine Zuwachssicherung ausführen, wird der Sicherungstyp dann automatisch in eine vollständige Sicherung konvertiert.

e. Wenn ein Verschlüsselungsalgorithmus ausgewählt wird, müssen Sie ein Verschlüsselungskennwort angeben (und es bestätigen).

   - Das Verschlüsselungskennwort kann höchstens aus 23 Zeichen bestehen.
   - Eine vollständige Sicherung und alle verknüpften Zuwachssicherungen verwenden das gleiche Kennwort zur Datenverschlüsselung.

- Wenn Sie auf Amazon S3 sichern möchten, gehen Sie folgendermaßen vor:

  a. Wählen Sie **CIFS-Freigabe** aus, und geben Sie den Amazon S3-Speicher in folgendem Format ein:

     s3://S3-Region/S3-Bucket-Name

  b. Klicken Sie auf den Pfeil, und geben Sie die Informationen zum Zugreifen auf Amazon S3 ein.

4. Wenn Sie **Arcserve UDP-Recovery Point Server** als Zieltyp auswählen, gehen Sie folgendermaßen vor:

   - Recovery Point Server: Wählen Sie den Ziel-Recovery Point Server in der Drop-down-Liste aus.
   - Datenspeicher: Wählen Sie den Zieldatenspeicher in der Drop-down-Liste aus.
   - Kennwortschutz: Aktivieren Sie das Kontrollkästchen **Kennwortschutz**, geben Sie das Sitzungskennwort ein, und geben Sie es zur Bestätigung erneut ein.

     Hinweis: Das Sitzungskennwort ist optional, wenn das Sicherungsziel ein unverschlüsselter RPS-Datenspeicher ist.
   - Um bei Festlegung des Sicherungsnetzwerks das Netzwerk zwischen Linux-Sicherungsserver und Recovery Point Server (RPS) auszuwählen, aktivieren Sie das Kontrollkästchen **Ausgewähltes Netzwerk für den Sicherungsdatenverkehr verwenden**, und wählen Sie dann das Netzwerk in der Drop-down-Liste aus.

     Hinweis: Um den Job mit dem verfügbaren Netzwerk oder dem Standardnetzwerk fortzusetzen, falls das ausgewählte Sicherungsnetzwerk nicht zugänglich ist, aktivieren Sie das Kontrollkästchen **Führen Sie den Job weiter aus, selbst wenn keine Verbindung zum ausgewählten Sicherungsnetzwerk hergestellt werden kann**.

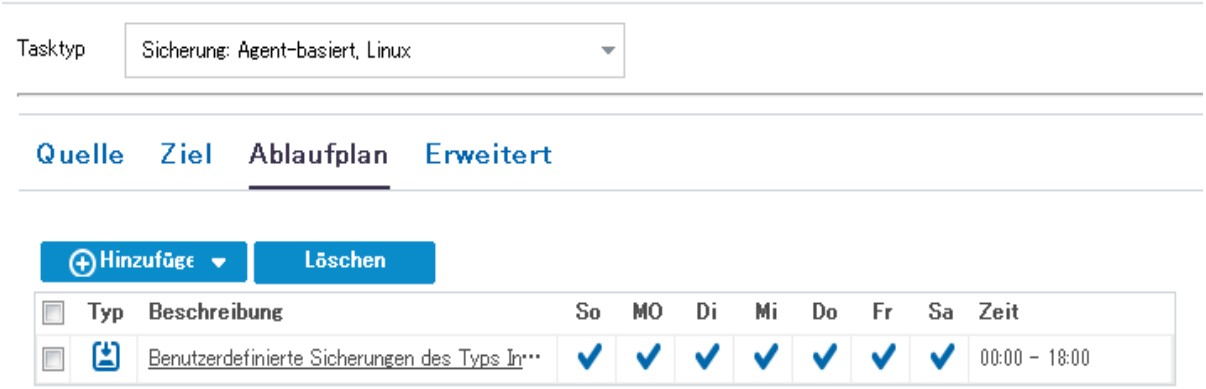
     Wenn das Sicherungsziel ein Datenspeicher mit Deduplizierung ist, werden Daten direkt zwischen dem Linux-Quellserver und dem Recovery Point Server (RPS) übertragen, auch wenn die Option "Netzwerk angeben" zwischen dem Linux-Quellserver und dem Linux-Sicherungsserver konfiguriert ist. Wenn das Sicherungsziel jedoch ein Datenspeicher ohne Deduplizierung ist, wird der Datenverkehr über den Linux-Sicherungsserver geleitet.

   Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan für Sicherungen definieren, damit sie zu festgelegten Intervallen wiederholt werden. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben. Wenn der lokale Datenträger oder ein freigegebener Ordner das Sicherungsziel ist, dann ist der Standardwert eine benutzerdefinierte Zuwachssicherung jeden Abend um 22 Uhr. Wenn RPS-Server das Sicherungsziel ist, dann ist der Standardwert eine tägliche Zuwachssicherung jeden Abend um 22 Uhr.

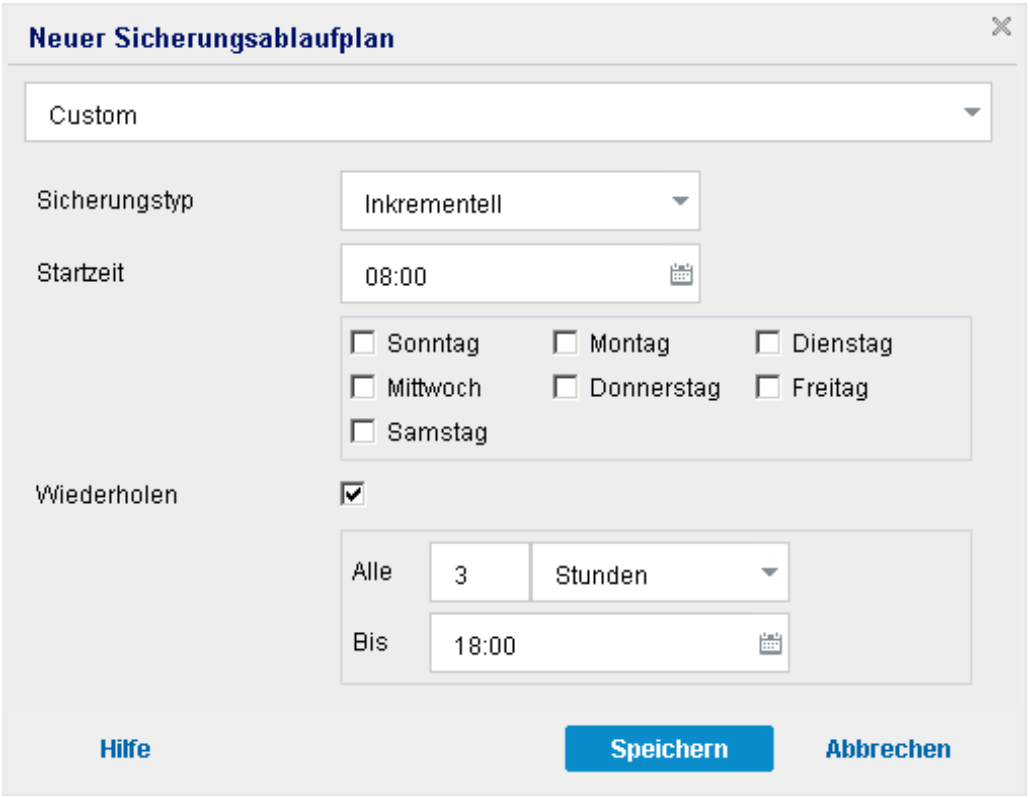
Sie können einen Jobplan der Sicherung bearbeiten oder löschen.



Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ablaufplan**.
2. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

   Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



a. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

b. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke

des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Überprüfen

Legt den Ablaufplan für Überprüfungssicherungen fest.

Arcserve UDP überprüft die Gültigkeit und Vollständigkeit der geschützten Daten durch einen Vergleich des gespeicherten Sicherungs-Images mit der Sicherungsquelle. Im Bedarfsfall wird das Image neu synchronisiert. Bei einer Überprüfungssicherung wird die letzte Sicherung jedes einzelnen Blocks mit den Inhalten und Informationen der Quelle verglichen. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht (zumeist aufgrund von Änderungen seit der letzten Sicherung), aktualisiert Arcserve UDP die Sicherung dieses Blocks (Neusynchronisierung). In seltenen Fällen kann eine Überprüfungssicherung auch durchgeführt werden, um eine vollständige Sicherung zu erhalten, ohne den erforderlichen Speicherplatz einer vollständigen Sicherung zu verwenden.

Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteile: Die Sicherung benötigt viel Zeit, da alle Quellenblöcke mit den Blöcken der letzten Sicherung verglichen werden.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die seit der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Diese ist der optimale Weg, um eine Sicherung durchzuführen.

c. Geben Sie die Startzeit für die Sicherung an.

d. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

e. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

3. Geben Sie die Einstellungen für die Aufbewahrung an, wenn das Ziel ein freigegebener oder ein Netzwerkordner ist.

   Hinweis: Weitere Informationen zu den Wiederherstellungssätzen finden Sie unter Funktionsweise der Wiederherstellungssätze.

   Geben Sie die Anzahl der Wiederherstellungssätze an, die aufbewahrt werden sollen

   Gibt die Anzahl der aufbewahrten Wiederherstellungssätze an.

   Einen neuen Wiederherstellungssatz starten jeden:

   Ausgewählten Tag der Woche

   Gibt den Wochentag an, der für das Starten eines neuen Wiederherstellungssatzes ausgewählt wurde.

   Ausgewählten Tag des Monats

   Gibt den Monatstag an, der für das Starten eines neuen Wiederherstellungssatzes ausgewählt wurde. Geben Sie einen Wert zwischen 1 und 31 oder den letzten Tag des Monats an.

   Hinweis: Die Linux Backup Server überprüft die Anzahl an Recovery-Sätzen im konfigurierten Backup-Speicher alle 15 Minuten und löscht jeden zusätzlichen Recovery-Satz aus dem Backup-Speicherverzeichnis.

4. Wenn Sie Arcserve Recovery Point Server als Ziel ausgewählt haben, führen Sie die folgenden zusätzlichen Schritte aus.

   Hinzufügen eines Zusammenführungsplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zusammenführungsplan hinzufügen** aus.

      Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

   b. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

   c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

   d. Klicken Sie auf **Speichern**.

      Der Zusammenführungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

   Hinzufügen eines Drosselungsplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

      Das Dialogfeld Drosselungsplan hinzufügen wird geöffnet.

   b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

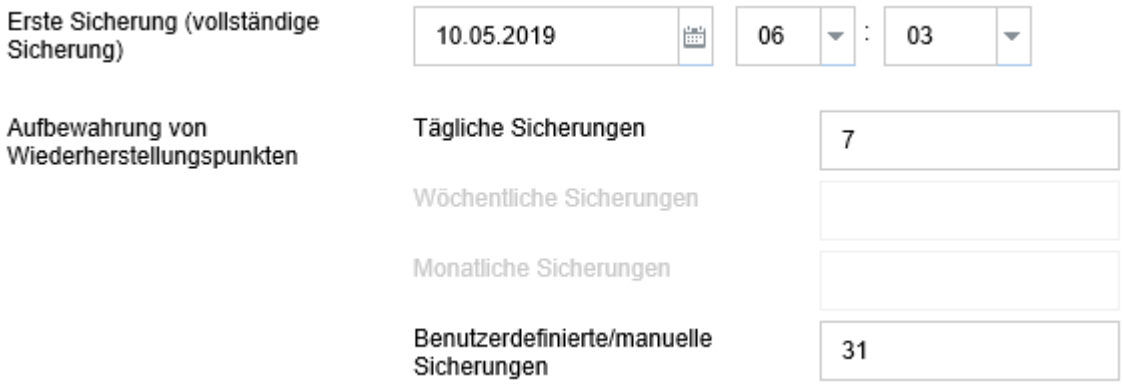
c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Drosselungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

5. Geben Sie die Startzeit für die geplante Sicherung an.



6. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld "Sicherungsablaufplan" übernommen.

Der Sicherungsablaufplan ist nun angegeben.

Funktionsweise der Wiederherstellungssätze

Ein Wiederherstellungssatz ist eine Speichereinstellung, bei der eine Gruppe von Wiederherstellungspunkten, die über einen angegebenen Zeitraum gesichert wurden, als ein Satz gespeichert wird. Ein Wiederherstellungssatz umfasst eine Serie von Sicherungen, beginnend bei einer vollständigen Sicherung, gefolgt von einer Reihe von Zuwachs-, Überprüfungs- oder vollständigen Sicherungen. Sie können die Anzahl der Wiederherstellungssätze angeben, die beibehalten werden soll.

Die **Einstellungen des Wiederherstellungssatzes** stellen sicher, dass eine periodische Wartung der Wiederherstellungssätze erfolgt. Wenn das angegebene Limit überschritten ist, wird der älteste Wiederherstellungssatz gelöscht. Folgende Werte definieren die standardmäßigen, die minimalen und die maximalen Wiederherstellungssätze in Arcserve Unified Data Protection Agent for Linux:

Standard: 2

Mindestwert: 1

Höchstanzahl an Wiederherstellungssätzen: 100

Hinweis: Wenn Sie einen Wiederherstellungssatz löschen möchten, um Sicherungsspeicherplatz zu sparen, reduzieren Sie die Anzahl der aufbewahrten Sätze, und der Sicherungsserver löscht automatisch den ältesten Wiederherstellungssatz. Versuchen Sie nicht, den Wiederherstellungssatz manuell zu löschen.

Beispiel-Satz 1:

- Vollständige Sicherung
- Zuwachssicherung
- Zuwachssicherung
- Überprüfen
- Zuwachssicherung

Beispiel-Satz 2:

- Vollständige Sicherung
- Zuwachssicherung
- Vollständige Sicherung
- Zuwachssicherung

Eine vollständige Sicherung ist erforderlich, um einen neuen Wiederherstellungssatz zu starten. Die Sicherung, die den Satz startet, wird automatisch in eine vollständige Sicherung konvertiert, auch wenn keine vollständige Sicherung zur Ausführung zu diesem Zeitpunkt konfiguriert oder geplant ist.

Nachdem die Einstellung des Wiederherstellungssatzes geändert wurde (zum Beispiel wenn der Ausgangspunkt des Wiederherstellungssatzes der ersten Sicherung von Montag auf die erste Sicherung von Donnerstag geändert wird), dann wird der Ausgangspunkt der vorhandenen Wiederherstellungssätze nicht geändert.

Hinweis: Ein unvollständiger Wiederherstellungssatz wird nicht mitgezählt, wenn ein vorhandener Wiederherstellungssatz berechnet wird. Ein Wiederherstellungssatz wird nur als vollständig erachtet, wenn die Anfangssicherung des nächsten Wiederherstellungssatzes erstellt wird.

Beispiel 1: Aufbewahren von einem Wiederherstellungssatz:

- Legen Sie die Zahl der Wiederherstellungssätze, die aufbewahrt werden sollen, auf 1 fest.

  Der Sicherungsserver bewahrt immer zwei Sätze auf, um einen vollständigen Satz beizubehalten, bevor der nächste Wiederherstellungssatz gestartet wird.

Beispiel 2 - Aufbewahren von 2 Wiederherstellungssätzen:

- Legen Sie die Zahl der Wiederherstellungssätze, die aufbewahrt werden sollen, auf 2 fest.

  Der Sicherungsserver löscht den ersten Wiederherstellungssatz, wenn der vierte Wiederherstellungssatz dabei ist, zu starten. Dadurch wird sichergestellt, dass, wenn die erste Sicherung gelöscht und die vierte Sicherung gestartet wird, noch zwei verfügbare Wiederherstellungssätze (Wiederherstellungssatz 2 und Wiederherstellungssatz 3) auf dem Datenträger vorhanden sind.

  Hinweis: Auch wenn Sie nur einen Wiederherstellungssatz aufbewahren möchten, benötigen Sie Speicherplatz für mindestens zwei vollständige Sicherungen.

Beispiel 3 - Aufbewahren von 3 Wiederherstellungssätzen:

- Die Startzeit der Sicherung ist 06:00 Uhr, 20. August 2012.
- Eine Zuwachssicherung wird alle 12 Stunden ausgeführt.
- Am Freitag beginnt ein neuer Wiederherstellungssatz. Standardmäßig wird der erste Sicherungsjob am Freitag der Beginn des neuen Wiederherstellungssatzes sein.
- Sie möchten 3 Wiederherstellungssätze aufbewahren.

  Mit der obigen Konfiguration wird jeden Tag eine Zuwachssicherung um 06:00 Uhr und um 18:00 Uhr ausgeführt. Der erste Wiederherstellungssatz wird erstellt, wenn die erste Sicherung (muss eine vollständige Sicherung sein) durchgeführt wurde. Dann wird die erste vollständige Sicherung als die Anfangssicherung des Wiederherstellungssatzes markiert. Wenn die am Freitag um 06:00 Uhr geplante Sicherung ausgeführt wird, dann wird diese Sicherung in

eine vollständige Sicherung konvertiert und als gestartete Sicherung des Wiederherstellungssatzes markiert.

Hinweis: Wenn Sie die Sicherung bis zum Ende des Tages wiederholt ausführen möchten, legen Sie den Ablaufplan bis 12:00 Uhr fest. Um den Sicherungsjob beispielsweise alle 15 Minuten während des gesamten Tages auszuführen, legen Sie den Ablaufplan von 00:00 Uhr bis 00:00 Uhr alle 15 Minuten fest.

Festlegen von erweiterten Einstellungen

Geben Sie in der Registerkarte "Erweitert" zusätzliche Einstellungen für den Sicherungsjob an, einschließlich Backup-Durchsatz und Pre-/Post-Skript-Einstellungen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Erweitert**.
2. Legen Sie den Wert zum Drosseln der Sicherung fest.

   Dies gilt nur, wenn das Sicherungsziel ein lokaler oder ein freigegebener Ordner ist.

   Sie können die Höchstgeschwindigkeit festlegen (MB/min), mit der Sicherungen geschrieben werden. Sie können die Sicherungsgeschwindigkeit drosseln, um die CPU- oder Netzwerkauslastung zu reduzieren. Allerdings wirkt sich die Einschränkung der Sicherungsgeschwindigkeit negativ auf das Sicherungsfenster aus. Wenn Sie die Höchstgeschwindigkeit für Sicherungen senken, dauert es länger, die Sicherung abzuschließen.

   Hinweis: Standardmäßig ist die Option "Sicherung drosseln" nicht aktiviert und die Sicherungsgeschwindigkeit wird nicht gesteuert.
3. Geben Sie Ihre Vorsicherungseinstellungen und Nachsicherungseinstellungen unter **Einstellungen vor/nach dem Skript** an.

   Diese Skripte führen Skriptbefehle für Aktionen aus, die vor dem Start des Jobs und/oder nach Abschluss des Jobs durchgeführt werden sollen.

   Hinweis: Die Felder für die Einstellungen vor/nach dem Skript werden nur aufgefüllt, wenn Sie bereits eine Skriptdatei erstellt und unter folgendem Speicherort auf dem Linux-Sicherungsserver platziert haben:

   /opt/Arcserve/d2dserver/usr/prepost

   Hinweis: Weitere Informationen zur Erstellung der Prä-/Post-Skripte finden Sie unter *Verwalten der Prä-/Post-Skripte für Automatisierung*.
4. Klicken Sie auf "E-Mail-Alerts aktivieren", um E-Mail-Einstellungen festzulegen und Job-Alerts auszuwählen.

   Gilt nur, wenn das Sicherungsziel ein Arcserve Recovery Point Server ist.
5. Klicken Sie auf **Speichern**.

   Die Änderungen werden gespeichert.

   Der Sicherungsplan wird erstellt und automatisch für den Quellknoten bereitgestellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit

manuelle Sicherungen ausführen.

Jetzt können Sie die folgenden Tasks zum Plan hinzufügen:

- Replizieren
- Zu einem remote verwalteten RPS replizieren
- Auf Band kopieren

(Optional) Verwalten der Prä-/Post-Skripte für Automatisierung

Mit Prä-/Post-Skripts können Sie Ihre eigene Geschäftslogik in bestimmten Phasen eines laufenden Jobs ausführen. Sie können in **Einstellungen vor/nach dem Skript** im **Sicherungsassistenten** und **Wiederherstellungsassistenten** in der Konsole angeben, wann Ihre Skripte ausgeführt werden sollen. Die Skripts können je nach Einstellung auf dem Sicherungsserver ausgeführt werden.

Das Verwalten von Prä-/Post-Skripts ist ein zweiteiliger Vorgang, der das Erstellen des Prä-/Post-Skripts und das Einfügen des Skripts in den "prepost"-Ordners umfasst.

Erstellen von Prä-/Post-Skripts

Gehen Sie wie folgt vor:

1. Melden Sie sich als Root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie eine Skriptdatei, indem Sie die Umgebungsvariablen in Ihrer bevorzugten Skripterstellungssprache verwenden.

   Umgebungsvariablen des Prä-/Post-Skripts

   Verwenden Sie die folgenden Umgebungsvariablen, um Ihr Skript zu erstellen:

   D2D_JOBNAME

   Gibt den Namen des Jobs an.

   D2D_JOBID

   Gibt die Job-ID an. Die Job-ID ist eine Nummer, die für den Job vergeben wird, wenn Sie den Job ausführen. Wenn Sie den gleichen Job erneut ausführen, erhalten Sie eine neue Jobnummer.

   D2D_TARGETNODE

   Identifiziert den Knoten, der gesichert oder wiederhergestellt wird.

   D2D_JOBTYPE

   Identifiziert den Typ des ausgeführten Jobs. Die folgenden Werte identifizieren die D2D_JOBTYPE-Variable:

   backup.full

   Identifiziert den Job als eine vollständige Sicherung.

   backup.incremental

   Identifiziert den Job als eine Zuwachssicherung.

backup.verify

Identifiziert den Job als eine Überprüfungssicherung.

restore.bmr

Identifiziert den Job als eine Bare-Metal-Recovery (BMR). Dies ist ein Wiederherstellungsjob.

restore.file

Identifiziert den Job als eine Wiederherstellung auf Dateiebene. Dies ist ein Wiederherstellungsjob.

D2D_SESSIONLOCATION

Identifiziert den Speicherort, an dem die Wiederherstellungspunkte gespeichert sind.

D2D_PREPOST_OUTPUT

Identifiziert eine Temp-Datei. Der Inhalt der Anfangszeile der Temp-Datei wird im Aktivitätsprotokoll angezeigt.

D2D_JOBSTAGE

Gibt die Phase des Jobs an. Die folgenden Werte identifizieren die D2D_ JOBSTAGE-Variable:

pre-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, bevor der Job startet.

post-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Job startet.

post-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Snapshot erfasst wird.

post-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Snapshot erfasst wird.

D2D_TARGETVOLUME

Identifiziert das Volume, das während eines Sicherungsjobs gesichert wird. Diese Variable ist anwendbar für Prä-/Post-Snapshot-Skripts für einen Sicherungsjob.

D2D_JOBRESULT

Identifiziert das Ergebnis für ein Post-Job-Skript. Die folgenden Werte identifizieren die D2D_JOBRESULT-Variable:

success

Identifiziert das Ergebnis als erfolgreich.

fail

Identifiziert das Ergebnis als nicht erfolgreich.

D2DSVR_HOME

Identifiziert den Ordner, in dem der Sicherungsserver installiert ist. Diese Variable ist anwendbar für die Skripts, die auf dem Sicherungsserver ausgeführt werden.

Das Skript ist erstellt.

Hinweis: Bei allen Skripten zeigt der Rückgabewert von Null eine erfolgreiche Erstellung an, und ein Rückgabewert, der ungleich Null ist, weist auf einen Fehler hin.

Einfügen des Skripts in den Ordner "Prepost" und Überprüfung des Skripts

Alle Prä-/Post-Skripts für einen Sicherungsserver werden zentral vom Ordner "prepost" am folgenden Speicherort verwaltet:

/opt/Arcserve/d2dserver/usr/prepost

Gehen Sie wie folgt vor:

1. Fügen Sie die Datei in folgenden Speicherort des Sicherungsservers ein:

   /opt/Arcserve/d2dserver/usr/prepost

2. Geben Sie der Skriptdatei Ausführungsberechtigungen.
3. Melden Sie sich bei der Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche an.
4. Öffnen Sie den **Sicherungsassistenten** oder **Wiederherstellungsassistenten**, und navigieren Sie zur Registerkarte **Erweitert**.

5. Wählen Sie die Skriptdatei in der Drop-down-Liste **Einstellungen vor/nach dem Skript** aus, und übergeben Sie den Job.
6. Klicken Sie auf "**Aktivitätsprotokoll**", und stellen Sie sicher, dass das Skript für den angegebenen Sicherungsjob ausgeführt wird.

   Das Skript wird ausgeführt.

   Die Prä-/Post-Skripte wurden erfolgreich erstellt und befinden sich im Ordner "pre-post".

(Optional) Ausführen einer manuellen Sicherung

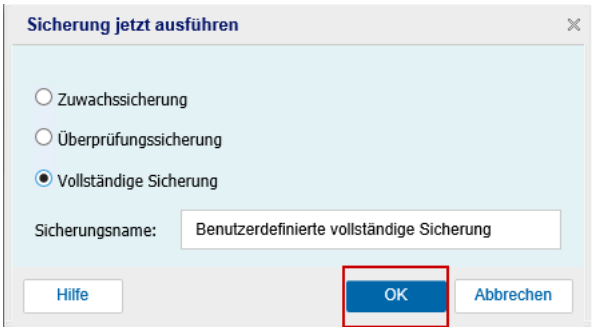
Normalerweise werden Ihre Sicherungen automatisch durchgeführt und von den Ablaufplan-Einstellungen gesteuert. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern. Wenn Sie z. B. einen Wiederholungsplan für vollständige Sicherungen, Zuwachssicherungen und Überprüfungssicherungen festgelegt haben und größere Veränderungen an Ihrem Rechner vornehmen möchten, müssen Sie sofort eine manuelle Sicherung durchführen, ohne auf die nächste geplante Sicherung zu warten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Navigieren Sie zu **Ressourcen** > **Plan** > **Alle Pläne**.

   Die Liste aller Pläne wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Plan, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
4. Wählen Sie im Dialogfeld "Sicherung jetzt ausführen" den gewünschten Sicherungstyp aus, und geben Sie dann gegebenenfalls den Sicherungsnamen an.



Es sind folgende Optionen verfügbar:

Zuwachssicherung

Startet eine Zuwachssicherung Ihres Rechners. Eine Zuwachssicherung sichert nur jene Blöcke, die seit der vorherigen Sicherung geändert wurden.

Hinweis: Wenn Sie eine Sicherung zum ersten Mal ausführen, wird automatisch die vollständige Sicherung initiiert, auch wenn Sie die Option "Zuwachssicherung" ausgewählt haben.

Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

Überprüfungssicherung

Startet eine Überprüfungssicherung Ihres Rechners, indem die aktuellste Sicherung von jedem einzelnen Block überprüft und der Inhalt und die Informationen mit der ursprünglichen Quelle verglichen wird. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht, aktualisiert Arcserve UDP Agent (Windows) die Sicherung dieses Blocks (Neusynchronisierung).

Vorteil: Im Vergleich zu einer vollständigen Sicherung wird nur ein sehr kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteil: Die Sicherung benötigt viel Zeit, da alle Blöcke des Quelldatenträgers mit den Blöcken der letzten Sicherung verglichen werden.

Vollständige Sicherung

Startet eine vollständige Sicherung Ihres gesamten Rechners oder der ausgewählten Volumes.

Hinweise:

- Wenn Sie der Sicherungsquelle ein neues Volume hinzufügen, wird das neue Volume vollständig gesichert, unabhängig davon, welche allgemeine Sicherungsmethode ausgewählt wurde.
- Wenn Sie keinen Sicherungsnamen angeben, wird automatisch der Name "Benutzerdefinierte vollständige Sicherung/Zuwachssicherung/Überprüfungssicherung" vergeben.

5. Klicken Sie auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.

6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.

7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Hinweis: Nur ein Job kann gleichzeitig ausgeführt werden. Wenn Sie versuchen, einen Sicherungsjob manuell zu starten, während gerade ein anderer Job ausgeführt wird, werden Sie in einer Warnmeldung darüber informiert, dass ein anderer Job ausgeführt wird, und aufgefordert, es später erneut zu versuchen.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Überprüfen der Sicherung

Um die Sicherung zu überprüfen, bestätigen Sie, dass Sie den Sicherungsplan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Sie können den Status von Sicherungsjobs auf der Registerkarte Jobs überprüfen.

Gehen Sie wie folgt vor: Zum Überprüfen von Plänen

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Wenden Sie zur Überprüfung von Sicherungsjobs eine der folgenden Methoden an:

Methode 1

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Methode 2

1. Navigieren Sie in der Arcserve UDP-Konsole zur Registerkarte **Jobs** > **Jobs erfolgreich abgeschlossen**.

   Die Liste der abgeschlossenen Sicherungsjobs wird im mittleren Fensterbereich angezeigt.
2. Klicken Sie auf den abgeschlossenen umgekehrten Replikationsjob. Der rechte Fensterbereich wird aktualisiert.
3. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
4. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Der Sicherungsjob wurde überprüft.

Fehlerbehebung

Jobstatus, Jobübersicht und Aktivitätsprotokoll nicht sichtbar

Jobstatus, Jobübersicht und Aktivitätsprotokoll nicht sichtbar

Problem

Jobstatus, Jobübersicht und Aktivitätsprotokoll für Linux-Knoten werden in der Arcserve UDP-Konsole nicht angezeigt.

Lösung

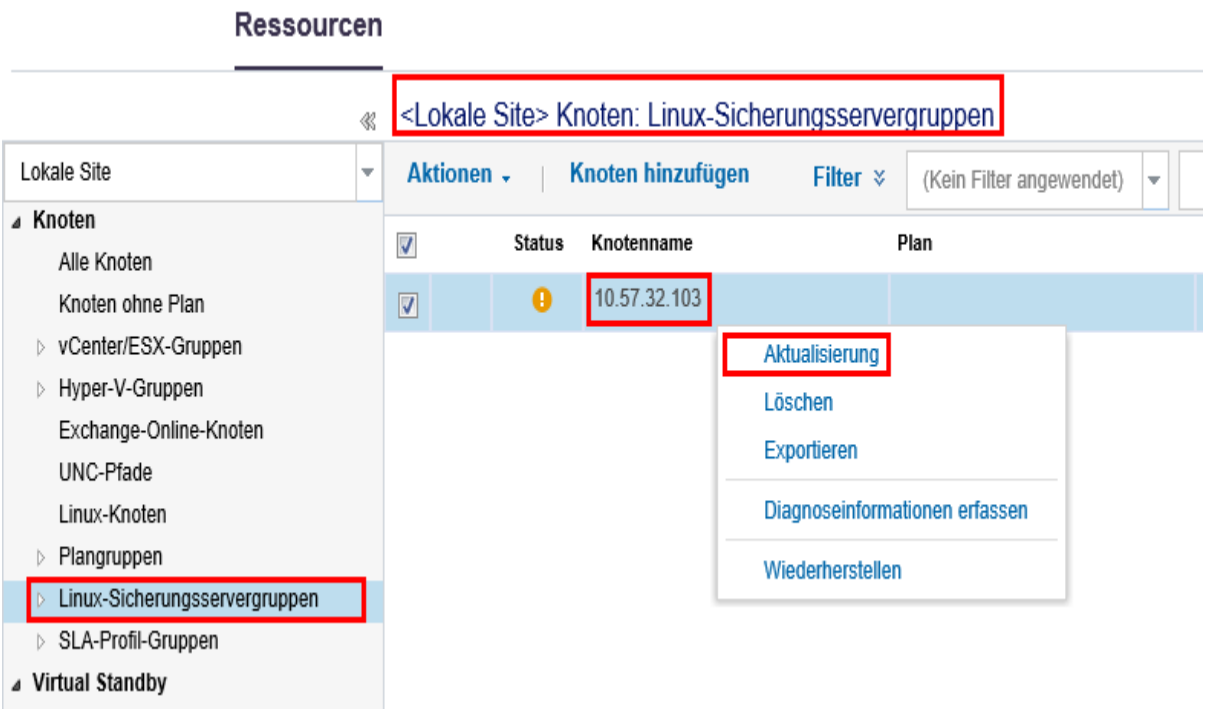
Der Linux-Sicherungsserver kann mit dem Hostnamen keine Verbindung mit Arcserve UDP herstellen.

Gehen Sie wie folgt vor:

1. Erstellen Sie die Datei server_ip.ini an folgendem Speicherort von Arcserve UDP:

   "UDP-Installationspfad"\Management\Configuration\server_ip.ini
2. Geben Sie die IP-Adresse von Arcserve UDP in dieser Datei ein.
3. Melden Sie sich bei der Arcserve UDP-Konsole an und aktualisieren Sie den Linux-Sicherungsserver und Linux-Knoten.

   Hinweis: Der Linux-Sicherungsserver kann nur über "Linux-Sicherungsservergruppen", wo alle Linux-Sicherungsserver aufgelistet werden, aktualisiert werden.



Jobstatus, Jobübersicht und Aktivitätsprotokoll sind nun sichtbar.

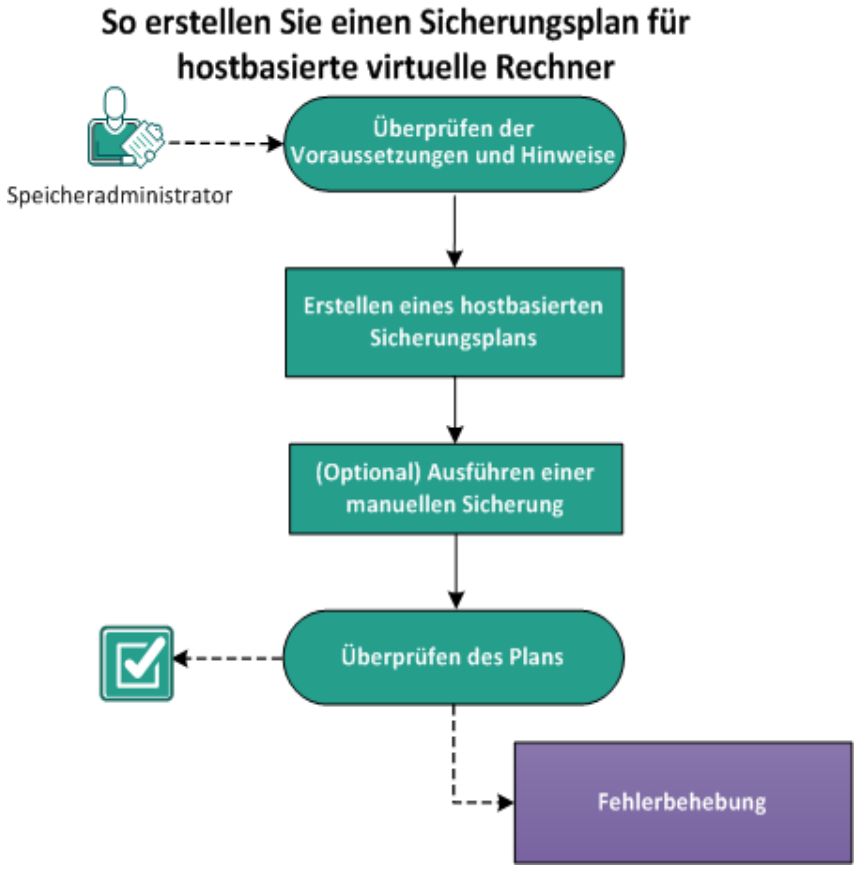
Erstellen eines Sicherungsplans für hostbasierte virtuelle Rechner

Um Ihre hostbasierten virtuellen Rechnerknoten zu schützen, müssen Sie einen hostbasierten Sicherungsplan erstellen. Ein Sicherungsplan für hostbasierte virtuelle Rechnerknoten besteht aus einem Sicherungstask. In diesem Sicherungstask können Sie die Knoten, die Sie schützen möchten, das Sicherungsziel und den Sicherungsablaufplan angeben. Beim Sicherungsziel kann es sich um ein lokales Ziel, einen freigegebenen Remote-Ordner oder den Recovery Point Server, auf dem Sie Ihre Sicherungsdaten speichern möchten, handeln.

Sie können auch Oracle-Datenbanken, SQL Server und Exchange Server sichern. Zum Sichern von Oracle-Datenbanken müssen gewisse Voraussetzunge erfüllt sein.. Zum Sichern von SQL Server und Exchange Server sind keine Voraussetzungen zu erfüllen. Überprüfen Sie folgende Voraussetzungen, um eine anwendungskonsistente Sicherung einer Oracle-Datenbank durchzuführen:

- Voraussetzung zur Erstellung einer anwendungskonsistenten Sicherung einer Oracle-Datenbank

Die folgende Abbildung veranschaulicht den Prozess zum Schützen hostbasierter virtueller Rechnerknoten.



Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen eines hostbasierten Sicherungsplans
3. (Optional) Ausführen einer manuellen Sicherung
4. Überprüfen des Plans
5. Fehlerbehebung

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich bei der Konsole an.
- Bereiten Sie einen hostbasierten Sicherungs-Proxy-Server vor, auf dem Arcserve Unified Data Protection Agent für Windows installiert ist.
- Um Funktionen wie Preflight-Check, Pre/Post-Befehle oder Anwendungsprotokoll bereinigen auszuführen, aktualisieren Sie die den virtuellen Computer in der Knotenlistenansicht der Arcserve UDP Konsole mit einer der folgenden Anmeldeinformationen für den virtuellen Gastcomputer:
  - Integrierte Anmeldeinformationen des Administratorbenutzers.
  - Integrierte Anmeldeinformationen des Domänen-Administratorbenutzers.
  - Deaktivieren Sie bei anderen Administratoranmeldeinformationen die Benutzerkontensteuerung (UAC) auf dem virtuellen Gastrechner.
- Um eine Wiederherstellung auf Datenbankebene (für Exchange und SQL Server) oder spezifische Wiederherstellung (Exchange) nach einer Sicherung durchführen zu können, müssen folgende Voraussetzungen erfüllt werden:
  - Die VM muss die anwendungskonsistente Sicherung unterstützen. Weitere Informationen zur anwendungskonsistenten Sicherung finden Sie unter So erstellen Sie anwendungskonsistente Snapshots für VMware oder So erstellen Sie anwendungskonsistente Snapshots für Hyper-V.
  - Bei VMware-VMs muss die Stilllegungsmethode für VMware-Snapshots der **VMware-Tools** im Plan für die Sicherung verwendet werden.
  - Für die Hyper-V-VM Arcserve UDP muss automatisch ein Dienstprogramm im Gast-BSder VM bereitgestellt werden, um Anwendungsmetadaten während einer Sicherung zu sammeln. Der Zugriff auf das Gast-BS der VM muss über den Sicherungs-Proxy-Server oder den Hyper-V-Host über ein Netzwerk erfolgen. Der VM-Knoten muss zur gleichen Zeit mit Administratoranmeldeinformationen in der Knotenansichtsliste der Arcserve UDP Konsole aktualisiert werden. Wenn der Zugriff auf das Gast-BS der VM vom Sicherungs-Proxy-Server und Hyper-V-Host aus irgendwelchen Gründen nicht möglich ist, gehen Sie folgendermaßen vor, um das Hilfsprogramm manuell auf dem Gast-BS der VM zu installieren:

a. Melden Sie sich beim Backup-Proxy-Server an, und navigieren Sie zum folgenden Ordner:

   <Arcserve UDP installation path>\Engine\BIN (Example, C:\Programme\Arcserve\Unified Data Protection\Engine\BIN)

b. Suchen Sie die ausführbare Datei **VMICService_32.exe** oder **VMICService_64.exe**.

c. Kopieren Sie die ausführbare Datei in einen Ordner innerhalb des Gast-BS der VM. (Kopieren Sie für ein 32-Bit-BS**VMICService_32.exe**, und andernfalls **VMICService_64.exe**).

   Zum Beispiel können Sie ein ISO-Image erstellen, indem Sie diese ausführbare Datei einfügen und sie auf das DVD-Gerät der VM laden.

d. Melden Sie sich beim Gast-BS des virtuellen Computers an und führen Sie entweder **VMICService_32.exe-Installation** oder **VMICService_64.exe-Installation** aus.

- Wenn Sie die Sicherungsdaten auf dem Recovery Point Server speichern möchten, installieren Sie die Serverkomponente, und erstellen Sie Datenspeicher.
- Überprüfen der Voraussetzungen zur Sicherung einer Oracle-Datenbank.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Für Hardwaresnapshots müssen folgende Voraussetzungen gegeben sein:

Für Hyper-V

- Installieren einen VSS-Hardwareanbieter auf den Hyper-V-Servern, und installieren Sie den VSS-Hardwareanbieter zur Unterstützung des übertragbaren Snapshots auch auf dem Sicherungs-Proxy-Server. Eine typische Konfiguration eines VSS-Hardwareanbieters umfasst:
  - Angeben eines Servers, der die LUN steuert.
  - Angeben der Anmeldeinformationen des Datenträger-Arrays für den Zugriff auf das Datenträger-Array.

  Weitere Informationen zur Konfiguration des VSS-Hardwareanbieters erhalten Sie beim Hersteller des Hardwareanbieters.
- Auf dem Hyper-V-Server und dem Proxy-Server muss jeweils eine ähnliche Betriebssystemversion installiert sein.
- Wenn der Hyper-V-Server zu einem Cluster gehört, sollte der Proxy-Server nicht Teil des Hyper-V-Clusters sein.

- Deinstallieren Sie UDP-CBT über "Programme und Funktionen" in der Systemsteuerung auf dem Hyper-V-Host.

Für VMware

- Arcserve UDP unterstützt NetApp iSCSI- und NetApp NFS-LUNs.
- Fügen Sie zum Erstellen eines Hardware-Snapshots für VMware das Speicher-Array zur Konsole hinzu. Weitere Informationen zum Hinzufügen eines Speicher-Arrays finden Sie unter Hinzufügen eines Speicher-Arrays.
- Um den Hardware-Snapshot zu verwenden, ist eine Flexclone Lizenz für NetApp-Speicher-Arrays mit Data ONTAP erforderlich, die im 7- und Cluster-Modus ausgeführt werden.

Hinweise für die Sicherung der VM:

- **Auswirkungen einer Volume-Defragmentierung auf kontinuierliche Sicherungen**

  Die systemeigene Defragmentierung von Windows wirkt sich auf die Größe des Backups auf Blockebene aus, da Arcserve UDP weiterhin alle geänderten Blöcke inkrementell sichert. Das bedeutet, dass Blöcke, die während der Defragmentierung verschoben wurden, auch dann in die Sicherung eingeschlossen werden, wenn sich keine Daten in den Dateien geändert haben. Dadurch wird die Sicherungsgröße erhöht. Dieses Verhalten ist normal.

- **So schützen Sie virtuelle Rechner in Hyper-V 2016 mit der Windows-Funktion "Robuste Änderungsnachverfolgung"**

  Um VMs in Hyper-V 2016 zu schützen, wird für inkrementelle Sicherungen die Nutzung der Windows-Funktion "Robuste Änderungsnachverfolgung" (RCT) empfohlen. Arcserve UDP verwendet automatisch die Windows-Funktion "Robuste Änderungsnachverfolgung" (RCT), wenn VMs mit der Konfigurationsversion 8.0 oder höher gesichert werden, die auf einem Hyper-V 2016-Host bzw. in einem Hyper-V 2016-Cluster ausgeführt wird. Wenn Ihr Hyper-V von einer vorherigen Version aktualisiert wird, aktualisieren Sie auch Ihre VM-Konfiguration. Verwenden Sie hierzu die Microsoft-Dokumentation. Wenn die Aktualisierung für alle virtuellen Rechner abgeschlossen ist, die von Arcserve UDP geschützt werden, wird empfohlen, den Arcserve UDP-CBT-Dienst auf dem Hyper-V-Host zu deinstallieren.

Überlegungen bei einer bestimmten Netzwerksicherung:

- Hypervisor, Windows Proxy und RPS müssen sich im selben Netzwerk befinden.
- Wenn ESXi mit **Hostname** zum vCenter hinzugefügt wird, muss die Auswahl des Sicherungsnetzwerks das Standardnetzwerk von ESXi sein.

  Hinweis: Das Standardnetzwerk ist das Netzwerk, das durch DNS.

- Wenn ESXi mit IP zum vCenter hinzugefügt wird, sollte die Auswahl des Sicherungsnetzwerks das gleiche Netzwerk sein, das ESXi zum Anfügen an das vCenter verwendet.

Szenario #	Hat vCenter	Was wird zum Hinzufügen in vCenter verwendet?	Könnte das Sicherungsnetzwerk verwendet werden?	Funktioniert der Datei-Workaround für DNS/Hosts?
1	Nein	N/V	Ja	N/V
2	Ja	Hostname von ESXi – Die Produktions-IP des Hostnamens wird aufgelöst	Nein	Ja. Aktualisieren Sie das DNS oder die Hostdatei auf dem Proxyserver.
3	Ja	Hostname von ESXi – Die Sicherungsnetzwerk-IP des Hostnamens wird aufgelöst	Ja	N/V
4	Ja	Produktions-IP von ESXi	Nein	Nein
5	Ja	Sicherungsnetzwerk-IP von ESXi	Ja	N/V

Prüfen der Voraussetzungen für eine anwendungskonsistente Sicherung der Oracle Datenbank

Um eine Oracle-Datenbank mit konsistenten Daten zu sichern, stellen Sie sicher, dass der ARCHIVELOG-Modus aktiviert ist, damit die Redo-Protokolle archiviert werden.

Hinweis: Das Daten-Volume muss Oracle-Datendateien, Kontrolldateien, Server-Parameterdateien und Online-Redo-Protokolle enthalten. Die archivierten Redo-Protokolle müssen sich physisch auf einem separaten Volume befinden.

Befolgen Sie diese Schritte, um zu überprüfen, ob der ARCHIVELOG-Modus aktiviert ist:

a. Auf dem Oracle Server als Oracle-Benutzer mit SYSDBA-Berechtigungen anmelden.

b. Geben Sie folgenden Befehl ein, wenn die SQL*Plus-Eingabeaufforderung angezeigt wird:

   ARCHIVE LOG LIST;

   Einstellungen des Archivprotokolls für die aktuelle Instanz werden angezeigt.

c. Konfigurieren Sie folgende Einstellungen:

   Datenbankprotokollierungsmodus: Archivierungsmodus

   Automatische Archivierung: aktiviert

d. Starten Sie den ARCHIVELOG-Modus.

   Hinweis: Wenn der ARCHIVELOG-Modus nicht aktiviert ist, starten Sie den ARCHIVELOG-Modus, um die Datenbank zu sichern.

Befolgen Sie diese Schritte, um den ARCHIVELOG-Modus zu starten:

a. Fahren Sie den Oracle-Server herunter.

b. Führen Sie die folgenden Anweisungen in Oracle aus:

   CONNECT SYS/SYS_PASSWORD AS SYSDBA

   STARTUP MOUNT;

   ALTER DATABASE ARCHIVELOG;

   ALTER DATABASE OPEN;

   Standardmäßig werden Protokolle im Flash-Wiederherstellungsbereich gespeichert. Wenn Archivprotokolle nicht im Flash-Wiederherstellungsbereich gespeichert werden sollen, stellen Sie das LOG_ARCHIVE_DEST_n-Parameter auf den Speicherort ein, in dem die Archivprotokolle gespeichert werden sollen.

SQL>ALTER SYSTEM SET LOG_ARCHIVE_DEST_
1='LOCATION=e:\app\administrator\oradata\<Name_der_Oracle-Datenbank>\arch'
SCOPE= BOTH;

System geändert.

SQL> ARCHIVE LOG LIST;

Einstellungen des Archivprotokolls für die aktuelle Instanz werden angezeigt.

c. Konfigurieren Sie folgende Einstellungen:

Datenbankprotokollierungsmodus: Archivierungsmodus

Automatische Archivierung: aktiviert

Archivziel: E:\app\oracle\oradata\<Name_der_Oracle-Datenbank>\arch

Älteste Online-Protokollsequenz: 21

Aktuelle Protokollsequenz: 23

Der Oracle VSS Writer Service wurde gestartet und funktioniert ordnungsgemäß.

Erstellen eines hostbasierten Sicherungsplans

Ein Sicherungsplan besteht aus einem Sicherungstask, der eine Sicherung des virtuellen Rechners ausführt und die Daten am angegebenen Ziel speichert. Jeder Task besteht aus Parametern, die Quelle, Ziel, Ablaufplan und weitere Sicherungsdetails definieren.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

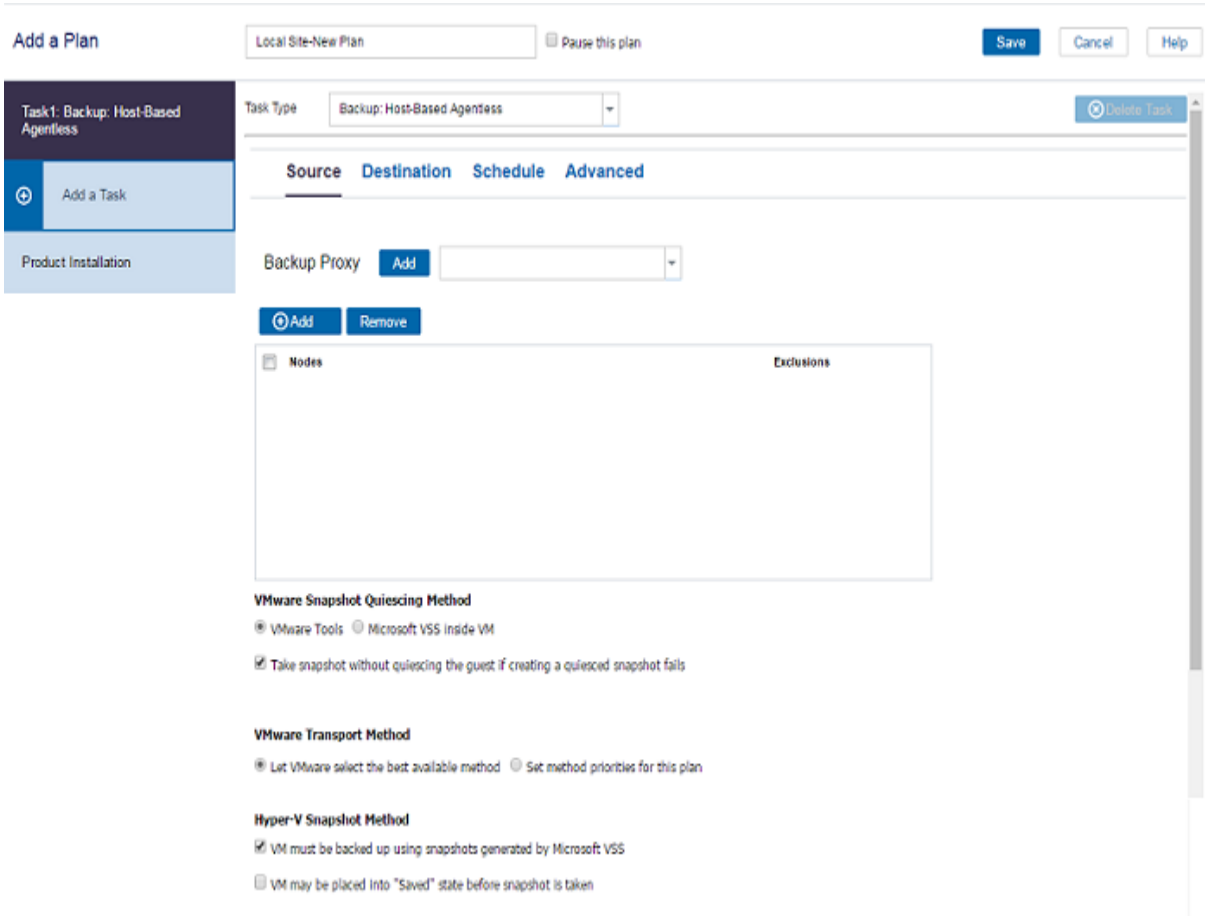
   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Sicherung, Hostbasiert und**

ohne Agent aus.



Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die Quellknoten angeben, die Sie schützen möchten. Sie können mehrere Knoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Knoten hinzufügen, wenn Sie einen Plan auf der Quellenseite erstellen oder ändern. Sie können einen Plan speichern, ohne Quellknoten hinzuzufügen. Der Plan wird erst bereitgestellt, wenn Sie Quellknoten hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Quelle**, und fügen Sie einen Sicherungs-Proxy-Server hinzu.

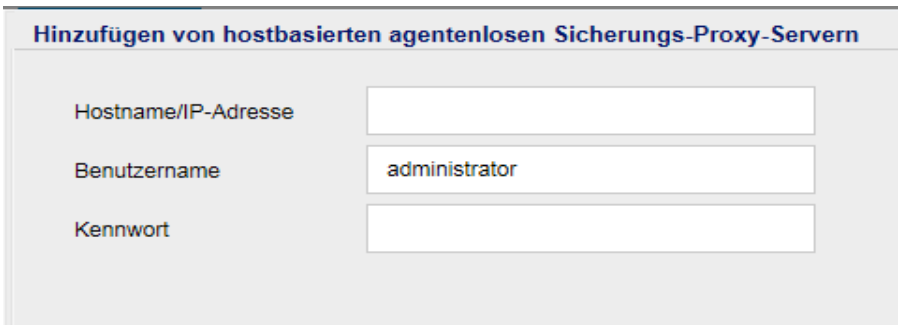
   Der Proxy-Server ist ein Knoten, auf dem Sie Arcserve Unified Data Protection Agent für Windows installieren. Wenn der Agent nicht auf diesem Proxy-Server installiert ist, wenn Sie den Plan speichern, wird dem Proxy-Server der Agent bereitgestellt. Die Einstellung für die Agent-Bereitstellung befindet sich im Task "Agent-Installation" des Plans.

   - Wenn der Sicherungs-Proxy bereits hinzugefügt wurde, wählen Sie ihn aus der Drop-Down-Liste aus.

   - Wenn der Sicherungs-Proxy nicht hinzugefügt wurde, klicken Sie auf **Hinzufügen**.

     Das Dialogfeld **Hinzufügen eines hostbasierten agentenlosen Sicherungs-Proxy-Servers** wird geöffnet.

     Geben Sie die Details zum Proxy-Server an, und klicken Sie auf **OK**.

   Sie müssen Portnummer und Protokoll nicht hinzufügen. Portnummer und Protokoll werden auf der Registerkarte **Einstellungen** der Konsole konfiguriert.

Hinweis: Wenn Sie einen Plan durch Ändern des Sicherungs-Proxy bearbeiten, aber die im Plan enthaltenen Knoten über laufende Jobs verfügen, schlägt die Planbereitstellung fehl. Befolgen Sie diese Schritte, um den Proxy eines Plans zu ändern:

a. Unterbrechen Sie den Plan.

b. Warten Sie, bis alle Knoten im Plan die laufenden Sicherungsjobs ausgeführt haben. (Oder Sie brechen die laufenden Jobs ab).

c. Ändern Sie den Proxy des Plans und speichern Sie ihn.

d. Nehmen Sie den Plan wieder auf.

2. Klicken Sie auf **Knoten hinzufügen**, um eine der folgenden Optionen zum Hinzufügen zu schützender Knoten auszuwählen:

Zu schützende Knoten auswählen

Öffnet das Dialogfeld **Zu schützende Knoten auswählen**, in dem Sie die Knoten aus der angezeigten Liste auswählen können. Wählen Sie diese Option aus, wenn Sie die Knoten bereits zu der Konsole hinzugefügt haben.

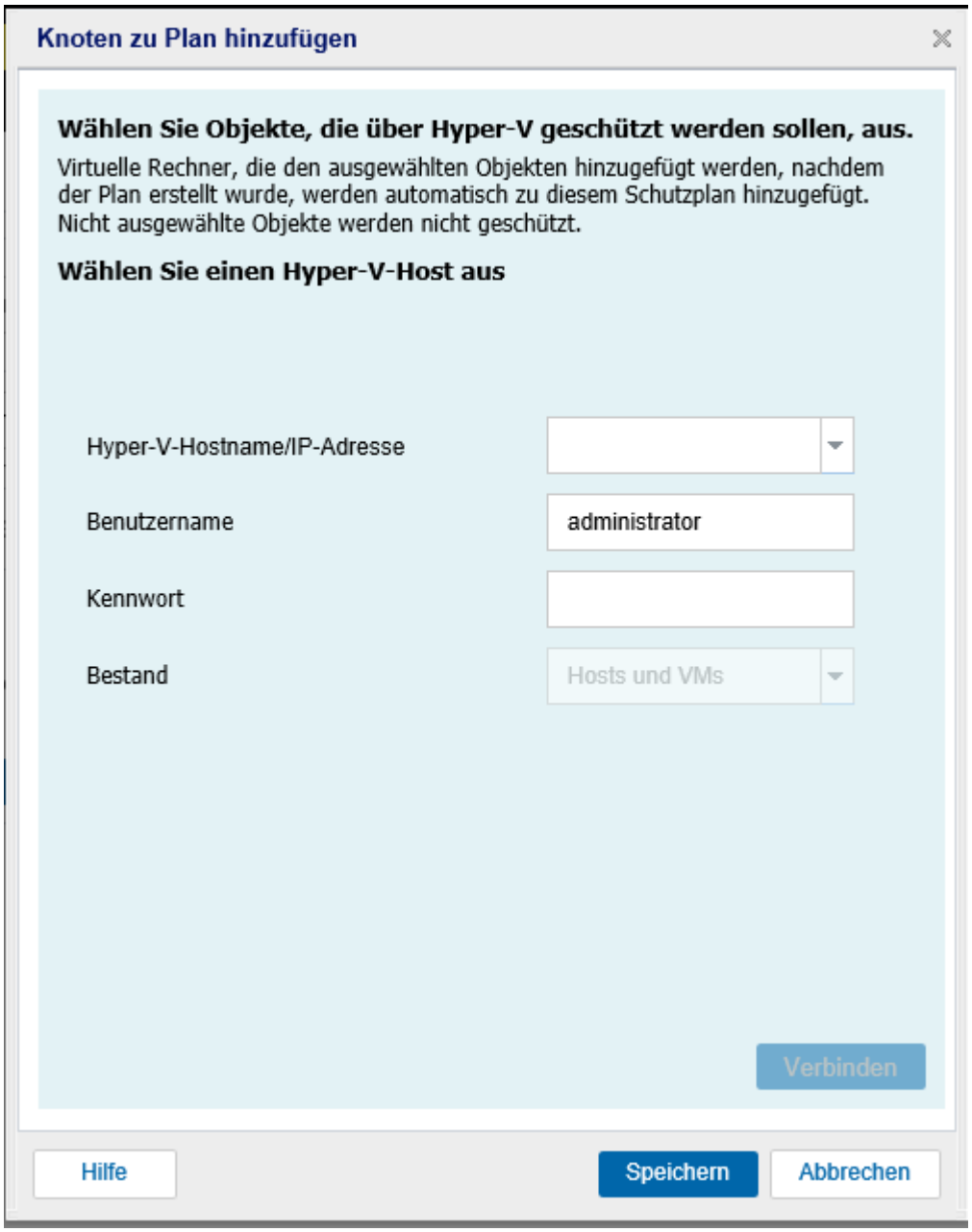
Hinzufügen von Knoten von einem Hyper-V

Öffnet das Dialogfeld **Knoten zu Arcserve UDP-Konsole hinzufügen**. Sie können einem Plan einzelne VM-Knoten oder VM-Containerobjekte (einschließlich Hyper-V-Cluster, Hyper-V-Host, den Speicherort) hinzufügen. Sobald Sie ein VM-Containerobjekt zum Plan hinzufügen, schützt der Plan alle zugewiesenen VMs automatisch. Eine neu unter dem VM-Containerobjekt erstellte oder aus einem anderen Ort in das VM-Containerobjekt verschobene VM wird automatisch von Arcserve UDP geschützt. Wenn die VM aus dem VM-Containerobjekt gelöscht (oder aus dem VM-Containerobjekt verschoben) wird, schützt Arcserve UDP die VM nicht mehr.

Um einem VM-Containerobjekt einen Plan hinzuzufügen, gehen Sie folgendermaßen vor:

a. Geben Sie die Hyper-V Serverdetails an, wählen Sie einen Suchmodus für die VMs in der Drop-down-Liste "Bestand" (Hosts und VMs, Speicher und VMs) und klicken Sie auf "Verbinden".

Eine Hyper-V-Hierarchiestruktur wird angezeigt.

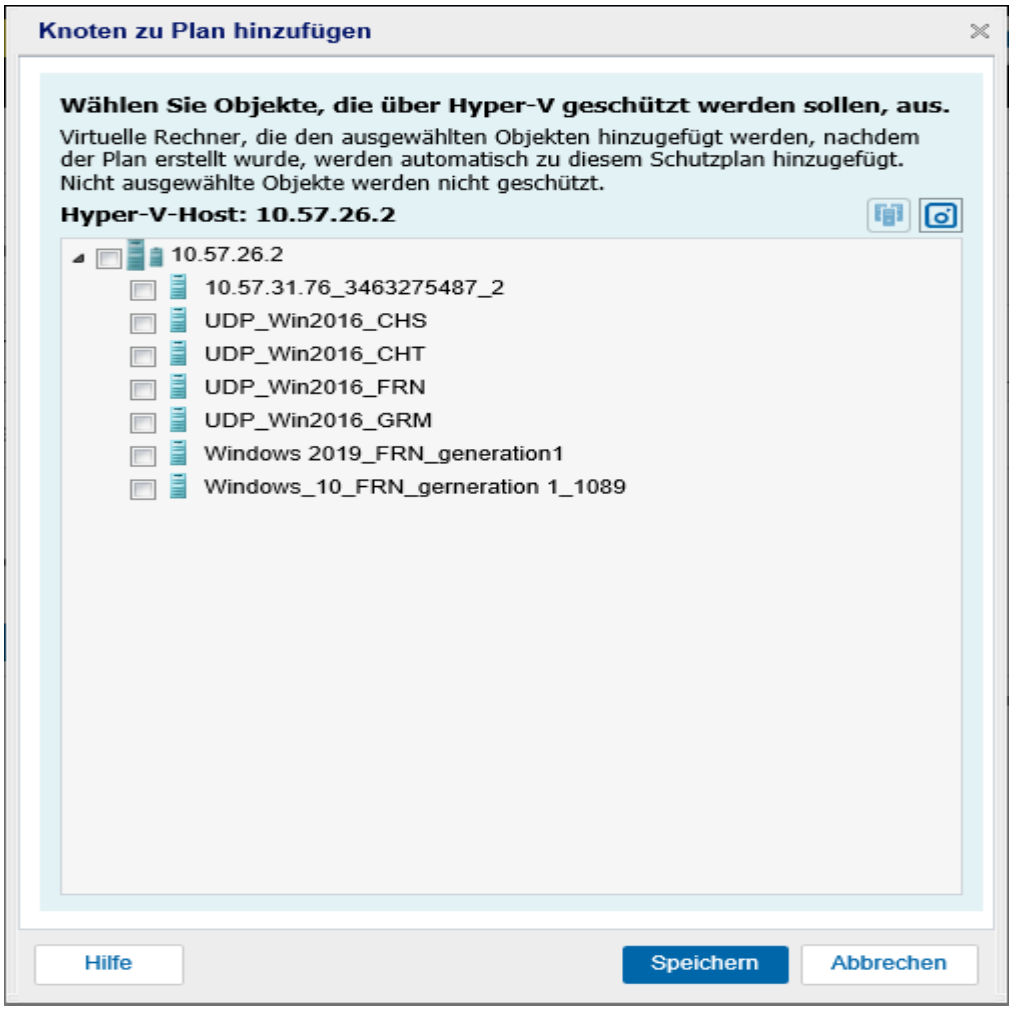


b. Erweitern Sie die Hyper-V-Hierarchiestruktur, um folgende Optionen auszuführen:

Hinweis: Je nach der Auswahl in der Drop-down-Liste "Bestand" werden andere Hierarchiestrukturen angezeigt – Hosts und VMs oder Speicher und VMs. Um zwischen verschiedenen Ansichten zu wechseln, klicken Sie auf die Schaltflächen oben rechts in der Struktur.

i. **Eine einzelne VM hinzufügen**

Aktivieren Sie das Kontrollkästchen der VM, die Sie aus der Liste hinzufügen möchten, und klicken Sie auf **Speichern**.



ii. **Fügen Sie ein VM-Containerobjekt hinzu**

Aktivieren Sie das Kontrollkästchen des VM-Containerobjekts, das Sie aus der Liste hinzufügen möchten, und klicken Sie auf "Speichern". Während Sie ein VM-Containerobjekt zum Schützen auswählen, können Sie auch die Auswahl einer untergeordneten VM oder eines untergeordneten VM-Containerobjekts unterhalb des Objekts deaktivieren. Dadurch wird die untergeordnete VM oder das untergeordnete VM-Containerobjekt vom Schutz ausgeschlossen.

Hinweis: Arcserve UDP verwendet Hyper-V-Cluster-/Host-Name, Volume-Name oder SMB-Freigabename, um das Containerobjekt in der Hyper-V-Liste eindeutig zu identifizieren. Dadurch können Sie Plänen dasselbe VM-Containerobjekt mehrmals hinzufügen.

Fügen Sie beispielsweise einen Hyper-V-Host anhand des Host-Namens hinzu, und fügen Sie dann unter Verwendung der IP-Adresse denselben Hyper-V-Host erneut zu. Ein weiteres Beispiel ist, eine SMB-Freigabe hinzuzufügen, die den Host-Namen des Host-Rechners verwendet, und

dieselbe SMB-Freigabe hinzuzufügen, die die IP-Adresse des Host-Rechners verwendet.

Wichtig!Arcserve UDP lässt Sie dasselbe Containerobjekt nicht zweimal zu einem Plan hinzufügen, um unvorhersehbares Verhalten zu vermeiden.

Hinzufügen von Knoten von vCenter/ESX

Öffnet das Dialogfeld **Knoten zu Arcserve UDP-Konsole hinzufügen**. Sie können einem Plan einzelne VM Knoten, Vorlagen oder VM-Containerobjekte hinzufügen. Sobald Sie ein VM-Containerobjekt zum Plan hinzufügen, schützt der Plan alle zugewiesenen VMs automatisch. Wenn eine neue VM unter dem VM-Containerobjekt erstellt oder aus einem anderen Speicherort in das VM-Containerobjekt verschoben wird, schützt Arcserve UDP die VM automatisch. Wenn die VM aus dem VM-Containerobjekt gelöscht oder aus dem VM-Containerobjekt verschoben wird, schützt Arcserve UDP die VM nicht mehr.

Hinweis: neben den VM-Containerobjekten in vSphere, behandelt Arcserve UDP auch Tags und Tag-Kategorien als VM Containerobjekt, sodass sie dem agentenlosen Sicherungsplan hinzugefügt werden. In einem solchen Fall werden automatisch alle VMs und Vorlagen geschützt, denen das betreffende Tag zugewiesen ist. Falls einem allgemeinem VM-Containerobjekt zudem ein Tag zugewiesen wird, wird dasselbe Tag auch allen VMs unter diesem VM-Containerobjekt virtuell zugewiesen. Weisen Sie beispielsweise einem Ressourcenpool ein Tag zu, wird allen VMs in diesem Pool automatisch dasselbe Tag zugewiesen, selbst wenn ihnen in vCenter kein Tag zugewiesen ist. Die automatische Sicherung auf Tag-Basis wird nur für vCenter 6.0 und 6.5 unterstützt.

Um einem VM-Containerobjekt einen Plan hinzuzufügen, gehen Sie folgendermaßen vor:

a. Geben Sie die Details des vCenter/ESX-Servers ein, wählen Sie in der Drop-down-Liste "Inventory" aus, in welcher Struktur die VMs angezeigt werden sollen ("Hosts and Clusters", "VMs and Templates" oder "VMs and Tags"), und klicken Sie auf **Verbinden**.

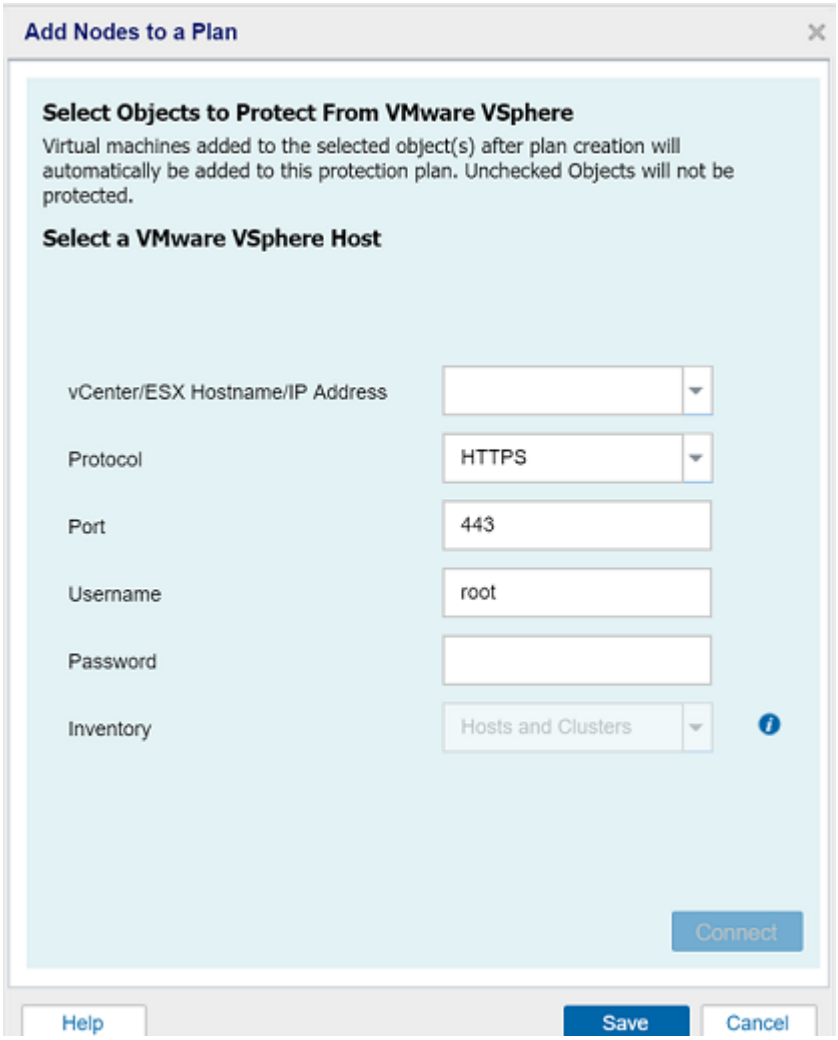
   Eine vSphere-Hierarchiestruktur wird angezeigt.

   Hinweis: Beachten Sie Folgendes:

   - Das VMware Virtual Disk Development Kit (VDDK) 6.x.x.x ist im Lieferumfang von Arcserve UDP 7.0 enthalten. VDDK 6.x.x.x unterstützt jedoch kein HTTP. Außerdem unterstützen vCenter

und ESX HTTPS-Verbindungen nur standardmäßig.

- Wählen Sie HTTPS-**Protokoll** aus, wenn Sie das integrierte VDDK 6.x.x manuell durch eine andere Version ersetzen möchten, und um vCenter/ESX manuell so zu konfigurieren, dass HTTP-Verbindungen zugelassen werden.

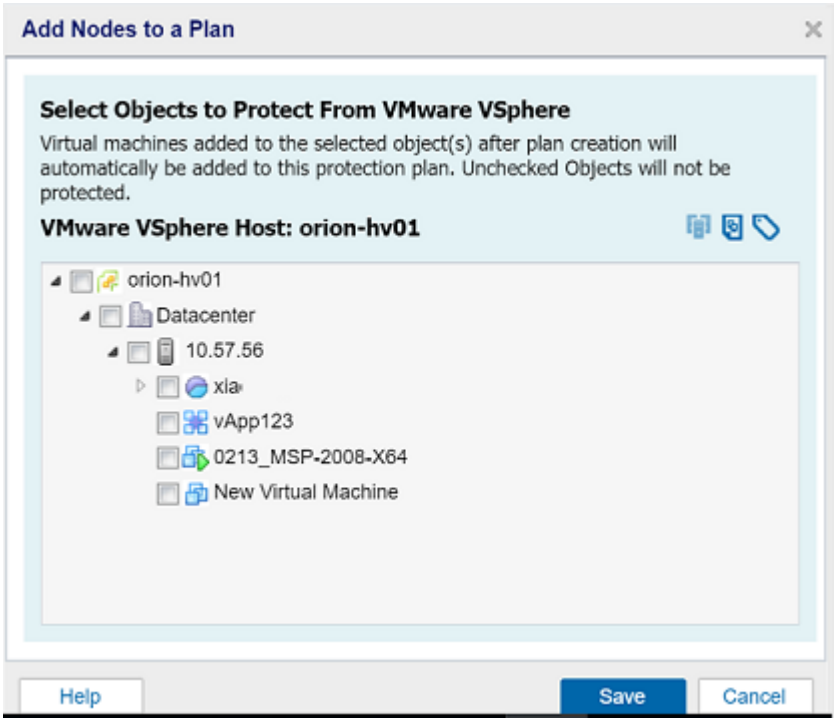


b. Erweitern Sie die vSphere-Liste, um Folgendes hinzuzufügen:

Hinweis: Je nachdem, welche Option Sie in der Drop-down-Liste "Bestandsaufnahme" auswählen, wird jeweils eine andere Hierarchiestrukturansicht angezeigt ("Hosts und Cluster", "VMs und Vorlagen" oder "VMs und Tags"). Durch Klicken auf die Schaltflächen oben rechts neben der Struktur können Sie zwischen den verschiedenen Strukturansichten wechseln.

i. **Hinzufügen einer einzelnen VM**

Aktivieren Sie das Kontrollkästchen der VM, die Sie aus der Liste hinzufügen möchten, und klicken Sie auf **Speichern**.



ii. **Fügen Sie ein VM-Containerobjekt hinzu**

Aktivieren Sie das Kontrollkästchen des Containers, den Sie aus der Liste hinzufügen möchten, und klicken Sie auf **Speichern**. Während Sie den Container zum Schützen auswählen, können Sie auch eine untergeordnete VM oder ein untergeordnetes VM-Containerobjekt deaktivieren. Dadurch wird die untergeordnete VM oder das untergeordnete VM-Containerobjekt vom Schutz ausgeschlossen.

Hinweis: Arcserve UDP verwendet vCenter-ESX-Name und vSphere MoRef ID (verwaltete Objektverweis-ID) zur eindeutigen Identifizierung des VM- Containerobjekts in der **vSphere** Liste. Dadurch können Sie einem Plan dasselbe VM-Containerobjekt mehrmals hinzufügen.

Beispiel:

a. Fügen Sie einem vCenter ein VM-Containerobjekt hinzu, indem Sie sich über den Hostnamen mit dem vCenter verbinden, und fügen Sie dasselbe VM-Containerobjekt dann erneut hinzu, indem Sie sich über die vCenter-IP-Adresse verbinden.

b. Fügen Sie einem vCenter ein VM-Containerobjekt hinzu, und fügen Sie es dann erneut direkt vom ESX Server hinzu.

Wichtig: Arcserve UDP lässt Sie einem Plan nicht zweimal dasselbe VM-Containerobjekt hinzufügen, da dies zu unvorhersehbarem Verhalten führen kann.

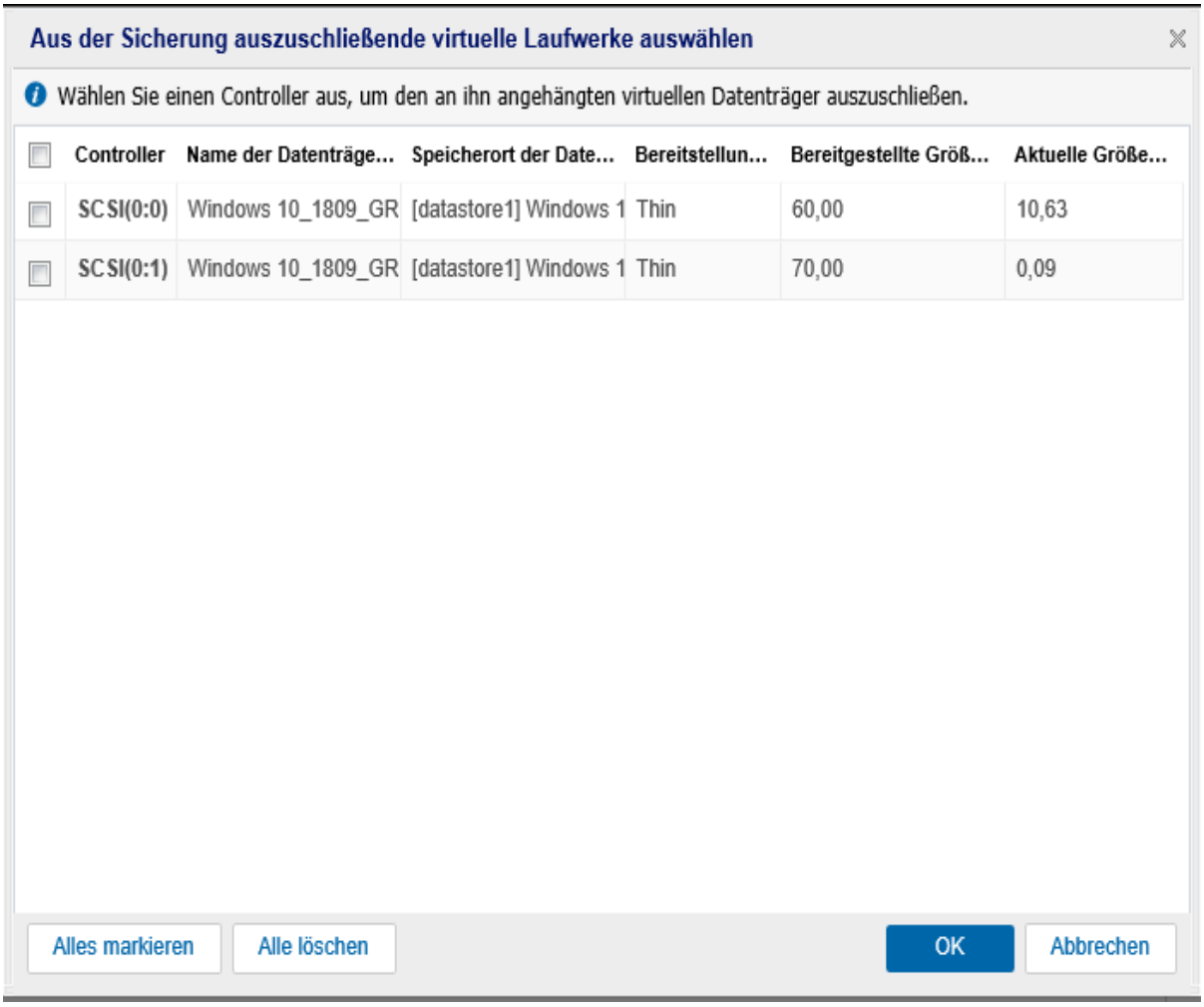
3. (Optional) Wählen Sie ein virtuelles Laufwerk, das den von dem Sicherungsjob ausgeschlossen werden kann.

   Standardmäßig wird die ganze VM einschließlich aller zugehörigen virtuellen Laufwerke durch den agentenlosen Sicherungsjob gesichert. Aber Sie können ein oder mehrere virtuelle Laufwerke angeben, die während der Sicherung übersprungen werden.

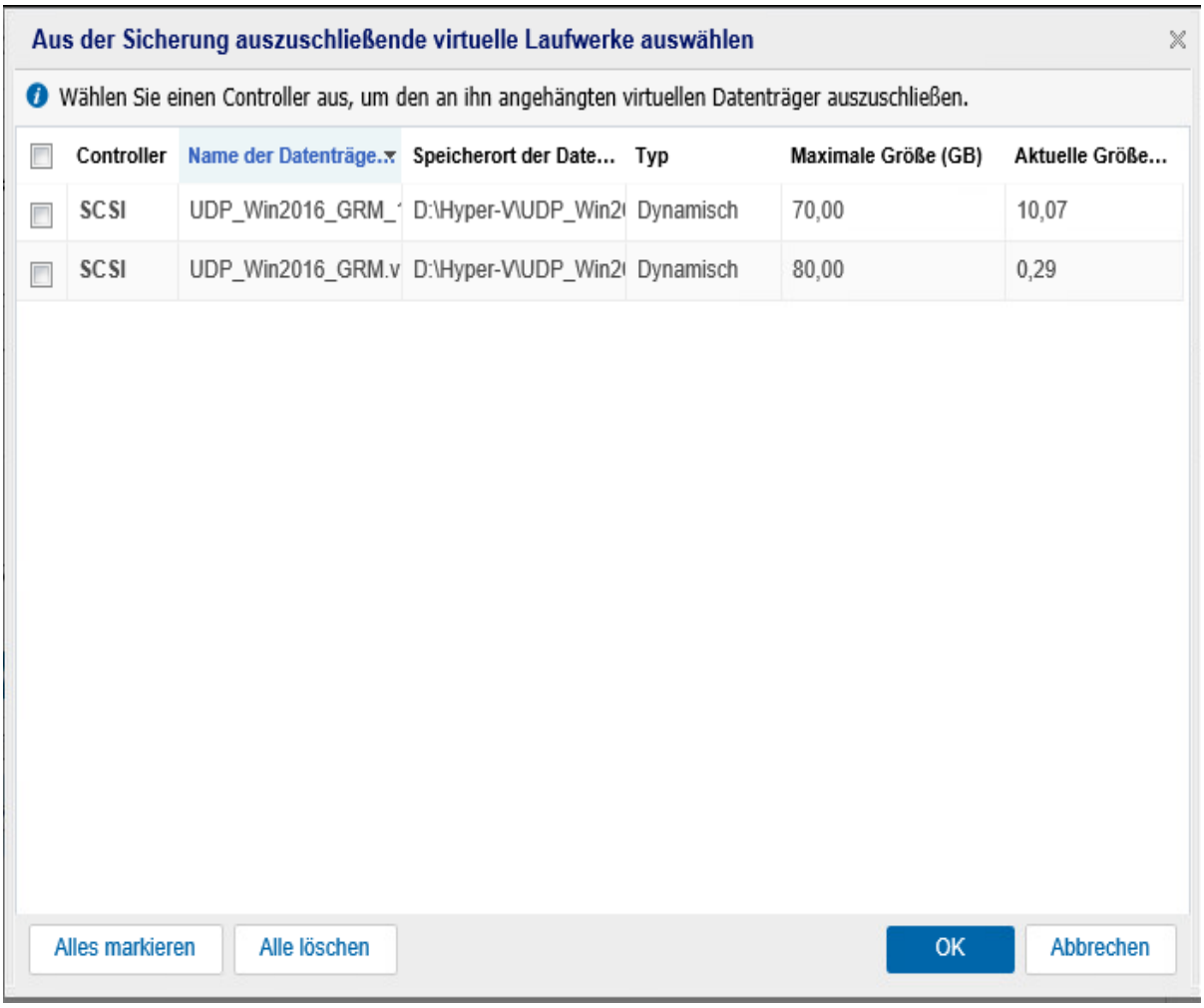
   a. Nach Hinzufügen eines VM-Knotens in den Plan, klicken Sie auf die Schaltfläche "Konfigurieren" auf der rechten Seite des Knotens.

      Ein Dialogfeld wird angezeigt.

      Dialogfeld für VMware-VM



      Dialogfeld für Hyper-V-VM



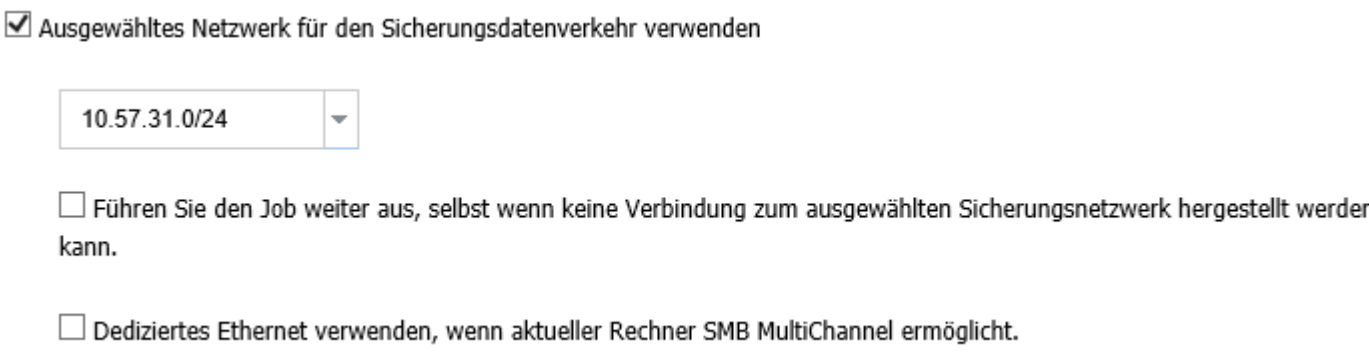
b. Aktivieren Sie das Kontrollkästchen für das virtuelle Laufwerk, das Sie vom Backup ausschließen möchten und klicken Sie zum Speichern auf **OK**.

Hinweise:

- Virtuelles Laufwerk wird statt dem Namen der virtuellen Datei vom Controller ausgeschlossen..
- Falls das virtuelle Laufwerk mit dem System-Volume des Gast-BS von der Sicherung ausgeschlossen ist, kann das wiederhergestellte VM nicht gestartet werden.
- Falls die VM eine Anwendung (SQL Server oder Exchange) installiert hat und ein virtuelles Laufwerk von der Sicherung ausgeschlossen ist, ist die Wiederherstellung auf Dateiebene DB nicht zulässig.

4. (Optional) Aktivieren Sie das Kontrollkästchen **Ausgewähltes Netzwerk für Sicherungsdatenverkehr verwenden**, und führen Sie die folgenden Schritte aus:

a. Um die Kommunikation zwischen dem Windows-Proxy- und dem Hypervisor-Server zu aktivieren, wählen Sie das CIDR-Netzwerk im Drop-down-Menü aus.



b. Wenn die Sicherungstask auch dann fortgesetzt werden soll, wenn das ausgewählte Netzwerk zwischen Proxyserver und Hypervisor-Server nicht verfügbar ist, aktivieren Sie das Kontrollkästchen **Weiter ausführen, auch wenn keine Verbindung mit dem ausgewählten Sicherungsnetzwerk hergestellt werden kann**.

c. Um die Einschränkung für den SMB-Multichannel zu definieren, sodass die Datenübertragung nur über das ausgewählte Netzwerk übertragen wird, aktivieren Sie das Kontrollkästchen **Dediziertes Ethernet verwenden, wenn der aktuelle Computer SMB Multichannel ermöglicht**.

Hinweise:

- Diese Option ist nicht standardmäßig verfügbar. Um diese Option zu aktivieren, wechseln Sie zu dem folgenden Ordnerspeicherort: C:\Program Files\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. Ändern Sie dann den Wert für useDedicatedEthernet zu "True".

```
- <SpecifyNetwork>
      <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

- Die SMB-Multichannel-Funktion ist standardmäßig in Windows aktiviert.

5. Geben Sie Netzwerkeinstellungen für die hostbasierte Hyper-V VM-Sicherung an:

Registrierungseinstellung: SMBSpecifiedIONetwork

Speicherort: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll oder HKEY_LOCAL_

MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\VMInstUUID

Typ: Multi-Zeichenfolgewert

Wertname: SMBSpecifiedIONetwork

Wertdaten: Zeichenfolge in der Form CIDR (ip/maskBitCount)

Beispiel: 192.168.10.0/24

Wenn sich die Hyper-V/Hyper-V-Cluster-VM-Datenträger auf der SMB-Freigabe befinden, kann der Benutzer auch ein anderes Netzwerk definieren, das für die Datenübertragung zwischen dem SMB-Server und dem Proxycomputer verwendet werden soll.

Hinweis: Die Zuordnung zwischen dem angegebenen IP- und SMB-Server-Hostnamen muss in der Domäne registriert sein.

6. (Optional) Wählen Sie eine der folgenden Stilllegungsmethoden für VMware aus. Diese Optionen gelten nur für VMware.

   VMware-Tools

   Gibt an, dass Arcserve UDP die VMware Tools für das Stilllegen des virtuellen Rechners verwendet. Wenn Sie die Option **Microsoft-VSS innerhalb der VM** im vorherigen Sicherungsjob verwendet haben, erfordert der nachfolgende Sicherungsjob mit dieser Option die Angabe der Anmeldedaten für den Zugriff auf den virtuellen Rechner. Dies liegt daran, dass Arcserve UDP die erforderlichen Tools vom virtuellen Rechner entfernt. Außerdem muss VMware Tools auf dem virtuellen Rechner installiert und aktualisiert werden.

   Microsoft-VSS innerhalb der VM

   Gibt an, dass Arcserve UDP Microsoft-VSS im Gastbetriebssystem für das Stilllegen des virtuellen Rechners verwendet. Dies gilt nur für virtuelle Rechner mit Windows-Gastbetriebssystem. VMware Tools muss im Gastbetriebssystem installiert werden, und die Tools müssen aktualisiert werden. Wenn Sie diese Option verwenden, muss der virtuelle Rechner eingeschaltet sein und mit den integrierten Administratoranmeldedaten aktualisiert werden. Weitere Informationen zum Aktualisieren von Knoten finden Sie unter Aktualisieren von Knoten.

   Hinweis: Der mit dieser Option von VMware bereitgestellte Snapshot ist möglicherweise nicht anwendungskonsistent. Oder anders ausgedrückt: Bei der mit dieser Option erstellten Sicherung handelt es sich unter Umständen nicht um eine anwendungskonsistente Sicherung. Die Umgehungslösung besteht darin, die Stilllegungsmethode für VMware-Snapshots der VMware-Tools zu nutzen und gleichzeitig die VSS-Writer *MSSearch Service Writer* und *Shadow Copy*

Optimization Writer im Gast-BS der VM zu deaktivieren, bevor das Problem behoben wird.

Snapshot ohne Stilllegung des Gastes aufnehmen, wenn Stilllegungs-Snapshot fehlschlägt

Gibt an, dass Arcserve UDP den Sicherungsjob durch Aufnahme eines Snapshots ohne Stilllegung des virtuellen Rechners fortsetzt, wenn der Snapshot beim Sicherungsjob nicht mit der Stilllegungsoption erstellt werden konnte.

Hinweise:

- Die Option **Microsoft-VSS innerhalb der VM** unterstützt die Anwendungs-Datenbankebene und die spezifische Ebene einer Sicherung nicht.
- Beide Stilllegungsmethoden sind nicht anwendbar, wenn der virtuelle Rechner ausgeschaltet ist. Wenn der Sicherungsjob gestartet wird, während der virtuelle Rechner ausgeschaltet ist, ignoriert der Sicherungsjob beide Stilllegungsmethoden.
- Für beide Stilllegungsmethoden gilt: Wenn der Sicherungsjob aus irgendwelchen Gründen nicht fortgesetzt werden kann (z. B., weil die Anmeldedaten nicht korrekt sind), schlägt der Sicherungsjob in Arcserve UDP fehl. Weitere Informationen zum Fehlschlagen eines Sicherungsjobs finden Sie unter dem Thema Fehlerbehebung.

7. (Optional) Wählen Sie eine der Transportmethoden für VMware aus. Diese Optionen sind für VMware anwendbar.

Lassen Sie VMware die beste verfügbare Methode auswählen.

Gibt an, dass VMware die Datentransferoption auswählt. Sie müssen keine Datentransferoption manuell festlegen.

Methodenprioritäten für diesen Plan festlegen

Gibt an, dass Sie die Datentransferoption auswählen und die Priorität für jede Option festlegen können. Verwenden Sie die Pfeilschaltfläche, um den Transportmodus zu priorisieren.

- HOTADD-Transportmodus
- NBD-Transportmodus
- NBDSSL-Transportmodus
- SAN-Transportmodus

Hinweis: Wenn Sie den Transportmodus sowohl in der Konsole als auch im Registrierungsschlüssel angegeben haben, dann überschreibt die von der Konsole festgelegte Priorität die im Registrierungsschlüssel festgelegte Priorität. Weitere

Informationen über das Festlegen der Priorität mithilfe des Registrierungsschlüssels finden Sie unter Definieren eines Transportmodus für hostbasierte agentenlose Sicherung und Wiederherstellung.

8. (Optional) Wählen Sie die Hyper-V-Snapshot-Methode aus. Diese Optionen gelten nur für Hyper-V.

   VM muss mithilfe von Snapshots gesichert werden, die über die Microsoft VSS-Methode generiert wurden

   Gibt an, dass Arcserve UDP die systemeigenen Snapshot-Methoden von Microsoft – online und offline – für den Sicherungsjob verwendet. Dies ist die Standardoption. Wenn dieses Kontrollkästchen nicht aktiviert ist und die Microsoft-Online- und -Offline-Methoden nicht verfügbar sind, verwendet der Sicherungsjob die Arcserve UDP-Methode, um den virtuellen Rechner zu sichern.

   Wenn die Microsoft-Offline-Methode für die Sicherung verwendet wird und sich der virtuelle Rechner im Zustand "Gespeichert" befinden muss, aktivieren Sie auch das Kontrollkästchen **VM kann in den Status "Gespeichert" abgelegt werden, bevor ein Snapshot aufgenommen wird**. Wenn Sie dieses Kontrollkästchen aktivieren, schlägt der Sicherungsjob fehl.

   Die Online-Sicherung ist die empfohlene Sicherungsmethode, da sie die anwendungskonsistente Sicherung unterstützt, ohne die Verfügbarkeit des virtuellen Rechners einzuschränken. Der Zugriff auf den virtuellen Rechner ist während der Sicherung möglich. Die Online-Sicherungsmethode muss einige Voraussetzungen erfüllen, wie z. B. installierte und aktualisierte Integrationsservices. Wird eine der Voraussetzungen nicht erfüllt, wird nur die Offline-Sicherungsmethode verwendet.

   Die Microsoft-Offline-Sicherungsmethode verfügt über zwei Ansätze: Zustand "Gespeichert" und Checkpoint. Wenn der Hyper-V-Host über das Betriebssystem Windows 2012 R2 mit KB 2919355 (oder höher) verfügt, wird der Checkpoint-Ansatz verwendet. Andernfalls wird der Ansatz des Zustands "Gespeichert" verwendet.

   Der Hauptunterschied zwischen diesen beiden Ansätzen ist, dass für den Ansatz des Zustands "Gespeichert" der virtuelle Rechner für kurze Zeit nicht verfügbar sein darf. Der virtuelle Rechner muss einige Minuten lang in den Zustand "Gespeichert" versetzt werden, während der Snapshot erstellt wird.

   Neben den systemeigenen Snapshot-Methoden von Microsoft verfügt Arcserve UDP auch über eine eigene Snapshot-Methode, die verwendet werden kann, wenn die systemeigenen Snapshot-Methoden von Microsoft nicht verfügbar sind.

Hinweis: Sowohl die Microsoft-Offlinemethode als auch die Arcserve UDP-Methode sind absturzkonsistente Sicherungsmethoden. Beide Methoden können die Datenintegrität nicht garantieren. Der Hauptunterschied zwischen den Methoden ist, dass die Microsoft-Offlinemethode dem Zustand nach einer plötzlichen Abschaltung der VM entspricht, die Arcserve UDP-Methode hingegen dem Zustand nach einer plötzlichen Abschaltung des Hyper-V-Hosts.

VM kann in den Status "Gespeichert" abgelegt werden, bevor ein Snapshot aufgenommen wird

Gibt an, dass der virtuelle Rechner wenn erforderlich in den Zustand "Gespeichert" versetzt wird, bevor der VSS-Snapshot erstellt wird. Wählen Sie diese Option aus, wenn der virtuelle Rechner die Onlinesicherung nicht unterstützt. Wenn der virtuelle Rechner die Onlinesicherung unterstützt, wird der virtuelle Rechner selbst bei Aktivierung dieser Option nicht in den Zustand "Gespeichert" versetzt.

Die Sicherungsquelle ist nun angegeben.

Definieren eines Transportmodus in der Registrierung für hostbasierte agentenlose Sicherung und Wiederherstellung

Sie können einen Transportmodus (für die Datenübertragung) definieren, der für den UDP-Agenten als Proxy verwendet werden soll, um hostbasierte agentenlose Sicherungen oder Wiederherstellungen für virtuelle Rechner auf VMware ESX-Servern auszuführen. Standardmäßig wird für hostbasierte agentenlose Sicherungen oder Wiederherstellungen ein Modus verwendet, der die Leistung (Geschwindigkeit) der Datenübertragung bei hostbasierten agentenlosen Sicherungen bzw. Wiederherstellungen verbessert. Wenn Sie für Sicherungen oder Wiederherstellungen jedoch einen spezifischen Transportmodus angeben möchten, konfigurieren Sie den Registrierungsschlüssel. Der entsprechende Vorgang ist in diesem Abschnitt beschrieben.

Hinweis: Für die Sicherung hat der im Plan definierte Transportmodus Vorrang vor dem, was in der Registry definiert ist.

Hostbasierte VM-Sicherungen können bei der Sicherung die folgenden Transportmodi verwenden:

- HOTADD-Transportmodus
- NBD-Transportmodus
- NBDSSL-Transportmodus
- SAN-Transportmodus

Beachten Sie Folgendes:

- Dies ist ein optionaler Konfigurationstask. Standardmäßig wird bei der Ausführung hostbasierter agentenloser Sicherungen ein Transportmodus eingesetzt, der die Leistung des Sicherungsvorgangs optimiert.
- Wenn Sie diesen Registrierungsschlüssel für die Verwendung eines spezifischen Transportmodus konfigurieren und dieser Modus nicht verfügbar ist, wird bei der Ausführung hostbasierter agentenloser Sicherungen ein verfügbarer Standardtransportmodus verwendet.
- Sie können den Transportmodus für alle VMs definieren, die für Sicherungen über den Proxy-Server verwendet werden (Proxy-Ebene), oder für eine einzelne VM (VM-Ebene). Wenn Sie sowohl den Proxy-Server als auch die VM konfigurieren, hat die Registrierung auf VM-Ebene Vorrang vor der Registrierung auf Proxy-Ebene.

Führen Sie diese Schritte durch, um den Transportmodus auf der Ebene des Proxy-Servers zu definieren (gilt sowohl für Sicherungen als auch für Wiederherstellungen):

1. Melden Sie sich beim Arcserve Unified Data Protection Agent für Windows-Sicherungs-Proxy-Server an.
2. Öffnen Sie die Windows-Registrierung, und suchen Sie nach dem folgenden Registrierungsschlüssel:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine]
3. Klicken Sie mit der rechten Maustaste auf "VDDKEnforceTransport", und klicken Sie im Pop-up-Menü auf "Ändern". Das Dialogfeld "Zeichenfolge bearbeiten" wird geöffnet.
4. Geben Sie im Feld "Wertdaten" den Transportmodus an, den Sie während des Sicherungsjobs verwenden möchten. Geben Sie einen oder mehrere der folgenden Werte an. Trennen Sie sie durch ":" voneinander ab. (Beispiel: nbd oder san:nbd:nbdssl:)

   hotadd

   HOTADD-Transportmodus

   nbd

   NBD-Transportmodus

   nbdssl

   NBDSSL-Transportmodus

   san

   SAN-Transportmodus
5. Klicken Sie auf "OK", um den Wert anzuwenden und das Dialogfeld "Zeichenfolge bearbeiten" zu schließen.

   Der Transportmodus ist definiert und wird das nächste Mal, wenn der Job ausgeführt wird, verwendet.

   Hinweis: Um Virtual Machine Disks (VMDK) des Typs Thin wiederherzustellen, wird standardmäßig der nicht erweiterte Transportmodus (LAN-Transportmodus) verwendet. Um den erweiterten Transportmodus für VMDKs des Typs Thin zu aktivieren, aktualisieren Sie den Registrierungsschlüssel wie im folgenden Beispiel:

   a. Öffnen Sie die Windows-Registrierung, und suchen Sie nach dem folgenden Registrierungsschlüssel:

      ```
      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine]
      ```

b. Erstellen Sie einen Schlüssel namens "AFRestoreDll".

c. Erstellen Sie innerhalb des Schlüssels "AFRestoreDll" einen Zeichenfolgenwert namens "EnforceTransportForRecovery".

d. Geben Sie den Transportmodus an, den Sie während des Wiederherstellungsjobs verwenden möchten. (Beispiel: "san:nbd:nbdssl")

Beispiel

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFRestoreDll]

"EnforceTransportForRecovery"="san:hotadd:nbd:nbdssl"

Führen Sie folgende Schritte durch, um den Transportmodus auf VM-Ebene zu definieren (gilt nur für Sicherungen):

1. Melden Sie sich beim Sicherungs-Proxy-System für die virtuellen Rechner von Arcserve Unified Data Protection Agent für Windows an.
2. Öffnen Sie die Windows-Registrierung, und suchen Sie nach dem folgenden Registrierungsschlüssel:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\{VM-InstanceUUID}
3. Klicken Sie mit der rechten Maustaste auf "VM-InstanceUUID", und wählen Sie "Neu" aus.
4. Klicken Sie im Pop-up-Menü auf "Zeichenfolgenwert".
5. Benennen Sie den neuen Zeichenfolgenwert folgendermaßen.

   EnforceTransport
6. Klicken Sie mit der rechten Maustaste auf "EnforceTransport". Klicken Sie dann im Pop-up-Menü auf "Ändern", um das Dialogfeld "Zeichenfolge bearbeiten" zu öffnen.
7. Geben Sie im Feld "Wertdaten" den Transportmodus an, den Sie während des Sicherungsjobs verwenden möchten. Legen Sie einen der folgenden Werte fest:

   hotadd

   HOTADD-Transportmodus

   nbd

   NBD-Transportmodus

   nbdssl

   NBDSSL-Transportmodus

   san

SAN-Transportmodus

8. Klicken Sie auf "OK", um den Wert anzuwenden und das Dialogfeld "Zeichenfolge bearbeiten" zu schließen.

   Der Transportmodus ist definiert und wird das nächste Mal, wenn der Job ausgeführt wird, verwendet.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Wählen Sie einen der folgenden **Zieltypen** aus:

   Lokaler Datenträger oder freigegebener Ordner

   Gibt an, dass das Sicherungsziel ein lokales Ziel oder ein freigegebener Ordner ist. Wenn Sie diese Option auswählen, können Sie Daten als Wiederherstellungspunkte oder Wiederherstellungssätze speichern. Die Optionen für Wiederherstellungspunkte und Wiederherstellungssätze sind auf der Registerkarte **Ablaufplan** verfügbar.

   Arcserve UDP-Recovery Point Server

   Gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.

2. Wenn Sie **Arcserve UDP-Recovery Point Server** ausgewählt haben, geben Sie folgende Details an:

   a. Wählen Sie einen Recovery Point Server aus.

   b. Wählen Sie einen Datenspeicher aus. Die Liste enthält alle Datenspeicher, die am angegebenen Recovery Point Server erstellt wurden.

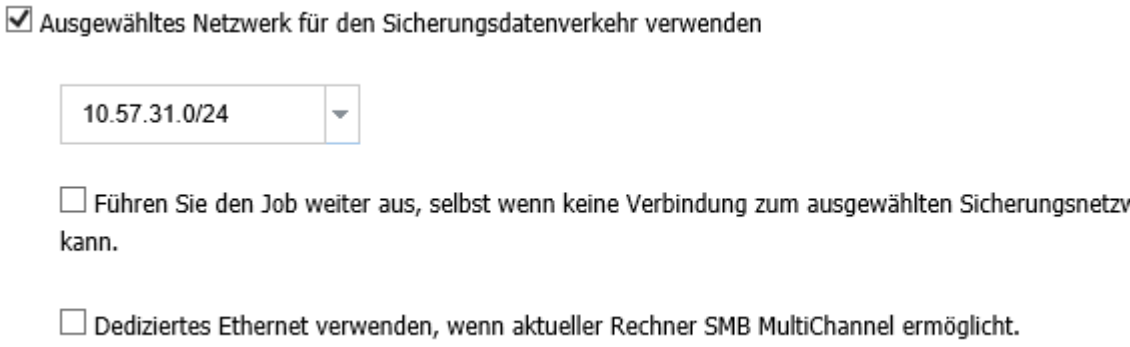
   c. Geben Sie ein Sitzungskennwort ein.

   Hinweis: Das Sitzungskennwort ist optional, wenn das Sicherungsziel ein unverschlüsselter RPS-Datenspeicher ist.

   d. Bestätigen Sie das Sitzungskennwort.

   e. (Optional) Aktivieren Sie das Kontrollkästchen **Ausgewähltes Netzwerk für Sicherungsdatenverkehr verwenden**, und führen Sie die folgenden Schritte aus:

      1. Um die Kommunikation zwischen dem Windows-Proxy- und dem Wiederherstellungspunktserver zu aktivieren, wählen Sie das CIDR-Netzwerk im Drop-down-Menü aus.



2. Wenn die Sicherungstask auch dann fortgesetzt werden soll, wenn das ausgewählte Netzwerk zwischen Proxyserver und Recovery Point Server nicht verfügbar ist, aktivieren Sie das Kontrollkästchen **Weiter ausführen, auch wenn keine Verbindung mit dem ausgewählten Sicherungsnetzwerk hergestellt werden kann**.
3. Um den SMB-Multichannel zu deaktivieren, sodass die Datenübertragung nur über das ausgewählte Netzwerk übertragen wird, aktivieren Sie das Kontrollkästchen **Dediziertes Ethernet verwenden, wenn der aktuelle Computer SMB Multichannel ermöglicht**.

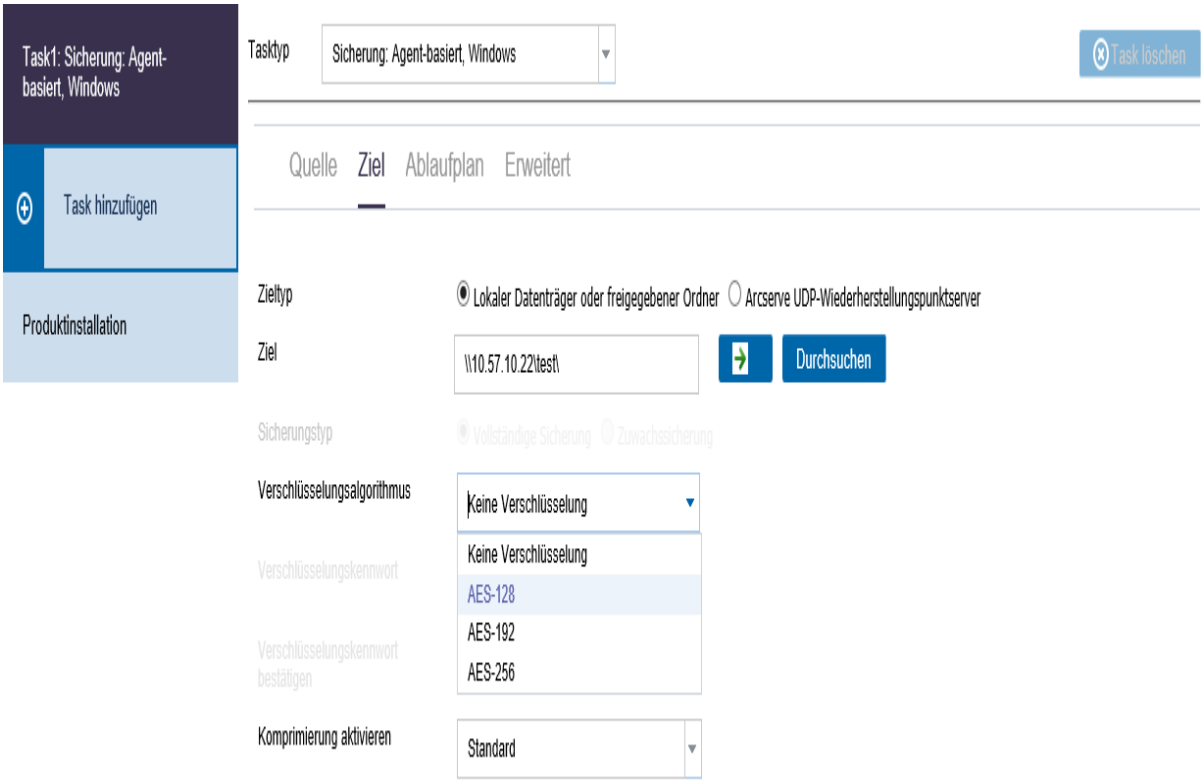
Hinweise:

- Diese Option ist nicht standardmäßig verfügbar. Um diese Option zu aktivieren, wechseln Sie zu dem folgenden Ordnerspeicherort: C:\Program Files\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. Ändern Sie dann den Wert für *useDedicatedEthernet* zu "True".

```
- <SpecifyNetwork>
      <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

  Die Funktion "Netzwerk angeben" wird im Falle eines Remotedatenspeichers deaktiviert, der den freigegebenen Netzwerkordner als Ziel verwendet hat.
- Die SMB-Multichannel-Funktion ist standardmäßig in Windows aktiviert.

3. Wenn Sie **Lokaler Datenträger oder freigegebener Ordner** ausgewählt haben, geben Sie folgende Details an:



   a. Geben Sie den vollständigen Pfad des lokalen Ziels oder Netzwerkziels an. Geben Sie für das Netzwerkziel Anmeldeinformationen für ein Konto mit Schreibzugriff an. Sie können auf "Durchsuchen" klicken, um das Ziel zu suchen oder auf das Pfeilsymbol, um die Verbindung zu testen und die Anmeldeinformationen für den Zielordner anzugeben.

   b. Wählen Sie aus der Liste der Dropdown-Optionen den Verschlüsselungsalgorithmus. Weitere Informationen finden Sie unter Verschlüsselungseinstellungen.

   c. Geben Sie optional ein Verschlüsselungskennwort an.

   d. Geben Sie Verschlüsselungskennwort zur Bestätigung erneut ein.

   e. Wählen Sie einen Komprimierungstyp aus. Weitere Informationen finden Sie unter "Komprimierungstyp".

Hinweis: Wenn Sie die Daten auf einem lokalen Datenträger oder in einem freigegebenen Ordner speichern, können Sie die Daten nicht auf einem anderen Reco-

very Point Server replizieren. Die Replikation wird nur unterstützt, wenn Sie die Daten auf einem Recovery Point Server speichern.

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein regulärer Ablaufplan, der basierend auf der Anzahl von Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

Gehen Sie wie folgt vor:

1. (Optional) Wählen Sie die Option für die Verwaltung von Wiederherstellungspunkten aus. Diese Option ist nur sichtbar, wenn Sie als Sicherungsziel "Lokaler oder freigegebener Ordner" ausgewählt haben.

   Nach Wiederherstellungspunkten aufbewahren

   Die Sicherungsdaten werden als Wiederherstellungspunkte gespeichert.

   Nach Wiederherstellungssätzen aufbewahren

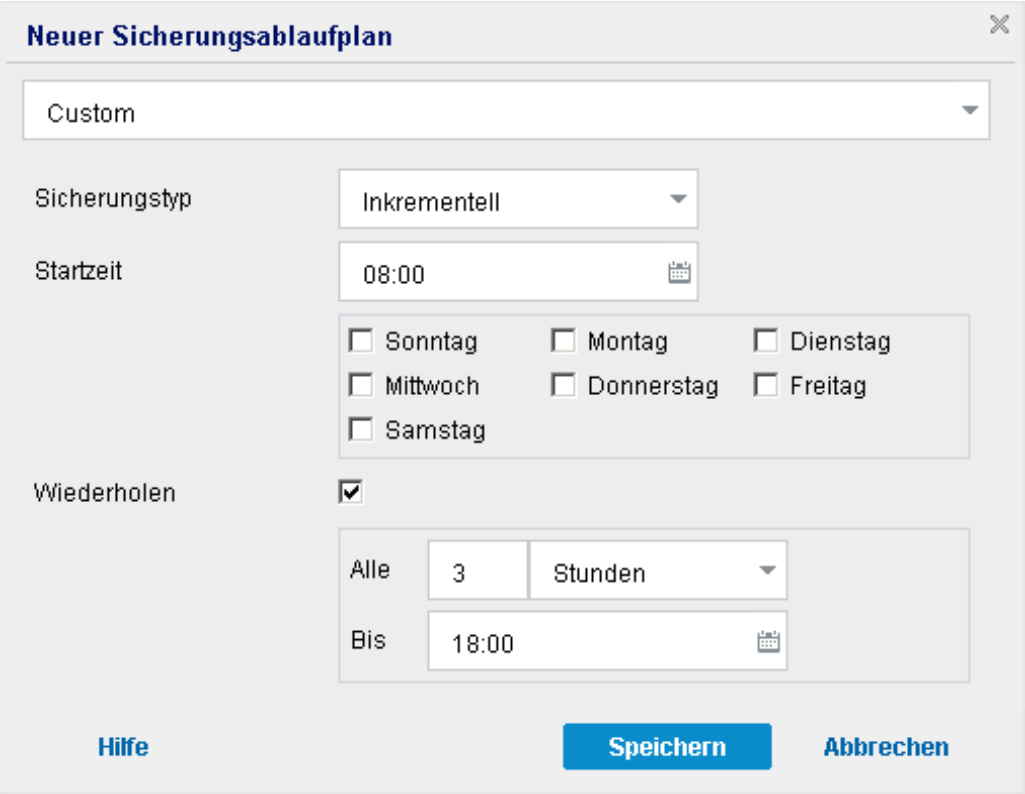
   Die Sicherungsdaten werden als Wiederherstellungssätze gespeichert.

2. Fügen Sie Ablaufpläne für Sicherungen, Zusammenführungen und Drosselungsvorgänge hinzu.

   Hinzufügen eines Sicherungsablaufplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke

des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Überprüfen

Legt den Ablaufplan für Überprüfungssicherungen fest.

Als Teil eines Ablaufplans wird Arcserve UDP die Gültigkeit und Vollständigkeit der geschützten Daten durch einen Vergleich des gespeicherten Sicherungs-Images mit der ursprünglichen Sicherungsquelle überprüfen. Im Bedarfsfall wird das Image neu synchronisiert. Bei einer Überprüfungssicherung wird die letzte Sicherung jedes einzelnen Blocks mit den Inhalten und Informationen der Quelle verglichen. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht (zumeist aufgrund von Änderungen seit der letzten Sicherung), aktualisiert Arcserve UDP die Sicherung dieses Blocks (Neusynchronisierung). In sehr seltenen Fällen kann eine Überprüfungssicherung auch durchgeführt werden, um eine vollständige Sicherung zu erhalten, ohne den erforderlichen Speicherplatz einer vollständigen Sicherung zu verwenden.

Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteile: Die Sicherung benötigt viel Zeit, da alle Quellenblöcke mit den Blöcken der letzten Sicherung verglichen werden.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die seit der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Es ist die optimale Methode zur Durchführung von Sicherungen, die standardmäßig verwendet werden sollte.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zusammenführungsplan hinzufügen** aus.

b. Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

c. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Zusammenführungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Drosselungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

b. Das Dialogfeld Drosselungsplan hinzufügen wird geöffnet.

c. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

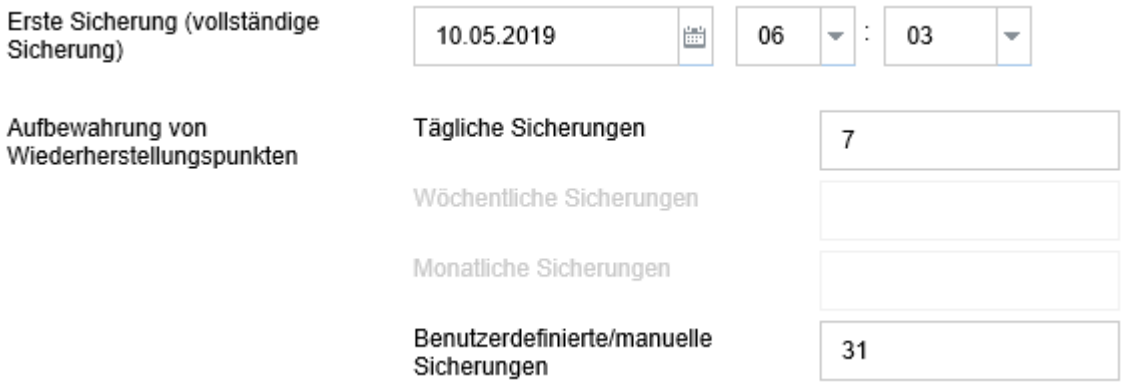
d. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

e. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

f. Klicken Sie auf **Speichern**.

Die Drosselung ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

3. Geben Sie die Startzeit für die geplante Sicherung an.



4. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld "Sicherungsablaufplan" übernommen.

5. Geben Sie die Katalogdetails an.

   Mit Katalogen können Sie den Dateisystemkatalog generieren. Der Dateisystemkatalog ist erforderlich, um schnellere und einfachere Suchvorgänge auszuführen. Die Kataloge werden je nach der Art der Sicherung, die Sie angegeben haben, aktiviert.

   Der Ablaufplan ist nun angegeben.

Funktionsweise der erweiterten Planung und Aufbewahrung

Mit der Ablaufplanoption können Sie einen benutzerdefinierten Ablaufplan, einen Ablaufplan für tägliche/wöchentliche/monatliche Sicherungen oder beides festlegen. Im benutzerdefinierten Ablaufplan können Sie den Sicherungsablaufplan für jeden Tag der Woche konfigurieren und bis zu vier Sicherungsablaufpläne für jeden Tag hinzufügen. Sie können einen bestimmten Wochentag auswählen und ein Zeitfenster erstellen, um anzugeben, wann und wie oft die Sicherung durchgeführt werden soll.

Ablaufplan	Unterstützter Job	Kommentare
Sichern	Sicherungsjob	Gibt Zeitfenster für die Ausführung von Sicherungsjobs an.
Sicherungsdrosselung	Sicherungsjob	Gibt die Zeitfenster an, um die Sicherungsgeschwindigkeit zu steuern.
Zusammenführen	Zusammenführungsjob	Gibt an, wann Zusammenführungsjobs ausgeführt werden sollen.
Täglicher Ablaufplan	Sicherungsjob	Gibt an, wann tägliche Sicherungsjobs ausgeführt werden sollen.
Wöchentlicher Ablaufplan	Sicherungsjob	Gibt an, wann wöchentliche Sicherungsjobs ausgeführt werden sollen.
Monatlicher Ablaufplan	Sicherungsjob	Gibt an, wann monatliche Sicherungsjobs ausgeführt werden sollen.

Sie können auch die Aufbewahrungseinstellungen für die Wiederherstellungspunkte angeben.

Hinweis: Legen Sie innerhalb der einzelnen Pläne Einstellungen für die Aufbewahrungszeit fest, um zu steuern, wie die Daten für die Knoten des entsprechenden Plans im Zieldatenspeicher aufbewahrt werden.

Ablaufpläne für tägliche/wöchentliche/monatliche Sicherungen sind vom benutzerdefinierten Ablaufplan und voneinander unabhängig. Sie können die Ausführung einer täglichen, wöchentlichen oder monatlichen Sicherung konfigurieren, ohne einen benutzerdefinierten Ablaufplan zu konfigurieren.

Jobplan der Sicherung

Sie können vier Zeitfenster pro Tag in Ihrem Sicherungsablaufplan hinzufügen. Ein gültiges Zeitfenster liegt im Bereich 12:00 Uhr bis 23:59 Uhr. Sie können kein Zeitfenster wie z. B. 18:00 Uhr bis 06:00 Uhr angeben. In solchen Fällen müssen Sie manuell zwei verschiedene Zeitfenster angeben.

Für jedes Zeitfenster wird die Startzeit einbezogen, und die Endzeit wird nicht einbezogen. Zum Beispiel haben Sie das Ausführen einer Zuwachssicherung konfiguriert, die stündlich zwischen 06:00 Uhr und 09:00 Uhr stattfinden soll, und die Sicherung wird um 06:00 Uhr gestartet. Das bedeutet, dass die Sicherung um 06:00 Uhr, 07:00 Uhr und 08:00 Uhr ausgeführt wird, NICHT aber um 09:00 Uhr.

Hinweis: Wenn Sie die Sicherung bis zum Ende des Tages wiederholt ausführen möchten, legen Sie den Ablaufplan bis 12:00 Uhr fest. Um den Sicherungsjob beispielsweise alle 15 Minuten während des gesamten Tages auszuführen, legen Sie den Ablaufplan von 00:00 Uhr bis 00:00 Uhr alle 15 Minuten fest.

Drosselungsplan der Sicherung

Mit dem Drosselungsplan der Sicherung können Sie die Geschwindigkeit des Sicherungsdurchsatzes steuern, die wiederum die Ressourcenverwendung (Datenträger-E/A, CPU, Netzwerkbandbreite) des Servers, der gesichert wird, steuert. Dies ist hilfreich, wenn die Serverleistung während der Geschäftszeiten nicht beeinträchtigt werden soll. Sie können vier Zeitfenster pro Tag in Ihrem Drosselungsplan der Sicherung hinzufügen. Für jedes Zeitfenster können Sie einen Wert in MB pro Minute angeben. Dieser Wert wird verwendet, um den Sicherungsdurchsatz zu steuern. Gültige Werte liegen im Bereich zwischen 1 MB/Minute bis 99.999 MB/Minute.

Wenn ein Sicherungsjob die angegebene Zeit überschreitet, dann wird das Drosselungslimit entsprechend dem angegebenen Zeitfenster angepasst. Zum Beispiel haben Sie als Drosselungslimit der Sicherung den Wert 500 MB/Minute von 08:00 Uhr bis 20:00 Uhr und 2500 MB/Minute von 20:00 Uhr bis 22:00 Uhr angegeben. Wenn ein Sicherungsjob um 19:00 Uhr startet und drei Stunden ausgeführt wird, dann hat das Drosselungslimit von 19:00 Uhr bis 20:00 Uhr den Wert 500 MB/Minute. Von 20:00 Uhr bis 22:00 Uhr hat das Drosselungslimit den Wert 2.500 MB/Minute.

Wenn Sie keinen Sicherungsablaufplan und keinen Ablaufplan für den Sicherungsdurchsatz angeben, dann wird die Sicherung so schnell wie möglich ausgeführt.

Ablaufplan für Zusammenführung

Ermöglicht es Ihnen, Wiederherstellungspunkte basierend auf dem angegebenen Ablaufplan zusammenzuführen.

Beachten Sie folgende Punkte für den Zusammenführungsjob:

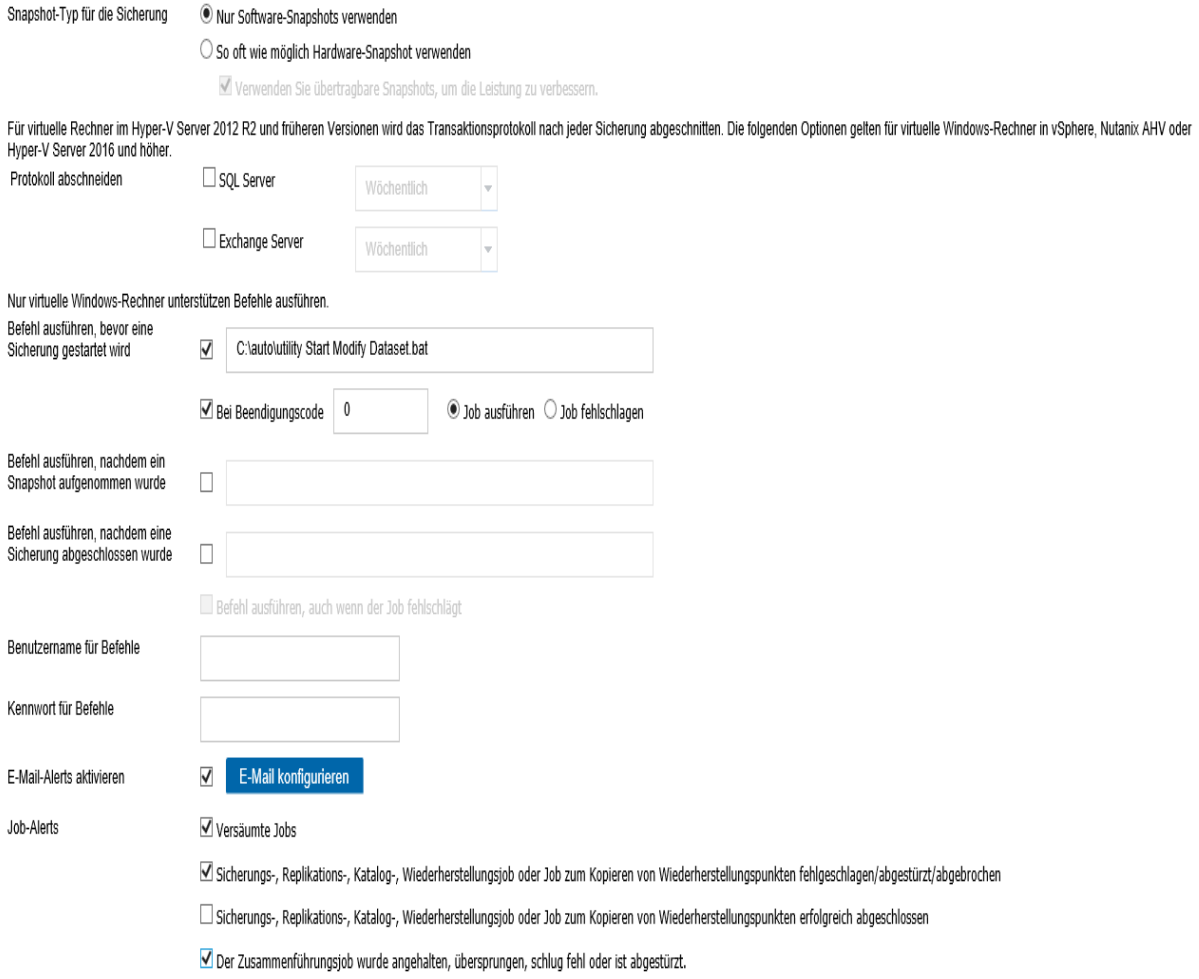
- Es kann immer nur ein Zusammenführungsjob für einen Knoten ausgeführt werden.

- Wenn ein Zusammenführungsjob gestartet wird, muss er abgeschlossen werden, bevor der nächste Zusammenführungsjob gestartet werden kann. Das bedeutet: Wenn ein oder mehrere Sätze an Wiederherstellungspunkten zusammengeführt werden, dann kann der neue Wiederherstellungspunkt nicht zu diesem Zusammenführungsprozess hinzugefügt werden, bis der Zusammenführungsprozess für den aktuellen Satz an Wiederherstellungspunkten abgeschlossen ist.
- Wenn ein Zusammenführungsjob mehr als einen Satz an Wiederherstellungspunkten bearbeitet (zum Beispiel Satz [1~4], Satz [5~11] und Satz [12~14], also drei Sätze), dann werden diese Sätze nacheinander vom Recovery Point Server bearbeitet.
- Wenn ein Zusammenführungsjob nach einer Pause fortgesetzt wird, erkennt der Job an welchem Punkt er unterbrochen wurde, und die Zusammenführung wird ab der Abbruchstelle fortgesetzt.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen den Snapshot-Typ für die Sicherung, die Einstellungen für die Protokollkürzung sowie die Angabe des Speicherorts für sämtliche Skripte und E-Mail-Einstellungen. Überprüfen Sie die Voraussetzungen, bevor Sie den Hardware-Snapshot-Typ auswählen.

Die folgende Abbildung zeigt die Registerkarte "Erweitert":



Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

   Art des Snapshots für die Sicherung

   Wählen Sie eine der folgenden Optionen für den Sicherungs-Snapshot aus.

   Nur Software-Snapshot verwenden

Gibt an, dass der Sicherungstyp nur den Software-Snapshot verwendet. Der Hardware-Snapshot wird von UDP nicht überprüft. Der Software-Snapshot nutzt weniger Ressourcen auf den virtuellen Rechnern. Diese Option eignet sich für Server mit niedrigeren Konfigurationen und Verarbeitungsgeschwindigkeiten.

So oft wie möglich Hardware-Snapshot verwenden

Gibt an, dass beim Sicherungstyp erst auf einen Hardware-Snapshot geprüft wird. Wenn alle Kriterien erfüllt sind, verwendet der Sicherungstyp den Hardware-Snapshot.

Hinweis: Weitere Informationen zu den Hardware-Snapshot-Kriterien finden Sie in den Voraussetzungen.

Für Hyper-V verwendet Arcserve UDP den Hardwareanbieter zum Erstellen eines VSS-Snapshots der Volumes auf dem Hyper-V-Host und zum Importieren des Hardware-Snapshots auf dem Proxy-Server. Auf dem Proxy-Server muss ein geeigneter Hardwareanbieter installiert sein. Für VMware erstellt Arcserve UDP für einen kurzen Zeitraum einen vSphere-Software-Snapshot und dann einen Hardware-Snapshot. Dieser Hardware-Snapshot wird auf den VMware ESX-Server geladen, und der Software-Snapshot wird gelöscht. Arcserve UDP verwendet dann den Inhalt im Hardware-Snapshot für die Sicherung der zur VM gehörigen Dateien.

Leistung mithilfe von übertragbaren Snapshots verbessern

Gibt an, dass für den Hardware-Snapshot ein übertragbarer Snapshot verwendet wird. Durch einen übertragbaren Snapshot wird der Sicherungsdurchsatz erhöht. Diese Option ist nur auf Hyper-V-Server anwendbar.

Protokoll abschneiden

Ermöglicht es Ihnen, den Ablaufplan anzugeben, um Protokolle für SQL Server und Exchange Server zu kürzen. Sie können den Ablaufplan als **Täglich**, **Wöchentlich** oder **Monatlich** angeben. Dies gilt nur für VMware.

Befehl ausführen, bevor eine Sicherung gestartet wird

Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, unter dem das Skript innerhalb des Gast-BS des virtuellen Rechners gespeichert ist. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt. Dies gilt nur für Windows-VMs.

Hinweise: (gilt auch für die Befehle "Nach Erstellen eines Snapshots" und "Nach Abschluss der Sicherung")

- Es wird empfohlen, den vollständigen Pfad des Befehls/Skripts anzugeben. Verwenden Sie zum Beispiel "C:\Windows\System32\Ping.exe" statt nur "Ping.exe".
- Um zu vermeiden, dass der Sicherungsjob hängen bleibt, weil der Befehl/das Skript hängt, wird der Befehl/das Skript standardmäßig beendet, wenn er/es innerhalb von 3 Minuten nicht beendet werden kann. Wenn Sie die Standardeinstellung für das Zeitlimit ändern möchten, führen Sie folgende Schritte auf Proxy-Server- oder VM-Ebene durch:

  Auf Proxy-Server-Ebene (gilt für alle Sicherungsjobs, die auf diesem Proxy-Server ausgeführt werden)

  a. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

     [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

  b. Fügen Sie einen DWORD-Wert mit dem Namen "PrePostCMDTimeoutInMinute" hinzu, und geben Sie den Wert mit dem Zeitlimit in Minuten an.

  Auf VM-Ebene

  a. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

     [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

  b. Fügen Sie einen DWORD-Wert mit dem Namen "PrePostCMDTimeoutInMinute" hinzu, und geben Sie den Wert mit dem Zeitlimit in Minuten an.

     Hinweis: Wenn Sie den Registrierungswert sowohl im VM als auch in der Registrierung auf Proxy-Ebene hinzufügen, hat die Einstellung in der Registrierung auf VM-Ebene Priorität über die Einstellung in der Registrierung auf Proxy-Ebene.

Befehl ausführen, nachdem ein Snapshot aufgenommen wurde

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungs-Snapshot aufgenommen wurde. Geben Sie den Pfad an, unter dem das Skript innerhalb des Gast-BS des virtuellen Rechners gespeichert ist. Dies gilt nur für Windows-VMs.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den Pfad an, unter dem das Skript innerhalb des Gast-BS des virtuellen Rechners gespeichert ist. Dies gilt nur für Windows-VMs.

Befehl ausführen, auch wenn der Job fehlschlägt

Wenn dieses Kontrollkästchen aktiviert ist, wird das unter "Befehl ausführen, nachdem eine Sicherung abgeschlossen ist" angegebene Skript ausgeführt, selbst wenn der Sicherungsjob fehlschlägt. Andernfalls wird das Skript nur dann ausgeführt, wenn der Sicherungsjob erfolgreich abgeschlossen wurde.

Benutzername für Befehle

Ermöglicht die Angabe des Benutzernamens zum Ausführen der Befehle.

Kennwort für Befehle

Ermöglicht die Angabe des Kennworts zum Ausführen der Befehle.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Typen der Warnmeldungen angeben, die Sie in einer E-Mail erhalten möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers.

Job-Alerts

Ermöglicht es Ihnen, die Arten von Job-Alerts auszuwählen, die Sie per E-Mail empfangen möchten.

2. Klicken Sie auf **Speichern**.

Die Aktualisierungen werden gespeichert und es wird ein grünes Häkchen neben dem Tasknamen angezeigt. Die Planungsseite wird geschlossen.

Hinweis:

- Wenn Sie einen anderen Task hinzufügen, wählen Sie den Plan aus der Registerkarte Ressourcen und ändern Sie den Plan. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern.
- Wenn Sie einen Knoten auswählen, auf dem kein Arcserve UDP-Agent als Backup-Proxy installiert ist, stellt die UDP-Konsole automatisch einen Agenten diesem Knoten bereit, nachdem der Plan gespeichert wurde.

Der hostbasierte agentenlose Sicherungsplan für den virtuellen Rechner wurde erstellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

Ausführen von Skripten oder Befehlen und Protokollkürzung mit einem zusätzlichen Administratorkonto

Zusätzliche Administratorkonten sind jene Konten, bei denen es sich nicht um Standardadministratoren handelt. Die folgenden beiden Konten sind betroffen, wenn Sie Befehle oder Skripten ausführen:

1. Bei "Knoten aktualisieren" festgelegtes Konto
2. Auf der Registerkarte "Erweitert" eines Plans festgelegtes Konto

Für virtuelle VMware- bzw. Hyper-V-Rechner gelten jeweils eigene Bedingungen für die Verwendung der zusätzlichen Administratorkonten.

Virtuelle VMware-Rechner

Wenn beide Konten festgelegt sind, verwenden Sie das erste Konto, um sich beim virtuellen Rechner anzumelden. (Das vSphere-SDK wird zur Kommunikation mit dem virtuellen Rechner verwendet, so dass der Netzwerkzugriff zwischen dem Proxy-Server und dem virtuellen Rechner nicht erforderlich ist.) Verwenden Sie anschließend das zweite Konto, um den Befehl oder das Skript im virtuellen Rechner auszuführen.

Wenn eines der beiden Konten nicht festgelegt ist, verwenden Sie für die Anmeldung beim virtuellen Rechner das verfügbare Konto, und führen Sie den Befehl oder das Skript aus.

Es wird empfohlen, für beide Konten das integrierte Administratorkonto oder das integrierte Domänenadministratorkonto zu verwenden.

Wenn Sie ein zusätzliches (nicht integriertes) Administratorkonto verwenden, ist der Vorgang anders.

Gehen Sie wie folgt vor:

1. Um sich mit dem hinzugefügten Administratorkonto anzumelden, befolgen Sie den Schritt im Thema Aktualisieren von Knoten, um sicherzustellen, dass das Konto über die erforderlichen Berechtigungen verfügt.
2. Um den Befehl oder das Skript mithilfe des zusätzlichen Administratorkontos auszuführen, stellen Sie sicher, dass das Konto über die erforderliche Berechtigung verfügt. Melden Sie sich mit dem zusätzlichen Administratorkonto beim virtuellen Gastrechner an, führen Sie den Befehl oder das Skript aus, und bestätigen Sie, dass der Befehl oder Skript erfolgreich abgeschlossen werden kann.

Virtuelle Hyper-V-Rechner

Für virtuelle Hyper-V-Rechner benötigen Sie nur ein Konto. Wenn beide Konten festgelegt sind, verwenden Sie das zweite (auf der Registerkarte "Erweitert" eines Plans festgelegte) Konto, um eine Verbindung mit dem virtuellen Rechner herzustellen und den Befehl oder das Skript zu starten. Die Windows-Verwaltungsinstrumentation (WMI) wird zur Kommunikation mit dem virtuellen Rechner verwendet, sodass zwischen dem Proxy-Server und dem virtuellen Rechner Netzwerkzugriff erforderlich ist.

Wenn eines der beiden Konten nicht festgelegt ist, verwenden Sie für die Anmeldung beim virtuellen Rechner das verfügbare Administratorkonto, und starten Sie den Befehl oder das Skript.

Gehen Sie wie folgt vor:

1. Greifen Sie mit Remote-WMI auf den virtuellen Rechner zu. Stellen Sie sicher, dass Sie für das zusätzliche Administratorkonto über die erforderlichen Berechtigungen verfügen. Die Voraussetzungen für das Konto sind im Thema Aktualisieren von Knoten beschrieben.
2. Um den Befehl oder das Skript mithilfe des zusätzlichen Administratorkontos auszuführen, stellen Sie sicher, dass das Konto über die erforderliche Berechtigung verfügt. Melden Sie sich mit dem zusätzlichen Administratorkonto beim virtuellen Gastrechner an, führen Sie den Befehl oder das Skript aus, und bestätigen Sie, dass der Befehl oder Skript erfolgreich abgeschlossen werden kann.

Überprüfen Sie auch, ob WMI von der Firewall der Gast-VM zugelassen wird. Wenn dies nicht aktiviert ist, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei der Gast-VM an.
2. Öffnen Sie die Systemsteuerung.
3. Öffnen Sie die Windows-Firewall.
4. Klicken Sie auf "Eine App oder ein Feature durch die Windows-Firewall zulassen".
5. Aktivieren Sie die Windows-Verwaltungsinstrumentation (WMI).
6. Klicken Sie auf "OK".

Definieren einer Beschränkung der Anzahl von gleichzeitigen Sicherungen

Sie können eine Beschränkung der Anzahl an Sicherungsjobs definieren, die gleichzeitig ausgeführt werden können. Diese Funktion ermöglicht es Ihnen, die Leistung des hostbasierten VM-Sicherungs-Proxy-Servers in Ihrer Sicherungsumgebung zu optimieren. Standardmäßig kann Host-Based VM Backup bis zu vier VMware-VM-Sicherungsjobs, zehn Hyper-V-VM-Sicherungsjobs und vier Nutanix AHV-VM-Sicherungsjobs gleichzeitig ausführen. Bei Umgebungen mit vielen virtuellen Rechnern, die einem Proxy-Server zugeordnet sind, kann sich eine große Anzahl von gleichzeitigen Sicherungen negativ auf Netzwerk- und Sicherungsleistung auswirken.

Hinweis: Wenn die Anzahl an gleichzeitigen Jobs die angegebene Grenze überschreitet, gelangen die Jobs, die die Grenze überschreiten, in die Jobwarteschlange.

Hinweis: Wenn die Höchstanzahl an gleichzeitigen VMware-Sicherungsjobs das ESX-Server-Verbindungslimit überschreitet, dann können Kommunikationsfehler zwischen dem ESX-Server und dem Sicherungs-Proxy auftreten, und das Dateisystem des ESX-Server-Datenspeichers kann gesperrt bleiben. Starten Sie in solchen Fällen den ESX-Server neu, oder migrieren Sie den gesperrten virtuellen Rechner in einen anderen Datenspeicher, um die VM zu entsperren. Weitere Details finden Sie im entsprechenden VMware-Dokument (VMware-KB:1022543).

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Proxy-System des virtuellen Arcserve UDP-Rechners an.
2. Öffnen Sie die Windows-Registrierung, und suchen Sie nach dem folgenden Registrierungsschlüssel:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
   ```

3. Suchen Sie folgende Schlüssel:

   ```
   VMwareMaxJobNum
   HyperVMaxJobNum
   AHVMaxJobNum
   ```

   Hinweis: Beide Schlüssel sind bereits angelegt und der Standardwert ist 4 bzw. 10.

4. Klicken Sie mit der rechten Maustaste auf VMMaxJobNum, HyperVMaxJobNum oder AHVMaxJobNum, und klicken Sie dann im Pop-up-Menü auf "Ändern".

   Das Dialogfeld "Zeichenfolge bearbeiten" wird geöffnet.

5. Geben Sie im Feld "Wertdaten" die Anzahl an Sicherungsjobs an, die gleichzeitig ausgeführt werden dürfen.

- **Untergrenze:** 1
- **Maximale Anzahl--**Keine
- **Standard**--10 für Hyper-V und 4 für VMware und Nutanix AHV

6. Klicken Sie auf OK.

   Das Limit ist jetzt definiert.

   Das Limit an gleichzeitigen Sicherungsjobs ist definiert.

(Optional) Ausführen einer manuellen Sicherung

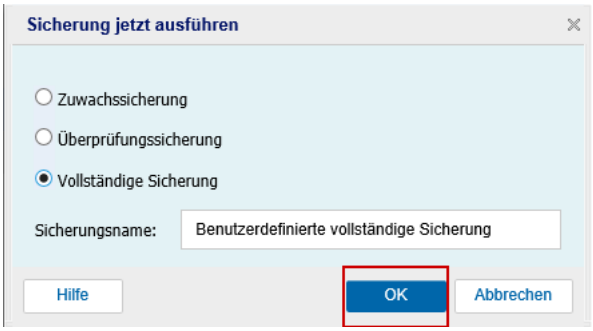
Normalerweise werden Ihre Sicherungen automatisch durchgeführt und von den Ablaufplan-Einstellungen gesteuert. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern. Wenn Sie z. B. einen Wiederholungsplan für vollständige Sicherungen, Zuwachssicherungen und Überprüfungssicherungen festgelegt haben und größere Veränderungen an Ihrem Rechner vornehmen möchten, müssen Sie sofort eine manuelle Sicherung durchführen, ohne auf die nächste geplante Sicherung zu warten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Navigieren Sie zu **Ressourcen** > **Plan** > **Alle Pläne**.

   Die Liste aller Pläne wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Plan, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
4. Wählen Sie im Dialogfeld "Sicherung jetzt ausführen" den gewünschten Sicherungstyp aus, und geben Sie dann gegebenenfalls den Sicherungsnamen an.



Es sind folgende Optionen verfügbar:

Zuwachssicherung

Startet eine Zuwachssicherung Ihres Rechners. Eine Zuwachssicherung sichert nur jene Blöcke, die seit der vorherigen Sicherung geändert wurden.

Hinweis: Wenn Sie eine Sicherung zum ersten Mal ausführen, wird automatisch die vollständige Sicherung initiiert, auch wenn Sie die Option "Zuwachssicherung" ausgewählt haben.

Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

Überprüfungssicherung

Startet eine Überprüfungssicherung Ihres Rechners, indem die aktuellste Sicherung von jedem einzelnen Block überprüft und der Inhalt und die Informationen mit der ursprünglichen Quelle verglichen wird. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht, aktualisiert Arcserve UDP Agent (Windows) die Sicherung dieses Blocks (Neusynchronisierung).

Vorteil: Im Vergleich zu einer vollständigen Sicherung wird nur ein sehr kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteil: Die Sicherung benötigt viel Zeit, da alle Blöcke des Quelldatenträgers mit den Blöcken der letzten Sicherung verglichen werden.

Vollständige Sicherung

Startet eine vollständige Sicherung Ihres gesamten Rechners oder der ausgewählten Volumes.

Hinweise:

- Wenn Sie der Sicherungsquelle ein neues Volume hinzufügen, wird das neue Volume vollständig gesichert, unabhängig davon, welche allgemeine Sicherungsmethode ausgewählt wurde.
- Wenn Sie keinen Sicherungsnamen angeben, wird automatisch der Name "Benutzerdefinierte vollständige Sicherung/Zuwachssicherung/Überprüfungssicherung" vergeben.

5. Klicken Sie auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.

6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.

7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Hinweis: Nur ein Job kann gleichzeitig ausgeführt werden. Wenn Sie versuchen, einen Sicherungsjob manuell zu starten, während gerade ein anderer Job ausgeführt wird, werden Sie in einer Warnmeldung darüber informiert, dass ein anderer Job ausgeführt wird, und aufgefordert, es später erneut zu versuchen.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Hinweis: Sie können auch eine manuelle Sicherung auslösen. Klicken Sie mit der rechten Maustaste auf einen Plan, und wählen Sie in den Optionen **Jetzt sichern** aus. Wenn der Plan für die Sicherung von vSphere-Containerobjekten konfiguriert ist, veranlasst UDP die Sicherung aller VMs, die unter diesem Container verfügbar sind.

Überprüfen des Plans

Um Ihre Sicherung zu überprüfen, bestätigen Sie, dass Sie den Sicherungsplan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Sie können den Status von Sicherungsjobs auf der Registerkarte Jobs überprüfen.

Gehen Sie wie folgt vor: Zum Überprüfen von Plänen

1. Klicken Sie auf die Registerkarte "Ressourcen".
2. Navigieren Sie im linken Fensterbereich zu Knoten, und klicken Sie auf Alle Knoten.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Gehen Sie wie folgt vor: Zum Überprüfen von Sicherungsjobs

1. Klicken Sie auf die Registerkarte Jobs.
2. Klicken Sie im linken Fensterbereich auf "Alle Jobs".

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Erstellen eines Plans für ein Virtual Standby in AWS EC2

Virtual Standby konvertiert die Wiederherstellungspunkte in Formate für virtuelle Rechner auf der festgelegten Cloud und bereitet einen Snapshot vor, damit Ihre Daten bei Bedarf auf einfache Weise wiederhergestellt werden können. Diese Funktion deckt auch die Hochverfügbarkeitsfunktion ab und stellt sicher, dass der virtuelle Rechner sofort übernehmen kann, wenn der Quellrechner ausfällt. Der Virtual Standby-Rechner wird erstellt, indem Wiederherstellungspunkte in das Amazon AWS EC2-Format für virtuelle Rechner konvertiert werden.

Hinweis: Der Virtual Standby-Task wird nur ausgeführt, wenn der Sicherungstask einen gültigen Snapshot des Wiederherstellungspunkts erstellt. Wenn der Sicherungstask fehlschlägt, dann wird der Virtual Standby-Task übersprungen.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen eines Plans mit einem Sicherungstask
3. Hinzufügen eines "Virtual Standby auf EC2-Tasks" zum Plan
4. (Optional) Manuelles Ausführen eines "Virtual Standby auf EC2"-Tasks
5. Unterbrechen und Wiederaufnehmen des Virtual Standby-Jobs
6. Überprüfen des Plans
7. Beenden von EC2-Ressourcen

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich bei der Konsole an.
- Wenn Sie die Sicherungsdaten auf Recovery Point Servern speichern möchten, installieren Sie die Serverkomponente, und erstellen Sie Datenspeicher.
- Sie haben einen gültigen Wiederherstellungspunkt, um einen Virtual Standby-Rechner zu erstellen. Die Wiederherstellungspunkte können aus folgenden Tasks stammen:
  - Sicherung: agentenbasiert, Windows
  - Sicherung: hostbasiert, agentenlos
  - Replizieren
  - Replizieren von einem Remote-Recovery Point Server
- Sichern des gesamten Rechners, um Virtual Standby-Task zu aktivieren. Sie können einen Virtual Standby-Task nicht erstellen, wenn es sich bei der Sicherung nicht um eine vollständige Sicherung handelt.
- Installieren Sie das Systemvolume auf dem ersten Datenträger. Stellen Sie sicher, dass sich das Systemvolume und das Startvolume des Quellrechners auf demselben Datenträger befinden.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.
- Konfigurieren Sie die Sicherheitsgruppeneinstellung auf EC2, um die zugehörigen Ports für den eingehenden Zugriff, einschließlich TCP 8014 und TCP 4091, zu öffnen.
- Überprüfen Sie, ob das Amazon AWS-Konto auf AWS S3 und AWS EC2 zugreifen kann. Arcserve UDP stellt das Konto nicht bereit.
- Sie müssen das Systemvolume auf dem ersten Datenträger installieren. Stellen Sie sicher, dass sich das Systemvolume und das Startvolume des Quellrechners auf demselben Datenträger befinden.
- Für Amazon IAM-Benutzer sind spezielle AWS-API Berechtigungen erforderlich, um Steuerung und Interaktion mit AWS-APIs für VSB auf EC2 zu ermöglichen. Weitere Informationen finden Sie unter So konfigurieren Sie spezifische IAM-Berechtigungen für IAM-Benutzer mit VSB auf EC2.

Besondere Aspekte:

- Virtual Standby zu EC2-Task unterstützt aufgrund einer Amazon AWS EC2-Einschränkung NICHT das Starten des Quellrechners von UEFI-Firmware.
- Auf dem Quellrechner wird .NET Framework 4.5 benötigt, um den Amazon-PV-Treiber für den Virtual Standby zu EC2-Task zu installieren.
- Aufgrund einer AWS-Einschränkung müssen sich das Systemvolume und das Startvolume des Quellknoten im VSB-auf-EC2-Plan auf dem ersten Datenträger befinden.
- Aufgrund eines AWS-Einschränkung kann die Konfiguration der TCP/IP-Einstellung auf der EC2-Instanz nicht auf die erste Netzwerkschnittstelle angewendet werden.
- Die Zuweisung einer elastischen IP-Adresse ist nur für die erste Netzwerkschnittstelle auf der EC2-Instanz verfügbar.
- Die Konfiguration der TCP/IP-Einstellung gilt nur für Szenarien, in denen Direktzugriff oder VPN zwischen dem primären Standort und dem AWS-Netzwerk konfiguriert ist. Andernfalls führt die Anpassung dazu, dass die EC2-Instanz nicht mehr zugänglich ist.
- Sie können die Aktivierung/Deaktivierung der automatischen Zuweisung öffentlicher IP-Adressen für die im Plan vorhandenen Knoten nicht ändern und Aktualisierungen betreffen nur neue Knoten, die zum Plan hinzugefügt werden.
- Sie müssen die PowerShell-Version 3.0 oder höher auf dem Quellrechner installieren, bevor Sie den VSB auf EC2 für die folgenden Instanztypen konfigurieren:

  C5, C5d, C5n, F1, G3, G4, H1, I3, I3en, Inf1, m4.16xlarge, M5, M5a, M5ad, M5d, M5dn, M5n, P2, P3, R4, R5, R5a, R5ad, R5d, R5dn, R5n, T3, T3a, X1, X1e und z1d

Konfigurieren von detaillierteren IAM-Berechtigungen für IAM-Benutzer mit VSB auf EC2

In diesem Abschnitt werden die Schritte und die API-Berechtigungsrichtlinie erläutert, die für den auf dem VSB-Cloud-proxy innerhalb von Amazon EC2 Web Services installierten Arcserve UDP-Agenten erforderlich sind. Die Berechtigungen ermöglichen das Ausführen der nötigen Aktionen zur Übertragung von Daten zu AWS EC2 Cloud und für das Virtual auf die AWS EC2 Cloud.

Mit der Vorgehensweise können Sie einem Amazon IAM-Benutzer helfen, mit der AWS-API zu interagieren und die Kontrolle zu erlangen. Die Berechtigungsrichtlinie wird nicht nur für den Benutzer direkt angewendet, sondern auch für eine Rolle und Gruppe innerhalb der IAM-Sicherheitsschnittstelle in Amazon Web Services.

Gehen Sie wie folgt vor:

1. Melden Sie sich als Administrator bei Amazon Web Services an.
2. Wählen Sie "Meine Anmeldeinformationen" aus, klicken Sie links auf **Benutzer** und klicken Sie dann auf die Schaltfläche **Neue Benutzer erstellen**.
3. Geben Sie den gewünschten Benutzernamen ein.

   Hinweis: Überprüfen Sie, ob die Option **Für jeden Benutzer einen Zugriffsschlüssel generieren** aktiviert ist.
4. Klicken Sie auf die Schaltfläche **Erstellen**.
5. Klicken Sie auf **Anmeldeinformationen herunterladen**.

   Die Anmeldeinformationen enthalten Ihren Zugriffsschlüssel und Ihr Geheimnis, die Sie später in der UDP-Konsole benötigen.
6. Wählen Sie in der Ansicht "Benutzer" den Benutzer aus der Liste der Benutzer aus, und klicken Sie dann auf die Registerkarte "Berechtigungen", die im unteren Bereich verfügbar ist.
7. Erstellen Sie über die Option "Benutzerdefinierte Richtlinie" eine benutzerdefinierte Inline-Richtlinie für den Benutzer.
8. Geben Sie einen Namen für die Richtlinie ein, und fügen Sie den folgenden Inhalt in das Richtliniendokument ein.

   {

   "Version": "2012-10-17",

   "Statement": [

   {

"Sid": "Stmt1477881304097",
"Aktion": [
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:AttachNetworkInterface",
"ec2:AttachVolume",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:CreateSnapshot",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteVolume",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeBundleTasks",
"ec2:DescribeClassicLinkInstances",
"ec2:DescribeConversionTasks",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeExportTasks",
"ec2:DescribeFlowLogs",
"ec2:DescribeHosts",
"ec2:DescribeHostReservations",
"ec2:DescribeHostReservationOfferings",
"ec2:DescribeIdentityIdFormat",
"ec2:DescribeIdFormat",

"ec2:DescribeImageAttribute",

"ec2:DescribeImages",

"ec2:DescribeImportImageTasks",

"ec2:DescribeImportSnapshotTasks",

"ec2:DescribeInstanceAttribute",

"ec2:DescribeInstanceStatus",

"ec2:DescribeInstances",

"ec2:DescribeInternetGateways",

"ec2:DescribeKeyPairs",

"ec2:DescribeMovingAddresses",

"ec2:DescribeNatGateways",

"ec2:DescribeNetworkAcls",

"ec2:DescribeNetworkInterfaceAttribute",

"ec2:DescribeNetworkInterfaces",

"ec2:DescribePlacementGroups",

"ec2:DescribePrefixLists",

"Ec2:DescribeRe",

"ec2:DescribeReservedInstances",

"ec2:DescribeReservedInstancesListings",

"ec2:DescribeReservedInstancesModifications",

"ec2:DescribeReservedInstancesOfferings",

"ec2:DescribeRouteTables",

"ec2:DescribeSecurityGroups",

"ec2:DescribeSnapshotAttribute",

"ec2:DescribeSnapshots",

"ec2:DescribeSpotDatafeedSubscription",

"ec2:DescribeSpotFleetInstances",

"ec2:DescribeSpotFleetRequestHistory",

"ec2:DescribeSpotFleetRequests",

"ec2:DescribeSpotInstanceRequests",

"ec2:DescribeSpotPriceHistory",

"ec2:DescribeStaleSecurityGroups",

"ec2:DescribeSubnets",

"ec2:DescribeTags",

"ec2:DescribeVolumeAttribute",

"ec2:DescribeVolumeStatus",

"ec2:DescribeVolumes",

"ec2:DescribeVpcAttribute",

"ec2:DescribeVpcClassicLink",

"ec2:DescribeVpcEndpointServices",

"ec2:DescribeVpcEndpoints",

"ec2:DescribeVpcPeeringConnections",

"ec2:DescribeVpcs",

"ec2:DescribeVpnConnections",

"ec2:DescribeVpnGateways",

"ec2:DetachClassicLinkVpc",

"ec2:DetachInternetGateway",

"ec2:DetachNetworkInterface",

"ec2:DetachVolume",

"ec2:DetachVpnGateway",

"ec2:DisableVgwRoutePropagation",

"ec2:DisableVpcClassicLink",

"ec2:DisableVpcClassicLinkDnsSupport",

"ec2:DescribeVpcClassicLinkDnsSupport",

"ec2:DetachNetworkInterface",

"ec2:DetachVolume",

"ec2:DisassociateAddress",

"ec2:ModifyInstanceAttribute",

"ec2:ModifyNetworkInterfaceAttribute",

"ec2:ModifySnapshotAttribute",

"ec2:ModifySubnetAttribute",

"ec2:ModifyVolumeAttribute",

```
            "ec2:RevokeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:RunInstances",
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Effect": "Allow",
        "Resource": [
        "*"
        ]
    },
    {
        "Sid": "Stmt1477880716900",
        "Aktion": [
            "s3:CreateBucket",
            "s3:DeleteBucket",
            "s3:DeleteObject",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:PutObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "Stmt1477883239716",
        "Aktion": [
            "iam:GetUser"
```

```
        ],
        "Effect": "Allow",
        "Resource": [
            "*"
        ]
    }
    ]
    }
```

9. Klicken Sie auf **Richtlinie anwenden**.
10. Verwenden Sie in der UDP-Konsole den Zugriffsschlüssel des IAM-Benutzers und den Sicherheits-Zugriffsschlüssel, um einen VSB-auf-EC2-Plan zu erstellen.

Erstellen eines Plans mit einem Sicherungstask

Ein Plan umfasst verschiedene Arten von Tasks, die Sie ausführen möchten. Um einen Virtual Standby-Rechner zu erstellen, erstellen Sie einen Plan, der einen Sicherungstask und einen Virtual Standby-Task enthält. Ein Sicherungstask führt eine Sicherung der Quellknoten aus und speichert die Daten am angegebenen Ziel. Diese Sicherungsdaten werden von der Virtual Standby-Funktion verwendet und in ein Format für virtuelle Rechner konvertiert.

Sie können einen Virtual Standby-Rechner aus einer Agent-basierten Windows-Sicherung oder aus einer hostbasierten Sicherung ohne Agent erstellen. Sie können auch einen Virtual Standby-Rechner aus Daten erstellen, die mithilfe des **Replikationstasks** repliziert werden. Folgender Vorgang ist ein Beispiel für die Erstellung einer Agent-basierten Windows-Sicherung.

Hinweise:

- Weitere Informationen zu hostbasierten agentenlosen Sicherungen finden Sie unter Erstellen eines Sicherungsplans für hostbasierte virtuelle Rechner.
- Weitere Informationen zur Replikation von Sicherungsdaten finden Sie unter Replizieren von Daten zwischen Datenspeichern, die von einer UDP-Konsole verwaltet werden und die von unterschiedlichen UDP-Konsolen verwaltet werden.
- Aufgrund von Einschränkungen bei Amazon AWS EC2 unterstützt die Option "Virtual Standby auf EC2" auf Quellrechnern KEINE Starts von UEFI-Firmware.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

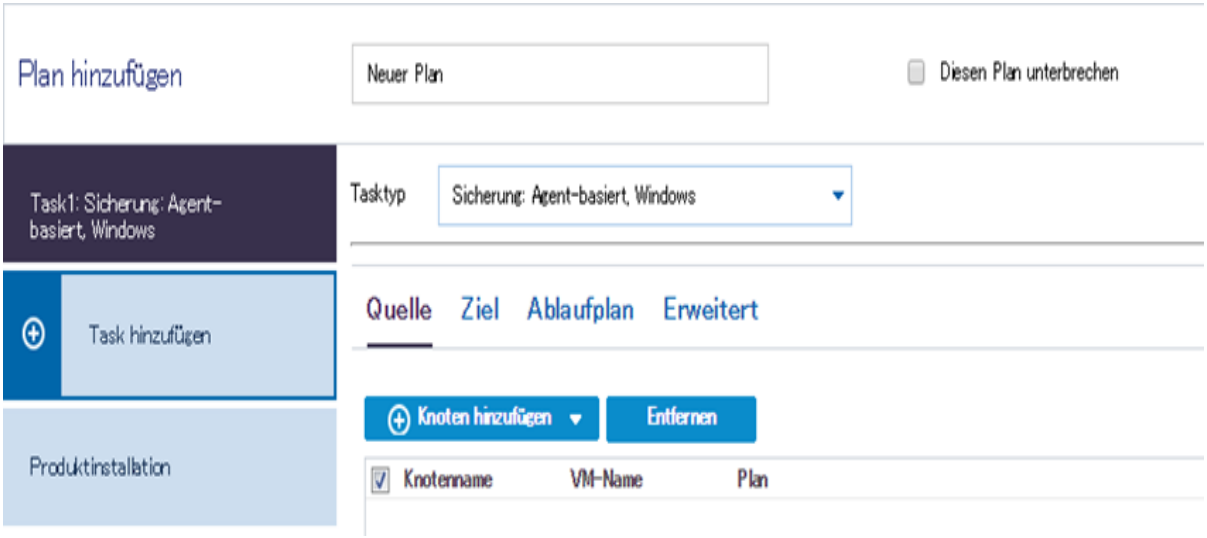
   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.

6. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Sicherung, Agent-basiertes Windows** aus.



Geben Sie nun Quelle, Ziel, Zeitplan und Erweitert-Details an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die Quellknoten angeben, die Sie schützen möchten. Sie können mehrere Knoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Knoten hinzufügen, wenn Sie einen Plan auf der Quellenseite erstellen oder ändern. Sie können einen Plan auch speichern, ohne Quellknoten hinzuzufügen. Der Plan wird erst bereitgestellt, wenn Sie Quellknoten hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Quelle" auf **Hinzufügen**.
2. Wählen Sie eine der folgenden Optionen:

   Wählen Sie zu sichernden Knoten in Arcserve UDP aus

   Öffnet das Dialogfeld "Wählen Sie zu sichernden Knoten in Arcserve UDP aus". Wählen Sie die Knoten in der angezeigten Liste aus. Wählen Sie diese Option aus, wenn Sie die Knoten bereits zu der Konsole hinzugefügt haben.

   Windows-Knoten hinzufügen

   Öffnet das Dialogfeld "Knoten zu Plan hinzufügen". Wählen Sie diese Option aus, wenn Sie die Knoten nicht hinzugefügt haben und Sie die zu schützenden Knoten manuell hinzufügen möchten.

   Knoten aus Active Directory erkennen

   Öffnet das Dialogfeld Knoten zu Arcserve UDP-Konsole hinzufügen. Wählen Sie diese Option, wenn Sie Knoten aus Active Directory erkennen und hinzufügen möchten.

3. Wenn Sie die Option **Wählen Sie zu sichernden Knoten in Arcserve UDP aus** ausgewählt haben, gehen Sie im Dialogfeld "Zu schützende Knoten auswählen" folgendermaßen vor:

   a. (Optional) Wählen Sie einen Filter aus der Dropdown-Liste "Gruppen" aus, um nach Knoten zu filtern. Sie können Schlüsselwörter eingeben, um den Knotenfilter weiter einzuschränken.

      Die Knoten werden in der Spalte "Verfügbare Knoten" angezeigt.

   b. Wählen Sie die Knoten aus der Spalte "Verfügbare Knoten" aus, und klicken Sie dann auf den einfachen Nach-rechts-Pfeil (>) oder den doppelten Nach-rechts-Pfeil (>>), um die ausgewählten Knoten bzw. alle Knoten in die Spalte "Ausgewählte Knoten" zu verschieben.

Die Knoten werden in der Spalte "Ausgewählte Knoten" angezeigt.

c. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

4. Wählen Sie zum Festlegen des Schutztyps eine der folgenden Optionen aus:

Alle Volumes sichern

Bereitet einen Sicherungs-Snapshot aller Volumes vor.

Ausgewählte Volumes sichern

Bereitet einen Sicherungs-Snapshot des ausgewählten Volumes vor.

Die Sicherungsquelle ist nun angegeben.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Wählen Sie einen der folgenden **Zieltypen** aus:

   Lokaler Datenträger oder freigegebener Ordner

   Gibt an, dass das Sicherungsziel ein lokales Ziel oder ein freigegebener Ordner ist. Wenn Sie diese Option auswählen, können Sie Daten als Wiederherstellungspunkte oder Wiederherstellungssätze speichern. Die Optionen für Wiederherstellungspunkte und Wiederherstellungssätze sind auf der Registerkarte **Ablaufplan** verfügbar.

   Arcserve UDP-Recovery Point Server

   Gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.

2. Wenn Sie **Arcserve UDP-Recovery Point Server** ausgewählt haben, geben Sie folgende Details an:
   a. Wählen Sie einen Recovery Point Server aus.
   b. Wählen Sie einen Datenspeicher aus. Die Liste enthält alle Datenspeicher, die am angegebenen Recovery Point Server erstellt wurden.
   c. Geben Sie ein Sitzungskennwort ein.
   d. Bestätigen Sie das Sitzungskennwort.
3. Wenn Sie **Lokaler Datenträger oder freigegebener Ordner** ausgewählt haben, geben Sie folgende Details an:
   a. Geben Sie den vollständigen Pfad des lokalen Ziels oder Netzwerkziels an. Geben Sie für das Netzwerkziel Anmeldeinformationen für ein Konto mit Schreibzugriff an.
   b. Wählen Sie den Verschlüsselungsalgorithmus aus. Weitere Informationen finden Sie unter Verschlüsselungseinstellungen.
   c. Geben Sie optional ein Verschlüsselungskennwort an.
   d. Bestätigen Sie das Verschlüsselungskennwort.

e. Wählen Sie einen Komprimierungstyp aus. Weitere Informationen finden Sie unter "Komprimierungstyp".

Hinweis: Wenn Sie die Daten auf einem lokalen Datenträger oder in einem freigegebenen Ordner speichern, können Sie die Daten nicht auf einem anderen Recovery Point Server replizieren. Die Replikation wird nur unterstützt, wenn Sie die Daten auf einem Recovery Point Server speichern.

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

Gehen Sie wie folgt vor:

1. (Optional) Wählen Sie die Option für die Verwaltung von Wiederherstellungspunkten aus. Diese Option ist nur sichtbar, wenn Sie als Sicherungsziel "Lokaler oder freigegebener Ordner" ausgewählt haben.

   Nach Wiederherstellungspunkten aufbewahren

   Die Sicherungsdaten werden als Wiederherstellungspunkte gespeichert.

   Nach Wiederherstellungssätzen aufbewahren

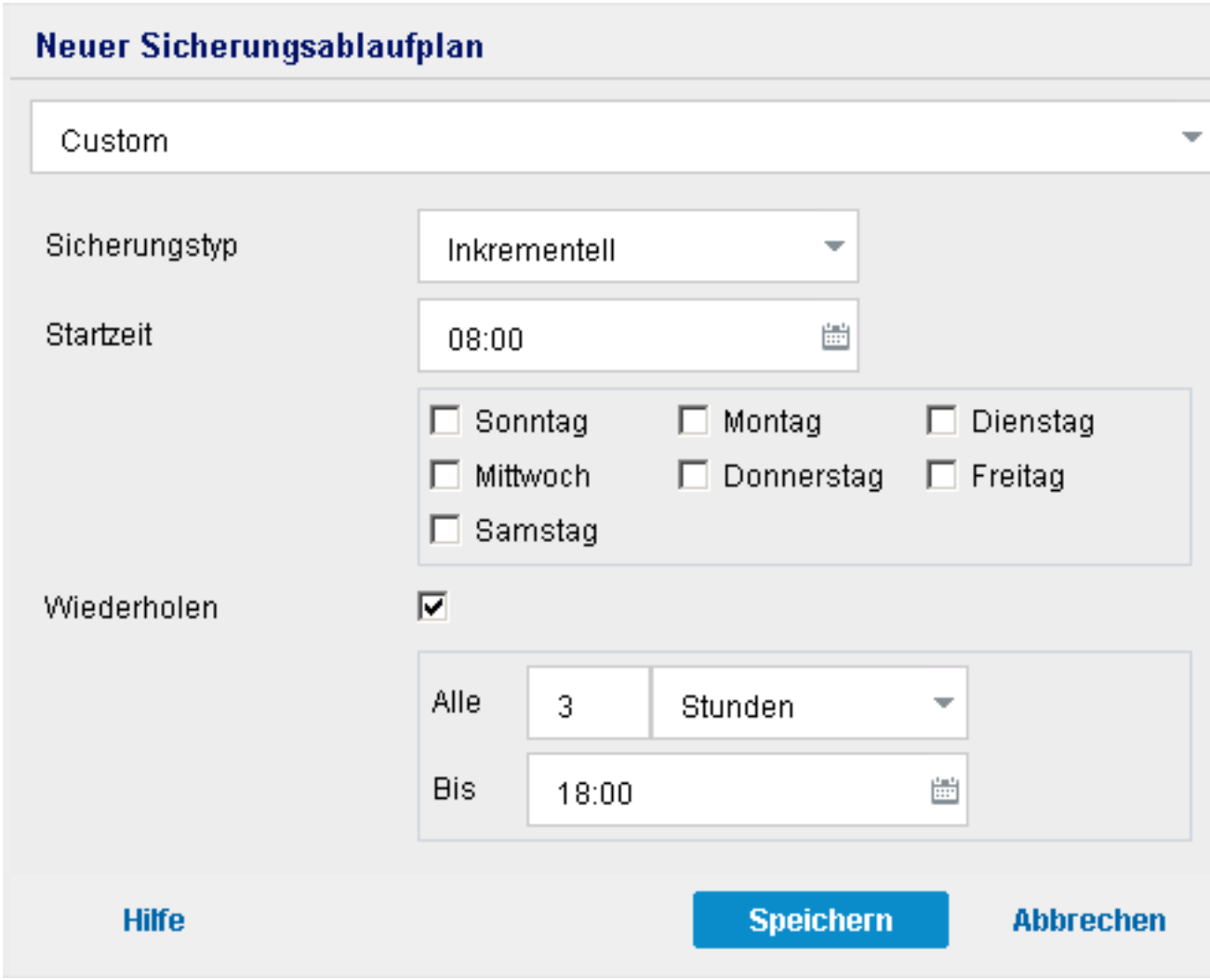
   Die Sicherungsdaten werden als Wiederherstellungssätze gespeichert.

2. Fügen Sie Ablaufpläne für Sicherungen, Zusammenführungen und Drosselungsvorgänge hinzu.

   Hinzufügen eines Sicherungsablaufplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Überprüfen

Legt den Ablaufplan für Überprüfungssicherungen fest.

Arcserve UDP überprüft die Gültigkeit und Vollständigkeit der geschützten Daten durch einen Vergleich des gespeicherten Sicherungs-Images mit der Sicherungsquelle. Im Bedarfsfall wird das Image neu synchronisiert. Bei einer Überprüfungssicherung wird die letzte Sicherung jedes einzelnen Blocks mit den Inhalten und Informationen der Quelle verglichen. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht (zumeist aufgrund von Änderungen seit der letzten Sicherung), aktualisiert Arcserve UDP die Sicherung dieses Blocks (Neusynchronisierung). In seltenen Fällen kann eine Überprüfungssicherung auch durchgeführt werden, um eine vollständige Sicherung zu erhalten, ohne den erforderlichen Speicherplatz einer vollständigen Sicherung zu verwenden.

Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteile: Die Sicherung benötigt viel Zeit, da alle Quellenblöcke mit den Blöcken der letzten Sicherung verglichen werden.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die seit der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf Hinzufügen, und wählen Sie Zusammenführungsplan hinzufügen aus.

Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

b. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

d. Klicken Sie auf **Speichern**.

Der Zusammenführungsablaufplan ist auf der Seite **Ablaufplan** angegeben und wird dort angezeigt.

Hinzufügen eines Drosselungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

Das Dialogfeld Drosselungsplan hinzufügen wird geöffnet.

b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

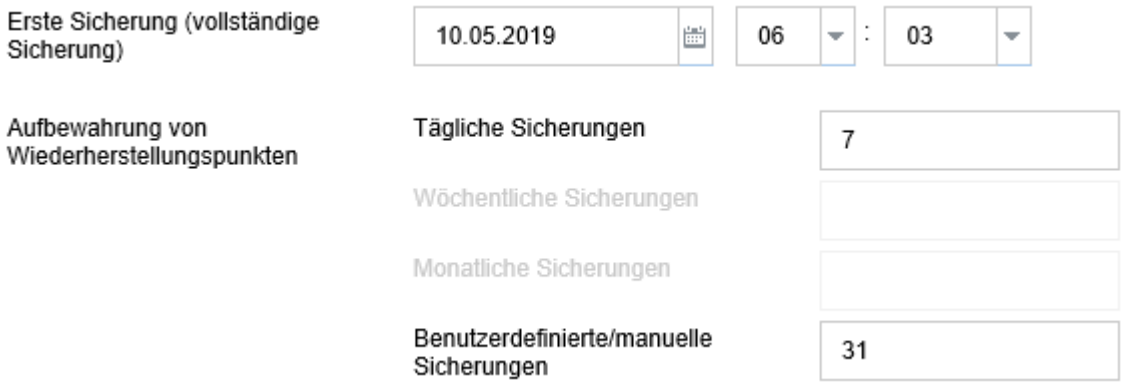
c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Drosselungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

3. Geben Sie die Startzeit für die geplante Sicherung an.



4. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld "Sicherungsablaufplan" übernommen.

5. Geben Sie die Katalogdetails an.

   Mit Katalogen können Sie den Dateisystemkatalog generieren. Der Dateisystemkatalog ist erforderlich, um schnellere und bessere Suchvorgänge auszuführen. Wenn Sie die Kontrollkästchen für den Katalog aktivieren, werden die Kataloge je nach der Sicherungsart, die Sie angegeben haben, aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Kataloggenerierung zu deaktivieren.

   Der Ablaufplan ist nun angegeben.

Funktionsweise der erweiterten Planung und Aufbewahrung

Mit der Ablaufplanoption können Sie einen benutzerdefinierten Ablaufplan, einen Ablaufplan für tägliche/wöchentliche/monatliche Sicherungen oder beides festlegen. Im benutzerdefinierten Ablaufplan können Sie den Sicherungsablaufplan für jeden Tag der Woche konfigurieren und bis zu vier Sicherungsablaufpläne für jeden Tag hinzufügen. Sie können einen bestimmten Wochentag auswählen und ein Zeitfenster erstellen, um anzugeben, wann und wie oft die Sicherung durchgeführt werden soll.

Ablaufplan	Unterstützter Job	Kommentare
Sichern	Sicherungsjob	Gibt Zeitfenster für die Ausführung von Sicherungsjobs an.
Sicherungsdrosselung	Sicherungsjob	Gibt die Zeitfenster an, um die Sicherungsgeschwindigkeit zu steuern.
Zusammenführen	Zusammenführungsjob	Gibt an, wann Zusammenführungsjobs ausgeführt werden sollen.
Täglicher Ablaufplan	Sicherungsjob	Gibt an, wann tägliche Sicherungsjobs ausgeführt werden sollen.
Wöchentlicher Ablaufplan	Sicherungsjob	Gibt an, wann wöchentliche Sicherungsjobs ausgeführt werden sollen.
Monatlicher Ablaufplan	Sicherungsjob	Gibt an, wann monatliche Sicherungsjobs ausgeführt werden sollen.

Sie können auch die Aufbewahrungseinstellungen für die Wiederherstellungspunkte angeben.

Hinweis: Legen Sie innerhalb der einzelnen Pläne Einstellungen für die Aufbewahrungszeit fest, um zu steuern, wie die Daten für die Knoten des entsprechenden Plans im Zieldatenspeicher aufbewahrt werden.

Ablaufpläne für tägliche/wöchentliche/monatliche Sicherungen sind vom benutzerdefinierten Ablaufplan und voneinander unabhängig. Sie können die Ausführung einer täglichen, wöchentlichen oder monatlichen Sicherung konfigurieren, ohne einen benutzerdefinierten Ablaufplan zu konfigurieren.

Jobplan der Sicherung

Sie können vier Zeitfenster pro Tag in Ihrem Sicherungsablaufplan hinzufügen. Ein gültiges Zeitfenster liegt im Bereich 12:00 Uhr bis 23:59 Uhr. Sie können kein Zeitfenster wie z. B. 18:00 Uhr bis 06:00 Uhr angeben. In solchen Fällen müssen Sie manuell zwei verschiedene Zeitfenster angeben.

Für jedes Zeitfenster wird die Startzeit einbezogen, und die Endzeit wird nicht einbezogen. Zum Beispiel haben Sie das Ausführen einer Zuwachssicherung konfiguriert, die stündlich zwischen 06:00 Uhr und 09:00 Uhr stattfinden soll, und die Sicherung wird um 06:00 Uhr gestartet. Das bedeutet, dass die Sicherung um 06:00 Uhr, 07:00 Uhr und 08:00 Uhr ausgeführt wird, NICHT aber um 09:00 Uhr.

Hinweis: Wenn Sie die Sicherung bis zum Ende des Tages wiederholt ausführen möchten, legen Sie den Ablaufplan bis 12:00 Uhr fest. Um den Sicherungsjob beispielsweise alle 15 Minuten während des gesamten Tages auszuführen, legen Sie den Ablaufplan von 00:00 Uhr bis 00:00 Uhr alle 15 Minuten fest.

Drosselungsplan der Sicherung

Mit dem Drosselungsplan der Sicherung können Sie die Geschwindigkeit des Sicherungsdurchsatzes steuern, die wiederum die Ressourcenverwendung (Datenträger-E/A, CPU, Netzwerkbandbreite) des Servers, der gesichert wird, steuert. Dies ist hilfreich, wenn die Serverleistung während der Geschäftszeiten nicht beeinträchtigt werden soll. Sie können vier Zeitfenster pro Tag in Ihrem Drosselungsplan der Sicherung hinzufügen. Für jedes Zeitfenster können Sie einen Wert in MB pro Minute angeben. Dieser Wert wird verwendet, um den Sicherungsdurchsatz zu steuern. Gültige Werte liegen im Bereich zwischen 1 MB/Minute bis 99.999 MB/Minute.

Wenn ein Sicherungsjob die angegebene Zeit überschreitet, dann wird das Drosselungslimit entsprechend dem angegebenen Zeitfenster angepasst. Zum Beispiel haben Sie als Drosselungslimit der Sicherung den Wert 500 MB/Minute von 08:00 Uhr bis 20:00 Uhr und 2500 MB/Minute von 20:00 Uhr bis 22:00 Uhr angegeben. Wenn ein Sicherungsjob um 19:00 Uhr startet und drei Stunden ausgeführt wird, dann hat das Drosselungslimit von 19:00 Uhr bis 20:00 Uhr den Wert 500 MB/Minute. Von 20:00 Uhr bis 22:00 Uhr hat das Drosselungslimit den Wert 2.500 MB/Minute.

Wenn Sie keinen Sicherungsablaufplan und keinen Ablaufplan für den Sicherungsdurchsatz angeben, dann wird die Sicherung so schnell wie möglich ausgeführt.

Ablaufplan für Zusammenführung

Ermöglicht es Ihnen, Wiederherstellungspunkte basierend auf dem angegebenen Ablaufplan zusammenzuführen.

Beachten Sie folgende Punkte für den Zusammenführungsjob:

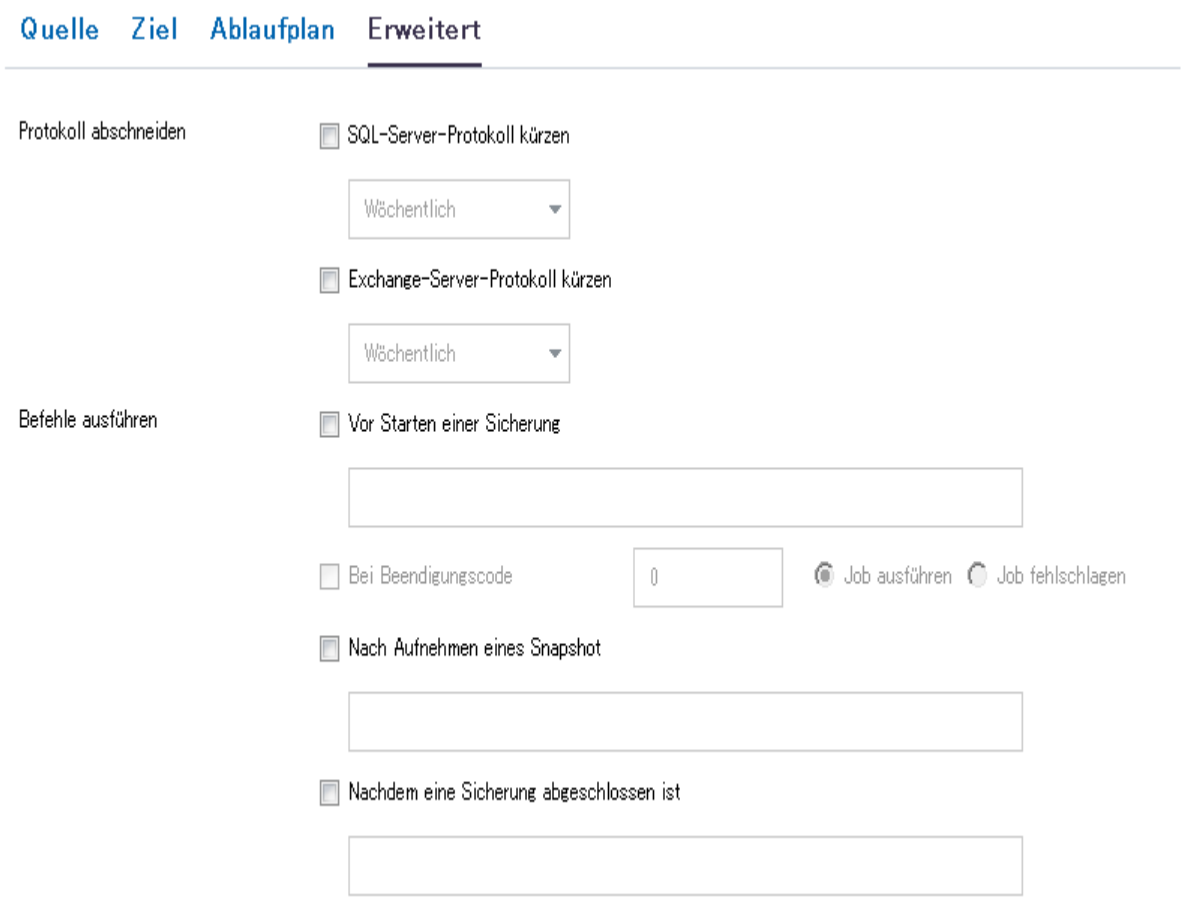
- Es kann immer nur ein Zusammenführungsjob für einen Knoten ausgeführt werden.

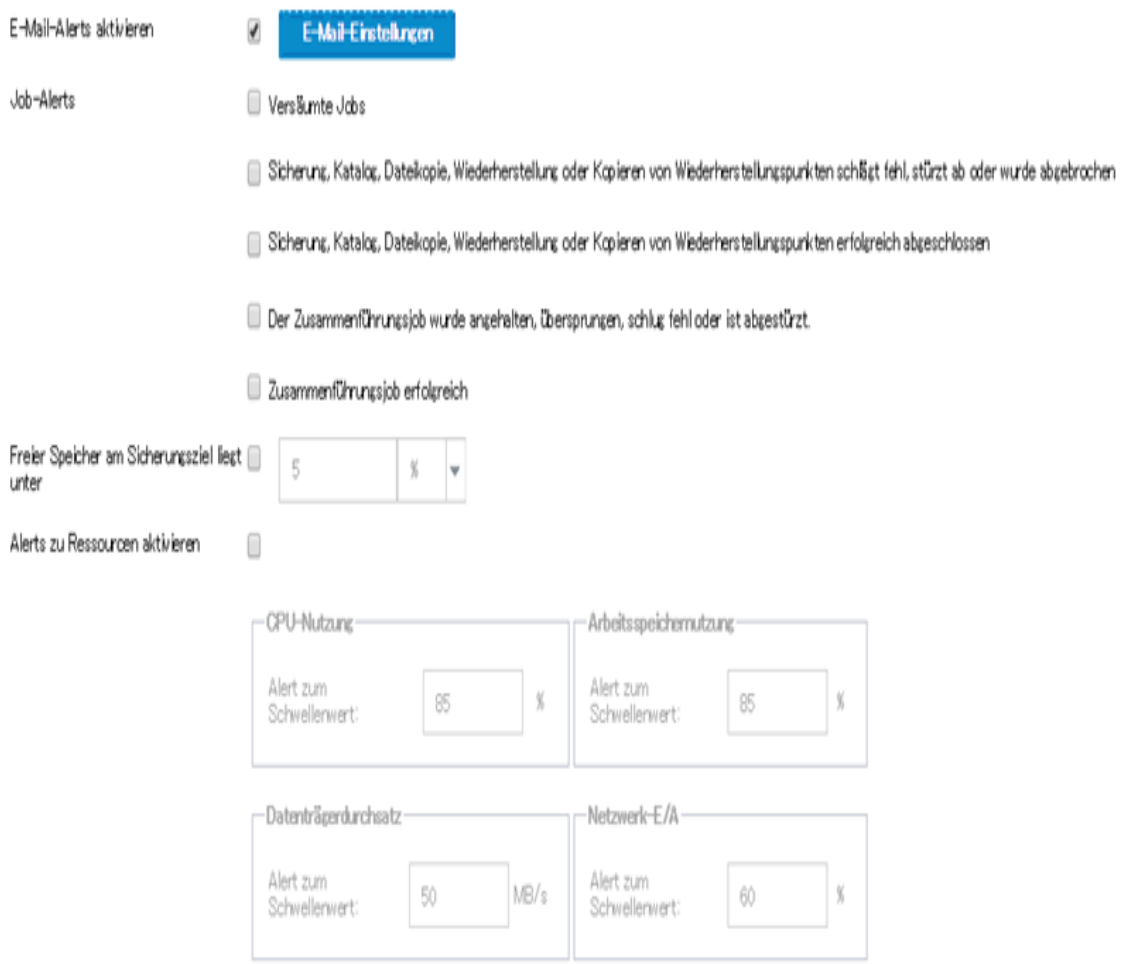
- Wenn ein Zusammenführungsjob gestartet wird, muss er abgeschlossen werden, bevor der nächste Zusammenführungsjob gestartet werden kann. Das bedeutet: Wenn ein oder mehrere Sätze an Wiederherstellungspunkten zusammengeführt werden, dann kann der neue Wiederherstellungspunkt nicht zu diesem Zusammenführungsprozess hinzugefügt werden, bis der Zusammenführungsprozess für den aktuellen Satz an Wiederherstellungspunkten abgeschlossen ist.
- Wenn ein Zusammenführungsjob mehr als einen Satz an Wiederherstellungspunkten bearbeitet (zum Beispiel Satz [1~4], Satz [5~11] und Satz [12~14], also drei Sätze), dann werden diese Sätze nacheinander vom Recovery Point Server bearbeitet.
- Wenn ein Zusammenführungsjob nach einer Pause fortgesetzt wird, erkennt der Job an welchem Punkt er unterbrochen wurde, und die Zusammenführung wird ab der Abbruchstelle fortgesetzt.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen die Einstellungen zum Abschneiden von Protokollen, das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte "Erweitert":





Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

Protokoll abschneiden

Ermöglicht es Ihnen, den Ablaufplan anzugeben, um Protokolle für SQL Server und Exchange Server zu kürzen. Sie können den Ablaufplan als **Täglich**, **Wöchentlich** oder **Monatlich** angeben.

Benutzername

Ermöglicht es Ihnen, den Benutzer anzugeben, der zur Ausführung eines Skripts autorisiert ist.

Kennwort

Ermöglicht es Ihnen, das Kennwort des Benutzers anzugeben, der zur Ausführung des Skripts autorisiert ist.

Befehl ausführen, bevor eine Sicherung gestartet wird

Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, in dem das Skript gespeichert wird. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem ein Snapshot aufgenommen wurde

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungs-Snapshot aufgenommen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Arten der Alerts angeben, die Sie in Form von E-Mails empfangen möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers.

Job-Alerts

Ermöglicht es Ihnen, die Typen der Job-E-Mails auszuwählen, die Sie erhalten möchten.

Warnmeldungen zu Ressourcen aktivieren

Ermöglicht es Ihnen, einen Schwellenwert für CPU-Auslastung, Speicherverwendung, Datenträgerdurchsatz, Netzwerk-E/A anzugeben. Sie können den Wert in Prozent angeben. Sie erhalten eine E-Mail, wenn der Wert "Warnmeldung zum Schwellenwert" überschritten ist.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Knoten installiert ist und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung

an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agenten oder kein Agent installiert ist. Um den Agenten auf diesen Knoten zu installieren bzw. um ein Upgrade des Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus, und klicken Sie auf "Speichern".

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie eine andere Task hinzufügen müssen, müssen Sie den Plan aus der Registerkarte **Ressourcen** auswählen und den Plan ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern.

Der Sicherungsplan wird erstellt und automatisch für den Quellknoten bereitgestellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

Hinzufügen eines "Virtual Standby auf EC2-Tasks" zum Plan

Erstellen Sie einen "Virtual Standby auf EC2"-Task, damit die Sicherungsdaten in ein Format für virtuelle Rechner konvertiert werden und ein virtueller Rechner erstellt wird.

Hinweise:

- Virtual Standby auf EC2 unterstützt das automatische Starten des virtuellen Rechners nicht.
- Wenn Sie den Plan unterbrechen, wird der Virtual Standby-Job nicht gestartet. Wenn Sie den Plan wieder aufnehmen, wird der Virtual Standby-Job nicht automatisch fortgesetzt. Sie müssen einen anderen Sicherungsjob manuell ausführen, damit der Virtual Standby-Job gestartet wird. Darüber hinaus ist die Option "Virtual Standby unterbrechen/wiederaufnehmen" nicht verfügbar, wenn der Plan unterbrochen ist. Wenn der virtuelle Rechner nach einer Unterbrechung des Plans nicht automatisch starten soll, müssen Sie das Heartbeat-Signal für die Knoten manuell unterbrechen.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Fensterbereich auf **Task hinzufügen**.

   Ein neuer Task wird im linken Fensterbereich hinzugefügt.

2. Wählen Sie im Drop-down-Menü **Tasktyp** die Option **Virtual Standby** aus.

   Der Virtual Standby-Task wird hinzugefügt.

3. Wählen Sie auf der Registerkarte **Quelle** eine Quelle für den Virtual Standby-Task aus.

4. Klicken Sie auf die Registerkarte **Virtualisierungsserver**.

5. Wählen Sie EC2 als Virtualisierungstyp aus, und geben Sie Details ein.

   Virtualisierungstyp: EC2

   Kontoname

   Wählen Sie das vorhandene Amazon AWS-Konto für den Zugriff auf AWS EC2 aus. Sie können auch ein neues Konto hinzufügen, indem Sie auf **Hinzufügen** klicken. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos für Amazon EC2.

   EC2-Region

Wählen Sie die EC2-Region aus, in der sich Ihr Cloud-Proxy befindet. Arcserve UDP unterstützt alle globalen EC2-Regionen und die EC2-Region China.

Hinweis: Das angegebene Konto muss ein Administratorkonto oder ein Konto mit Administratorberechtigungen für EC2 sein.

VSB-Cloud-Proxy

Definieren Sie eine EC2-Instanz in der ausgewählten Region als Cloud-Proxy.

Hinweis: In der EC2-Instanz muss der Arcserve UDP-Agent installiert sein.

Benutzername und Kennwort

Geben Sie die Anmeldeinformationen für die Anmeldung beim VSB-Cloud-Proxy an.

Protokoll

Geben Sie entweder HTTP oder HTTPS als das Protokoll an, das Sie für die Kommunikation des Arcserve Unified Data Protection-Quellagenten auf dem VSB-Cloud-Proxy verwenden möchten.

Port

Legen Sie den Port fest, den Sie für die Kommunikation zwischen dem Quellserver und dem VSB-Cloud-Proxy verwenden möchten.

Hinweis: Da der Cloud-Proxy für den Datentransfer verwendet wird, müssen die zugehörigen Ports für den Zugriff auf den Inbound in der AWS EC2-Sicherheitsgruppe, einschließlich TCP 8014 und 4091, aktiviert sein.

6. Klicken Sie auf die Registerkarte **Virtueller Rechner**, und geben Sie Details für die Grundeinstellungen, die Cloud-Speicher-Einstellungen und die Netzwerkeinstellungen ein.

   Amazon AWS EC2

   Wenden Sie die folgenden Optionen für virtuelle Rechner auf Amazon AWS EC2 an:

   Präfix des Namens des virtuellen Rechners

   Geben Sie das Präfix an, das Sie dem Anzeigenamen des virtuellen Rechners in der AWS EC2-Cloud voranstellen möchten.

   Standardwert: UDPVM_

   Wiederherstellungspunkt-Snapshots

   Geben Sie die Anzahl an Wiederherstellungspunkt-Snapshots (Wiederherstellungspunkten) für den Virtual Standby-Rechner an. Die Höchstanzahl von Wiederherstellungspunkt-Snapshots für AWS EC2 beträgt 29.

Kombinieren Sie alle unkonvertierten Sitzungen in Wiederherstellungspunkt-Snapshots.

Geben Sie an, ob alle unkonvertierten Sitzungen in einem einzigen Wiederherstellungspunkt-Snapshot kombiniert werden sollen, wenn der nächste geplante VSB-Auftrag stattfindet.

Standard: Ausgewählt

Instanzentyp

Amazon EC2 stellt eine Vielzahl von Instanzentypen zur Auswahl, die für unterschiedliche Anwendungsfälle optimiert sind. Instanzen sind virtuelle Server, die Anwendungen ausführen können. Sie können unterschiedliche Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazität haben, sodass Sie flexibel den passenden Ressourcenmix für Ihre Anwendungen auswählen können. Weitere Informationen zu Instanzentypen und dazu, welcher Typ zu welchen Datenverarbeitungsanforderungen passt, finden Sie unter diesem Link.

Typen von EBS-Volumes

Volumes des Typs "Standard-SSD" bieten eine maximale E/A-Rate von 3.000 IOPS und stellen eine konstante Baseline von 3 IOPS/GiB bereit. Volumes des Typs "Bereitgestellte E/A\Sek.-SSD" können bis zu 20.000 IOPS bereitstellen und sind die beste Wahl für EBS-optimierte Instanzen. Volumes des Typs "Magnetfestplatte", früher Standard-Volumes genannt, stellen durchschnittlich 100 IOPS bereit und können maximal mehrere Hundert IOPS liefern. Weitere Informationen zu den verschiedenen Typen von EBS-Volumes finden Sie unter diesem Link.

Netzwerk

Erlaubt die Definition der VPC sowie der Subnetze, der NICs und der Sicherheitsgruppe für den Virtual Standby-Rechner auf AWS EC2.

Hinweis: Wenn die automatische Zuweisung der öffentlichen IP aktiviert ist, wird aufgrund der Einschränkung von AWS EC2 nur eine NIC auf AWS EC2 abgebildet und andere werden verworfen.

Gleiche Zahl an Netzwerkadaptern wie die Quelle bei der letzten Sicherung

Aktivieren Sie diese Option, um zu definieren, auf welche Weise die virtuelle NIC zum Netzwerk auf EC2 zugeordnet werden soll. Aktivieren Sie diese Option, wenn der virtuelle Rechner virtuelle NICs und ein virtuelles Netzwerk enthält.

Hinweis: Diese Einstellungen sind nur dann konfigurierbar, wenn die automatische Zuweisung der öffentlichen IP deaktiviert ist.

7. Klicken Sie auf **Speichern**.

Die Änderungen werden gespeichert, und der Virtual Standby-Task wird automatisch auf dem Virtual Standby-Server bereitgestellt.

Sie haben den Virtual Standby-Plan erfolgreich erstellt und bereitgestellt.

Hinzufügen eines Drosselungsplans für Datenübertragungen zur Cloud

Mit dem Drosselungsplan können Sie die Geschwindigkeit des Datenübertragungsdurchsatzes zur Cloud steuern, die wiederum die Ressourcenverwendung (Netzwerkbandbreite) des Servers, der zur Cloud übertragen wird, steuert. Dies ist hilfreich, wenn die Serverleistung während der Geschäftszeiten nicht beeinträchtigt werden soll. Sie können vier Zeitfenster pro Tag in Ihrem Drosselungsplan für Datenübertragungen zur Cloud hinzufügen. Für jedes Zeitfenster können Sie einen Wert in Mbit/s bzw. Kbit/s pro Minute angeben. Dieser Wert wird verwendet, um den Übertragungsdurchsatz zur Cloud zu steuern. Gültige Werte liegen zwischen 1 Mbit/s bzw. Kbit/s und 99.999 Mbit/s bzw. Kbit/s.

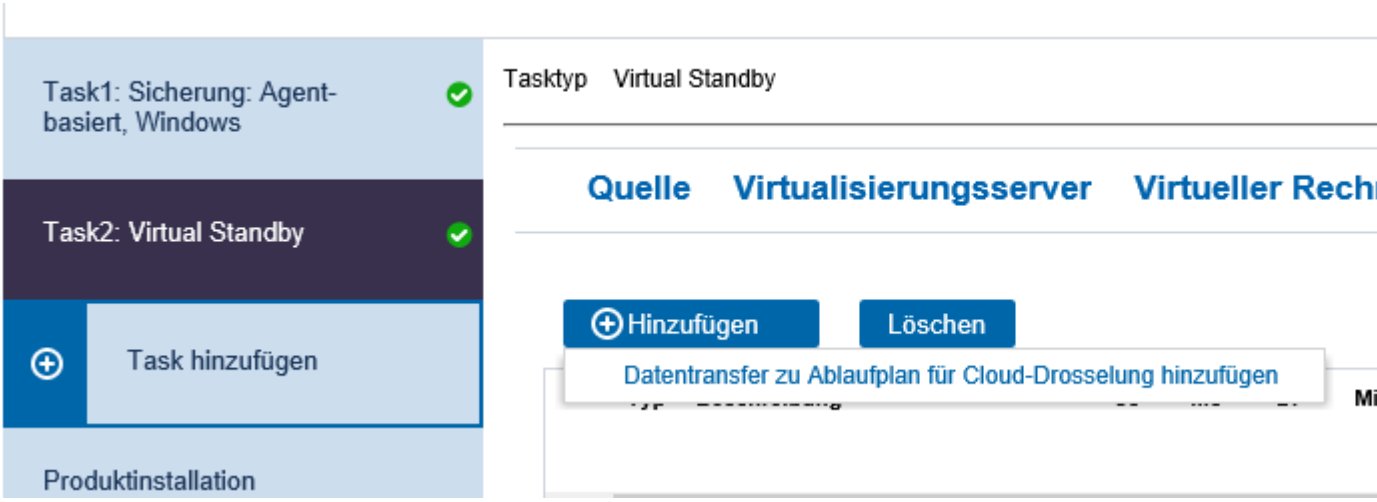
Wenn ein Datenübertragungsjob die angegebene Zeit überschreitet, dann wird das Drosselungslimit entsprechend dem angegebenen Zeitfenster angepasst. Zum Beispiel haben Sie als Drosselungslimit für die Übertragung den Wert 500 Mbit/s von 08:00 Uhr bis 20:00 Uhr und 2.500 Mbit/s von 20:00 Uhr bis 22:00 Uhr angegeben. Wenn ein Datenübertragungsjob um 19:00 Uhr startet und drei Stunden ausgeführt wird, dann hat das Drosselungslimit von 19:00 Uhr bis 20:00 Uhr den Wert 500 Mbit/s. Von 20:00 Uhr bis 22:00 Uhr hat das Drosselungslimit den Wert 2.500 Mbit/s.

Wenn des Sicherungstask mehr als einen Quellknoten mit Virtual Standby zur Cloud umfasst, wird das Drosselungslimit gleichmäßig aufgeteilt. Beispiel: Sie haben 500 Mbit/s als Drosselungslimit festgelegt und der Plan umfasst zwei Quellknoten. Wenn diese Knoten gleichzeitig Daten zur Cloud übertragen, liegt das Drosselungslimit für jeden Knoten bei 250 Mbit/s. Bei Abschluss des Übertragungstasks eines Knotens ändert sich das Drosselungslimit für den anderen Knoten, der den Task noch ausführt, in 500 Mbit/s.

Wenn Sie keinen Drosselungsplan festlegen, dann wird die Datenübertragung zur Cloud so schnell wie möglich ausgeführt.

Gehen Sie wie folgt vor:

1. Klicken Sie auf "Hinzufügen" und wählen Sie die Option zum Hinzufügen eines Drosselungsplans für Datenübertragungen zur Cloud aus.



Das Dialogfeld "Drosselungsplan hinzufügen" wird geöffnet.

2. Geben Sie die Begrenzung für den Durchsatz in Mbit/s bzw. Kbit/s an.

   Die Seite "Standby-VM - Netzwerkkonfiguration - <Knotenname>" wird geöffnet.

3. Geben Sie die Startzeit an, zu der die Drosselung starten soll.
4. Nehmen Sie eine Eingabe unter "Bis" vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.
5. Klicken Sie auf "Speichern".

   Der Drosselungsplan ist nun festgelegt und wird auf der Seite "Ablaufplanung" angezeigt.

Konfigurieren des Standby-VM-Netzwerks

Sie können die Standby-VM auf AWS EC2 mit benutzerdefinierten Netzwerkeinstellungen einschalten. Sie können folgende Netzwerkeinstellungen auf der Standby-VM konfigurieren:

- Geben Sie auf der Registerkarte **Netzwerkadapter-Einstellungen** das virtuelle Netzwerk und die NIC (Network Interface Card, Netzwerkkarte) sowie TCP/IP-Einstellungen für die einzelnen Netzwerkadapter an.
- Aktualisieren Sie die DNS-Server auf der Registerkarte **DNS-Aktualisierungseinstellungen**, um Clients basierend auf den TCP/IP-Einstellungen vom Quellrechner zu den virtuellen Virtual Standby-Rechnern umzuleiten.

Gehen Sie wie folgt vor:

1. Navigieren Sie auf der Registerkarte **Ressourcen** zur Knotengruppe **Virtual Standby**.

   Die Virtual Standby-Knoten werden im mittleren Fensterbereich angezeigt.

2. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Standby-VM - Netzwerkkonfiguration**.

   Die Seite "Standby-VM - Netzwerkkonfiguration - <Knotenname>" wird geöffnet.

3. Wählen Sie auf der Registerkarte **Netzwerkadapter-Einstellungen** das virtuelle Netzwerk aus der Liste **Standby-VM - Virtuelles Netzwerk** aus.

4. Wählen Sie das Subnetz aus der Subnetzliste aus.

5. Wählen Sie die elastische IP-Adresse aus der Liste **Elastic IP (Elastische IP)** aus.

6. Wählen Sie **TCP-/IP-Einstellungen anpassen** aus.

7. Klicken Sie auf die Schaltfläche **Adresse hinzufügen**, und fügen Sie **IP-Adressen**, **Gateway-Adressen**, **DNS-Adressen** und **WINS-Adressen** hinzu.

   Hinweis: Wenn Sie **DNS-Adressen** hinzufügen, dann konfigurieren Sie die DNS-Server auf der Registerkarte **DNS-Aktualisierungseinstellungen**.

8. Klicken Sie auf **Speichern**.

   Die Seite "Standby-VM - Netzwerkkonfiguration - <Knotenname>" wird geschlossen.

   Das Standby-VM-Netzwerk ist konfiguriert.

(Optional) Manuelles Ausführen eines "Virtual Standby auf EC2"-Tasks

Um einen Virtual Standby-Job manuell auszuführen, müssen Sie zunächst eine manuelle Sicherung ausführen. Der Virtual Standby zu EC2-Task wird mit einem Sicherungstask verknüpft. Wenn ein Plan einen Sicherungstask und einen Virtual Standby zu EC2-Task enthält, wird der Virtual Standby-Job nach dem Abschluss des Sicherungsjobs automatisch ausgeführt.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Wenn Sie Pläne hinzugefügt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Wählen Sie die Knoten aus, die Sie sichern möchten und für die ein zugewiesener Plan vorliegt.
4. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Jetzt sichern**.

   Das Dialogfeld **Sicherung jetzt ausführen** wird geöffnet.
5. Wählen Sie den Sicherungstyp aus, und geben Sie einen Namen für den Sicherungsjob an.
6. Klicken Sie auf **OK**.

   Der Sicherungsjob wird ausgeführt.

   Der Virtual Standby zu EC2-Job wird sofort nach dem Sicherungsjob ausgeführt.

   Der Virtual Standby zu EC2-Job wird manuell ausgeführt.

Unterbrechen und Wiederaufnehmen eines Virtual Standby-Jobs

Virtuelle Konvertierung ist der Prozess, bei dem Virtual Standby die Arcserve Unified Data Protection-Wiederherstellungspunkte von Quellknoten in Formate für virtuelle Rechner konvertiert, die als Wiederherstellungspunkt-Snapshots bezeichnet werden. Wenn es einen Fehler auf einem Quellknoten gibt, verwendet die Virtual Standby-Funktion die Wiederherstellungspunkt-Snapshots, um einen virtuellen Rechner für den Quellknoten in Betrieb zu nehmen.

Die Best Practice besteht darin, zuzulassen, dass der virtuelle Konvertierungsprozess kontinuierlich in Betrieb ist. Wenn Sie den virtuellen Konvertierungsprozess jedoch auf lokalen und Remote-Virtual Standby-Servern vorübergehend unterbrechen möchten, können Sie dies über die Konsole tun. Nachdem Sie die Probleme auf dem Quellknoten behoben haben, können Sie den virtuellen Konvertierungsprozess wieder aufnehmen.

Wenn Sie Virtual Standby-Jobs (Konvertierungsjobs) unterbrechen, wird der Konvertierungsjob, der gegenwärtig durchgeführt wird, nicht unterbrochen. Der Unterbrechungsvorgang bezieht sich auf nur den Job, dessen Ausführung nach Beendigung des nächsten Sicherungsjobs erwartet wird. Dadurch startet der nächste Konvertierungsjob nicht, bis Sie den (unterbrochenen) Konvertierungsjob ausdrücklich wiederaufnehmen.

Wenn Sie Virtual Standby für Knoten wiederaufnehmen und wenn mehrere Sicherungssitzungen ohne Wiederherstellungspunkt-Snapshot vorhanden sind, dann wird ein Dialogfeld angezeigt, in dem Sie die Smart Copy-Option auswählen können. Wenn Sie auf "Ja" klicken, konvertiert Virtual Standby die kombinierte Sitzung in einen einzelnen Wiederherstellungspunkt-Snapshot. Wenn Sie auf "Nein" klicken, konvertiert Virtual Standby jede Sitzung einzeln

Hinweis: Optional können Sie Virtual Standby-Jobs direkt von den Knoten aus unterbrechen und wiederaufnehmen. Weitere Informationen finden Sie unter "Unterbrechen und Wiederaufnehmen von Virtual Standby-Jobs von den Knoten".

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Navigieren Sie im linken Fensterbereich zu "**Virtual Standby**", und klicken Sie auf "**Alle Knoten**".

Wenn Sie Knoten hinzugefügt haben, werden diese Knoten im mittleren Fensterbereich angezeigt.

4. Wählen Sie den Knoten aus, den Sie unterbrechen oder wiederaufnehmen möchten.
5. Klicken Sie im mittleren Fensterbereich auf "**Aktionen**", "**Virtual Standby**", "**Unterbrechen**" oder "**Fortsetzen**".

   Die Virtual Standby-Funktion für den ausgewählten Knoten wird unterbrochen oder wiederaufgenommen.

Überprüfen des Plans

Um Ihre Virtual Standby-Funktion zu überprüfen, stellen Sie sicher, dass Sie den Virtual Standby-Plan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Nachdem der Sicherungsjob erfolgreich abgeschlossen wurde, wird der Virtual Standby-Job ausgeführt. Sie können den Status des Sicherungsjobs und Virtual Standby-Jobs in der Registerkarte **Jobs** überprüfen.

Folgen Sie diesen Schritten, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Folgen Sie diesen Schritten, um Virtual Standby-Jobs zu überprüfen:

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob und der Virtual Standby-Job erfolgreich ausgeführt werden.

   Der Plan für Virtual Standby wurde erfolgreich überprüft.

   Der Virtual Standby-Rechner wurde erstellt.

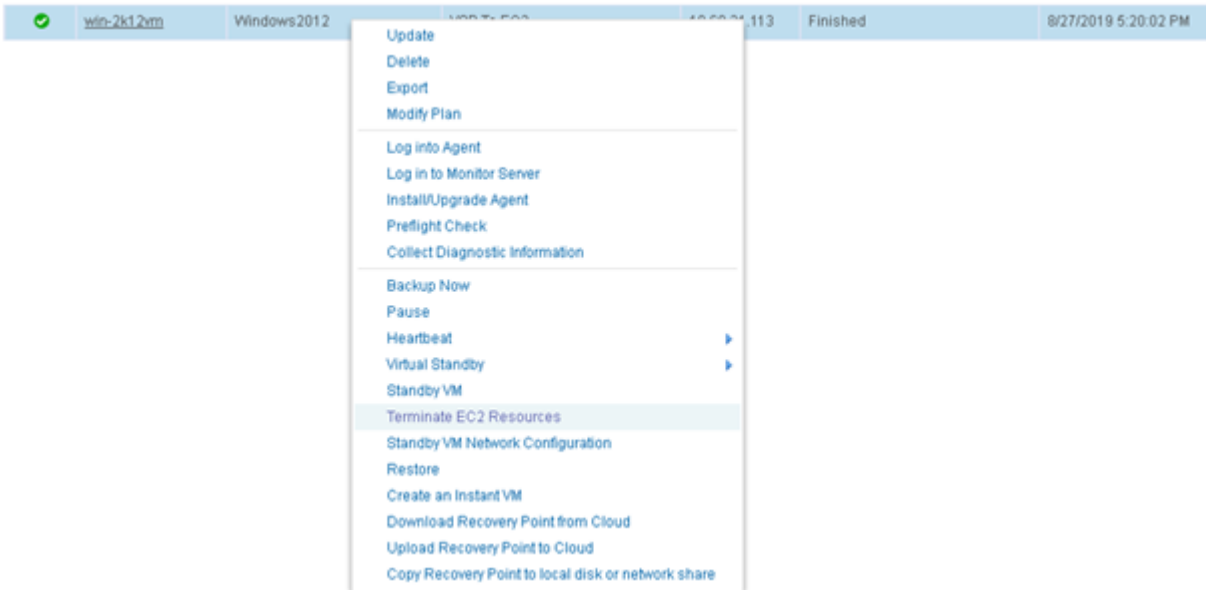
Beenden von EC2-Ressourcen

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

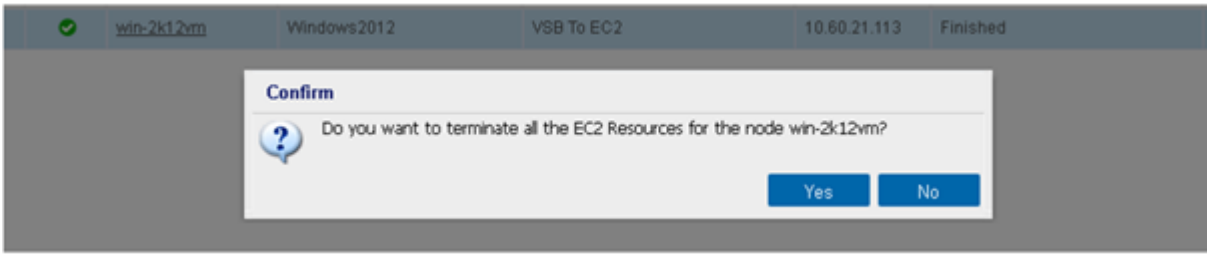
   Alle Knoten werden im mittleren Fensterbereich angezeigt.
3. Klicken Sie mit der rechten Maustaste auf einen Knoten, und wählen Sie "EC2-Ressourcen beenden" aus.

   Ein Bestätigungsdialogfeld wird geöffnet.



4. Klicken Sie auf **Ja**, um die AWS Cloud-Ressourcen zu bereinigen, die von Virtual Standby zu EC2-Task generiert werden. Klicken Sie auf **Nein**, um den Beendigungsprozess zu beenden.

   Hinweis: Wenn ein Knoten keine erfolgreichen VSB-zu-EC2-Aufträge hat, verfügt dieser Knoten nicht über die Option "EC2-Ressourcen beenden".



Erstellen eines Virtual Standby in einem Microsoft Azure Plan

Virtual Standby konvertiert die Wiederherstellungspunkte in Formate für virtuelle Rechner und bereitet einen Snapshot vor, damit Ihre Daten bei Bedarf auf einfache Weise wiederhergestellt werden können. Diese Funktion deckt auch die Hochverfügbarkeitsfunktion ab und stellt sicher, dass der virtuelle Rechner sofort übernehmen kann, wenn der Quellrechner ausfällt. Die Standby-VM wird durch die Konvertierung der Wiederherstellungspunkte in ein Microsoft VM-Format erstellt.

Hinweis: Der Virtual Standby-Task wird nur ausgeführt, wenn der Sicherungstask einen gültigen Snapshot des Wiederherstellungspunkts erstellt. Wenn der Sicherungstask fehlschlägt, dann wird der Virtual Standby-Task übersprungen.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen eines Plans mit einem Sicherungstask
3. Hinzufügen eines Virtual Standby zu Azure Task
4. (Optional) Manuelles Ausführen des Virtual Standby-Jobs
5. Unterbrechen und Wiederaufnehmen des Heartbeat-Signals
6. Unterbrechen und Wiederaufnehmen des Virtual Standby-Jobs
7. Überprüfen des Plans

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich bei der Konsole an.
- Wenn Sie die Sicherungsdaten auf Recovery Point-Servern speichern möchten, installieren Sie die Serverkomponente, und erstellen Sie Datenspeicher.
- Sie haben einen gültigen Wiederherstellungspunkt, um einen Virtual Standby-Rechner zu erstellen. Die Wiederherstellungspunkte können aus folgenden Aufgaben stammen:
  - Sicherung: Agent-basiert, Windows
  - Sicherung: hostbasiert, agentenlos
  - Replizieren
  - Replizieren von einem Remote-Recovery Point Server
- Überprüfen Sie, ob die Voraussetzungen zum Hinzufügen eines Microsoft Azure Cloud Kontos erfüllt sind.. Weitere Informationen finden Sie unter Voraussetzung zum Hinzufügen eines Microsoft Azure Cloud Kontos.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Erstellen eines Plans mit einem Sicherungstask

Ein Plan umfasst verschiedene Arten von Tasks, die Sie ausführen möchten. Um einen Virtual Standby-Rechner zu erstellen, erstellen Sie einen Plan, der einen Sicherungstask und einen Virtual Standby-Task enthält. Ein Sicherungstask führt eine Sicherung der Quellknoten aus und speichert die Daten am angegebenen Ziel. Diese Sicherungsdaten werden von der Virtual Standby-Funktion verwendet und in ein Format für virtuelle Rechner konvertiert.

Weitere Informationen finden Sie unter Erstellen Sie einen Plan mit einem Sicherungs-Task.

Hinzufügen eines Virtual Standby-Tasks zum Plan

Erstellen Sie einen Virtual Standby to Azure-Task, sodass die Backup-Daten in ein VM-Format konvertiert werden und eine Virtual Machine erstellt wird. Die Virtual Standby-Funktion überwacht auch das Heartbeat-Signal des Quellknotens, damit der virtuelle Rechner umgehend übernimmt, wenn der Quellknoten ausfällt.

Hinweise:

- Virtual Standby kann Wiederherstellungspunkt-Snapshots von hostbasierten VM-Knoten und Knoten, die von einem Remote-Recovery Point Server repliziert wurden, nicht automatisch einschalten. Das automatische Einschalten ist auch nicht möglich, wenn die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird. Sie müssen Wiederherstellungspunkt-Snapshots für solche Knoten manuell einschalten.
- Wenn Sie den Plan unterbrechen, wird der Virtual Standby-Job nicht gestartet. Wenn Sie den Plan wieder aufnehmen, wird der Virtual Standby-Job nicht automatisch fortgesetzt. Sie müssen einen anderen Sicherungsjob manuell ausführen, damit der Virtual Standby-Job gestartet wird. Darüber hinaus ist die Option "Virtual Standby unterbrechen/wiederaufnehmen" nicht verfügbar, wenn der Plan unterbrochen ist. Wenn der virtuelle Rechner nach einer Unterbrechung des Plans nicht automatisch starten soll, müssen Sie das Heartbeat-Signal für die Knoten manuell unterbrechen.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Fensterbereich auf **Task hinzufügen**.

   Ein neuer Task wird im linken Fensterbereich hinzugefügt.

2. Wählen Sie im Drop-down-Menü **Tasktyp** die Option **Virtual Standby** aus.

   Der Virtual Standby-Task wird hinzugefügt.

3. Wählen Sie auf der Registerkarte **Quelle** eine Quelle für den Virtual Standby-Task aus.

4. Klicken Sie auf die Registerkarte **Virtualisierungsserver**, und geben Sie die Details für Virtualisierungsserver und Überwachungsserver ein.

   Virtualisierungstyp – Azure

   Virtualisierungstyp

   Azure als Virtualisierungstyp angeben.

   Kontoname

Ein bestehendes Azure-Konto auswählen Sie können auch ein neues Konto hinzufügen, indem Sie auf **Hinzufügen** klicken.

Weitere Informationen finden Sie unter So fügen Sie ein Cloud-Konto hinzu.

Ressourcengruppe

Geben Sie eine Ressourcengruppe an. Sie sollten eine Ressourcengruppe in Azure haben.

Eine Anleitung hierzu finden Sie unter Ressourcengruppe in Azure in der Microsoft-Dokumentation.

Region

Wählen Sie den Azure-Bereich, wo Ihre Standby-VM gespeichert werden soll. Weitere Informationen zum Bereich finden Sie unter Bereiche in Azure.

Monitor

Legen Sie den Hostnamen des Servers fest, der den Status des Quellservers überwacht.

Hinweise:

- Sie können einem beliebigen physischen Computer oder virtuellen Rechner als Überwachungsserver verwenden.
- Sie können nicht den Sicherungsquellserver als Überwachungsserver verwenden.
- Der Überwachungsserver ist nicht erforderlich, wenn die Knoten von einem Remote-Recovery Point Server repliziert wurden oder die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird.
- Sie müssen den Überwachungsserver nicht konfigurieren, wenn die Virtual Standby-Quelle Replikationstask ist und sich der Replikationsziel-RPS-Server in Azure befindet.

Benutzername

Geben Sie den Benutzernamen für die Anmeldung beim Überwachungssystem an.

Kennwort

Geben Sie das Kennwort für den Benutzernamen für die Anmeldung beim Überwachungssystem an.

Protokoll

Geben Sie HTTP oder HTTPS als das Protokoll an, das Sie für die Kommunikation zwischen dem Arcserve Unified Data Protection und dem Überwachungsserver verwenden möchten.

Port

Geben Sie den Port an, den Sie für die Datenübertragung zwischen demArcserve Unified Data Protection und dem Überwachungsserver verwenden möchten..

5. Klicken Sie auf die Registerkarte **Virtueller Rechner**, und geben Sie die Details für VM-Grundeinstellungen, VM-Datenspeicher für VMware, VM-Pfad für Hyper-V und VM-Netzwerk ein.

Präfix des Namens des virtuellen Rechners

Geben Sie das Präfix an, das Sie dem Anzeigenamen für den virtuellen Rechner auf Azure hinzufügen möchten.

Standardwert: UDPVM_

Wiederherstellungspunkt-Snapshots

Geben Sie die Anzahl an Wiederherstellungspunkt-Snapshots (Wiederherstellungspunkten) für den virtuellen Standby-Rechner an. Die maximale Anzahl von Wiederherstellungspunkt-Snapshots ist 29 für Azure.

Standardwert: 5

Kombinieren Sie alle unkonvertierten Sitzungen in Wiederherstellungspunkt-Snapshots.

Geben Sie an, ob alle unkonvertierten Sitzungen in einem einzigen Wiederherstellungspunkt-Snapshot kombiniert werden sollen, wenn der nächste geplante VSB-Auftrag stattfindet.

Standard: Ausgewählt

Größe des virtuellen Rechners

Microsoft Azure bietet eine große Auswahl an Größen virtueller Rechner an, die für verschiedene Nutzungsfälle optimiert wurden. Sie haben unterschiedliche Kombinationen von CPU, Arbeitsspeicher, Speicher und Netzwerkkapazität. Weitere Informationen zu Größen virtueller Rechner und wie sie Ihren PC-Anforderungen entsprechen, finden Sie bei den Größen fürVirtuelle Windows-Rechner in Azure.

Speicherkontoname

Wählen Sie ein Speicherkonto. Sie müssen einen Speicherkontonamen in Azure haben. Wählen Sie als Speicherkonto entweder "Speicher" (allgemein v1) oder

"Speicher V2" (allgemein v2). Weitere Informationen finden Sie unter Speicherkonto in Azure in der Microsoft-Dokumentation.

Virtuelles Netzwerk

Wählen Sie ein virtuelles Netzwerk. Sie sollten ein virtuelles Netzwerk in Azure haben. Weitere Informationen finden Sie unter Virtuelles Netzwerk in Azure in der Microsoft-Dokumentation.

Subnetz

Wählen Sie ein Subnetz je nach ausgewähltem virtuellen Netzwerk. Sie sollten ein Subnetz in Azure haben. Weitere Informationen finden Sie unter Subnetz in Azure in der Microsoft-Dokumentation.

Netzwerk-Sicherheitsgruppe

Wählen Sie eine Netzwerk-Sicherheitsgruppe. Sie sollten eine Netzwerk-Sicherheitsgruppe in Azure haben. Konfigurieren Sie die Regeln der Sicherheitsgruppe zum Öffnen der verknüpften Ports, darunter 3389 für Remote-Desktop, 8014, 8015 für Arcserve UDP Kommunikation. Eine Anleitung hierzu finden Sie unter Netzwerk-Sicherheitsgruppe in der Microsoft-Dokumentation.

Automatische Zuweisung einer öffentlichen IP-Adresse aktivieren

Wenn die automatische Zuweisung einer öffentlichen IP-Adresse aktiviert ist, wird die öffentliche IP-Adresse der Standby-VM automatisch zugewiesen, wenn sie in Azure gestartet ist.

6. Klicken Sie auf die Registerkarte **Erweitert**, und geben Sie folgende Details an:

Virtuellen Rechner automatisch starten

Geben Sie an, ob Sie den virtuellen Rechner automatisch starten möchten.

Hinweis: Diese Option ist nicht verfügbar für hostbasierte VM-Knoten und Knoten, die von einem Remote-Wiederherstellungspunktserver repliziert werden und die Quelle des Virtual Standby-Tasks ist diejenige, die an einen anderen Standort repliziert wird. Die Virtual Standby-Quelle ist der Replikationstask und der Replikationsziel-RPS-Server in Azure.

Zeitlimit

Geben Sie an, wie lange der Überwachungsserver auf ein Heartbeat-Signal warten muss, bevor er einen Wiederherstellungspunkt-Snapshot einschaltet.

Häufigkeit

Legen Sie die Häufigkeit fest, mit der der Quellserver ein Heartbeat-Signal an den Überwachungsserver sendet.

Beispiel: Der festgelegte Wert für das Zeitlimit ist 60. Der festgelegte Häufigkeitswert ist 10. Der Quellserver sendet Heartbeat-Signale in 10-Sekunden-Intervallen. Wenn der Überwachungsserver innerhalb von 60 Sekunden nach dem letzten erkannten Heartbeat-Signal kein Heartbeat-Signal erkennt, schaltet der Überwachungsserver unter Verwendung des letzten Wiederherstellungspunkt-Snapshot einen virtuellen Rechner ein.

Jobparameter anpassen

Sie können Jobparameter für die folgenden Optionen anpassen:

- *Anzahl der Threads, die für jeden Auftrag hochladen*: Standardwert: 4
- *Puffergröße für jeden Thread*: Standardwert: 4096 KB

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu erhalten, abhängig von den Einstellungen, die Sie angeben. Wenn Sie diese Option auswählen, werden weitere Kategorien der E-Mail-Alerts für Ihre Auswahl aktiviert.

- **Fehlendes Heartbeat-Signal für Quellrechner**: Virtual Standby sendet Alert-Benachrichtigungen, wenn der Überwachungsserver kein Heartbeat-Signal vom Quellserver erkennt.

  Hinweis: Für Knoten, die von einem Remote-Wiederherstellungspunktserver repliziert wurden oder wenn die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird, ist diese Option nicht verfügbar.

- **VM eingeschaltet für Quellrechner, der mit automatischer Einschaltung konfiguriert ist**: Virtual Standby sendet Alert-Benachrichtigungen, wenn ein virtueller Rechner in Betrieb genommen wird, der so konfiguriert wurde, dass eine automatische Inbetriebnahme erfolgt, wenn kein Heartbeat-Signal entdeckt wird.

  Hinweis: Für Knoten, die von einem Remote-Wiederherstellungspunktserver repliziert wurden oder wenn die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird, ist diese Option nicht verfügbar. Für hostbasierte Knoten eines virtuellen Rechners ist diese Option ebenfalls nicht verfügbar.

- **VM eingeschaltet für Quellrechner, der mit manueller Einschaltung konfiguriert ist**: Virtual Standby sendet Alert-Benachrichtigungen, wenn ein virtueller Rechner manuell eingeschaltet wird.

- **Virtual Standby-Fehler/-Ausfall/-Absturz**: Virtual Standby sendet Alert-Benachrichtigungen, wenn ein Fehler entdeckt wird, der während des Konvertierungsprozesses aufgetreten ist.
- **Virtual-Standby-Erfolg**: Virtual Standby sendet Alert-Benachrichtigungen, wenn festgestellt wird, dass der virtuelle Rechner erfolgreich eingeschaltet wurde.
- **Virtual Standby wurde nicht erfolgreich vom Wiederherstellungspunkt-Snapshot gestartet**: Virtual Standby sendet Alert-Benachrichtigungen, wenn festgestellt wird, dass ein virtueller Rechner nicht automatisch eingeschaltet wurde und die Option zur Aushilfswiederherstellung "Virtuellen Rechner automatisch starten" aktiviert ist.

7. Klicken Sie auf **Speichern**.

   Die Änderungen werden gespeichert, und der Virtual Standby-Task wird automatisch auf dem Virtual Standby-Server bereitgestellt.

   Hinweis: Wenn der Virtual Standby-Task abgeschlossen ist, wird das VM-Standby-Volume erstellt. Der virtuelle Standby-Rechner wird erst erstellt, nachdem der virtuelle Rechner von Arcserve UDP eingeschaltet wurde.

   Sie haben den Virtual Standby to Azure-Plan erfolgreich erstellt und angewandt.

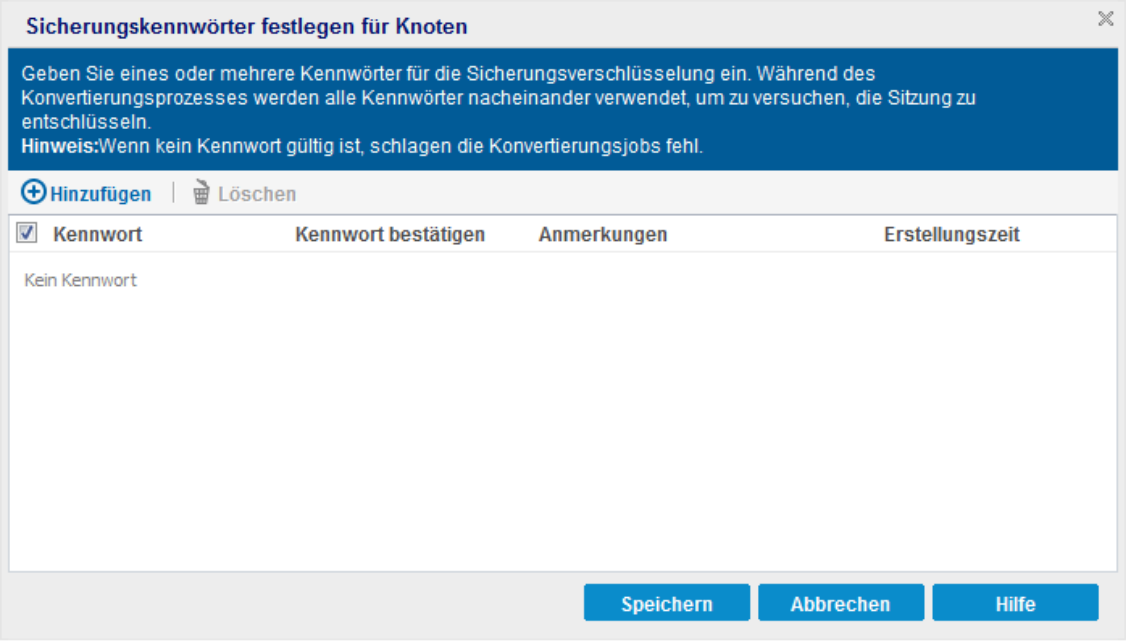
Festlegen von Sicherungskennwörtern für einen oder mehrere Knoten

Um sicherzustellen, dass der Konverter die Snapshots der replizierten Wiederherstellungspunkte konvertieren kann, können Sie in Virtual Standby Sicherungskennwörter für die Daten angeben, die der Konverter verwenden kann, um die Daten zu konvertieren.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.
3. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Sicherungskennwörter festlegen**.

   Das Dialogfeld **Sicherungskennwörter festlegen für Knoten** wird geöffnet.

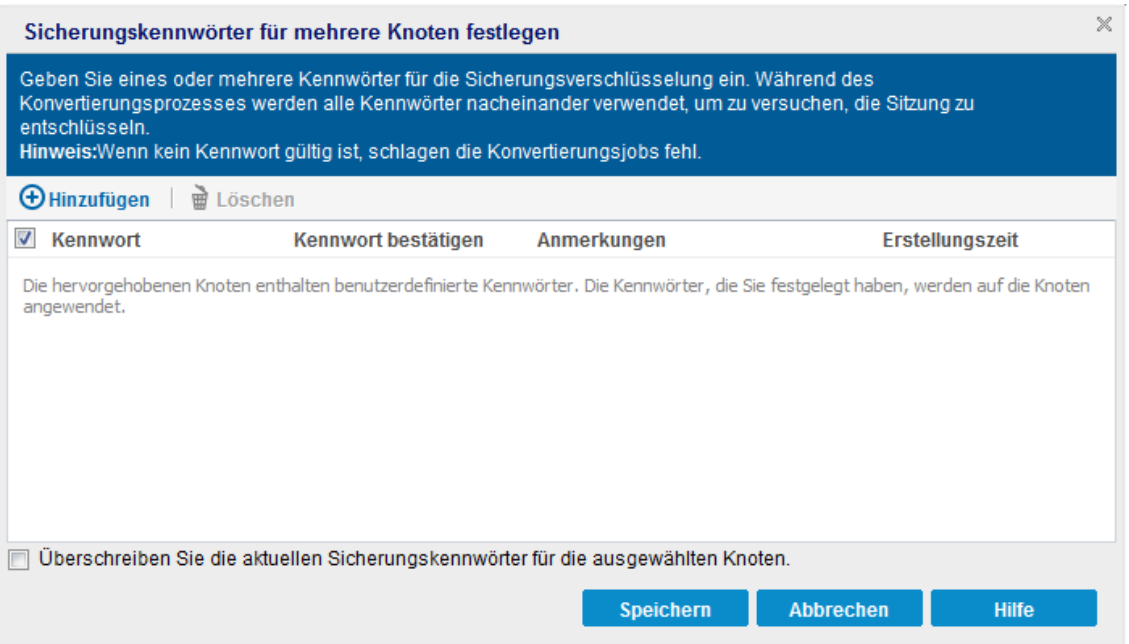


4. Führen Sie im Dialogfeld **Sicherungskennwörter festlegen** folgende Tasks für einen oder mehrere Knoten aus:

   Hinzufügen: Klicken Sie auf **Hinzufügen**, um Sicherungskennwörter zu den ausgewählten Knoten hinzuzufügen.

   Löschen: Klicken Sie auf **Löschen**, um Sicherungskennwörter aus den ausgewählten Knoten zu löschen.

Hinweis: Sie können die aktuellen Sicherungskennwörter für mehrere Knoten überschreiben, indem Sie das Kontrollkästchen **Überschreiben Sie die aktuellen Sicherungskennwörter für die ausgewählten Knoten** aktivieren.



5. Klicken Sie auf **Speichern**.

   Das Dialogfeld wird geschlossen und die Sicherungskennwörter wurden für die ausgewählten Remote-Knoten festgelegt.

(Optional) Manuelles Ausführen des Virtual Standby-Jobs

Um einen Virtual Standby-Job manuell auszuführen, müssen Sie zunächst eine manuelle Sicherung ausführen. Der Virtual Standby-Task wird mit einem Sicherungstask verknüpft. Wenn ein Plan einen Sicherungstask und einen Virtual Standby-Task enthält und Sie den Sicherungsjob manuell ausführen, wird der Virtual Standby-Job nach dem Abschluss des Sicherungsjobs automatisch ausgeführt.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte "**Ressourcen**".
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Zeigt die Pläne an, die Sie hinzugefügt haben.
3. Wählen Sie die Knoten aus, die gesichert werden sollen. Dem ausgewählten Knoten muss ein Plan zugewiesen sein.
4. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Jetzt sichern**.

   Das Dialogfeld **Sicherung jetzt ausführen** wird geöffnet.
5. Wählen Sie den Sicherungstyp aus, und geben Sie einen Namen für den Sicherungsjob an.
6. Klicken Sie auf **OK**.

   Der Sicherungsjob wird ausgeführt.

   Der Virtual Standby-Job wird sofort nach dem Sicherungsjob ausgeführt.

   Der Virtual Standby-Job wird manuell ausgeführt.

Aussetzen und Wiederaufnehmen von Heartbeat-Signalen

Mit der Arcserve Unified Data Protection-Lösung können Sie Heartbeat-Signale, die vom Überwachungsserver erkannt werden, unterbrechen und wiederaufnehmen. Beim Heartbeat-Signal handelt es sich um den Prozess, über den sich Quellserver und Überwachungsserver über den Zustand des Quellservers austauschen. Wenn der Überwachungsserver nach Ablauf eines festgelegten Zeitraums kein Heartbeat-Signal erkennt, stellt die Virtual Standby-Funktion den virtuellen Rechner bereit, damit dieser als Quellknoten fungiert.

Beispiele: Situationen zum Aussetzen oder Wiederaufnehmen von Heartbeat-Signalen

Die folgenden Beispiele beschreiben, wann Sie Heartbeat-Signale aussetzen und wann Sie sie fortsetzen sollten:

- Setzen Sie das Heartbeat-Signal aus, wenn Sie einen Knoten (Quellserver) für Wartungszwecke offline stellen möchten.
- Nehmen Sie das Heartbeat-Signal wieder auf, wenn die Wartungsaufgaben abgeschlossen sind und der Knoten (Quellserver) wieder online ist.

Beachten Sie Folgendes:

- Sie können Heartbeat-Signale auf Gruppenebene oder für einzelne Knoten aussetzen und wiederaufnehmen.
- Sie können Heartbeat-Signale für einen oder mehrere Knoten in einem Schritt aussetzen und wiederaufnehmen.
- Die Arcserve Unified Data Protection
- Wenn Sie ein Upgrade von Agent-Installationen auf Quellknoten durchführen, unterbricht Arcserve Unified Data Protection Um sicherzustellen, dass Überwachungsserver die Knoten, für die ein Upgrade durchgeführt wurde, überwachen, nehmen Sie das Heartbeat-Signal für die Knoten wieder auf, nachdem die Upgrades abgeschlossen wurden.

Gehen Sie wie folgt vor:

1. Melden Sie sich unter Arcserve Unified Data Protectionan.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Navigieren Sie im linken Fensterbereich zu **Virtual Standby** und klicken Sie auf **Alle Knoten**.

   Wenn Sie Knoten hinzugefügt haben, werden diese Knoten im mittleren Fensterbereich angezeigt.

4. Wählen Sie den Knoten aus, den Sie unterbrechen oder wiederaufnehmen möchten.
5. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Heartbeat-Signal**, **Unterbrechen** oder **Fortsetzen**.

   Das Heartbeat-Signal des ausgewählten Knotens wird unterbrochen bzw. wiederaufgenommen.

Unterbrechen und Wiederaufnehmen eines Virtual Standby-Jobs

Virtuelle Konvertierung ist der Prozess, bei dem Virtual Standby die Arcserve Unified Data Protection-Wiederherstellungspunkte von Quellknoten in Formate für virtuelle Rechner konvertiert, die als Wiederherstellungspunkt-Snapshots bezeichnet werden. Wenn es einen Fehler auf einem Quellknoten gibt, verwendet die Virtual Standby-Funktion die Wiederherstellungspunkt-Snapshots, um einen virtuellen Rechner für den Quellknoten in Betrieb zu nehmen.

Die Best Practice besteht darin, zuzulassen, dass der virtuelle Konvertierungsprozess kontinuierlich in Betrieb ist. Wenn Sie den virtuellen Konvertierungsprozess jedoch auf lokalen und Remote-Virtual Standby-Servern vorübergehend unterbrechen möchten, können Sie dies über die Konsole tun. Nachdem Sie die Probleme auf dem Quellknoten behoben haben, können Sie den virtuellen Konvertierungsprozess wieder aufnehmen.

Wenn Sie Virtual Standby-Jobs (Konvertierungsjobs) unterbrechen, wird der Konvertierungsjob, der gegenwärtig durchgeführt wird, nicht unterbrochen. Der Unterbrechungsvorgang bezieht sich auf nur den Job, dessen Ausführung nach Beendigung des nächsten Sicherungsjobs erwartet wird. Dadurch startet der nächste Konvertierungsjob nicht, bis Sie den (unterbrochenen) Konvertierungsjob ausdrücklich wiederaufnehmen.

Wenn Sie Virtual Standby für Knoten wiederaufnehmen und wenn mehrere Sicherungssitzungen ohne Wiederherstellungspunkt-Snapshot vorhanden sind, dann wird ein Dialogfeld angezeigt, in dem Sie die Smart Copy-Option auswählen können. Wenn Sie auf "Ja" klicken, konvertiert Virtual Standby die kombinierte Sitzung in einen einzelnen Wiederherstellungspunkt-Snapshot. Wenn Sie auf "Nein" klicken, konvertiert Virtual Standby jede Sitzung einzeln

Hinweis: Optional können Sie Virtual Standby-Jobs direkt von den Knoten aus unterbrechen und wiederaufnehmen. Weitere Informationen finden Sie unter "Unterbrechen und Wiederaufnehmen von Virtual Standby-Jobs von den Knoten".

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Navigieren Sie im linken Fensterbereich zu "**Virtual Standby**", und klicken Sie auf "**Alle Knoten**".

Wenn Sie Knoten hinzugefügt haben, werden diese Knoten im mittleren Fensterbereich angezeigt.

4. Wählen Sie den Knoten aus, den Sie unterbrechen oder wiederaufnehmen möchten.
5. Klicken Sie im mittleren Fensterbereich auf "**Aktionen**", "**Virtual Standby**", "**Unterbrechen**" oder "**Fortsetzen**".

   Die Virtual Standby-Funktion für den ausgewählten Knoten wird unterbrochen oder wiederaufgenommen.

Überprüfen des Plans

Um Ihre Virtual Standby-Funktion zu überprüfen, stellen Sie sicher, dass Sie den Virtual Standby-Plan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Nachdem der Sicherungsjob erfolgreich abgeschlossen wurde, wird der Virtual Standby-Job ausgeführt. Sie können den Status des Sicherungsjobs und Virtual Standby-Jobs in der Registerkarte **Jobs** überprüfen.

Folgen Sie diesen Schritten, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Folgen Sie diesen Schritten, um Virtual Standby-Jobs zu überprüfen:

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob und der Virtual Standby-Job erfolgreich ausgeführt werden.

   Der Plan für Virtual Standby wurde erfolgreich überprüft.

   Der Virtual Standby-Rechner wurde erstellt.

Erstellen eines Virtual Standby-Plans

Virtual Standby konvertiert die Wiederherstellungspunkte in Formate für virtuelle Rechner und bereitet einen Snapshot vor, damit Ihre Daten bei Bedarf auf einfache Weise wiederhergestellt werden können. Diese Funktion deckt auch die Hochverfügbarkeitsfunktion ab und stellt sicher, dass der virtuelle Rechner sofort übernehmen kann, wenn der Quellrechner ausfällt. Der virtuelle Standby-Rechner wird erstellt, indem die Wiederherstellungspunkte in ein VMware- oder Hyper-V-Format für virtuelle Rechner konvertiert werden.

Hinweis: Der Virtual Standby-Task wird nur ausgeführt, wenn der Sicherungstask einen gültigen Snapshot des Wiederherstellungspunkts erstellt. Wenn der Sicherungstask fehlschlägt, dann wird der Virtual Standby-Task übersprungen.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen eines Plans mit einem Sicherungstask
3. Hinzufügen eines Virtual Standby-Tasks zum Plan
4. (Optional) Manuelles Ausführen des Virtual Standby-Jobs
5. Unterbrechen und Wiederaufnehmen des Heartbeat-Signals
6. Unterbrechen und Wiederaufnehmen des Virtual Standby-Jobs
7. Überprüfen des Plans

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich bei der Konsole an.
- Wenn Sie die Sicherungsdaten auf Recovery Point Servern speichern möchten, installieren Sie die Serverkomponente, und erstellen Sie Datenspeicher.
- Sie haben einen gültigen Wiederherstellungspunkt, um einen Virtual Standby-Rechner zu erstellen. Die Wiederherstellungspunkte können aus folgenden Tasks stammen:
  - Sicherung: agentenbasiert, Windows
  - Sicherung: hostbasiert, agentenlos
  - Replizieren
  - Replizieren von einem Remote-Recovery Point Server
- Sichern des gesamten Rechners, um Virtual Standby-Task zu aktivieren. Sie können einen Virtual Standby-Task nicht erstellen, wenn es sich bei der Sicherung nicht um eine vollständige Sicherung handelt.
- Überprüfen Sie, ob Sie jeweils über die Mindestberechtigung zur Durchführung der erforderlichen VSB-Tasks verfügen. Weitere Informationen finden Sie unter Erforderliche Mindestberechtigungen für VSB-Tasks.
- Virtual Standby wird für Linux-Quellen nicht unterstützt. Eine Liste der unterstützten Betriebssysteme, Datenbanken und Browser finden Sie in der Kompatibilitätsmatrix.

Besondere Aspekte:

- Virtual Standby verwendet Thin Provisioning-Datenträger für vSphere.
- Virtual Standby verwendet virtuelle Festplatten mit dynamischer Erweiterung für Hyper-V.
- VMware verwendet einen separaten Rechner als Überwachungsserver mit installiertem Agenten.
- Hyper-V fungiert selbst als Überwachungsserver mit installiertem Agenten.

Hinweis: Als Best Practice wird empfohlen, Dateien vom Antivirusscanning auszuschließen, um sicherzustellen, dass Virtual Standby ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter Ausschließen von Dateien vom Antivirusscanning.

Erforderliche Mindestberechtigungen für VSB-Tasks

In der Tabelle sind die für die einzelnen VSB-Tasks erforderlichen Mindestberechtigungen aufgeführt.

Hinweis: Berechtigungen des Typs "Global" werden auf vCenter-Ebene festgelegt.

Tasks	Berechtigung
Datenspeicher	Speicherplatz zuweisen
	Datenspeicher durchsuchen
	Dateioperationen auf niedriger Ebene
Global	Methoden deaktivieren
	Methoden aktivieren
	Lizenzen
Host > Konfiguration	Speicherpartitionen konfigurieren
Netzwerk	Netzwerk zuweisen
Resource	Ressourcenpool virtuellen Rechner zuweisen
Virtueller Rechner > Konfiguration	Vorhandenen Datenträger hinzufügen
	Neuen Datenträger hinzufügen
	Gerät hinzufügen oder entfernen
	Erweitert
	CPU-Anzahl ändern
	Verfolgen von Datenträgeränderungen
	Arbeitsspeicher
Virtueller Rechner > Interaktion	Ausschalten
	Einschalten
	Konsoleninteraktion
Virtueller Rechner > Bestand	Aus vorhandenem erstellen
	Neu erstellen
	Entfernen
Virtueller Rechner > Bereitstellung	Festplattenzugriff erlauben
	Schreibgeschützten Datenträger-Zugriff erlauben
	Download durch virtuellen Rechner erlauben
Virtueller Rechner > Snapshot-Verwaltung	Snapshot erstellen
	Snapshot entfernen
	Auf Snapshot zurücksetzen

Erstellen eines Plans mit einem Sicherungstask

Ein Plan umfasst verschiedene Arten von Tasks, die Sie ausführen möchten. Um einen Virtual Standby-Rechner zu erstellen, erstellen Sie einen Plan, der einen Sicherungstask und einen Virtual Standby-Task enthält. Ein Sicherungstask führt eine Sicherung der Quellknoten aus und speichert die Daten am angegebenen Ziel. Die Virtual Standby-Funktion verwendet die Sicherungsdaten und konvertiert sie in ein Format für virtuelle Rechner.

Sie können einen Virtual Standby-Rechner aus einer Agent-basierten Windows-Sicherung oder aus einer hostbasierten Sicherung ohne Agent erstellen. Sie können auch einen Virtual Standby-Rechner aus Daten erstellen, die mithilfe des **Replikationstasks** repliziert werden. Folgender Vorgang ist ein Beispiel für die Erstellung einer Agent-basierten Windows-Sicherung.

Hinweise:

- Weitere Informationen zu hostbasierten agentenlosen Sicherungen finden Sie unter Erstellen eines Sicherungsplans für hostbasierte virtuelle Rechner.
- Weitere Informationen zur Replikation von Sicherungsdaten finden Sie unter Replizieren von Daten zwischen Datenspeichern, die von einer UDP-Konsole verwaltet werden und die von unterschiedlichen UDP-Konsolen verwaltet werden.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

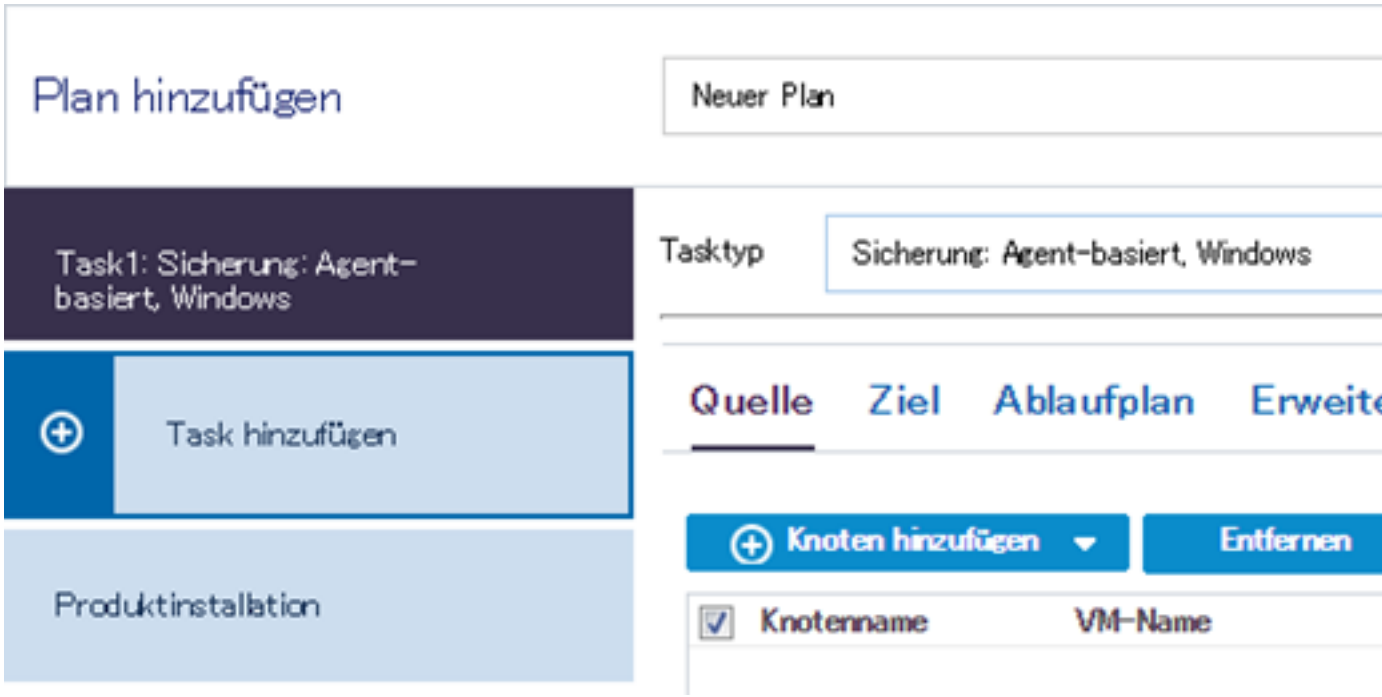
   Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen

Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.

6. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Sicherung, Agent-basiertes Windows** aus.



Geben Sie nun Quelle, Ziel, Zeitplan und Erweitert-Details an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die Quellknoten angeben, die Sie schützen möchten. Sie können mehrere Knoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Knoten hinzufügen, wenn Sie einen Plan auf der Quellenseite erstellen oder ändern. Sie können einen Plan auch speichern, ohne Quellknoten hinzuzufügen. Der Plan wird erst bereitgestellt, wenn Sie Quellknoten hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Quelle" auf **Hinzufügen**.
2. Wählen Sie eine der folgenden Optionen:

   Wählen Sie zu sichernden Knoten in Arcserve UDP aus

   Öffnet das Dialogfeld "Wählen Sie zu sichernden Knoten in Arcserve UDP aus". Wählen Sie die Knoten in der angezeigten Liste aus. Wählen Sie diese Option aus, wenn Sie die Knoten bereits zu der Konsole hinzugefügt haben.

   Windows-Knoten hinzufügen

   Öffnet das Dialogfeld "Knoten zu Plan hinzufügen". Wählen Sie diese Option aus, wenn Sie die Knoten nicht hinzugefügt haben und Sie die zu schützenden Knoten manuell hinzufügen möchten.

   Knoten aus Active Directory erkennen

   Öffnet das Dialogfeld Knoten zu Arcserve UDP-Konsole hinzufügen. Wählen Sie diese Option, wenn Sie Knoten aus Active Directory erkennen und hinzufügen möchten.

3. Wenn Sie die Option **Wählen Sie zu sichernden Knoten in Arcserve UDP aus** ausgewählt haben, gehen Sie im Dialogfeld "Zu schützende Knoten auswählen" folgendermaßen vor:

   a. (Optional) Wählen Sie einen Filter aus der Dropdown-Liste "Gruppen" aus, um nach Knoten zu filtern. Sie können Schlüsselwörter eingeben, um den Knotenfilter weiter einzuschränken.

      Die Knoten werden in der Spalte "Verfügbare Knoten" angezeigt.

   b. Wählen Sie die Knoten aus der Spalte "Verfügbare Knoten" aus, und klicken Sie dann auf den einfachen Nach-rechts-Pfeil (>) oder den doppelten Nach-rechts-Pfeil (>>), um die ausgewählten Knoten bzw. alle Knoten in die Spalte "Ausgewählte Knoten" zu verschieben.

Die Knoten werden in der Spalte "Ausgewählte Knoten" angezeigt.

c. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

4. Wählen Sie zum Festlegen des Schutztyps eine der folgenden Optionen aus:

Alle Volumes sichern

Bereitet einen Sicherungs-Snapshot aller Volumes vor.

Ausgewählte Volumes sichern

Bereitet einen Sicherungs-Snapshot des ausgewählten Volumes vor.

Die Sicherungsquelle ist nun angegeben.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Wählen Sie einen der folgenden **Zieltypen** aus:

   Lokaler Datenträger oder freigegebener Ordner

   Gibt an, dass das Sicherungsziel ein lokales Ziel oder ein freigegebener Ordner ist. Wenn Sie diese Option auswählen, können Sie Daten als Wiederherstellungspunkte oder Wiederherstellungssätze speichern. Die Optionen für Wiederherstellungspunkte und Wiederherstellungssätze sind auf der Registerkarte **Ablaufplan** verfügbar.

   Arcserve UDP-Recovery Point Server

   Gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.

2. Wenn Sie **Arcserve UDP-Recovery Point Server** ausgewählt haben, geben Sie folgende Details an:
   a. Wählen Sie einen Recovery Point Server aus.
   b. Wählen Sie einen Datenspeicher aus. Die Liste enthält alle Datenspeicher, die am angegebenen Recovery Point Server erstellt wurden.
   c. Geben Sie ein Sitzungskennwort ein.
   d. Bestätigen Sie das Sitzungskennwort.
3. Wenn Sie **Lokaler Datenträger oder freigegebener Ordner** ausgewählt haben, geben Sie folgende Details an:
   a. Geben Sie den vollständigen Pfad des lokalen Ziels oder Netzwerkziels an. Geben Sie für das Netzwerkziel Anmeldeinformationen für ein Konto mit Schreibzugriff an.
   b. Wählen Sie den Verschlüsselungsalgorithmus aus. Weitere Informationen finden Sie unter Verschlüsselungseinstellungen.
   c. Geben Sie optional ein Verschlüsselungskennwort an.
   d. Bestätigen Sie das Verschlüsselungskennwort.

e. Wählen Sie einen Komprimierungstyp aus. Weitere Informationen finden Sie unter "Komprimierungstyp".

Hinweis: Wenn Sie die Daten auf einem lokalen Datenträger oder in einem freigegebenen Ordner speichern, können Sie die Daten nicht auf einem anderen Recovery Point Server replizieren. Die Replikation wird nur unterstützt, wenn Sie die Daten auf einem Recovery Point Server speichern.

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

Gehen Sie wie folgt vor:

1. (Optional) Wählen Sie die Option für die Verwaltung von Wiederherstellungspunkten aus. Diese Option ist nur sichtbar, wenn Sie als Sicherungsziel "Lokaler oder freigegebener Ordner" ausgewählt haben.

   Nach Wiederherstellungspunkten aufbewahren

   Die Sicherungsdaten werden als Wiederherstellungspunkte gespeichert.

   Nach Wiederherstellungssätzen aufbewahren

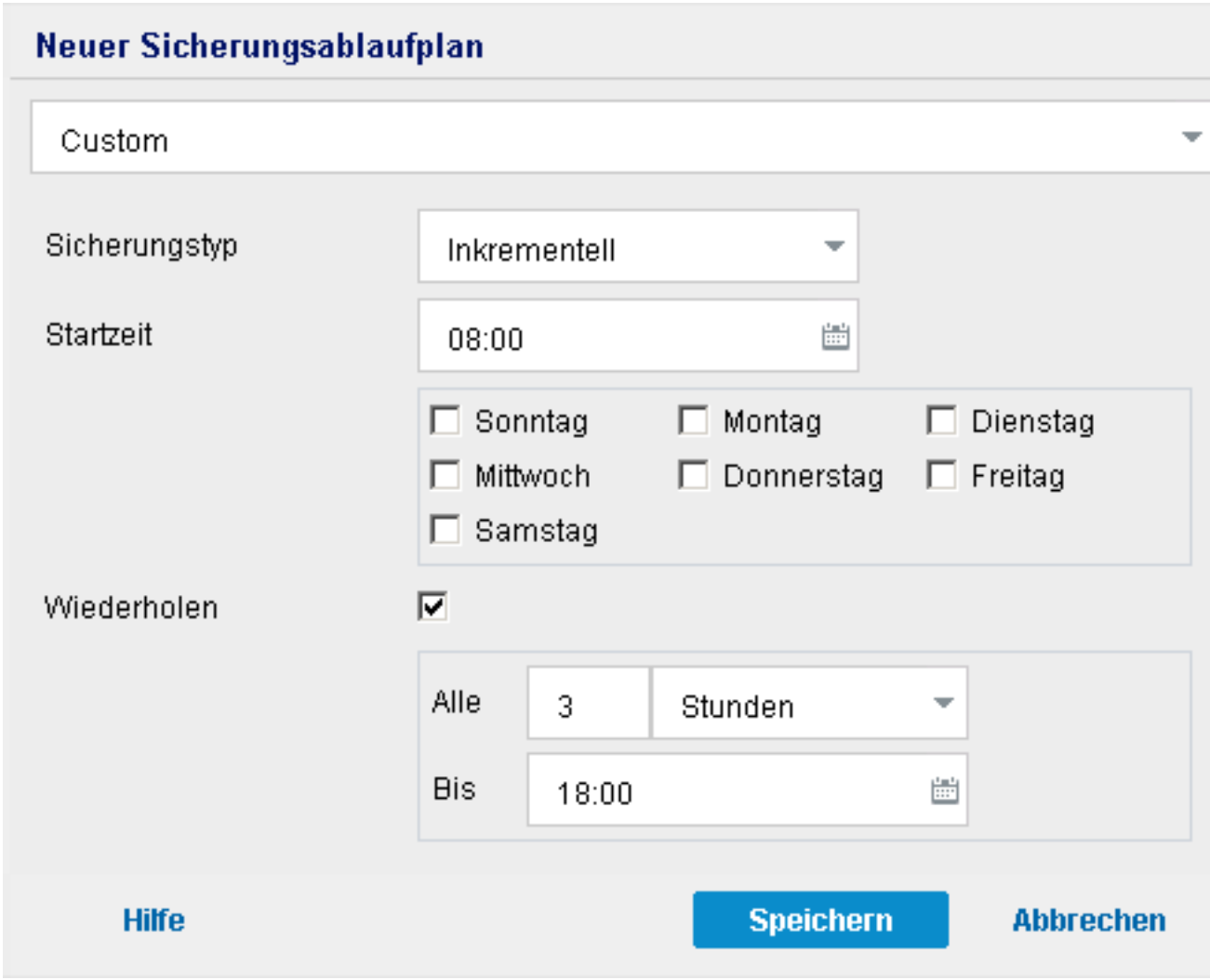
   Die Sicherungsdaten werden als Wiederherstellungssätze gespeichert.

2. Fügen Sie Ablaufpläne für Sicherungen, Zusammenführungen und Drosselungsvorgänge hinzu.

   Hinzufügen eines Sicherungsablaufplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Überprüfen

Legt den Ablaufplan für Überprüfungssicherungen fest.

Arcserve UDP überprüft die Gültigkeit und Vollständigkeit der geschützten Daten durch einen Vergleich des gespeicherten Sicherungs-Images mit der Sicherungsquelle. Im Bedarfsfall wird das Image neu synchronisiert. Bei einer Überprüfungssicherung wird die letzte Sicherung jedes einzelnen Blocks mit den Inhalten und Informationen der Quelle verglichen. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht (zumeist aufgrund von Änderungen seit der letzten Sicherung), aktualisiert Arcserve UDP die Sicherung dieses Blocks (Neusynchronisierung). In seltenen Fällen kann eine Überprüfungssicherung auch durchgeführt werden, um eine vollständige Sicherung zu erhalten, ohne den erforderlichen Speicherplatz einer vollständigen Sicherung zu verwenden.

Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteile: Die Sicherung benötigt viel Zeit, da alle Quellenblöcke mit den Blöcken der letzten Sicherung verglichen werden.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die seit der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf Hinzufügen, und wählen Sie Zusammenführungsplan hinzufügen aus.

Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

b. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

d. Klicken Sie auf **Speichern**.

Der Zusammenführungsablaufplan ist auf der Seite **Ablaufplan** angegeben und wird dort angezeigt.

Hinzufügen eines Drosselungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

Das Dialogfeld Drosselungsplan hinzufügen wird geöffnet.

b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

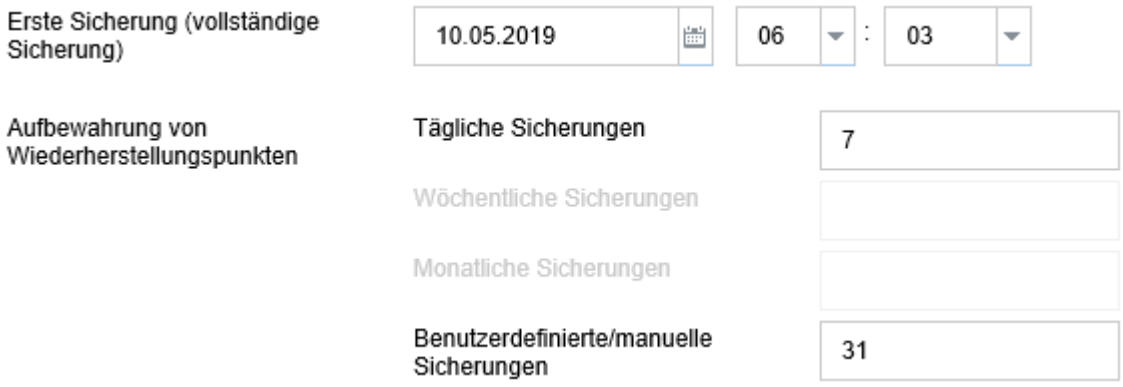
c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Drosselungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

3. Geben Sie die Startzeit für die geplante Sicherung an.



4. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld "Sicherungsablaufplan" übernommen.

5. Geben Sie die Katalogdetails an.

   Mit Katalogen können Sie den Dateisystemkatalog generieren. Der Dateisystemkatalog ist erforderlich, um schnellere und bessere Suchvorgänge auszuführen. Wenn Sie die Kontrollkästchen für den Katalog aktivieren, werden die Kataloge je nach der Sicherungsart, die Sie angegeben haben, aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Kataloggenerierung zu deaktivieren.

   Der Ablaufplan ist nun angegeben.

Funktionsweise der erweiterten Planung und Aufbewahrung

Mit der Ablaufplanoption können Sie einen benutzerdefinierten Ablaufplan, einen Ablaufplan für tägliche/wöchentliche/monatliche Sicherungen oder beides festlegen. Im benutzerdefinierten Ablaufplan können Sie den Sicherungsablaufplan für jeden Tag der Woche konfigurieren und bis zu vier Sicherungsablaufpläne für jeden Tag hinzufügen. Sie können einen bestimmten Wochentag auswählen und ein Zeitfenster erstellen, um anzugeben, wann und wie oft die Sicherung durchgeführt werden soll.

Ablaufplan	Unterstützter Job	Kommentare
Sichern	Sicherungsjob	Gibt Zeitfenster für die Ausführung von Sicherungsjobs an.
Sicherungsdrosselung	Sicherungsjob	Gibt die Zeitfenster an, um die Sicherungsgeschwindigkeit zu steuern.
Zusammenführen	Zusammenführungsjob	Gibt an, wann Zusammenführungsjobs ausgeführt werden sollen.
Täglicher Ablaufplan	Sicherungsjob	Gibt an, wann tägliche Sicherungsjobs ausgeführt werden sollen.
Wöchentlicher Ablaufplan	Sicherungsjob	Gibt an, wann wöchentliche Sicherungsjobs ausgeführt werden sollen.
Monatlicher Ablaufplan	Sicherungsjob	Gibt an, wann monatliche Sicherungsjobs ausgeführt werden sollen.

Sie können auch die Aufbewahrungseinstellungen für die Wiederherstellungspunkte angeben.

Hinweis: Legen Sie innerhalb der einzelnen Pläne Einstellungen für die Aufbewahrungszeit fest, um zu steuern, wie die Daten für die Knoten des entsprechenden Plans im Zieldatenspeicher aufbewahrt werden.

Ablaufpläne für tägliche/wöchentliche/monatliche Sicherungen sind vom benutzerdefinierten Ablaufplan und voneinander unabhängig. Sie können die Ausführung einer täglichen, wöchentlichen oder monatlichen Sicherung konfigurieren, ohne einen benutzerdefinierten Ablaufplan zu konfigurieren.

Jobplan der Sicherung

Sie können vier Zeitfenster pro Tag in Ihrem Sicherungsablaufplan hinzufügen. Ein gültiges Zeitfenster liegt im Bereich 12:00 Uhr bis 23:59 Uhr. Sie können kein Zeitfenster wie z. B. 18:00 Uhr bis 06:00 Uhr angeben. In solchen Fällen müssen Sie manuell zwei verschiedene Zeitfenster angeben.

Für jedes Zeitfenster wird die Startzeit einbezogen, und die Endzeit wird nicht einbezogen. Zum Beispiel haben Sie das Ausführen einer Zuwachssicherung konfiguriert, die stündlich zwischen 06:00 Uhr und 09:00 Uhr stattfinden soll, und die Sicherung wird um 06:00 Uhr gestartet. Das bedeutet, dass die Sicherung um 06:00 Uhr, 07:00 Uhr und 08:00 Uhr ausgeführt wird, NICHT aber um 09:00 Uhr.

Hinweis: Wenn Sie die Sicherung bis zum Ende des Tages wiederholt ausführen möchten, legen Sie den Ablaufplan bis 12:00 Uhr fest. Um den Sicherungsjob beispielsweise alle 15 Minuten während des gesamten Tages auszuführen, legen Sie den Ablaufplan von 00:00 Uhr bis 00:00 Uhr alle 15 Minuten fest.

Drosselungsplan der Sicherung

Mit dem Drosselungsplan der Sicherung können Sie die Geschwindigkeit des Sicherungsdurchsatzes steuern, die wiederum die Ressourcenverwendung (Datenträger-E/A, CPU, Netzwerkbandbreite) des Servers, der gesichert wird, steuert. Dies ist hilfreich, wenn die Serverleistung während der Geschäftszeiten nicht beeinträchtigt werden soll. Sie können vier Zeitfenster pro Tag in Ihrem Drosselungsplan der Sicherung hinzufügen. Für jedes Zeitfenster können Sie einen Wert in MB pro Minute angeben. Dieser Wert wird verwendet, um den Sicherungsdurchsatz zu steuern. Gültige Werte liegen im Bereich zwischen 1 MB/Minute bis 99.999 MB/Minute.

Wenn ein Sicherungsjob die angegebene Zeit überschreitet, dann wird das Drosselungslimit entsprechend dem angegebenen Zeitfenster angepasst. Zum Beispiel haben Sie als Drosselungslimit der Sicherung den Wert 500 MB/Minute von 08:00 Uhr bis 20:00 Uhr und 2500 MB/Minute von 20:00 Uhr bis 22:00 Uhr angegeben. Wenn ein Sicherungsjob um 19:00 Uhr startet und drei Stunden ausgeführt wird, dann hat das Drosselungslimit von 19:00 Uhr bis 20:00 Uhr den Wert 500 MB/Minute. Von 20:00 Uhr bis 22:00 Uhr hat das Drosselungslimit den Wert 2.500 MB/Minute.

Wenn Sie keinen Sicherungsablaufplan und keinen Ablaufplan für den Sicherungsdurchsatz angeben, dann wird die Sicherung so schnell wie möglich ausgeführt.

Ablaufplan für Zusammenführung

Ermöglicht es Ihnen, Wiederherstellungspunkte basierend auf dem angegebenen Ablaufplan zusammenzuführen.

Beachten Sie folgende Punkte für den Zusammenführungsjob:

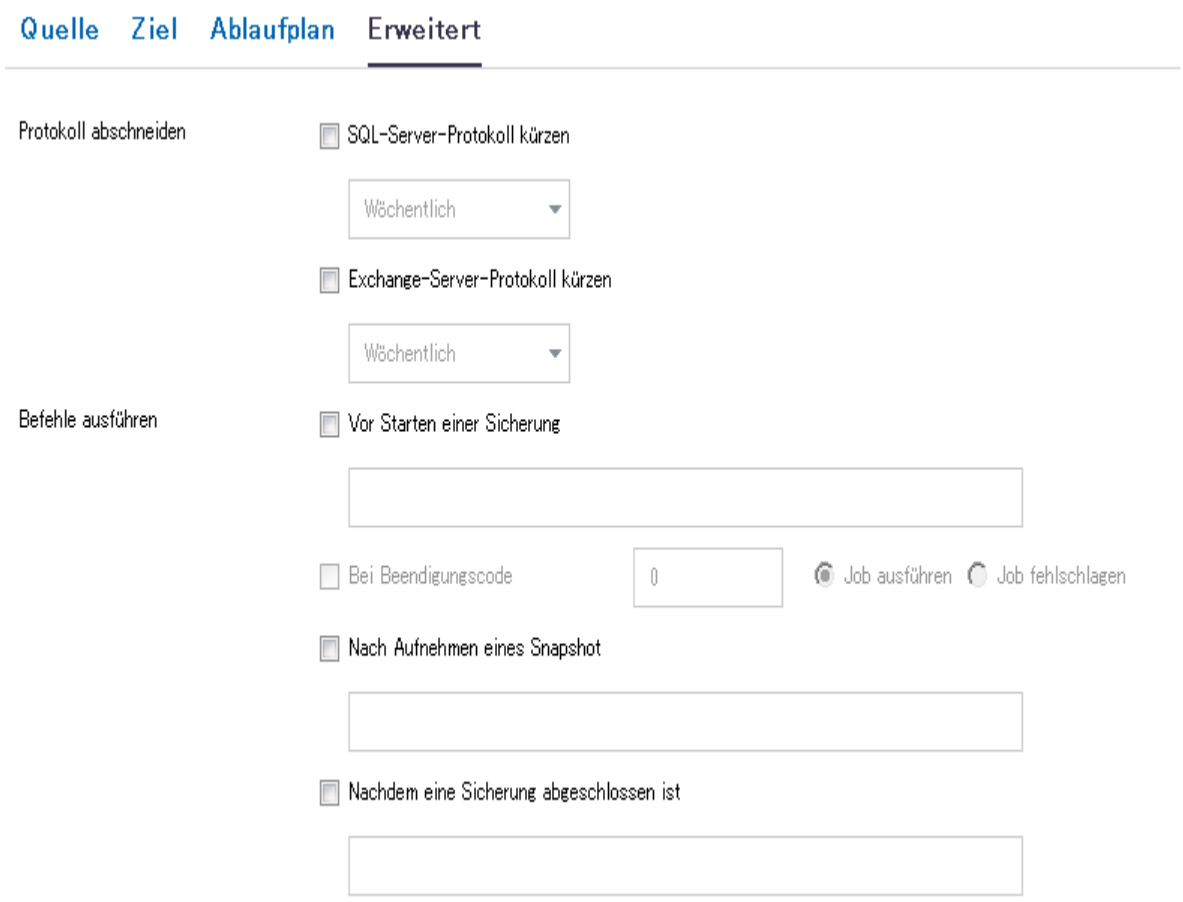
- Es kann immer nur ein Zusammenführungsjob für einen Knoten ausgeführt werden.

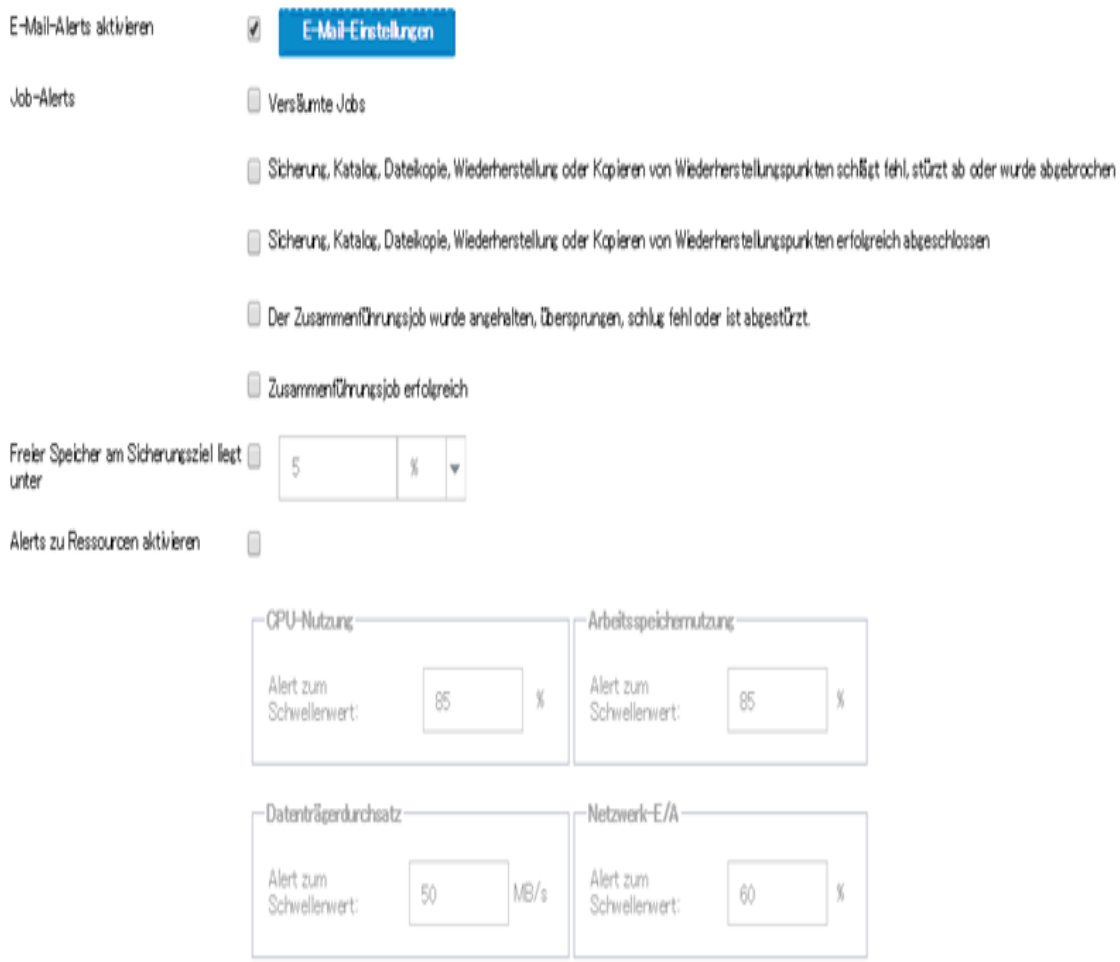
- Wenn ein Zusammenführungsjob gestartet wird, muss er abgeschlossen werden, bevor der nächste Zusammenführungsjob gestartet werden kann. Das bedeutet: Wenn ein oder mehrere Sätze an Wiederherstellungspunkten zusammengeführt werden, dann kann der neue Wiederherstellungspunkt nicht zu diesem Zusammenführungsprozess hinzugefügt werden, bis der Zusammenführungsprozess für den aktuellen Satz an Wiederherstellungspunkten abgeschlossen ist.
- Wenn ein Zusammenführungsjob mehr als einen Satz an Wiederherstellungspunkten bearbeitet (zum Beispiel Satz [1~4], Satz [5~11] und Satz [12~14], also drei Sätze), dann werden diese Sätze nacheinander vom Recovery Point Server bearbeitet.
- Wenn ein Zusammenführungsjob nach einer Pause fortgesetzt wird, erkennt der Job an welchem Punkt er unterbrochen wurde, und die Zusammenführung wird ab der Abbruchstelle fortgesetzt.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen die Einstellungen zum Abschneiden von Protokollen, das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte "Erweitert":





Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

   Protokoll abschneiden

   Ermöglicht es Ihnen, den Ablaufplan anzugeben, um Protokolle für SQL Server und Exchange Server zu kürzen. Sie können den Ablaufplan als **Täglich**, **Wöchentlich** oder **Monatlich** angeben.

   Benutzername

   Ermöglicht es Ihnen, den Benutzer anzugeben, der zur Ausführung eines Skripts autorisiert ist.

   Kennwort

   Ermöglicht es Ihnen, das Kennwort des Benutzers anzugeben, der zur Ausführung des Skripts autorisiert ist.

   Befehl ausführen, bevor eine Sicherung gestartet wird

Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, in dem das Skript gespeichert wird. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem ein Snapshot aufgenommen wurde

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungs-Snapshot aufgenommen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Arten der Alerts angeben, die Sie in Form von E-Mails empfangen möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers.

Job-Alerts

Ermöglicht es Ihnen, die Typen der Job-E-Mails auszuwählen, die Sie erhalten möchten.

Warnmeldungen zu Ressourcen aktivieren

Ermöglicht es Ihnen, einen Schwellenwert für CPU-Auslastung, Speicherverwendung, Datenträgerdurchsatz, Netzwerk-E/A anzugeben. Sie können den Wert in Prozent angeben. Sie erhalten eine E-Mail, wenn der Wert "Warnmeldung zum Schwellenwert" überschritten ist.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Knoten installiert ist und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung

an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agenten oder kein Agent installiert ist. Um den Agenten auf diesen Knoten zu installieren bzw. um ein Upgrade des Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus, und klicken Sie auf "Speichern".

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie eine andere Task hinzufügen müssen, müssen Sie den Plan aus der Registerkarte **Ressourcen** auswählen und den Plan ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern.

Der Sicherungsplan wird erstellt und automatisch für den Quellknoten bereitgestellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

Hinzufügen eines Virtual Standby-Tasks zum Plan

Erstellen Sie einen Virtual Standby-Task, damit die Sicherungsdaten in ein Format für virtuelle Rechner konvertiert werden und ein virtueller Rechner erstellt wird. Die Virtual Standby-Funktion überwacht auch das Heartbeat-Signal des Quellknotens, damit der virtuelle Rechner umgehend übernimmt, wenn der Quellknoten ausfällt.

Hinweise:

- Virtual Standby kann Wiederherstellungspunkt-Snapshots von hostbasierten VM-Knoten und Knoten, die von einem Remote-Recovery Point Server repliziert wurden, nicht automatisch einschalten. Das automatische Einschalten ist auch nicht möglich, wenn die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird. Sie müssen Wiederherstellungspunkt-Snapshots für solche Knoten manuell einschalten.
- Wenn Sie den Plan unterbrechen, wird der Virtual Standby-Job nicht gestartet. Wenn Sie den Plan wieder aufnehmen, wird der Virtual Standby-Job nicht automatisch fortgesetzt. Sie müssen einen anderen Sicherungsjob manuell ausführen, damit der Virtual Standby-Job gestartet wird. Darüber hinaus ist die Option "Virtual Standby unterbrechen/wiederaufnehmen" nicht verfügbar, wenn der Plan unterbrochen ist. Wenn der virtuelle Rechner nach einer Unterbrechung des Plans nicht automatisch starten soll, müssen Sie das Heartbeat-Signal für die Knoten manuell unterbrechen.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Fensterbereich auf **Task hinzufügen**.

   Ein neuer Task wird im linken Fensterbereich hinzugefügt.

2. Wählen Sie im Drop-down-Menü **Tasktyp** die Option **Virtual Standby** aus.

   Der Virtual Standby-Task wird hinzugefügt.

3. Wählen Sie auf der Registerkarte **Quelle** eine Quelle für den Virtual Standby-Task aus.

4. Klicken Sie auf die Registerkarte **Virtualisierungsserver**, und geben Sie die Details für Virtualisierungsserver und Überwachungsserver ein.

   Virtualisierungstyp: VMware

   ESX-Host/vCenter

   Legen Sie den Hostnamen des ESX- oder vCenter Server-Systems fest.

   Benutzername

Legen Sie den Benutzernamen fest, der für die Anmeldung beim VMware-System erforderlich ist.

Hinweis: Das Konto, das Sie angeben, muss ein administratives Konto oder ein Konto mit administrativen Berechtigungen für das ESX- oder vCenter Server-System sein.

Kennwort

Legen Sie das Kennwort für den Benutzernamen fest, das für die Anmeldung beim VMware-System erforderlich ist.

Protokoll

Geben Sie als Protokoll, das Sie für die Kommunikation zwischen dem Quellagenten von Arcserve Unified Data Protection und dem Überwachungsserver verwenden möchten, HTTP oder HTTPS an.

Port

Legen Sie den Port fest, den Sie für die Kommunikation zwischen dem Quellserver und dem Überwachungsserver verwenden möchten.

ESX-Knoten

Die Werte in diesem Feld variieren basierend auf dem Wert, der im Feld "ESX-Host/vCenter" angegeben wird:

ESX Server-Systeme

Wenn Sie im Feld "ESX-Host/vCenter" ein ESX Server-System angeben, wird in diesem Feld der Hostname des ESX Server-Systems angezeigt.

vCenter Server-Systeme

Wenn Sie ein vCenter Server-System im Feld "ESX-Host/vCenter" angeben, können Sie in diesem Feld (aus einer Drop-down-Liste) das ESX Server-System angeben, das Sie mit diesem Plan verknüpfen möchten.

Monitor

Legen Sie den Hostnamen des Servers fest, der den Status des Quellservers überwacht.

Hinweise:

- Sie können einem beliebigen physischen Computer oder virtuellen Rechner als Überwachungsserver verwenden.
- Sie können nicht den Sicherungsquellserver als Überwachungsserver verwenden.

- Der Überwachungsserver ist nicht erforderlich, wenn die Knoten von einem Remote-Recovery Point Server repliziert wurden oder die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird.
- Sie müssen den Überwachungsserver nicht konfigurieren, wenn die Virtual Standby-Quelle Replikationstask ist und sich der Replikationsziel-RPS-Server in Azure befindet.

Benutzername

Geben Sie den Benutzernamen für die Anmeldung beim Überwachungssystem an.

Kennwort

Geben Sie das Kennwort für den Benutzernamen für die Anmeldung beim Überwachungssystem an.

Protokoll

Geben Sie als Protokoll, das Sie für die Kommunikation zwischen dem Arcserve Unified Data Protection-System und dem ESX Server-System (Überwachungsserver) verwenden möchten, HTTP oder HTTPS an.

Port

Legen Sie den Port fest, den Sie für den Datentransfer zwischen dem Arcserve Unified Data Protection-System und dem ESX Server-System (Überwachungsserver) verwenden möchten.

Überwachungsserver als Proxy für den Datentransfer verwenden

Aktivieren Sie diese Option, um zuzulassen, dass der Überwachungsserver die Konvertierungsdaten aus dem Knoten des Arcserve Unified Data Protection-Agenten in den ESX Server-Datenspeicher kopiert. Wenn diese Option aktiviert ist, überträgt die Virtual Standby-Funktion die Konvertierungsdaten vom Agent-Knoten zum ESX Server-Datenspeicher mithilfe der Fibre-Channel-Kommunikation, die für die Datenübertragung schneller ist als die LAN-Kommunikation. Nur der Schreibvorgang für die Konvertierung erfolgt per Fibre Channel. Der Lesevorgang erfolgt über das LAN.

Hinweis: Die Option "Überwachungsserver als Proxy für den Datentransfer verwenden" ist standardmäßig aktiviert. Sie können diese Option deaktivieren, um zuzulassen, dass der Knoten des Arcserve Unified Data Protection-Agenten die Konvertierungsdaten direkt in den Datenspeicher im ESX Server-System kopiert.

Virtualisierungstyp: Hyper-V

Hyper-V-Hostname

Legen Sie den Hostnamen des Hyper-V-Systems fest.

Benutzername

Legen Sie den Benutzernamen fest, der für die Anmeldung beim Hyper-V-System erforderlich ist.

Hinweis: Das Konto, das Sie angeben, muss ein Admin-Konto oder ein Konto mit administrativen Berechtigungen für das Hyper-V-System sein.

Kennwort

Legen Sie das Kennwort für den Benutzernamen fest, das für die Anmeldung beim Hyper-V-System erforderlich ist.

Protokoll

Geben Sie als Protokoll, das Sie für die Kommunikation zwischen dem Arcserve Unified Data Protection-Server und dem Hyper-V Server-System (Überwachungsserver) verwenden möchten, HTTP oder HTTPS an.

Port

Legen Sie den Port fest, den Sie für den Datentransfer zwischen dem Arcserve Unified Data Protection-Server und dem Hyper-V Server-System (Überwachungsserver) verwenden möchten.

Hinweis: Klicken Sie auf **Verbinden**, um das Hyper-V-System zu validieren.

5. Klicken Sie auf die Registerkarte **Virtueller Rechner**, und geben Sie die Details für VM-Grundeinstellungen, VM-Datenspeicher für VMware, VM-Pfad für Hyper-V und VM-Netzwerk ein.

   VMware-Systeme:

   Wenden Sie die folgenden Optionen für virtuelle Rechner auf VMware-Systeme an:

   Präfix des Namens des virtuellen Rechners

   Geben Sie das Präfix an, das Sie dem Anzeigenamen des virtuellen Rechners auf dem ESX Server-System voranstellen möchten.

   Standardwert: UDPVM_

   Ressourcenpool

   Legen Sie den Namen des Ressourcenpools fest, in den der Virtual Standby-Rechner eingruppiert werden soll.

   CPU-Zähler

Legen Sie die Mindestanzahl und Höchstanzahl von CPUs fest, die vom Virtual Standby-Rechner unterstützt werden.

Arbeitsspeicher

Legen Sie den Gesamtwert für den RAM, der für den Virtual Standby-Rechner zugewiesen werden soll, in MB fest.

Hinweis: Der angegebene RAM-Wert muss ein Vielfaches von zwei sein.

Wiederherstellungspunkt-Snapshots

Geben Sie die Anzahl an Wiederherstellungspunkt-Snapshots (Wiederherstellungspunkten) für den virtuellen Standby-Rechner an. Die Höchstanzahl von Wiederherstellungspunkt-Snapshots für VMware-Virtualisierungsserver beträgt 29.

Alle virtuellen Datenträger verwenden denselben Datenspeicher

Aktivieren Sie diese Option, um alle zum virtuellen Rechner gehörigen Datenträger auf denselben Datenspeicher zu kopieren.

Deaktivieren Sie das Kontrollkästchen, um datenträgerbezogene Informationen zum virtuellen Rechner in den entsprechenden Datenspeicher zu kopieren. Legen Sie den Speicherort fest, an dem Sie die Konvertierungsdaten speichern möchten.

Netzwerk

Ermöglicht es Ihnen, die NICs, virtuellen Netzwerke und Pfade zu definieren, die das ESX Server-System verwendet, um mit den virtuellen Rechnern zu kommunizieren.

Hinweis: VMware SR-IOV Passthrough und Flexibler Netzwerkadapter wird nicht unterstützt.

Gleiche Zahl an Netzwerkadaptern wie die Quelle bei der letzten Sicherung

Aktivieren Sie diese Option, um zu definieren, auf welche Weise die virtuelle NIC zum virtuellen Netzwerk zugeordnet werden soll. Aktivieren Sie diese Option, wenn der virtuelle Rechner virtuelle NICs und ein virtuelles Netzwerk enthält.

Deaktivieren Sie das Kontrollkästchen, um den Namen des virtuellen Netzwerks zu definieren, das die NIC für die Kommunikation verwenden soll.

Hyper-V-Systeme:

Wenden Sie die folgenden Optionen für virtuelle Rechner auf Hyper-V-Systeme an:

Grundeinstellungen

Geben Sie folgende Grundeinstellungen an:

Präfix des Namens des virtuellen Rechners

Geben Sie das Präfix an, das Sie dem Anzeigenamen des virtuellen Rechners auf dem Hyper-V-System voranstellen möchten.

Standardwert: UDPVM_

CPU-Zähler

Legen Sie die Mindestanzahl und Höchstanzahl von CPUs fest, die vom Virtual Standby-System unterstützt werden.

Arbeitsspeicher

Legen Sie den Gesamtwert für den RAM, der dem Virtual Standby-Rechner zugewiesen werden soll, in MB fest.

Hinweis: Der angegebene RAM-Wert muss ein Vielfaches von vier sein.

Wiederherstellungspunkt-Snapshots

Geben Sie die Anzahl von Wiederherstellungspunkt-Snapshots für den virtuellen Standby-Rechner an. Die Höchstanzahl von Wiederherstellungspunkt-Snapshots für Hyper-V-Virtualisierungsserver beträgt 24.

Alle virtuellen Datenträger verwenden denselben Pfad

Aktivieren Sie diese Option, um den Speicherort auf dem Hyper-V-Server, auf dem Sie die Konvertierungsdaten speichern möchten, festzulegen.

Deaktivieren Sie das Kontrollkästchen, um den Speicherort auf dem Hyper-V-Server, auf dem Sie die Konvertierungsdaten speichern möchten, für die virtuellen Datenträger jeweils einzeln festzulegen.

Hinweis: Arcserve UDP-Lösung unterstützt nicht die Erstellung virtueller Datenträgerabbilder (VHD-VHDX-Dateien) auf komprimierten Volumen und Volumen, die vom Dateisystem verschlüsselt werden. Wenn sich der angegebene Pfad auf komprimierten oder verschlüsselten Hyper-V-Volumes befindet, lässt Sie Arcserve UDP den Virtual Standby-Task nicht erstellen.

VM-Netzwerk

Ermöglicht es Ihnen, die NICs, virtuellen Netzwerke und Pfade zu definieren, die der Hyper-V-Server verwendet, um mit den virtuellen Rechnern zu kommunizieren. Geben Sie eine der folgenden Optionen an, und füllen Sie die erforderlichen Felder aus.

Gleiche Zahl an Netzwerkadaptern wie die Quelle bei der letzten Sicherung

Aktivieren Sie diese Option, um zu definieren, auf welche Weise die virtuelle NIC zum virtuellen Netzwerk zugeordnet werden soll. Aktivieren Sie diese

Option, wenn der virtuelle Rechner virtuelle NICs und ein virtuelles Netzwerk enthält.

Deaktivieren Sie das Kontrollkästchen, um den Namen des virtuellen Netzwerks zu definieren, das die NIC für die Kommunikation verwenden soll.

6. Klicken Sie auf die Registerkarte **Erweitert**, und geben Sie folgende Details an:

Virtuellen Rechner automatisch starten

Geben Sie an, ob Sie den virtuellen Rechner automatisch starten möchten.

Hinweis: Diese Option ist nicht verfügbar für hostbasierte VM-Knoten und Knoten, die von einem Remote-Wiederherstellungspunktserver repliziert werden und die Quelle des Virtual Standby-Tasks ist diejenige, die an einen anderen Standort repliziert wird.

Zeitlimit

Geben Sie an, wie lange der Überwachungsserver auf ein Heartbeat-Signal warten muss, bevor er einen Wiederherstellungspunkt-Snapshot einschaltet.

Häufigkeit

Legen Sie die Häufigkeit fest, mit der der Quellserver ein Heartbeat-Signal an den Überwachungsserver sendet.

Beispiel: Der festgelegte Wert für das Zeitlimit ist 60. Der festgelegte Häufigkeitswert ist 10. Der Quellserver sendet Heartbeat-Signale in 10-Sekunden-Intervallen. Wenn der Überwachungsserver innerhalb von 60 Sekunden nach dem letzten erkannten Heartbeat-Signal kein Heartbeat-Signal erkennt, schaltet der Überwachungsserver unter Verwendung des letzten Wiederherstellungspunkt-Snapshot einen virtuellen Rechner ein.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu erhalten, abhängig von den Einstellungen, die Sie angeben. Wenn Sie diese Option auswählen, werden weitere Kategorien der E-Mail-Alerts für Ihre Auswahl aktiviert.

- **Fehlendes Heartbeat-Signal für Quellrechner**: Virtual Standby sendet Alert-Benachrichtigungen, wenn der Überwachungsserver kein Heartbeat-Signal vom Quellserver erkennt.

  Hinweis: Für Knoten, die von einem Remote-Recovery Point Server repliziert wurden oder wenn die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird, ist diese Option nicht verfügbar.

- **VM eingeschaltet für Quellrechner, der mit automatischer Einschaltung konfiguriert ist**: Virtual Standby sendet Alert-Benachrichtigungen, wenn ein

virtueller Rechner in Betrieb genommen wird, der so konfiguriert wurde, dass eine automatische Inbetriebnahme erfolgt, wenn kein Heartbeat-Signal entdeckt wird.

Hinweis: Für Knoten, die von einem Remote-Recovery Point Server repliziert wurden oder wenn die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird, ist diese Option nicht verfügbar. Für hostbasierte Knoten eines virtuellen Rechners ist diese Option ebenfalls nicht verfügbar.

- **VM eingeschaltet für Quellrechner, der mit manueller Einschaltung konfiguriert ist**: Virtual Standby sendet Alert-Benachrichtigungen, wenn ein virtueller Rechner manuell eingeschaltet wird.
- **Virtual Standby-Fehler/-Ausfall/-Absturz**: Virtual Standby sendet Alert-Benachrichtigungen, wenn ein Fehler entdeckt wird, der während des Konvertierungsprozesses aufgetreten ist.
- **Virtual-Standby-Erfolg**: Virtual Standby sendet Alert-Benachrichtigungen, wenn festgestellt wird, dass der virtuelle Rechner erfolgreich eingeschaltet wurde.
- **Virtual Standby wurde nicht erfolgreich vom Wiederherstellungspunkt-Snapshot gestartet**: Virtual Standby sendet Alert-Benachrichtigungen, wenn festgestellt wird, dass ein virtueller Rechner nicht automatisch eingeschaltet wurde und die Option zur Aushilfswiederherstellung "Virtuellen Rechner automatisch starten" aktiviert ist.
- **Hypervisor ist nicht erreichbar**: Virtual Standby sendet Alert-Benachrichtigungen, wenn festgestellt wird, dass mit dem ESX Server-System oder Hyper-V-System keine Kommunikation möglich ist.
- **Freier VM-Speicherplatz beträgt weniger als**: Virtual Standby sendet Alert-Benachrichtigungen, wenn festgestellt wird, dass auf dem angegebenen Hypervisor-Pfad nicht genügend freier Speicherplatz vorhanden ist. Dies tritt auf, wenn der freie Speicherplatz weniger ist als der benutzerdefinierte Schwellenwert. Der Schwellenwert kann entweder als absoluter Wert (MB) oder als prozentualer Anteil an der Gesamtkapazität angegeben werden.

7. Klicken Sie auf **Speichern**.

   Die Änderungen werden gespeichert, und der Virtual Standby-Task wird automatisch auf dem Virtual Standby-Server bereitgestellt.

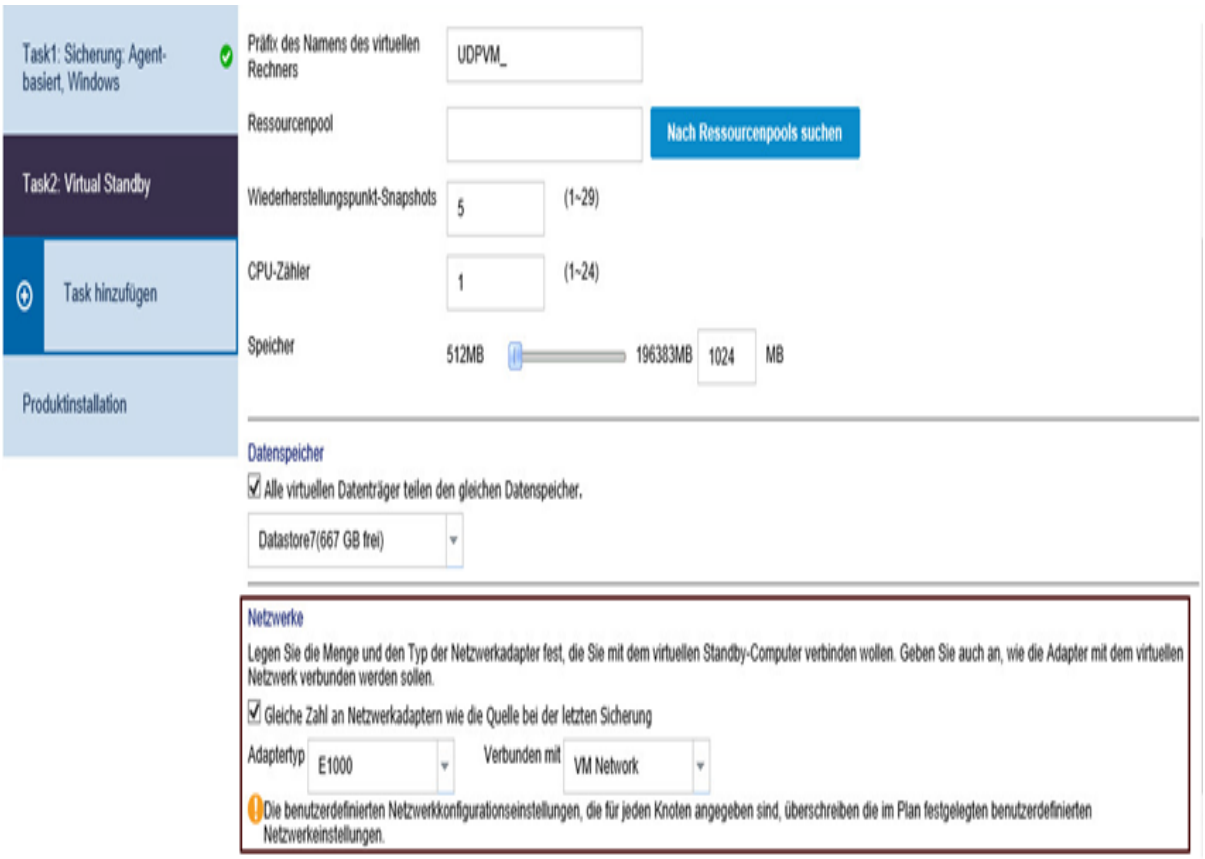
   Sie haben den Virtual Standby-Plan erfolgreich erstellt und bereitgestellt.

Bestimmung der Anzahl einzuschaltender NICs durch die Anwendung

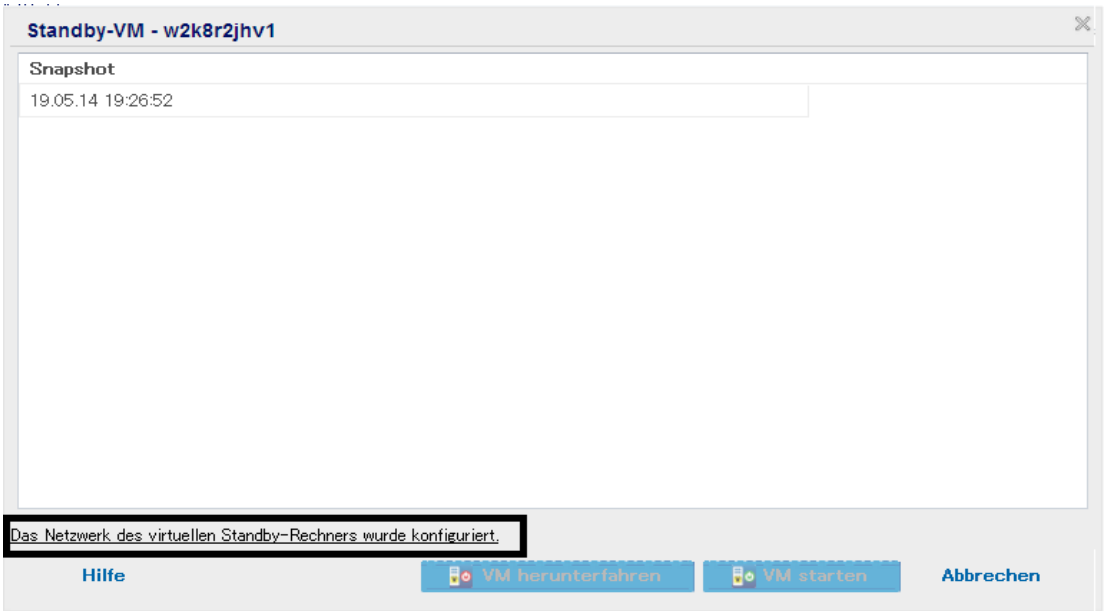
Beim Einschalten von virtuellen Rechnern bestimmt Virtual Standby die Anzahl von einzuschaltenden NICs (Netzwerkkarten) basierend darauf, ob das Netzwerk für Virtual Standby-Rechner konfiguriert ist. Folgende Tabelle veranschaulicht, wie Virtual Standby die Anzahl von NICs bestimmt, die benötigt werden, um Virtual Standby-Rechner einzuschalten:

Im Plan definierte Werte für das VM-Netzwerk	Die Option "Virtuellen Standby-Rechner mit benutzerdefinierten Netzwerkkonfigurationen starten" ist nicht aktiviert.	Die Option "Virtuellen Standby-Rechner mit benutzerdefinierten Netzwerkkonfigurationen starten" ist aktiviert.
Die definierten Werte sind die selben wie die des Quellrechners.	Virtual Standby schaltet die Anzahl von NICs ein, die zum Zeitpunkt des letzten Sicherungsjobs für den Quellrechner definiert war.	Virtual Standby schaltet die Anzahl von NICs ein, die dem größeren der folgenden Werte entspricht: ■ die in der benutzerdefinierten Netzwerkkonfiguration definierte Anzahl ■ die Anzahl von NICs ein, die zum Zeitpunkt des letzten Sicherungsjobs für den Quellrechner definiert war
Die definierten Werte sind benutzerdefinierte Werte.	Virtual Standby schaltet die Anzahl von benutzerdefinierten Netzwerken ein, die im Plan definiert sind.	Virtual Standby schaltet die Anzahl von NICs ein, die dem größeren der folgenden Werte entspricht: ■ die in der benutzerdefinierten Netzwerkkonfiguration definierte Anzahl ■ die Anzahl von NICs, die für die benutzerdefinierte Richtlinie definiert sind

Das folgende Dialogfeld (Bearbeiten eines Virtual Standby-Task in "Einen Plan ändern") des Virtual Standby-Tasks besteht aus benutzerdefinierten Konfigurationen für NICs, die eingeschaltet werden sollen:



Das folgende Dialogfeld (Standby-VM – <host_name>) veranschaulicht, wo Sie die Option zum Starten des Virtual Standby-Rechners mit benutzerdefinierten Netzwerkkonfigurationen aktivieren:

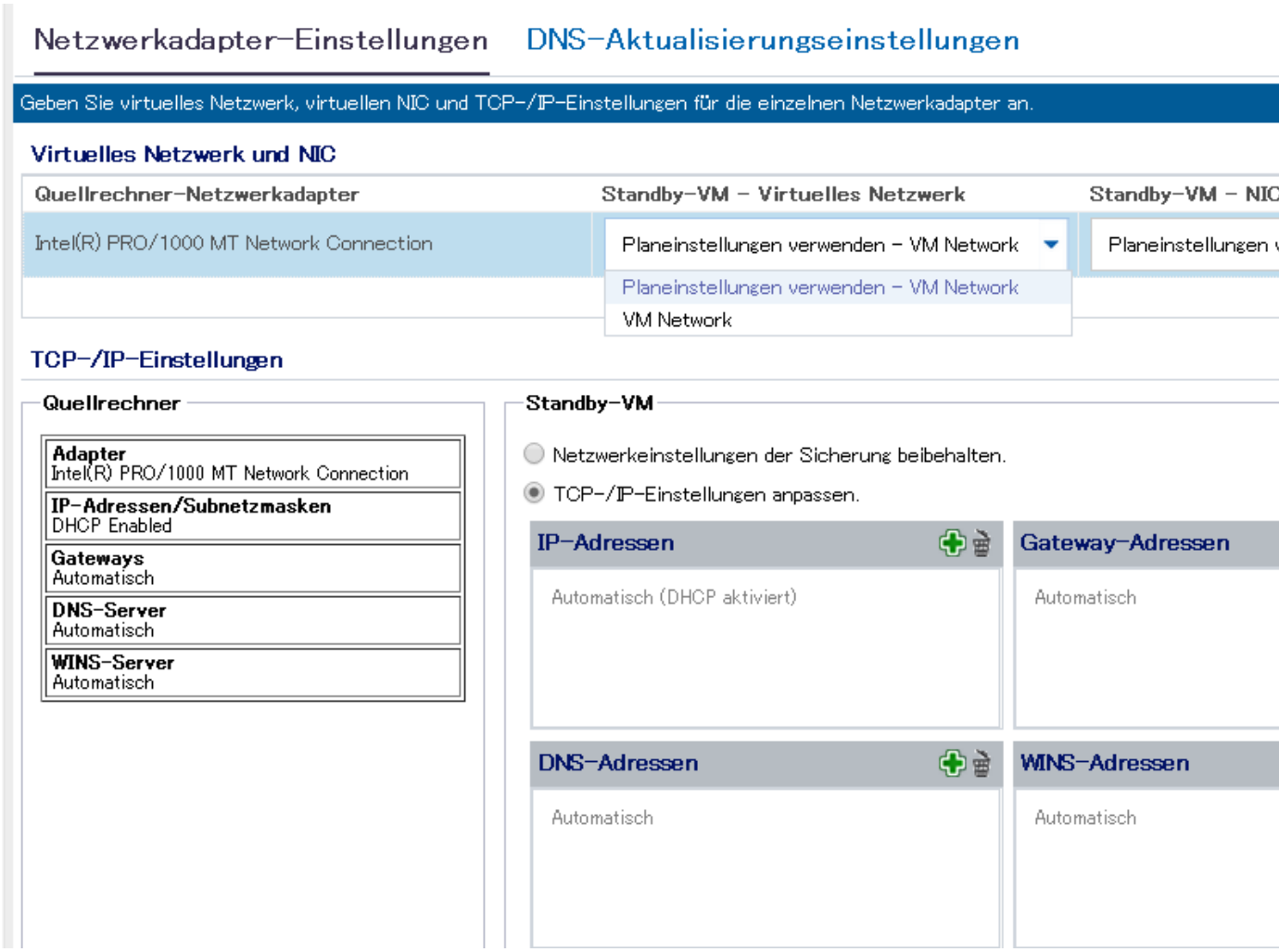


Konfigurieren des Standby-VM-Netzwerks

Sie können die Standby-VM mit benutzerdefinierten Netzwerkeinstellungen einschalten. Sie können folgende Netzwerkeinstellungen auf der Standby-VM konfigurieren:

- Geben Sie auf der Registerkarte **Netzwerkadapter-Einstellungen** das virtuelle Netzwerk und die NIC (Network Interface Card, Netzwerkkarte) sowie TCP/IP-Einstellungen für die einzelnen Netzwerkadapter an.
- Aktualisieren Sie die DNS-Server auf der Registerkarte **DNS-Aktualisierungseinstellungen**, um Clients basierend auf den TCP/IP-Einstellungen vom Quellrechner zu den virtuellen Virtual Standby-Rechnern umzuleiten.

Die folgende Abbildung zeigt die Registerkarte **Netzwerkadapter-Einstellungen** von **Standby-VM - Netzwerkkonfiguration**:



Gehen Sie wie folgt vor:

1. Navigieren Sie auf der Registerkarte **Ressourcen** zur Knotengruppe **Virtual Standby**.

   Die Virtual Standby-Knoten werden im mittleren Fensterbereich angezeigt.

2. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Standby-VM - Netzwerkkonfiguration**.

   Die Seite "Standby-VM - Netzwerkkonfiguration - <Knotenname>" wird geöffnet.

3. Wählen Sie auf der Registerkarte **Netzwerkadapter-Einstellungen** das virtuelle Netzwerk aus der Liste **Standby-VM - Virtuelles Netzwerk** aus.

4. Wählen Sie den NIC-Typ aus der Liste **Standby-VM - NIC-Typ** aus.

5. Wählen Sie **TCP-/IP-Einstellungen anpassen** aus.

6. Klicken Sie auf die Schaltfläche **Adresse hinzufügen**, und fügen Sie **IP-Adressen**, **Gateway-Adressen**, **DNS-Adressen** und **WINS-Adressen** hinzu.

   Hinweis: Wenn Sie **DNS-Adressen** hinzufügen, dann konfigurieren Sie die DNS-Server auf der Registerkarte **DNS-Aktualisierungseinstellungen**.

7. Klicken Sie auf **Speichern**.

   Die Seite "Standby-VM - Netzwerkkonfiguration - <Knotenname>" wird geschlossen.

   Das Standby-VM-Netzwerk ist konfiguriert.

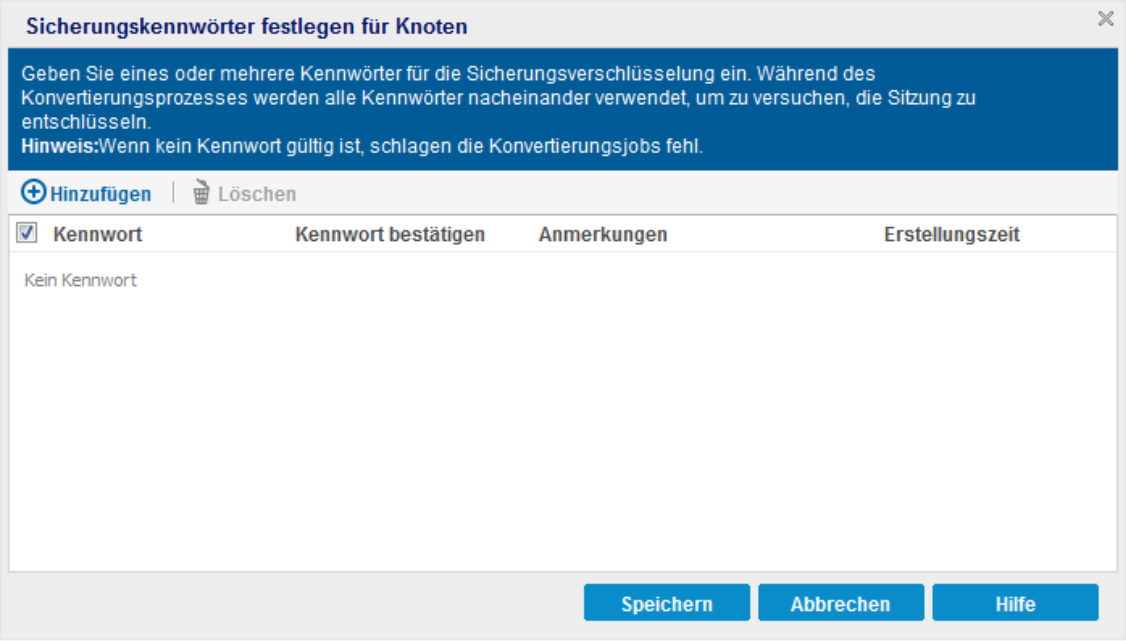
Festlegen von Sicherungskennwörtern für einen oder mehrere Knoten

Um sicherzustellen, dass der Konverter die Snapshots der replizierten Wiederherstellungspunkte konvertieren kann, können Sie in Virtual Standby Sicherungskennwörter für die Daten angeben, die der Konverter verwenden kann, um die Daten zu konvertieren.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.
3. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Sicherungskennwörter festlegen**.

   Das Dialogfeld **Sicherungskennwörter festlegen für Knoten** wird geöffnet.

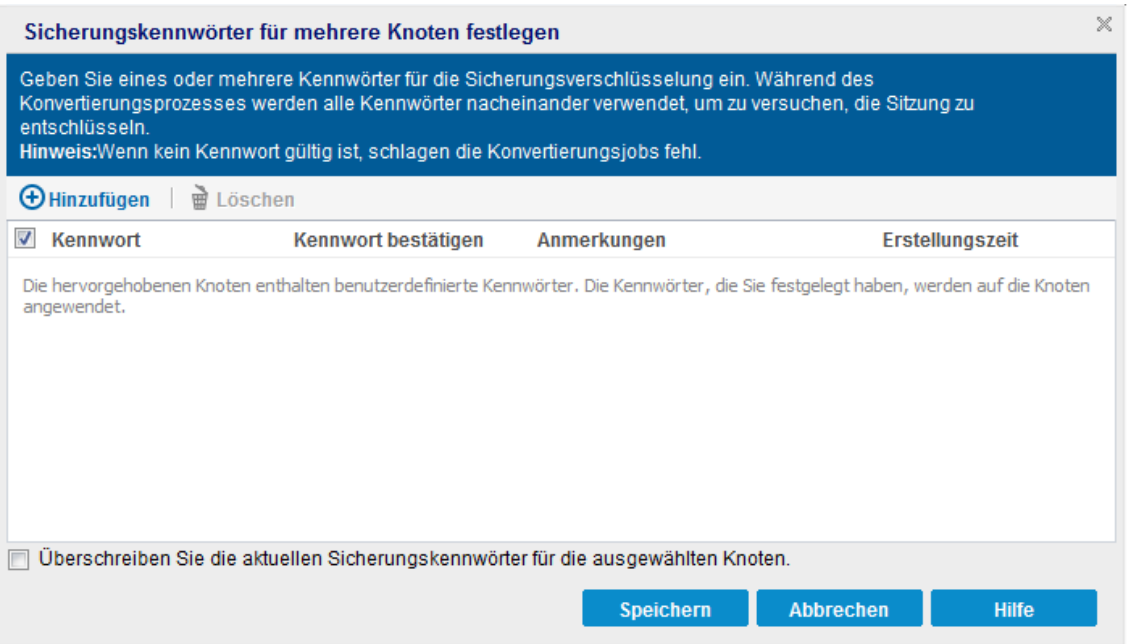


4. Führen Sie im Dialogfeld **Sicherungskennwörter festlegen** folgende Tasks für einen oder mehrere Knoten aus:

   Hinzufügen: Klicken Sie auf **Hinzufügen**, um Sicherungskennwörter zu den ausgewählten Knoten hinzuzufügen.

   Löschen: Klicken Sie auf **Löschen**, um Sicherungskennwörter aus den ausgewählten Knoten zu löschen.

Hinweis: Sie können die aktuellen Sicherungskennwörter für mehrere Knoten überschreiben, indem Sie das Kontrollkästchen **Überschreiben Sie die aktuellen Sicherungskennwörter für die ausgewählten Knoten** aktivieren.



5. Klicken Sie auf **Speichern**.

   Das Dialogfeld wird geschlossen und die Sicherungskennwörter wurden für die ausgewählten Remote-Knoten festgelegt.

(Optional) Manuelles Ausführen des Virtual Standby-Jobs

Um einen Virtual Standby-Job manuell auszuführen, müssen Sie zunächst eine manuelle Sicherung ausführen. Der Virtual Standby-Task wird mit einem Sicherungstask verknüpft. Wenn ein Plan einen Sicherungstask und einen Virtual Standby-Task enthält und Sie den Sicherungsjob manuell ausführen, wird der Virtual Standby-Job nach dem Abschluss des Sicherungsjobs automatisch ausgeführt.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte "**Ressourcen**".
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Zeigt die Pläne an, die Sie hinzugefügt haben.
3. Wählen Sie die Knoten aus, die gesichert werden sollen. Dem ausgewählten Knoten muss ein Plan zugewiesen sein.
4. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Jetzt sichern**.

   Das Dialogfeld **Sicherung jetzt ausführen** wird geöffnet.
5. Wählen Sie den Sicherungstyp aus, und geben Sie einen Namen für den Sicherungsjob an.
6. Klicken Sie auf **OK**.

   Der Sicherungsjob wird ausgeführt.

   Der Virtual Standby-Job wird sofort nach dem Sicherungsjob ausgeführt.

   Der Virtual Standby-Job wird manuell ausgeführt.

Aussetzen und Wiederaufnehmen von Heartbeat-Signalen

Mit der Arcserve Unified Data Protection-Lösung können Sie Heartbeat-Signale, die vom Überwachungsserver erkannt werden, unterbrechen und wiederaufnehmen. Beim Heartbeat-Signal handelt es sich um den Prozess, über den sich Quellserver und Überwachungsserver über den Zustand des Quellservers austauschen. Wenn der Überwachungsserver nach Ablauf eines festgelegten Zeitraums kein Heartbeat-Signal erkennt, stellt die Virtual Standby-Funktion den virtuellen Rechner bereit, damit dieser als Quellknoten fungiert.

Beispiele: Situationen zum Aussetzen oder Wiederaufnehmen von Heartbeat-Signalen

Die folgenden Beispiele beschreiben, wann Sie Heartbeat-Signale aussetzen und wann Sie sie fortsetzen sollten:

- Setzen Sie das Heartbeat-Signal aus, wenn Sie einen Knoten (Quellserver) für Wartungszwecke offline stellen möchten.
- Nehmen Sie das Heartbeat-Signal wieder auf, wenn die Wartungsaufgaben abgeschlossen sind und der Knoten (Quellserver) wieder online ist.

Beachten Sie Folgendes:

- Sie können Heartbeat-Signale auf Gruppenebene oder für einzelne Knoten aussetzen und wiederaufnehmen.
- Sie können Heartbeat-Signale für einen oder mehrere Knoten in einem Schritt aussetzen und wiederaufnehmen.
- Die Arcserve Unified Data Protection
- Wenn Sie ein Upgrade von Agent-Installationen auf Quellknoten durchführen, unterbricht Arcserve Unified Data Protection Um sicherzustellen, dass Überwachungsserver die Knoten, für die ein Upgrade durchgeführt wurde, überwachen, nehmen Sie das Heartbeat-Signal für die Knoten wieder auf, nachdem die Upgrades abgeschlossen wurden.

Gehen Sie wie folgt vor:

1. Melden Sie sich unter Arcserve Unified Data Protectionan.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Navigieren Sie im linken Fensterbereich zu **Virtual Standby** und klicken Sie auf **Alle Knoten**.

   Wenn Sie Knoten hinzugefügt haben, werden diese Knoten im mittleren Fensterbereich angezeigt.

4. Wählen Sie den Knoten aus, den Sie unterbrechen oder wiederaufnehmen möchten.
5. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Heartbeat-Signal**, **Unterbrechen** oder **Fortsetzen**.

   Das Heartbeat-Signal des ausgewählten Knotens wird unterbrochen bzw. wiederaufgenommen.

Unterbrechen und Wiederaufnehmen eines Virtual Standby-Jobs

Virtuelle Konvertierung ist der Prozess, bei dem Virtual Standby die Arcserve Unified Data Protection-Wiederherstellungspunkte von Quellknoten in Formate für virtuelle Rechner konvertiert, die als Wiederherstellungspunkt-Snapshots bezeichnet werden. Wenn es einen Fehler auf einem Quellknoten gibt, verwendet die Virtual Standby-Funktion die Wiederherstellungspunkt-Snapshots, um einen virtuellen Rechner für den Quellknoten in Betrieb zu nehmen.

Die Best Practice besteht darin, zuzulassen, dass der virtuelle Konvertierungsprozess kontinuierlich in Betrieb ist. Wenn Sie den virtuellen Konvertierungsprozess jedoch auf lokalen und Remote-Virtual Standby-Servern vorübergehend unterbrechen möchten, können Sie dies über die Konsole tun. Nachdem Sie die Probleme auf dem Quellknoten behoben haben, können Sie den virtuellen Konvertierungsprozess wieder aufnehmen.

Wenn Sie Virtual Standby-Jobs (Konvertierungsjobs) unterbrechen, wird der Konvertierungsjob, der gegenwärtig durchgeführt wird, nicht unterbrochen. Der Unterbrechungsvorgang bezieht sich auf nur den Job, dessen Ausführung nach Beendigung des nächsten Sicherungsjobs erwartet wird. Dadurch startet der nächste Konvertierungsjob nicht, bis Sie den (unterbrochenen) Konvertierungsjob ausdrücklich wiederaufnehmen.

Wenn Sie Virtual Standby für Knoten wiederaufnehmen und wenn mehrere Sicherungssitzungen ohne Wiederherstellungspunkt-Snapshot vorhanden sind, dann wird ein Dialogfeld angezeigt, in dem Sie die Smart Copy-Option auswählen können. Wenn Sie auf "Ja" klicken, konvertiert Virtual Standby die kombinierte Sitzung in einen einzelnen Wiederherstellungspunkt-Snapshot. Wenn Sie auf "Nein" klicken, konvertiert Virtual Standby jede Sitzung einzeln

Hinweis: Optional können Sie Virtual Standby-Jobs direkt von den Knoten aus unterbrechen und wiederaufnehmen. Weitere Informationen finden Sie unter "Unterbrechen und Wiederaufnehmen von Virtual Standby-Jobs von den Knoten".

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve Unified Data Protection an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Navigieren Sie im linken Fensterbereich zu "**Virtual Standby**", und klicken Sie auf "**Alle Knoten**".

Wenn Sie Knoten hinzugefügt haben, werden diese Knoten im mittleren Fensterbereich angezeigt.

4. Wählen Sie den Knoten aus, den Sie unterbrechen oder wiederaufnehmen möchten.
5. Klicken Sie im mittleren Fensterbereich auf "**Aktionen**", "**Virtual Standby**", "**Unterbrechen**" oder "**Fortsetzen**".

   Die Virtual Standby-Funktion für den ausgewählten Knoten wird unterbrochen oder wiederaufgenommen.

Überprüfen des Plans

Um Ihre Virtual Standby-Funktion zu überprüfen, stellen Sie sicher, dass Sie den Virtual Standby-Plan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Nachdem der Sicherungsjob erfolgreich abgeschlossen wurde, wird der Virtual Standby-Job ausgeführt. Sie können den Status des Sicherungsjobs und Virtual Standby-Jobs in der Registerkarte **Jobs** überprüfen.

Folgen Sie diesen Schritten, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Folgen Sie diesen Schritten, um Virtual Standby-Jobs zu überprüfen:

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob und der Virtual Standby-Job erfolgreich ausgeführt werden.

   Der Plan für Virtual Standby wurde erfolgreich überprüft.

   Der Virtual Standby-Rechner wurde erstellt.

Erstellen eines Assured Recovery-Plans

Um überprüfen zu können, ob auf die Daten zugegriffen werden kann und ob sie wiederherstellbar sind, müssen Sie einen Assured Recovery-Plan erstellen. Der Assured Recovery-Plan basiert auf einem Sicherungs-/Replikationsplan. Mit diesem Wiederherstellungstask können Sie einen Assured Recovery-Task zu einem vorhandenen Sicherungs- oder Replikationsplan hinzufügen. Der Assured Recovery-Task umfasst eine Quelle, Testeinstellungen, einen Ablaufplan und erweiterte Einstellungen. Sie können Assured Recovery-Jobs auch manuell ausführen.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Hinzufügen eines Assured Recovery-Tasks zum Plan
3. (Optional) Manuelles Ausführen von Assured Recovery-Testjobs

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie die folgenden erforderlichen Aufgaben durchgeführt haben:

- Melden Sie sich bei der Konsole an.
- Sie haben die Serverkomponente installiert und Datenspeicher erstellt, wenn Sie Sicherungsdaten auf Recovery Point Servern speichern möchten.
- Sie haben einen gültigen Wiederherstellungspunkt zum Erstellen einer Instant VM oder eines Instant Virtual Disk. Bei der Auswahl der Wiederherstellungspunkte können Sie aus folgenden Tasks wählen:
  - Sicherung: agentenbasiert, Windows
  - Sicherung: hostbasiert, agentenlos
  - Replizieren
  - Sicherung: Office 365 Exchange Online
  - Sicherung: Office 365 OneDrive
  - Sicherung: Office 365 SharePoint Online
  - Sicherung: Dateien unter dem UNC- oder NFS-Pfad
  - Sicherung: agentenbasiert, Linux
- Stellen Sie sicher, dass die Arcserve UDP-Agenten bereits auf dem Proxy-Server installiert sind.
- Sie haben sichergestellt, dass das Betriebssystem des Proxy-Servers Windows Server 2008 R2 (64 Bit) oder höher ist.

  Hinweis: Für Sicherungspläne des Typs "UNC-Pfad" und Office 365-Sicherungspläne (Exchange Online, OneDrive, SharePoint Online) sollte der Assured Recovery-Proxy-Server unter Windows Server 2012 oder höher ausgeführt werden.
- Sie haben sichergestellt, dass der Proxy-Server über ausreichend Speicherplatz für die Instant VM oder Instant Virtual Disk verfügt.

  Hinweis: Der notwendige Speicherplatz richtet sich maßgeblich nach der RAM-Größe, die Sie im AR-Task für den Testtypen AR IVM konfiguriert haben. Für jede IVM benötigt der Hypervisor die maximale bis gleiche Größe des Arbeitsspeichers, um die die temporären Daten in Auslagerungsdateien zu speichern. Wenn Ihnen beispielsweise 5 Knoten im selben Plan mit AR-IVM-Task vorliegen und die VM-Speichergröße auf 4 GB festgelegt ist, benötigen Sie mindestens 5 * 4 = 20 GB freien Speicher für die Auslagerungsdateien. Darüber

hinaus benötigen Sie möglicherweise 10 MB freien Speicherplatz für die VM-Konfigurationsdateien.

- Stellen Sie sicher, dass die Windows-Betriebssystemversion auf dem Assured Recovery-Proxy-Server mit der Windows-Betriebssystemversion auf der Quell-VM übereinstimmt oder höher ist.

Hinzufügen eines Assured Recovery-Tasks zum Plan

Ein Assured Recovery-Task fügt einen Assured Recovery-Task zu einem vorhandenen Sicherungs-/Replikationsplan hinzu. Jeder Task besteht aus Parametern, die Quelle, Taskeinstellungen, Ablaufplan und erweiterte Einstellungen definieren. Erstellen Sie einen Assured Recovery-Task auf Basis eines Sicherungs-/Replikationstasks, um zu überprüfen, ob auf die Daten zugegriffen werden kann und sie auf jeden Fall wiederhergestellt werden können, und um die Datenintegritätsprüfung durchzuführen.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Öffnen Sie im mittleren Fensterbereich einen vorhandenen Sicherungs- oder Replikationsplan.
4. Klicken Sie im ausgewählten Plan im linken Fensterbereich auf **Task hinzufügen**.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn Sie den Plan unterbrechen, wird der Assured Recovery-Job nicht gestartet. Wenn Sie den Plan wieder aufnehmen, wird der Assured Recovery-Job nicht automatisch fortgesetzt. Sie müssen einen anderen Sicherungsjob manuell ausführen, um den Assured Recovery-Job zu starten.
6. Wählen Sie im Drop-down-Menü **Tasktyp** die Option **Assured Recovery-Test** aus.
7. Legen Sie nun die Quelle, die Taskeinstellungen (IVM oder IVD), den Ablaufplan und die Details unter Erweitert fest.
8. Klicken Sie auf **Speichern**.

   Die Änderungen werden gespeichert, und der Assured Recovery-Task wird automatisch bereitgestellt.

Angeben der Quelle

Auf der Registerkarte "Quelle" können Sie den Quellwiederherstellungspunkt angeben, den Sie schützen möchten.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Quelle**.
2. Öffnen Sie die Drop-Down-Liste "Wiederherstellungspunktquelle für Assured Recovery-Test", und wählen Sie die gewünschte Option aus.
3. Wählen Sie Typen von Wiederherstellungspunkten für Assured Recovery-Tests aus. Folgende zwei Optionen stehen zur Auswahl:
   - Assured Recovery-Test aus ausgewählten Sicherungstypen

     Sie können "Tägliche Sicherungen", "Wöchentliche Sicherungen" oder "Monatliche Sicherungen" auswählen. Die Optionen für tägliche, wöchentliche oder monatliche Sicherungen werden in Abhängigkeit vom Ablaufplan der Quellsicherung aktiviert. Wenn für die Quellsicherung beispielsweise nur eine monatliche Sicherung geplant ist, ist bei der Option "Assured Recovery-Test aus ausgewählten Sicherungstypen" nur "Monatliche Sicherungen" aktiviert.
   - Assured Recovery Test von den letzten Wiederherstellungspunkten

Die Sicherungsquelle ist nun angegeben

Festlegen der Taskeinstellungen für den Testtyp "Instant Virtual Machine"

Wenn Sie als Testtyp "Instant Virtual Machine (VM)" auswählen, wird der virtuelle Rechner vom Wiederherstellungspunkt gestartet, und es wird optional das benutzerdefinierte Skript ausgeführt. Für den Wiederherstellungspunkt wird ein guter Zustand angenommen, wenn die VM erfolgreich startet und das Überprüfungsskript innerhalb des benutzerdefinierten Zeitintervalls einen Erfolg meldet.

Hinweis: Dieser Schritt ist nicht erforderlich, wenn Sie als Testtyp **Instant Virtual Disk** ausgewählt haben.

Sie können als Hypervisor-Typ VMware vSphere oder Microsoft Hyper-V auswählen und Details für die Proxy-Einstellungen und VM-Einstellungen eingeben, um die Taskeinstellungen für die IVM festzulegen.

Gehen Sie wie folgt vor:

1. Wählen Sie als Testtyp **Instant Virtual Machine** aus.

   Hinweis: Wenn die Quellenaufgabe Agent-basierte Linux-Sicherung/-Replikation ist, ist die Option "Instant VM" der einzige unterstützte Testtyp.

2. Wählen Sie eine der Hypervisor-Optionen aus, und geben Sie die entsprechenden Details ein:

   VMware vSphere

   Hinweis: Falls die AR-Taskeinstellung IVM in vSphere entspricht, ist die erforderliche VMware-Lizenz vergleichbar mit der Funktion, die für Instant VM erforderlich war.

   a. Führen Sie einen der folgenden Schritte durch, um einen Server unter "vCenter/ESX(i) Server" einzustellen:

      - Wenn Sie bereits einen VMware-Knoten zu dem ausgewählten Standort in der Konsole hinzugefügt haben, können Sie den Knoten aus der Drop-down-Liste "vCenter/ESX(i) Server" auswählen.
      - Wenn Sie noch keine VMware-Knoten hinzugefügt haben, klicken Sie auf **Hinzufügen**.

        Das Dialogfeld **Geben Sie das VM-Ziel an** wird geöffnet.

      - Geben Sie die Details zur VM an, und klicken Sie auf "OK".

        Alle ESX(i)- oder Ressourcenpools werden im mittleren Fensterbereich der Seite "VM-Ort" angezeigt.

b. Wählen Sie entweder "ESX(i)", "Cluster", "Ressourcenpool" oder "Virtuelle App" als Speicherort aus.

Der VMware vSphere-Rechner ist nun angegeben.

Hinweis: Geben Sie den Datenspeicher des ESX(i)-Servers an, wenn die Quellenaufgabe agentenbasierte Linux-Sicherung/-Replikation oder hostbasierte Sicherung/Replikation ohne Agent ist.

Festlegen von Microsoft Hyper-V

Führen Sie einen der folgenden Schritte durch, um Microsoft Hyper-V einzustellen:

- Wenn Sie bereits einen Hyper-V-Knoten zu dem ausgewählten Standort in der Konsole hinzugefügt haben, wählen Sie den Knoten aus der Drop-down-Liste Hyper-V-Server/Cluster aus.
- Wenn Sie noch keine Hyper-V-Knoten hinzugefügt haben, klicken Sie auf **Hinzufügen**.

  Das Dialogfeld Geben Sie das VM-Ziel an wird geöffnet.

  Hinweis: Wenn Sie eine Verbindung zu der Hyper-V-Instant VM mit einem nicht integrierten lokalen Administratorkonto herstellen, muss die Remote-UAC deaktiviert werden. Weitere Informationen zum Deaktivieren der Remote-UAC bei nicht integrierten Administratoren finden Sie unter So deaktivieren Sie eine Remote-UAC bei nicht integrierten Administratoren.
- Geben Sie die Details des Hyper-V-Servers an, und klicken Sie auf **OK**.

Die Hyper-V-VM ist nun angegeben.

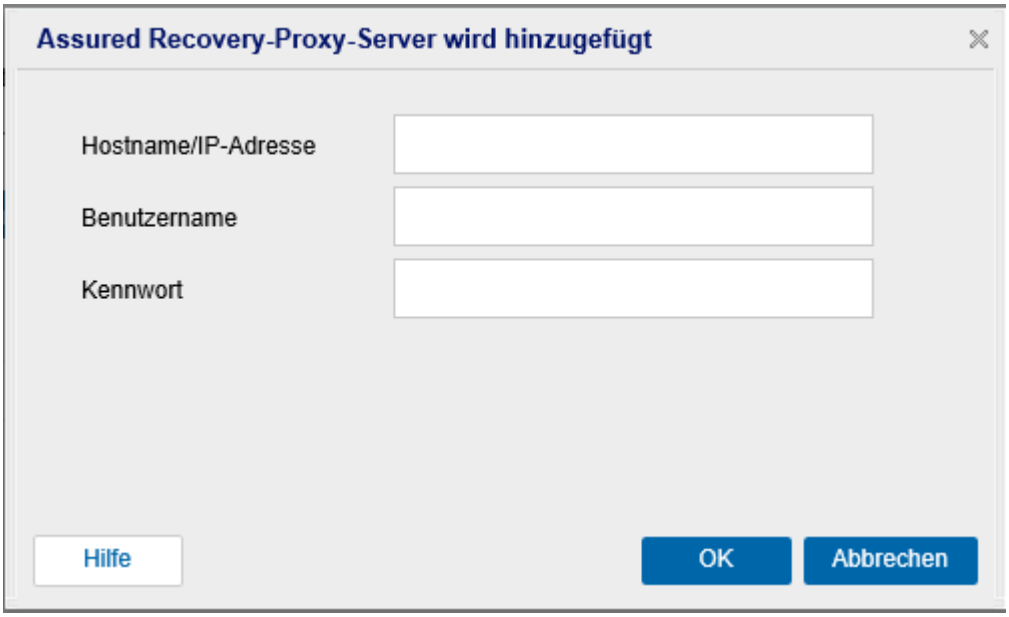
Geben Sie Nutanix AHV an.

Dies ist nur für Linux-VM-Unterstützung. Weitere Informationen finden Sie unter Schützen von Instant-VM auf Nutanix AHV für Linux-Knoten.

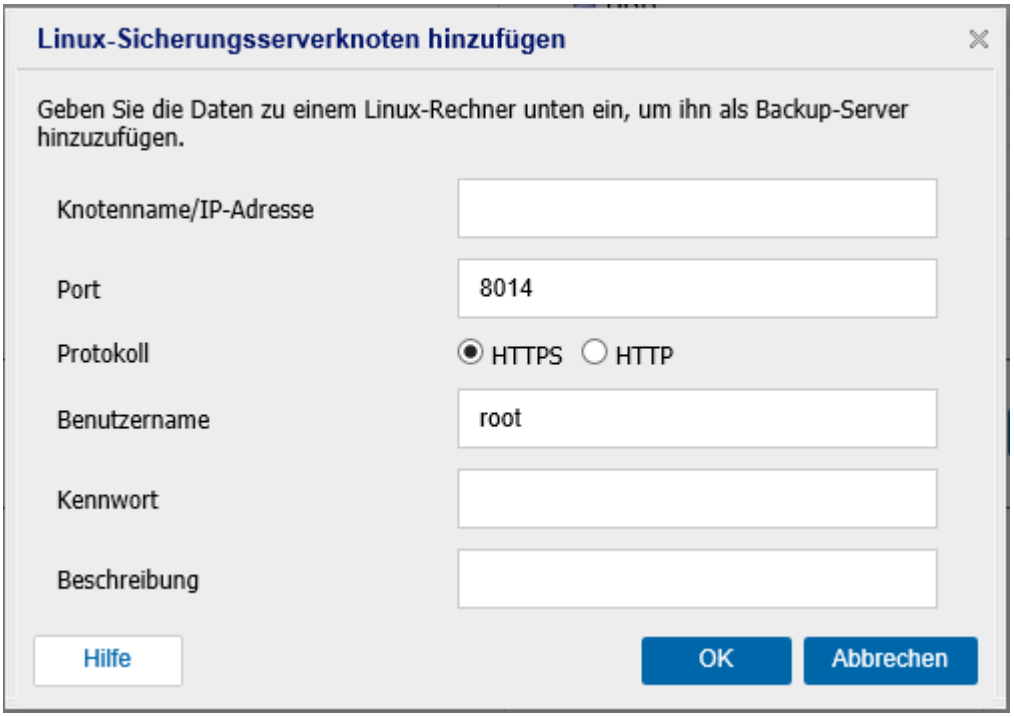
3. Wählen Sie eine der folgenden Optionen, um den **Proxy-Server** anzugeben:
   - Wenn Sie bereits einen Proxy-Knoten zu dem ausgewählten Standort in der Konsole hinzugefügt haben, können Sie den Knoten in der Drop-down-Liste mit den Proxy-Servern auswählen.
   - Wenn Sie noch keine Proxy-Knoten hinzugefügt haben, klicken Sie auf **Hinzufügen**.

Das Dialogfeld **Adding Assured Recovery Proxy Server (Assured Recovery-Proxy-Server hinzufügen)** wird geöffnet.

Für Windows-Proxy-Server



Für Linux-Proxy-Server



- Geben Sie die Details für den Proxy-Server an.
- Klicken Sie auf **OK**.

Die Knoten werden im Bereich **Verfügbare Knoten** angezeigt.

Hinweise:

- Sie müssen nur einen Proxy-Server auswählen, wenn der Hypervisor VMware vSphere ist.
- Wenn der Hypervisor VMware vSphere ist, müssen Sie die Windows-Netzwerkdateisystemrolle (Network File System, NFS) auf dem Recovery Point Server installieren. Der Instant VM-Prozess installiert NFS automatisch. Informationen zur manuellen Installation des Netzwerkdateisystems finden Sie unter So installieren Sie das Netzwerkdateisystem manuell auf einem Windows-Server.
- Wählen Sie Proxy-Server basierend auf ausgewählten Knotentypen im Plan aus. Beispielsweise Windows-Proxy-Server für Windows-Knoten und Linux-Proxy-Server für Linux-Knoten.

4. (Optional) Gehen Sie folgendermaßen vor, um die Gateway-Einstellungen für Assured Recovery festzulegen.

   Hinweis: Gilt nur für Linux.

   a. Mithilfe von DHCP-Einstellungen oder durch manuelle Angabe von IP-Adresse, Maske und Standard-Gateway.

   b. Wählen Sie aus der Drop-down-Liste ein virtuelles Netzwerk aus.

   Hinweis: Gateway-Einstellungen sind nur erforderlich, wenn die Quelle des Assured Recovery-Tests Agent-basierte Linux-Sicherung/-Replikation oder hostbasierte Sicherung/Replikation ohne Agent ist.

5. Geben Sie die Details für die **VM-Einstellungen** für Assured Recovery an.

   Präfix des Namens des virtuellen Rechners

   Gibt das Präfix des VM-Namens an. Der Name des Quellknotens mit einem Präfix ist der Standardname der Instant VM. Einige Sonderzeichen dürfen nicht im Namen verwendet werden, z. B. "@", "\ " usw.

   Standardwert: UDPARVM_

   VM-Dateiordner

   Geben Sie den Ordner an, in dem die Assured Recovery-VM auf dem Proxy-Server gespeichert ist. Sie können die Volume-Informationen des Proxy-Servers durchsuchen.

   CPU-Zähler

   Gibt die Anzahl der CPUs an, die Sie in der Assured Recovery-VM benötigen.

   Speichergröße

Gibt die Größe des Arbeitsspeichers an, den Sie in der Assured Recovery-VM benötigen.

Netzwerkeinstellungen

Legt die Netzwerkeinstellungen für die Assured Recovery-VM fest. Sie können die Option "Connect Assured Recovery VM to Network" (Assured Recovery-VM mit Netzwerk verbinden) aktivieren oder deaktivieren. Außerdem können Sie DHCP-Einstellungen für die Assured Recovery-VM verwenden oder die TCP/IP-Einstellungen der Sicherungssitzung.

Adaptertyp

Legt den Adaptertyp für die Assured Recovery-VM fest. Die verfügbaren Adaptertypen können je nach Hypervisor variieren.

Festlegen der Taskeinstellungen für den Testtyp "Instant Virtual Disk"

Wenn Sie Instant Virtual Disk als Testtyp in den Testeinstellungen auswählen, wird der Wiederherstellungspunkt als lokaler Datenträger bereitgestellt, die Integrität des Volumes/Dateisystems überprüft und optional das benutzerdefinierte Skript ausgeführt. Es wird davon ausgegangen, dass der Wiederherstellungspunkt sich in einem ordnungsgemäßen Zustand befindet, wenn er erfolgreich geladen werden kann und alle Tests ein positives Ergebnis zurückgeben.

Hinweis:

- Dieser Schritt ist nicht erforderlich, wenn Sie als Testtyp **Instant Virtual Machine** ausgewählt haben.
- Die Option **Sofortiger virtueller Datenträger** unterstützt keine Nicht-Windows-Knoten.

Gehen Sie wie folgt vor:

1. Führen Sie einen der folgenden Schritte durch, um einen Server unter **Windows-Proxy-Server:** einzustellen:
   a. Wählen Sie aus der Drop-down-Liste einen der verfügbaren Knoten aus.

      Hinweis: Wenn Sie bereits einen Proxy-Knoten zu dem ausgewählten Standort in der Konsole hinzugefügt haben, finden Sie eine Liste aller Knoten in der Drop-down-Liste **Windows-Proxy-Server**.

   b. Wenn Sie noch keine Proxy-Knoten hinzugefügt haben, gehen Sie wie folgt vor:
      i. Klicken Sie auf **Hinzufügen**.
      ii. Das Dialogfeld **Adding Assured Recovery Proxy Server (Assured Recovery-Proxy-Server hinzufügen)** wird geöffnet.
      iii. Geben Sie die Details zum Proxy-Server an, und klicken Sie auf **OK**.
2. **Navigieren Sie** zum Speicherort des Ordners der Virtual Hard Disk auf dem Proxy-Server.

Angeben eines Ablaufplans für Assured Recovery-Testjobs

Auf der Registerkarte "Ablaufplan" können Sie den Ablaufplan für Assured Recovery-Testjobs festlegen. Wenn Sie keinen Ablaufplan angeben, wird der Task sofort gestartet, nachdem Sie den primären Task abgeschlossen haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ablaufplan**.
2. Klicken Sie auf **Hinzufügen** und dann auf **Ablaufplan für Assured Recovery-Testjob hinzufügen**.

   Das Dialogfeld "Ablaufplan für Assured Recovery-Testjob hinzufügen" wird angezeigt.
3. Legen Sie den Ablaufplan fest, und klicken Sie auf **Speichern**.

   Das Dialogfeld wird geschlossen, und die Registerkarte "Ablaufplan" zeigt den angegebenen Plan an.

   Hinweise:

   - Wenn die Assured Recovery-Quelle über den Ablaufplan "Letzte Widerherstellungspunkte + Assured Recovery aktivieren" verfügt, ist der Standardwert 1. Dadurch wird standardmäßig der letzte Widerherstellungspunkt überprüft.

     Bei einem Wert< = 0 werden alle nicht verifizierten Widerherstellungspunkte getestet.
   - Wenn die Assured Recovery-Quelle über den Ablaufplan "Täglich/Wöchentlich/Monatlich + Assured Recovery aktivieren" verfügt, ist der Standardwert 9 (7 täglich + 1 wöchentlich + 1 monatlich).

     Bei einem Wert< = 0 werden alle nicht verifizierten Widerherstellungspunkte getestet.
   - Wenn Sie nicht den Standardwert verwenden möchten, können Sie einen DWORD-32-Bit-Registrierungsschlüssel an folgendem Ort hinzufügen:

     HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AssuredRecovery\MaxNumberOfRecoveryPoint

Festlegen von erweiterten Einstellungen

Auf der Registerkarte "Erweitert" können Sie andere für den Abschluss des Plans erforderliche Einstellungen festlegen. Diese Einstellungen sind optional und müssen nicht vorgenommen werden, wenn Sie keine weiteren Einstellungen hinzufügen müssen. Einige der Optionen auf der Registerkarte **Erweitert** variieren je nach Ihrer Auswahl auf der vorherigen Registerkarte. Zum Beispiel wird die Option "Eigenschaften der Heartbeat-Signale" nur angezeigt, wenn Sie unter **Testeinstellungen** als Testtyp "Sofortiger virtueller Rechner" ausgewählt haben.

Eigenschaften der Heartbeat-Signale

Hinweis: Die Option "Eigenschaften der Heartbeat-Signale" wird nur angezeigt, wenn Sie als Testtyp "Sofortiger virtueller Rechner" ausgewählt haben.

Zeitlimit

Gibt an, wie lange der Proxy-Server maximal auf das Heartbeat-Signal der Assured Recovery-VM warten darf. Wenn die Assured Recovery-VM über das definierte Zeitlimit hinaus nicht verfügbar ist, schlägt der Assured Recovery-Testjob fehl.

Häufigkeit

Gibt an, wie häufig der Proxy-Server den Heartbeat-Zustand der Assured Recovery-VM überprüft.

Hinweis: Diese Option wird nicht angezeigt, wenn Sie Agent-basierte Linux-Sicherung/-Replikation als Wiederherstellungspunktquelle des Assured Recovery-Tests ausgewählt haben.

Kontrollpunkte

Hinweis: Die Option wird nur angezeigt, wenn Sie als Testtyp "Instant Virtual Disk" ausgewählt haben.

Dateisystem überprüfen

Überprüft, ob das Dateisystem und die Größe des Volumes denen des Quellrechners entsprechen.

Befehl zum Prüfen des Datenträgers ausführen

Überprüft die Integrität der Daten durch Ausführung des Befehls zur Datenträgerüberprüfung für die Volumes der Instant Virtual Disk.

Benutzerdefinierter Befehlsspeicherort auf dem Proxy

Hinweis: Diese Option wird nicht angezeigt, wenn Sie Agent-basierte Linux-Sicherung/-Replikation als Wiederherstellungspunktquelle des Assured Recovery-Tests ausgewählt haben.

Gibt das benutzerdefinierte Skript an, das auf dem Proxy-Server gespeichert ist. Sie können die Volume-Informationen des Proxy-Servers durchsuchen. Wenn IVM als Assured Recovery-Typ ausgewählt ist, wird das Skript in die VM kopiert und ausgeführt, wenn die VM gestartet wird. Wenn IVHD als Assured Recovery-Typ ausgewählt ist, wird das Skript auf dem Proxy-Server ausgeführt.

Hinweis: Der Assured Recovery-Job unterstützt nur das ausführbare Windows-BAT-Skript oder die ausführbare Binärdatei. Diese Einschränkung schränkt jedoch Ihre Nutzung des Assured Recovery-Jobs nicht ein. Sie können ein zum Starten Ihres PowerShell-Skripts geschriebenes Windows-Batch-Skript verwenden, mit dem Namen "test.bat" und dem folgenden Inhalt:

Powershell.exe -NoProfile -ExecutionPolicy ByPass -Command "& '%ScriptPath%\AR-check.ps1'"

Darüber hinaus werden die folgenden Argumente gemäß Ihren Anforderungen an das Skript übergeben.

- set PlanName=%1%

- set NodeName=%2%

- set ProxyServer=%3%

- set RecoveryPointName=%3%

- set MountPointRootPathName=%5% (gilt nur für Instant Virtual Disk-Testtyp)

Dadurch wird das BAT-Skript aufgerufen und wie folgt ausgeführt:

Für den Testtyp Instant Virtual Machine:

"%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName

Für den Testtyp Instant Virtual Disk:

%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName MountPointRootPathName

Beendigungscode

Gibt den Beendigungscode für "Job erfolgreich durchführen" oder "Job fehlschlagen" an.

Job erfolgreich

Gibt an, dass der Assured Recovery-Job erfolgreich durchgeführt wird, wenn das Skript den Beendigungscode zurückgibt.

Job fehlschlagen

Gibt an, dass der Assured Recovery-Job fehlschlagen wird, wenn das Skript den Beendigungscode zurückgibt.

Job schlägt fehl, wenn die Ausführung länger dauert als

Gibt an, ob das Skript über die festgelegte Zeit hinaus ausgeführt wird.

Standardwert: 15 Minuten

Linux Prä-/Post-Skript-Einstellung auf Proxy

Hinweis: Diese Option wird nur angezeigt, wenn Sie Agent-basierte Linux-Sicherung/-Replikation oder hostbasierte Sicherung/Replikation ohne Agent als Wiederherstellungspunktquelle des Assured Recovery-Tests ausgewählt haben.

Auf Linux-Sicherungsserver nach Abschluss des Assured Recovery-Jobs ausführen

Gibt das Skript auf dem Linux-Proxy an, das nach Abschluss des Assured Recovery-Jobs auf dem Linux-Sicherungsserver ausgeführt wird.

Auf Assured Recovery-VM ausführen, nachdem eine Assured Recovery-VM gestartet wurde

Gibt das Skript auf dem Linux-Proxy an, das nach dem Start der Assured Recovery VM auf der Assured Recovery VM ausgeführt wird.

Job schlägt fehl, wenn die Ausführung länger dauert als

Gibt an, ob das Skript über die festgelegte Zeit hinaus ausgeführt wird.

E-Mail-Alerts

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Typen der Alerts angeben, die Sie in einer E-Mail erhalten möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

Hinweise: Für Jobs mit Linux-Sicherungsserver nicht verfügbar.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers im Dialogfenster **E-Mail-Einstellungen**.

Festlegen von Sicherungskennwörtern für einen oder mehrere Knoten

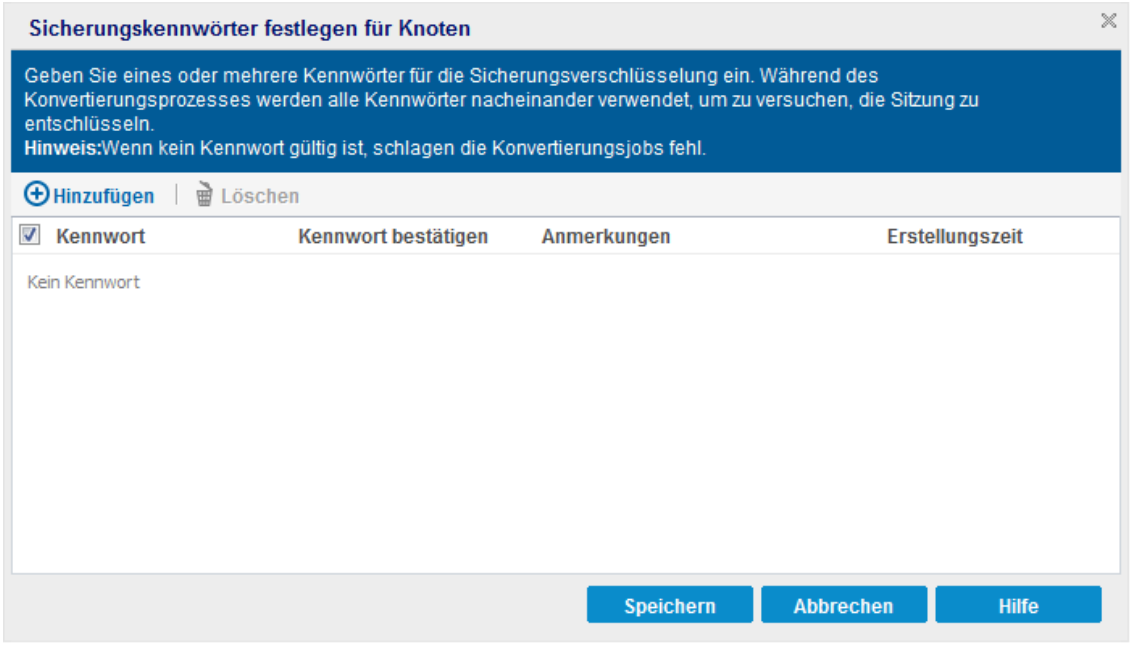
Um zu gewährleisten, dass der Assured Recovery-Auftrag die replizierten Wiederherstellungspunkte testen kann, lässt Assured Recovery Sie Sicherungskennwörter für die Daten bestimmen. Jobs mit Zugriff auf Backup-Sitzungen verwenden kontinuierlich Kennwörter, um die Sitzung zu entschlüsseln.

Hinweis: Wenn keines der Kennwörter gültig ist, schlägt der Zugriff des Jobs auf die Sicherungssitzung fehl.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.
3. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Sicherungskennwörter festlegen**.

   Das Dialogfeld **Sicherungskennwörter festlegen für Knoten** wird geöffnet.

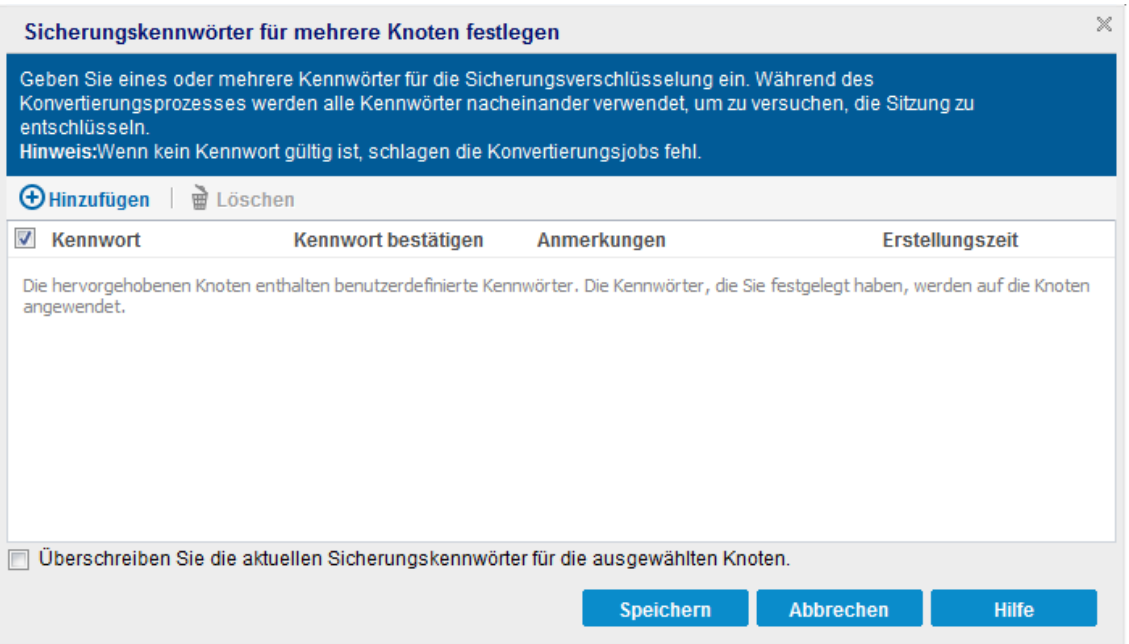


4. Führen Sie im Dialogfeld **Sicherungskennwörter festlegen** folgende Tasks für einen oder mehrere Knoten aus:

   Hinzufügen: Klicken Sie auf **Hinzufügen**, um Sicherungskennwörter zu den ausgewählten Knoten hinzuzufügen.

   Löschen: Klicken Sie auf **Löschen**, um Sicherungskennwörter aus den ausgewählten Knoten zu löschen.

Hinweis: Sie können die aktuellen Sicherungskennwörter für mehrere Knoten überschreiben, indem Sie das Kontrollkästchen **Überschreiben Sie die aktuellen Sicherungskennwörter für die ausgewählten Knoten** aktivieren.



5. Klicken Sie auf **Speichern**.

   Das Dialogfeld wird geschlossen und die Sicherungskennwörter wurden für die ausgewählten Remote-Knoten festgelegt.

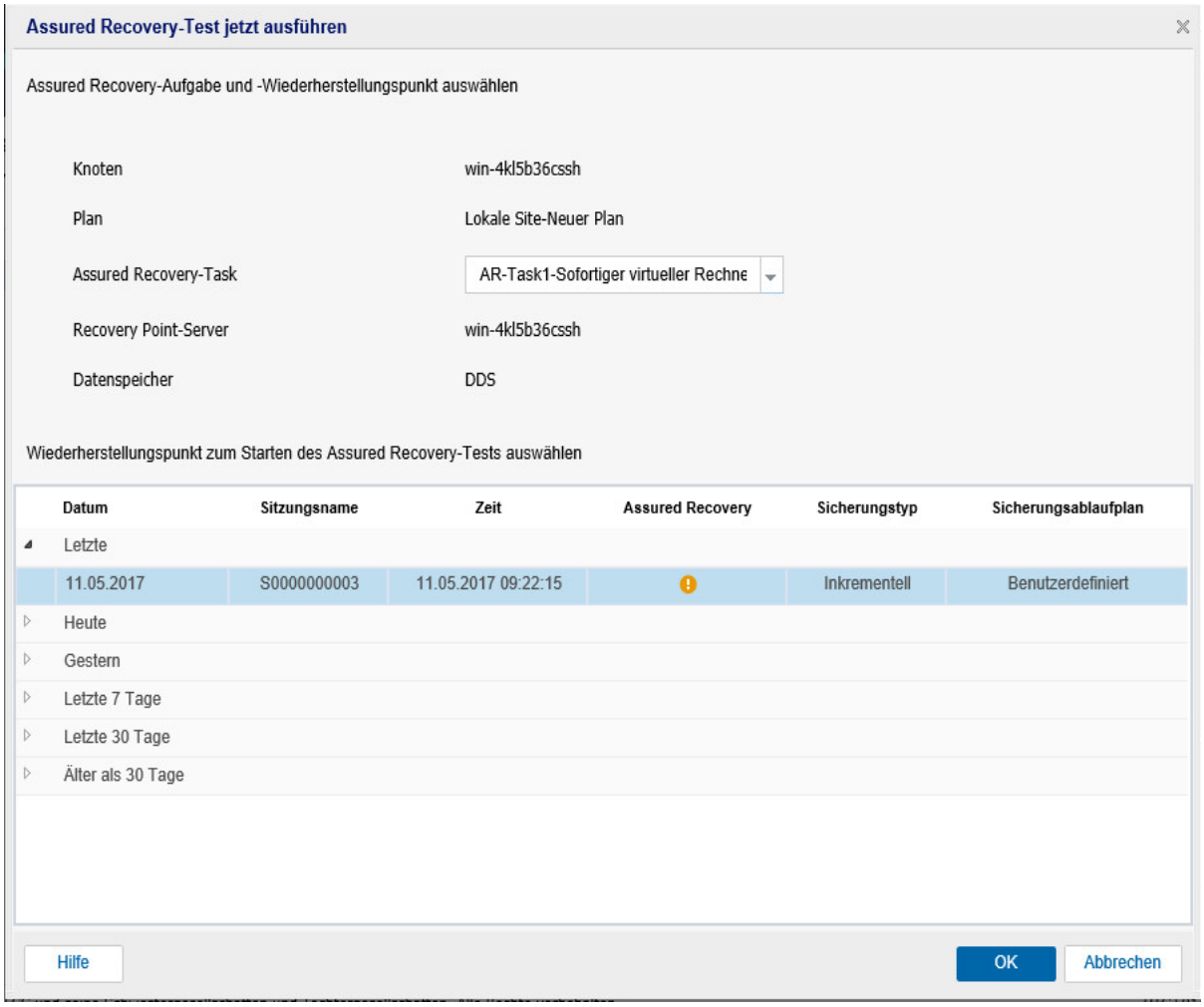
(Optional) Manuelles Ausführen von Assured Recovery-Testjobs

In Arcserve UDP werden alle Pläne, einschließlich Assured Recovery-Jobs, automatisch ausgeführt und über die Ablaufplaneinstellungen gesteuert. Für Assured Recovery-Jobs gilt: Arcserve UDP erlaubt neben der geplanten Ausführung auch die manuelle Ausführung von Assured Recovery-Tests für Knoten und Pläne. In diesem Artikel finden Sie zwei separate Anleitungen zur Durchführung von manuellen Assured Recovery-Tests für Knoten und Pläne.

Gehen Sie wie folgt vor, um einen manuellen Assured Recovery-Test für einen Knoten auszuführen:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu Knoten, und klicken Sie auf **Alle Knoten**.
3. Wählen Sie aus dem mittleren Fensterbereich die Knoten aus, denen ein Assured Recovery-Plan zugewiesen ist, und klicken Sie auf **Aktionen**.
4. Wählen Sie aus den unter "Aktionen" angezeigten Optionen die Option **Run Assured Recovery Test Now** aus.

   Das Dialogfeld "Assured Recovery" wird geöffnet.



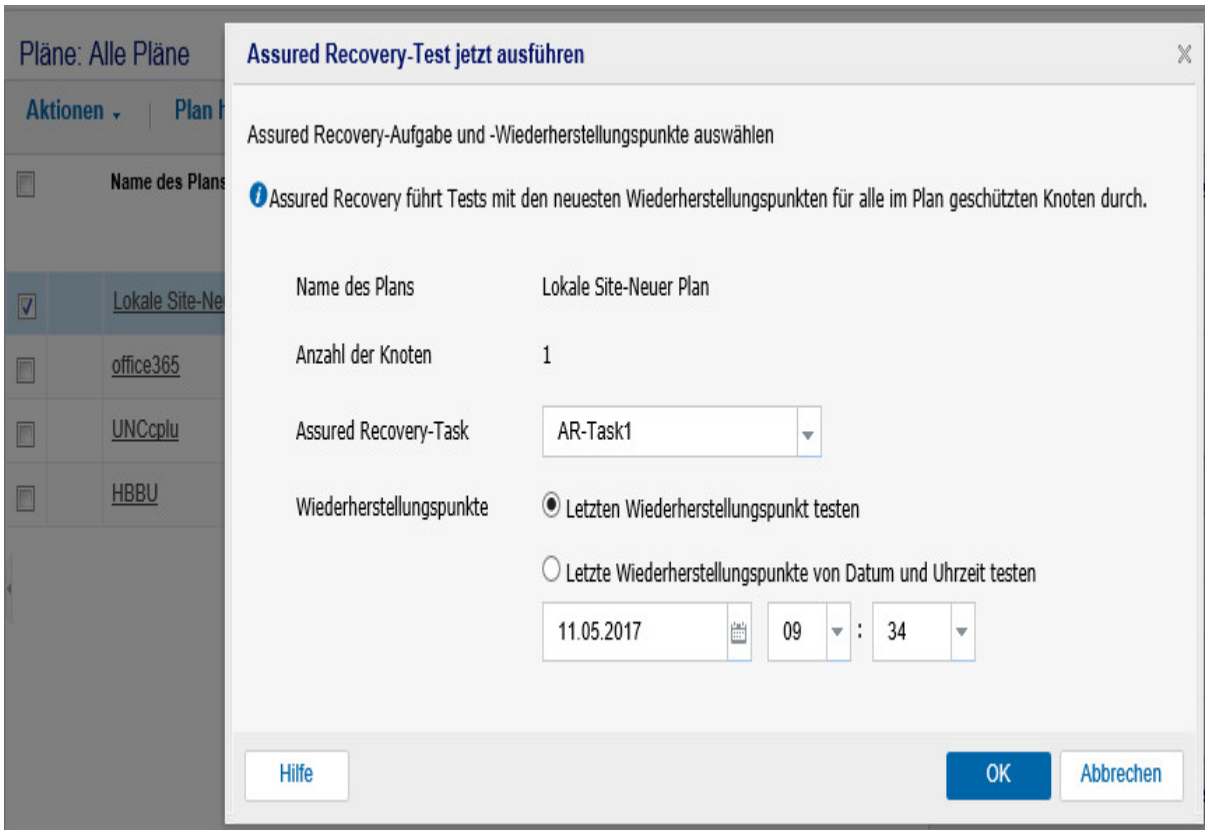
5. Wählen Sie einen Assured Recovery-Task und einen Wiederherstellungspunkt aus, und klicken Sie auf **OK**.

   Der Assured Recovery-Test für den Knoten wird ausgeführt.

   Gehen Sie wie folgt vor, um einen manuellen Assured Recovery-Test für einen Plan auszuführen:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu Pläne, und klicken Sie auf **Alle Pläne**.
3. Wählen Sie aus dem mittleren Fensterbereich einen Assured Recovery-Plan aus, und klicken Sie auf **Aktionen**.
4. Wählen Sie aus den unter "Aktionen" angezeigten Optionen die Option **Run Assured Recovery Test Now** aus.

   Das Dialogfeld "Assured Recovery" wird geöffnet.



5. Wählen Sie einen Assured Recovery-Task und eine der Optionen für den Wiederherstellungspunkt aus, und klicken Sie auf **OK**.

   Der Assured Recovery-Test für den Plan wird ausgeführt.

Erstellen eines Sicherungsplans für UNC/NFS-Pfade

Um Ihre Verzeichnisse und Dateien im UNC/NFS-Pfad zu schützen, müssen Sie einen Plan erstellen. Der Plan für den UNC/NFS-Pfad besteht aus einem Sicherungstask. In diesem Sicherungstask können Sie die Knoten, die Sie schützen möchten, das Sicherungsziel und den Ablaufplan für die Sicherung angeben. Beim Sicherungsziel handelt es sich um einen Recovery Point Server, auf dem Sie Ihre Sicherungsdaten speichern möchten. Das Ziel ist ein freigegebener Remote-Ordner. Bei einem UNC/NFS-Pfad beträgt die maximale Sicherungsgröße 128 TB.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen einer Dateifreigabe
3. Erstellen eines Sicherungsplans
4. (Optional) Ausführen einer manuellen Sicherung
5. Erstellen anderer Aufgaben im UNC/NFS-Plan
6. Überprüfen der Sicherung

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie die folgenden erforderlichen Aufgaben durchgeführt haben:

1. Melden Sie sich bei der Konsole an.
2. Bereiten Sie einen Sicherungs-Proxy-Server für UNC/NFS-Pfade vor, auf dem Arcserve Unified Data Protection Agent für Windows installiert ist.
3. Halten Sie Benutzeranmeldeinformationen bereit, die mindestens die Leseberechtigung für den UNC/NFS-Pfad beinhalten, den Sie schützen möchten.

   Hinweis: Informationen zum Hinzufügen, Aktualisieren und Löschen eines UNC/NFS-Pfad-Knotens finden Sie unter Hinzufügen und Verwalten eines UNC/NFS-Pfades.
4. Bereiten Sie einen Recovery Point Server mit einem Datenspeicher mit oder ohne Deduplizierung vor.
5. Erstellen Sie einen Datenspeicher zum Speichern Ihrer Sicherungsdaten.
6. Erstellen Sie eine Dateifreigabe im Nutanix Prism-Webportal.

Besondere Aspekte:

- Zusätzlicher Lizenzverbrauch für UNC-Pfade. Gehen Sie auf Fehlerbehebung, um das Problem zu lösen.
- Der Sicherungs-Proxy ist immer ein Windows-Rechner.
- Damit der Nutanix-NFS-Plan funktioniert, muss NfsUtils auf dem Sicherungs-Proxy-Rechner vorinstalliert sein (wie dies bei dem integrierten NFS-Plan der Fall ist).
- Wenn bei einem Nutanix File Server eine der FSVMs aus dem Cluster fehlschlägt, wird die andere FSVM zum primären Besitzer des File Servers, und HA wird für den FSVM-Cluster aktiviert.

Erstellen einer Dateifreigabe

Auf der Seite "Share/Export" können Sie verteilte oder standardmäßige Dateifreigaben erstellen. Eine verteilte Freigabe oder Stammfreigabe ist ein Repository, in dem sich die persönlichen Dateien eines Benutzers befinden, während die Standardfreigabe oder universelle Freigabe ein von der Gruppe gemeinsam genutztes Repository ist. Eine verteilte Freigabe wird in den Verzeichnissen der obersten Ebene verteilt, während sich die Standardfreigabe auf einer einzelnen Dateiserver-

VM (FSVM) befindet. Dieser Abschnitt enthält Informationen zum Erstellen einer Dateifreigabe zur Durchführung der UNC/NFS-Sicherung für Nutanix Files.

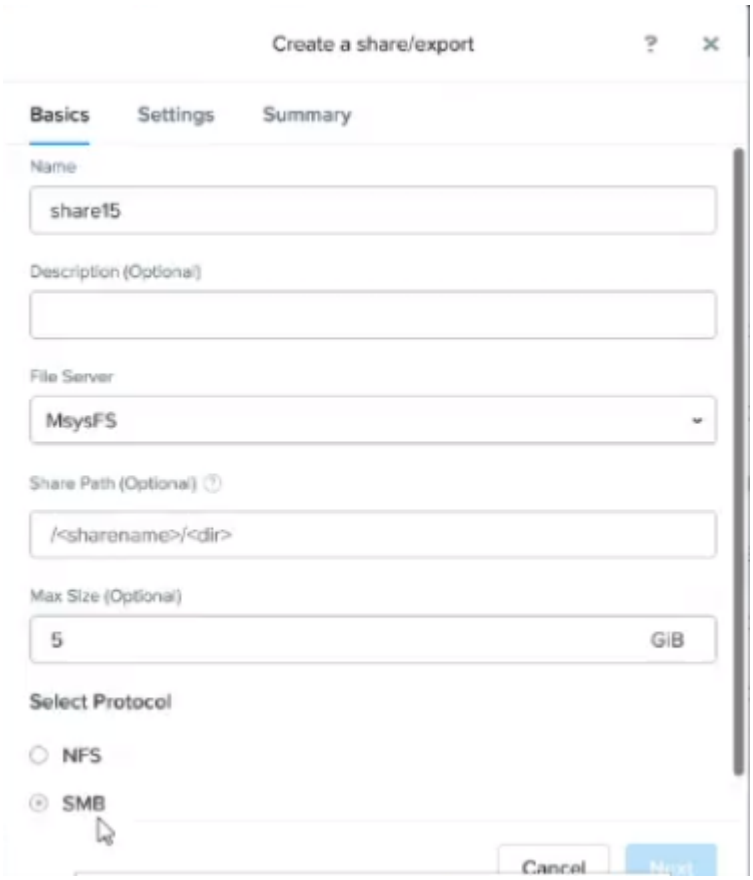
Gehen Sie wie folgt vor:

1. Melden Sie sich beim Nutanix Prism-Webportal an.
2. Navigieren Sie im Hauptmenü zu **File Server**, und klicken Sie dann im Dashboard "File Server" auf **Share/Export**.

   Das Fenster "Create a share/export" wird mit der Registerkarte "Basics" angezeigt.
3. Führen Sie auf der Registerkarte "Basics" die folgenden Schritte aus, und klicken Sie dann auf **Next**:
   - Name: Geben Sie einen Namen für die Freigabe ein.

     Hinweis: Für den Freigabenamen gelten die folgenden Namenskonventionen:
     - Jeder Name muss eindeutig sein.
     - Bei Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
     - Dateien dürfen Unicode-Zeichen enthalten.
     - Die maximale Namenslänge beträgt 80 Zeichen.
     - Ein Leerzeichen darf nicht als erstes oder letztes Zeichen im Namen verwendet werden.
     - Namen, die auf $ enden, sind versteckte Freigaben.
   - Description (optional): Geben Sie bei Bedarf eine Beschreibung für die Freigabe ein.
   - File Server: Wählen Sie in der Drop-down-Liste einen Dateiserver aus, auf dem sich die Freigabe befindet.
   - Share Path (optional): Geben Sie den Dateipfad zur Freigabe an.
   - Max Size (optional): Geben Sie die maximale Größe der Freigabe ein. Standardmäßig wird die Größe in GiB angegeben.
   - Select Protocol: Wählen Sie **SMB** als Protokoll aus.

     Hinweis: Um die Multiprotokollfunktion zu aktivieren, aktivieren Sie das Kontrollkästchen **Enable multiprotocol access for NFS**.



4. Behalten Sie auf der Registerkarte "Einstellungen" die Standardeinstellungen bei, oder nehmen Sie Änderungen nach Bedarf vor, und klicken Sie dann auf **Next**.

   Use "Distributed" share type instead of "Standard"

   Ermöglicht das Erstellen einer verteilten Freigabe.

   Hinweis: Standardmäßig werden bei Einzel-FSVM-Bereitstellungen Standardfreigaben erstellt.

   Enable Self Service Restore

   Ermöglicht die Wiederherstellung von Dateien aus früheren Snapshots.

   Enable File System Compression

   Ermöglicht es Ihnen, Speicherplatz zu sparen und die Datenmenge auf der Freigabe zu reduzieren, indem für die geschriebenen Daten eine Inline-Komprimierung durchgeführt wird.

   Hinweis: Stellen Sie sicher, dass Sie die Komprimierung auf Containerebene deaktivieren. Wenn Sie die Komprimierung aktiviert haben, wird die Option "Enable File System Compression" deaktiviert.

   Enable Access Based Enumeration (ABE)

Ermöglicht die Aktivierung von Access-Based Enumeration (ABE).

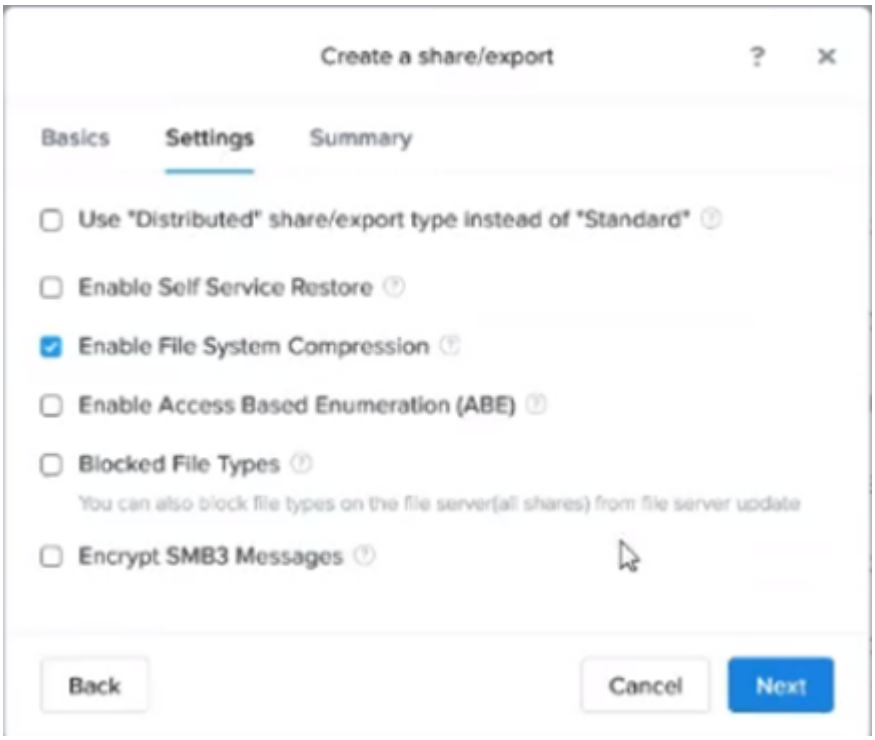
Blocked File Types

Ermöglicht die Angabe der blockierten Dateitypen.

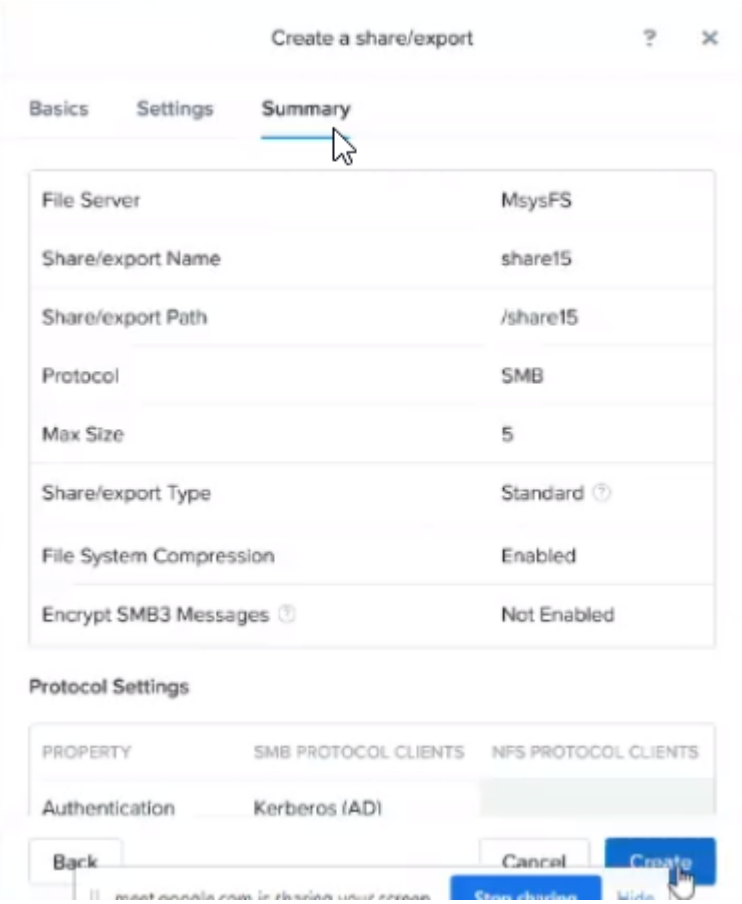
Geben Sie eine durch Kommas getrennte Liste von Dateitypen ein, die für die Freigabe gesperrt werden sollen.

Encrypt SMB3 Messages

Ermöglicht die Aktivierung der Nachrichtenverschlüsselung zwischen dem Dateiserver und dem Client.



5. Überprüfen Sie die Details auf der Seite "Summary", und klicken Sie dann auf **Create**.



Hinweis: Um Änderungen an den Einstellungen der vorherigen Seiten vorzunehmen, klicken Sie auf **Back**.

Die Dateifreigabe wird erfolgreich erstellt.

Hinweis: Kopieren Sie als Nächstes den Ladepfad, und ordnen Sie dann die neu erstellte Freigabe im lokalen UDP zu. Weitere Informationen hierzu Sie unter Schritt 6 (a1) von "Angeben der Quelle".

Erstellen eines Sicherungsplans mit einem UNC/NFS-Pfad-Task

Ein Sicherungsplan enthält einen Sicherungstask, der eine Sicherung eines physischen Knotens ausführt und die Daten an einem angegebenen Ziel speichert. Jeder Task besteht aus Parametern, die Quelle, Ziel, Ablaufplan und weitere Sicherungsdetails definieren.

Gehen Sie wie folgt vor:

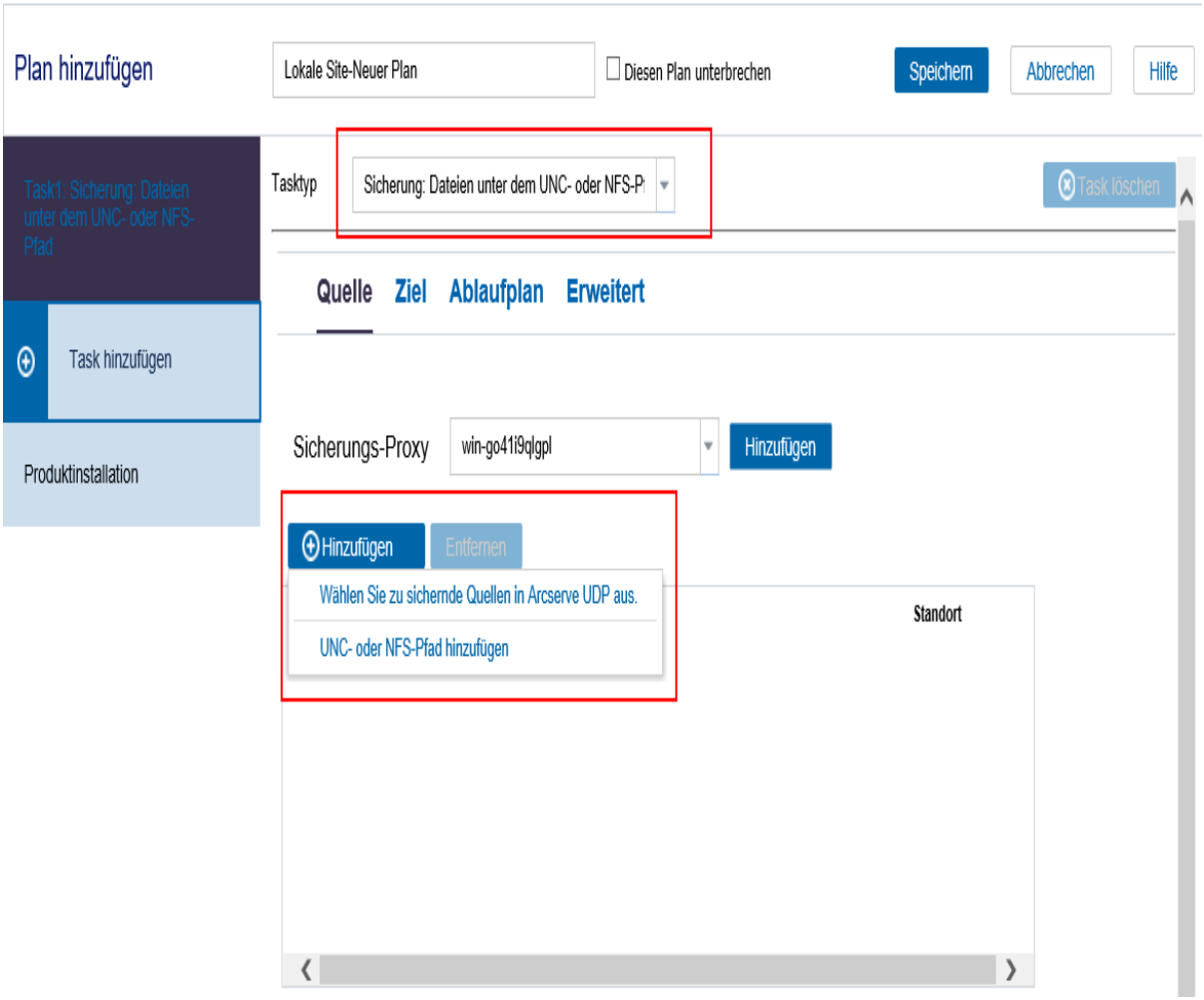
1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie dann auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
4. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Die Seite Plan hinzufügen wird geöffnet.
5. Geben Sie einen Plannamen ein.
6. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
7. Wählen Sie aus der Dropdown-Liste Tasktyp die Option **Sicherung: Dateien im UNC/NFS-Pfad** aus.



Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die Quellknoten angeben, die Sie schützen möchten. Sie können mehrere Knoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Knoten hinzufügen, wenn Sie einen Plan auf der Quellenseite erstellen oder ändern. Sie können einen Plan auch speichern, ohne Quellknoten hinzuzufügen. Der Plan wird erst bereitgestellt, wenn Sie Quellknoten hinzugefügt haben.

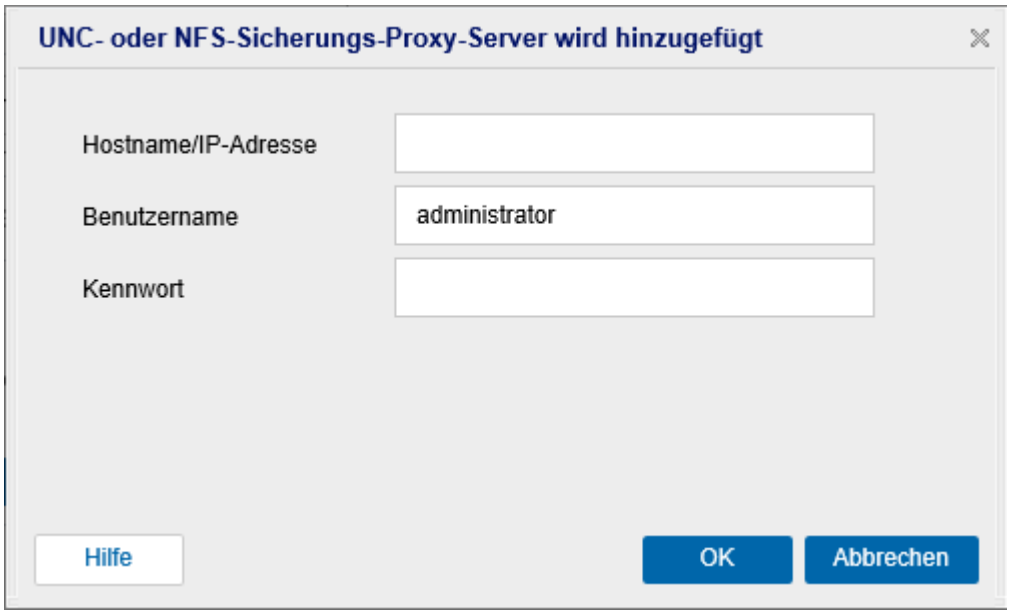
Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Quelle**.
2. Wenn der Sicherungs-Proxy bereits hinzugefügt wurde, wählen Sie ihn in der Drop-Down-Liste "Sicherungs-Proxy" aus.

   Der Proxyserver ist ein Knoten, auf dem Arcserve Unified Data Protection Agent für Windows installiert wird.

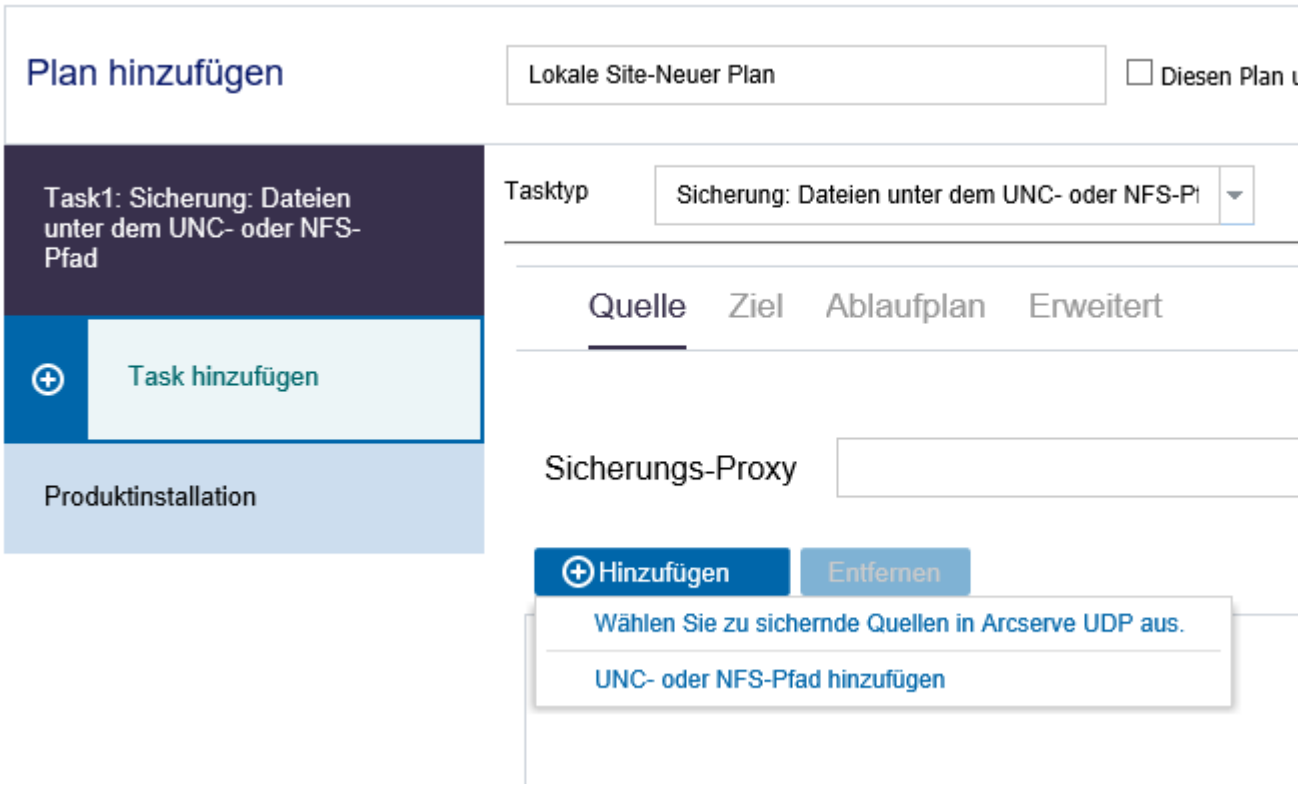
3. Wenn der Sicherungs-Proxy nicht hinzugefügt wurde, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf **Hinzufügen**.

      Das Dialogfeld "UNC oder NFS Backup Proxy Server hinzufügen" wird geöffnet.



b. Geben Sie die Details zum Proxy-Server an, und klicken Sie dann auf **OK**.

4. Um den UNC- oder NFS-Pfadknoten hinzuzufügen, klicken Sie auf **+Hinzufügen**, und wählen Sie dann eine der folgenden Optionen aus:



Auswählen von zu schützenden Quellen in Arcserve UDP

Öffnet das Dialogfeld Zu schützende Knoten auswählen, in dem Sie die Knoten aus der angezeigten Liste auswählen können. Wählen Sie diese Option aus, wenn Sie die Knoten bereits zu der Konsole hinzugefügt haben.

UNC- oder NFS-Pfad hinzufügen

Öffnet das Dialogfeld Knoten zu Arcserve UDP-Konsole hinzufügen. Wählen Sie diese Option aus, wenn Sie die Knoten nicht hinzugefügt haben und die zu schützenden Knoten manuell hinzufügen möchten.

5. Wenn Sie die Option **Auswählen von zu schützenden Quellen in Arcserve UDP** wählen, führen Sie folgende Schritte aus:

   a. (Optional) Wählen Sie einen Filter aus der Dropdown-Liste "Gruppen" aus, um nach Knoten zu filtern. Sie können Schlüsselwörter eingeben, um den Knotenfilter weiter einzuschränken.

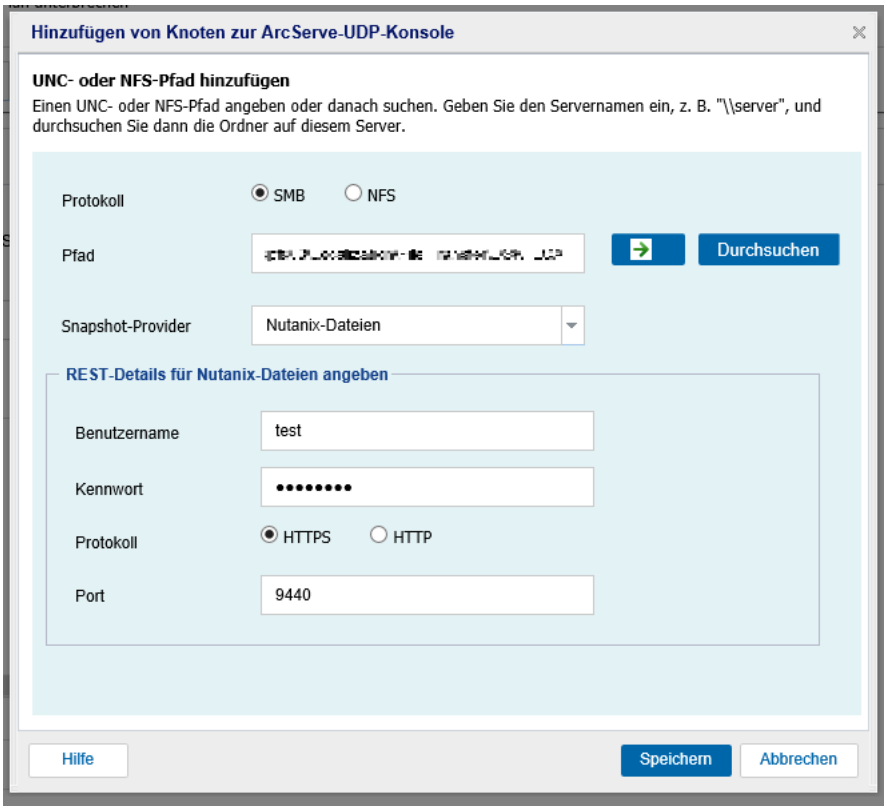
   Die Knoten werden im Bereich "Verfügbare Knoten" angezeigt.

   b. Wählen Sie die Knoten im Bereich Verfügbare Knoten aus, und klicken Sie dann auf das Symbol **Alle Knoten hinzufügen** (>>) oder **Ausgewählte Knoten hinzufügen** (>).

   Die ausgewählten Knoten werden im Bereich "Ausgewählte Knoten" angezeigt.

   c. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

6. Wenn Sie die Option **UNC- oder NFS-Pfad hinzufügen** auswählen, führen Sie auf der gleichnamigen Seite die folgenden Schritte aus:



a. Wählen Sie **SMB** oder **NFS** als Protokoll aus.

- Wenn Sie **SMB** auswählen, gehen Sie folgendermaßen vor:

1. Geben Sie den UNC-Pfad im folgenden Format ein:

   *Hostname**share*

   Hinweise:

   - Während die Nutanix-Dateifreigabe als Quelle für die Sicherung mit Nutanix-Dateien als Snapshot-Provider bereitgestellt wird, können Sicherungen nur auf Freigabeebene, jedoch nicht auf Unterordnerebene durchgeführt werden.
   - Gehen Sie folgendermaßen vor, um den UNC-Pfad abzurufen:

     a. Wählen Sie die neu erstellte Freigabe im mittleren Fensterbereich aus.

     b. Navigieren Sie in der Spalte SHARE/EXPORT DETAILS im Fensterbereich "Zusam-

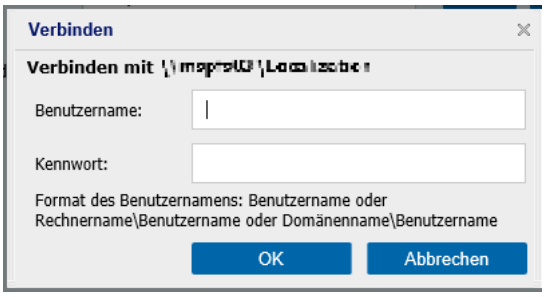
menfassung" zu **Mount Path**, und kopieren Sie dann den Ladepfad.

Wenn der UNC-Pfad gültig ist, werden ein Nach-rechts-Pfeil und die Option "Durchsuchen" aktiviert.

2. Klicken Sie auf den Pfeil nach rechts (>), um den UNC-Pfad zu validieren.

   Das Dialogfeld Verbinden wird angezeigt.

3. Geben Sie den Benutzernamen und das Kennwort nach Bedarf ein, und klicken Sie auf **OK**.



   Im Dialogfeld Knoten zu Arcserve UDP-Konsole hinzufügen wird der verifizierte UNC-Pfad angezeigt.

- Wenn Sie "NFS" auswählen, gehen Sie folgendermaßen vor:

  1. Geben Sie den UNC-Pfad im folgenden Format ein:

     *Hostname**share*

  2. Wählen Sie die Codierung aus den verfügbaren Optionen aus: "ANSI", "GB2312-80", "KSC5601", "BIG5", "SHIFT-JIS", "EUC-KR", "EUC-TW" und "EUC-JP".

     Der Standardwert ist ANSI.

     Hinweis: Während der Sicherung eines freigegebenen NFS-Ordners werden alle entsprechenden Dateien/Ordner, deren Name eine nicht unterstützte Sprachcodierung verwendet, übersprungen, oder es werden unbrauchbare Namen angezeigt.

b. Wählen Sie in der Drop-down-Liste "Snapshot Provider" die Option **Nutanix-Dateien** aus.

c. Geben Sie im Feld "REST-Details für Nutanix-Dateien angeben" die folgenden Anmeldeinformationen an:

   Benutzername

Bezieht sich auf den Benutzernamen, der vom REST-API-Benutzer mithilfe von Nutanix Prism erstellt wurde.

Kennwort

Bezieht sich auf das Kennwort für den Benutzernamen.

Protokoll

Gibt das Protokoll an, das Sie für die Kommunikation mit dem Zielserver verwenden möchten. Die verfügbaren Optionen sind HTTP und HTTPS.

Hinweis: Wählen Sie für sichere Kommunikation das HTTPS-Protokoll aus.

Port

Bezieht sich auf die Portnummer. Der Standardwert für den Port ist 9440; hiermit kann auf die REST-API-Aufrufe und Prism zugegriffen werden.

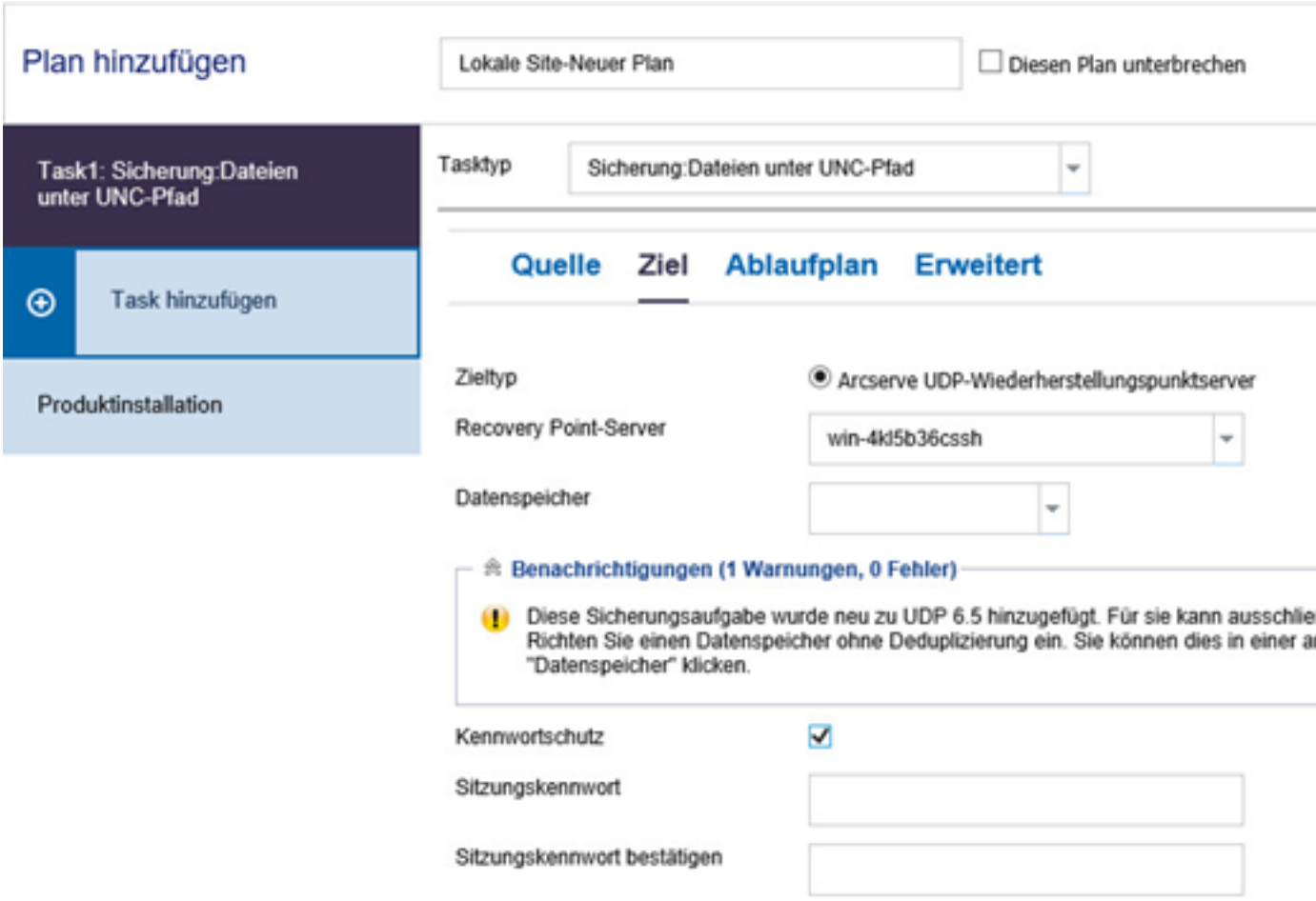
d. Klicken Sie auf **Speichern**.

Hinweis: Wenn die Verbindung zum Nutanix File Server fehlschlägt, wird das Fehlerdialogfeld/ein Benachrichtigungsfenster angezeigt. Klicken Sie auf **OK**, um das Fehlerdialogfeld zu schließen.

Die Sicherungsquelle ist nun angegeben.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.



Geben Sie die folgenden Details an:

- Zieltyp: Überprüfen Sie, ob die Option **Arcserve UDP-Recovery Point Server** standardmäßig ausgewählt ist.
- Recovery Point Server: Wählen Sie einen Recovery Point Server in der Drop-down-Liste aus.
- Datenspeicher: Wählen Sie einen Datenspeicher in der Drop-down-Liste aus.

  Die Liste enthält alle Datenspeicher, die am angegebenen Recovery Point Server erstellt wurden.
- Kennwortschutz: Geben Sie ein Sitzungskennwort an, und geben Sie es zur Bestätigung erneut ein.

Hinweis: Das Sitzungskennwort ist optional, wenn das Sicherungsziel ein unverschlüsselter RPS-Datenspeicher ist.

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

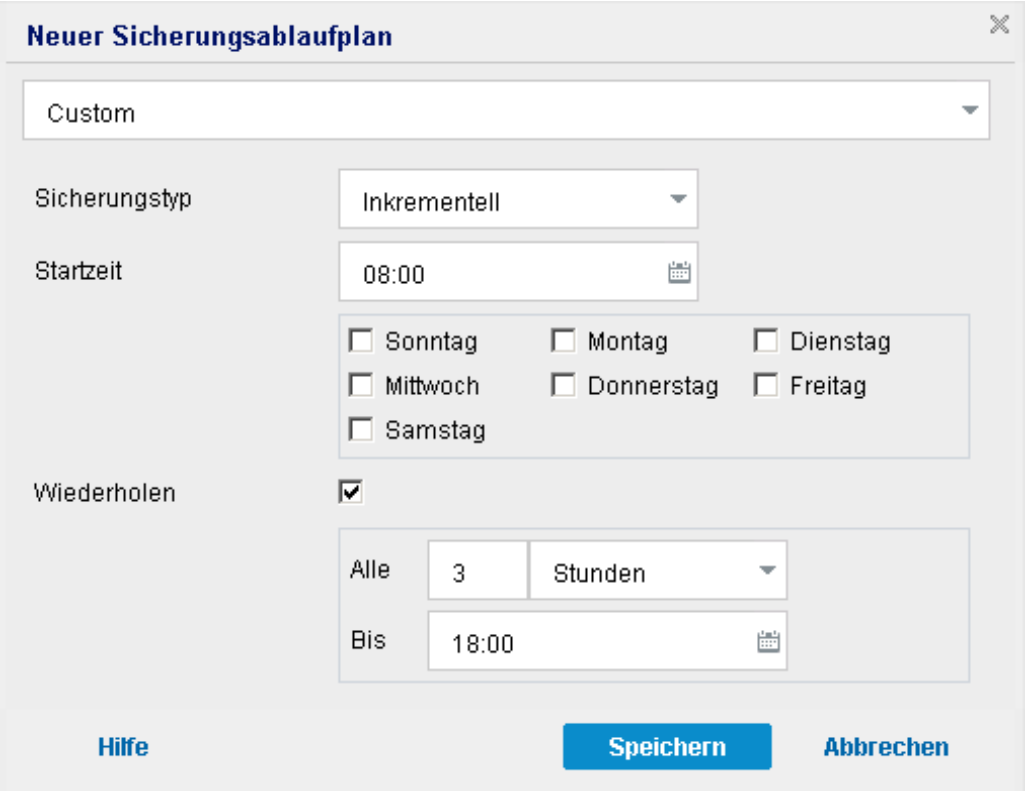
Gehen Sie wie folgt vor:

1. Hinzufügen von Backup, Zusammenführen, Drosselung für Datenträger-Lesevorgang und Ablaufpläne für die Netzwerkdrosselung.

Hinzufügen eines Sicherungsablaufplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

   Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke

des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Überprüfen

Legt den Ablaufplan für Überprüfungssicherungen fest.

Arcserve UDP überprüft die Gültigkeit und Vollständigkeit der geschützten Daten durch einen Vergleich des gespeicherten Sicherungs-Images mit der Sicherungsquelle. Im Bedarfsfall wird das Image neu synchronisiert. Bei einer Überprüfungssicherung wird die letzte Sicherung jedes einzelnen Blocks mit den Inhalten und Informationen der Quelle verglichen. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht (zumeist aufgrund von Änderungen seit der letzten Sicherung), aktualisiert Arcserve UDP die Sicherung dieses Blocks (Neusynchronisierung). In seltenen Fällen kann eine Überprüfungssicherung auch durchgeführt werden, um eine vollständige Sicherung zu erhalten, ohne den erforderlichen Speicherplatz einer vollständigen Sicherung zu verwenden.

Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteile: Die Sicherung benötigt viel Zeit, da alle Quellenblöcke mit den Blöcken der letzten Sicherung verglichen werden.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

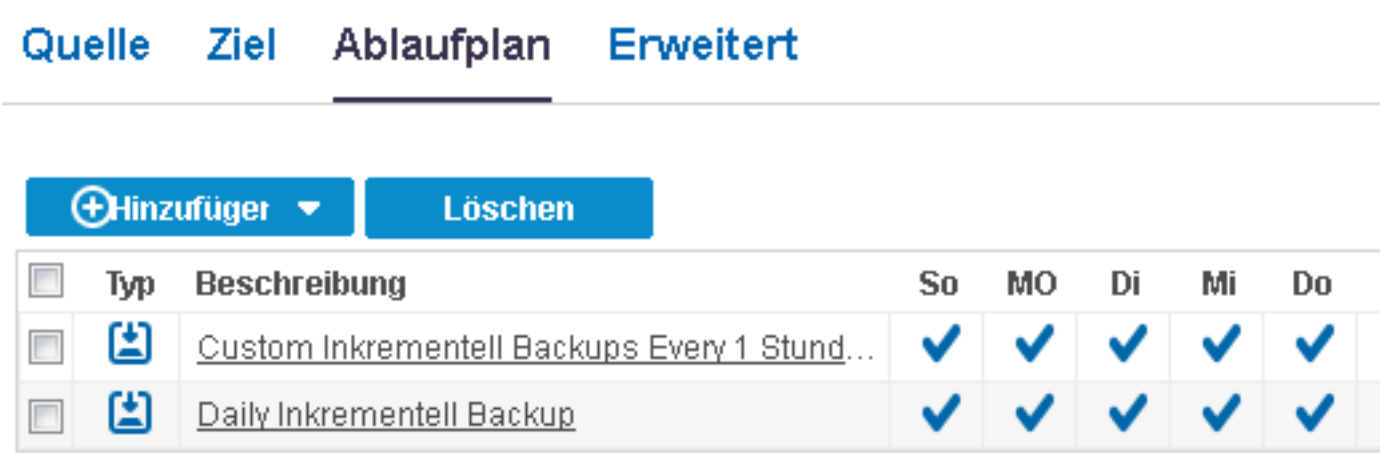
Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die nach der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Diese ist der optimale Weg, um eine Sicherung durchzuführen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

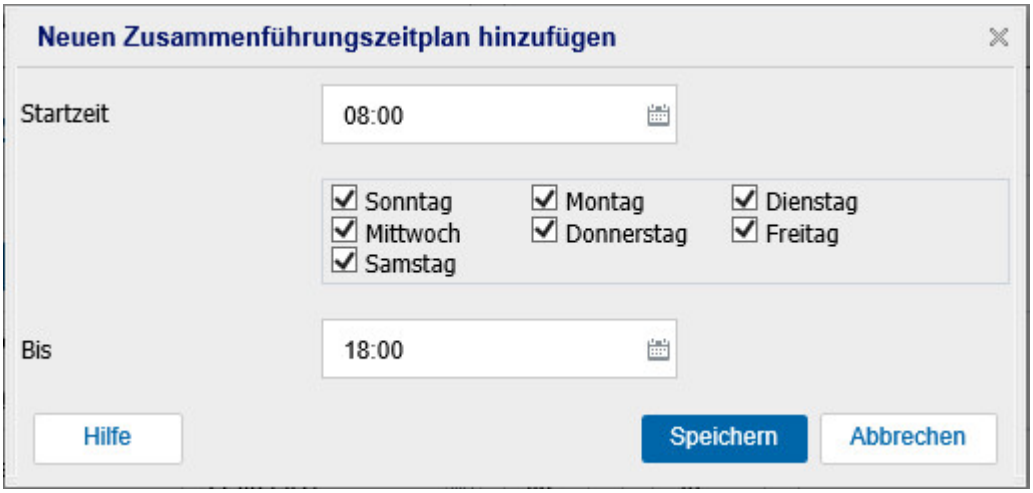
Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.



Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zusammenführungsplan hinzufügen** aus.

   Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.



b. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

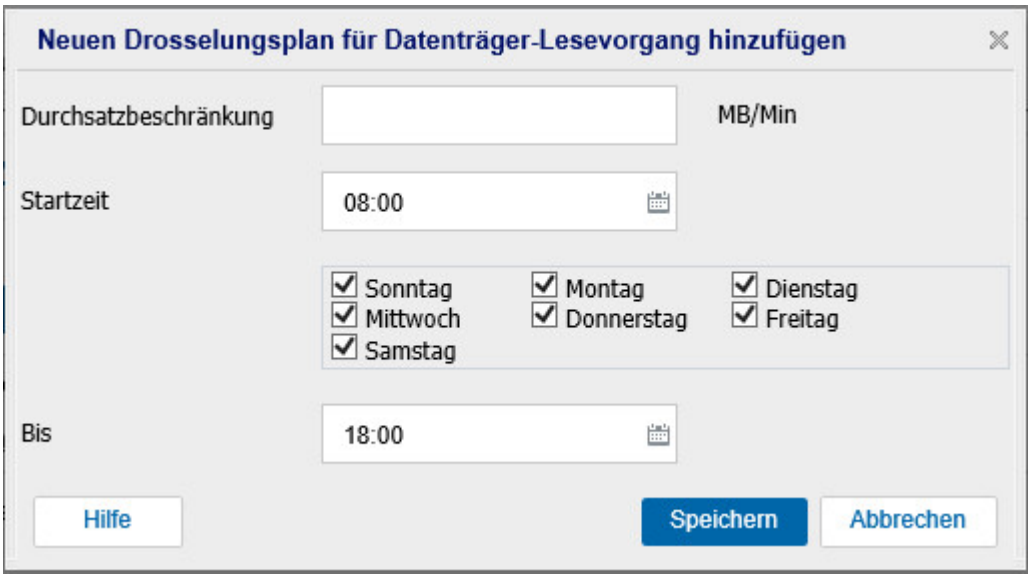
d. Klicken Sie auf **Speichern**.

Der Zusammenführungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Drosselungsplans für Datenträger-Lesevorgänge

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan für Datenträger-Lesevorgang hinzufügen** aus.

   Das Dialogfeld **Neuen Drosselungsplan für Datenträger-Lesevorgang hinzufügen** wird geöffnet.



b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

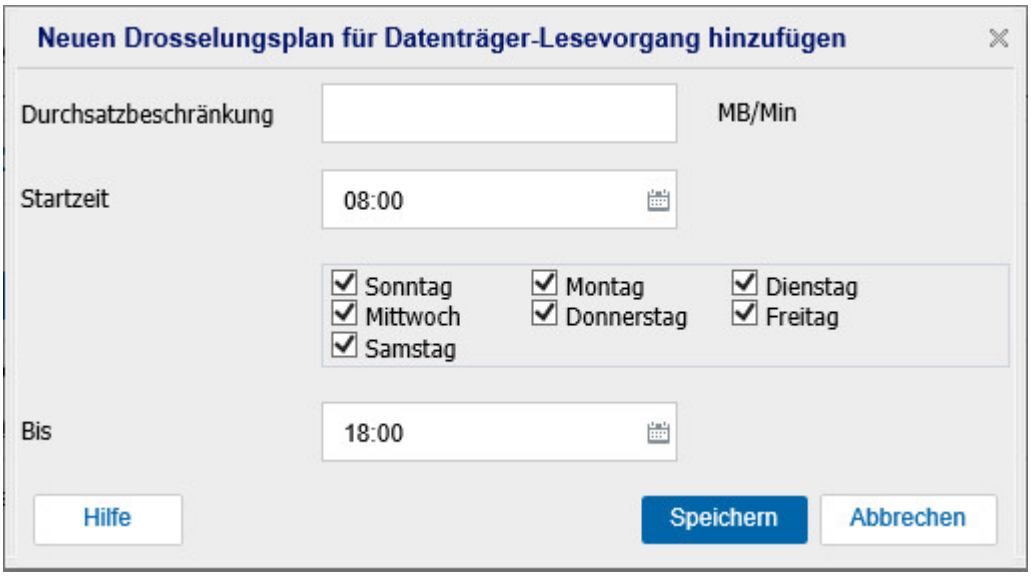
Der Drosselungsplan für Datenträger-Lesevorgänge ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Netzwerkdrosselungsplans

Hinweis: Die Option für Netzwerkdrosselungspläne wird für Sicherungen mit Windows-Agenten nur dann angezeigt, wenn Sie einen Datenspeicher mit Deduplizierung als Ziel für den Plan angeben.

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Netzwerk-Drosselungsplan hinzufügen** aus.

   Das Dialogfeld **Neuen Netzwerk-Drosselungsplan hinzufügen** wird geöffnet.



b. Definiert die Durchsatzbeschränkung in Mbps oder kbps.

Hinweis: Standard-Minimalwert: 500 kbps. Um den Standardwert zu ändern, führen Sie folgende Schritte aus:

i. Vom Registrierungspfad SOFTWARE\Arcserve\Unified Data Protection\Management\Console fügen Sie den Schlüssel MinNetworkThrottleValueInKpbs hinzu, der Typ ist REG_SZ, und legen Sie den Wert fest.

ii. Starten Sie den Arcserve UDP Verwaltungsdienst neu.

iii. Ändern Sie den Plan oder erstellen Sie einen neuen Plan.

Der benutzerdefinierte Wert wird wirksam.

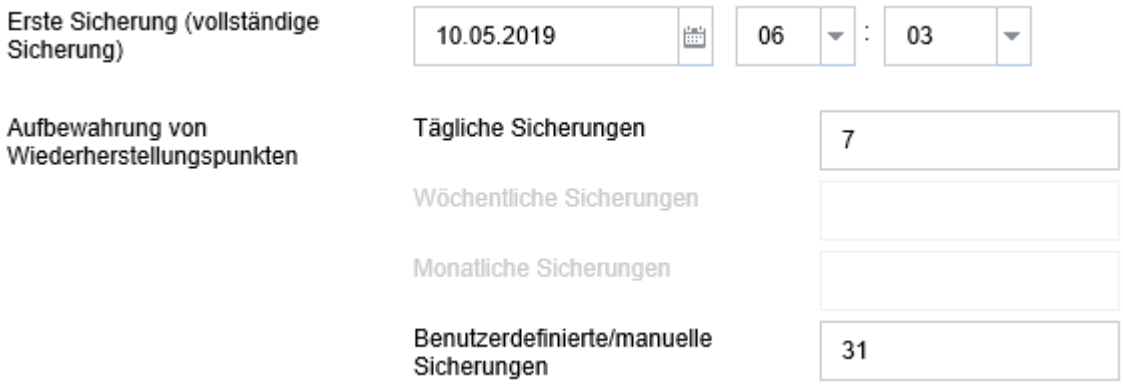
c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Netzwerkdrosselungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

2. Geben Sie die Startzeit für die geplante Sicherung an.



3. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

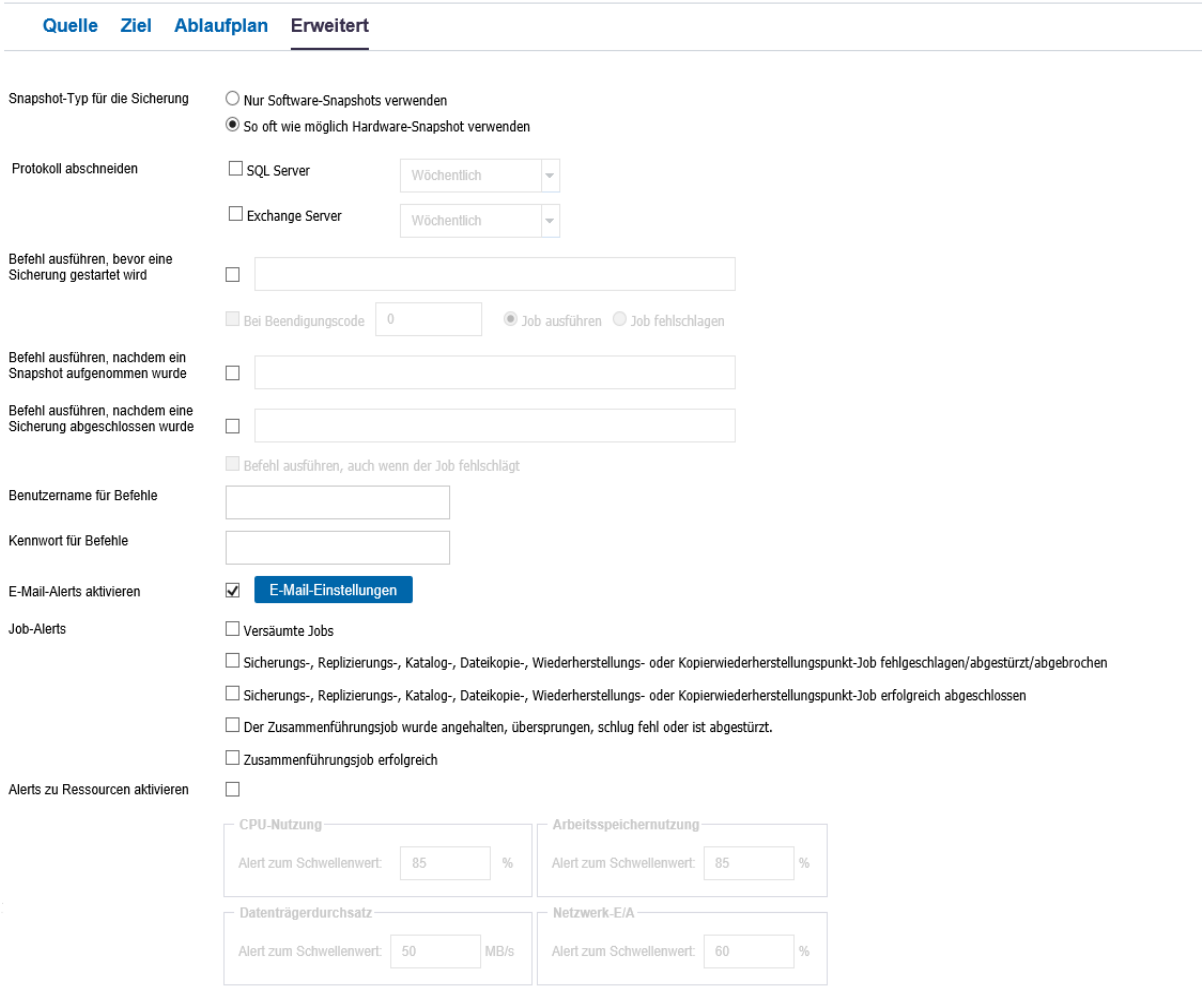
   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld "Sicherungsablaufplan" übernommen.

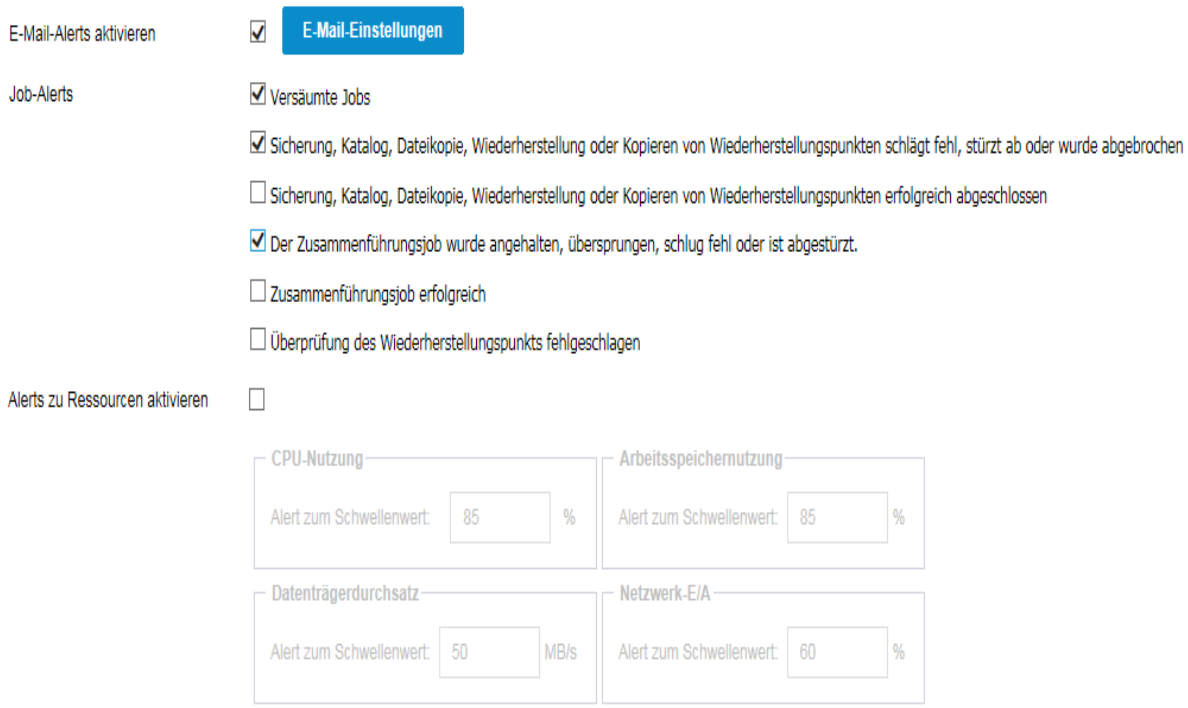
   Der Ablaufplan ist nun angegeben.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen die Einstellungen zum Abschneiden von Protokollen, das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte Erweitert:


Quelle
Ziel
Ablaufplan
Erweitert
Snapshot-Typ für die Sicherung
Nur Software-Snapshots verwenden
So oft wie möglich Hardware-Snapshot verwenden
Protokoll abschneiden
SQL Server
Wöchentlich
Exchange Server
Wöchentlich
Befehl ausführen, bevor eine Sicherung gestartet wird
Bei Beendigungscode
0
Job ausführen
Job fehlschlagen
Befehl ausführen, nachdem ein Snapshot aufgenommen wurde
Befehl ausführen, nachdem eine Sicherung abgeschlossen wurde
Befehl ausführen, auch wenn der Job fehlschlägt
Benutzername für Befehle
Kennwort für Befehle
E-Mail-Alerts aktivieren
E-Mail-Einstellungen
Job-Alerts
Versäumte Jobs
Sicherungs-, Replizierungs-, Katalog-, Dateikopie-, Wiederherstellungs- oder Kopierwiederherstellungspunkt-Job fehlgeschlagen/abgestürzt/abgebrochen
Sicherungs-, Replizierungs-, Katalog-, Dateikopie-, Wiederherstellungs- oder Kopierwiederherstellungspunkt-Job erfolgreich abgeschlossen
Der Zusammenführungsjob wurde angehalten, übersprungen, schlug fehl oder ist abgestürzt.
Zusammenführungsjob erfolgreich
Alerts zu Ressourcen aktivieren
CPU-Nutzung
Alert zum Schwellenwert:
85
%
Arbeitsspeichernutzung
Alert zum Schwellenwert:
85
%
Datenträgerdurchsatz
Alert zum Schwellenwert:
50
MB/s
Netzwerk-E/A
Alert zum Schwellenwert:
60
%



Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

   Art des Snapshots für die Sicherung

   Wählen Sie eine der folgenden Optionen für den Sicherungs-Snapshot aus.

   Nur Software-Snapshot verwenden

   Gibt an, dass der Sicherungstyp nur den Software-Snapshot verwendet. Der Hardware-Snapshot wird von UDP nicht überprüft. Der Software-Snapshot nutzt weniger Ressourcen auf den virtuellen Rechnern. Diese Option eignet sich für Server mit niedrigeren Konfigurationen und Verarbeitungsgeschwindigkeiten.

   So oft wie möglich Hardware-Snapshot verwenden

   Gibt an, dass beim Sicherungstyp erst auf einen Hardware-Snapshot geprüft wird. Wenn alle Kriterien erfüllt sind, verwendet der Sicherungstyp den Hardware-Snapshot.

   Hinweis: Weitere Informationen zu den Hardware-Snapshot-Kriterien finden Sie in den Voraussetzungen.

   Protokoll abschneiden

Ermöglicht es Ihnen, den Ablaufplan anzugeben, um Protokolle für SQL Server und Exchange Server zu kürzen. Sie können den Ablaufplan als **Täglich**, **Wöchentlich** oder **Monatlich** angeben.

Aktivieren Sie die Bereinigung von Protokollen im Stundentakt für SQL über einen Registrierungsschalter.

- Konfigurieren Sie die Planeinstellungen. Aktivieren Sie die Option "SQL Server" im Abschnitt "Protokoll verkürzen" unter der Registerkarte "Erweitert" und wählen Sie dann "Täglich".
- Legen Sie den Registrierungsschlüssel auf dem SQL-Server-Rechner fest, auf dem sich der UDP-Agent befindet. "PurgeSqlLogPerHour" ist das Intervall in Stunden für die Bereinigung des SQL-Protokolls.

  Pfad: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

  Wertname: PurgeSqlLogPerHour (gibt das Intervall in Stunden für die Bereinigung des SQL-Protokolls an.)

  Werttyp: REG_DWORD

Benutzername

Ermöglicht es Ihnen, den Benutzer anzugeben, der zur Ausführung eines Skripts autorisiert ist.

Kennwort

Ermöglicht es Ihnen, das Kennwort des Benutzers anzugeben, der zur Ausführung des Skripts autorisiert ist.

Befehl ausführen, bevor eine Sicherung gestartet wird

Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem ein Snapshot aufgenommen wurde

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungs-Snapshot aufgenommen wurde. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist.

Um das Skript nach dem Snapshot auch während eines Snapshot-Fehlers auszuführen, wählen Sie **Befehl ausführen, auch wenn der Snapshot fehlschlägt** aus.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Arten der Alerts angeben, die Sie in Form von E-Mails empfangen möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers. Weitere Informationen zur Konfiguration von E-Mail-Einstellungen finden Sie unter Konfigurieren von E-Mails und Alerts.

Job-Alerts

Ermöglicht es Ihnen, die Typen der Job-E-Mails auszuwählen, die Sie erhalten möchten.

Warnmeldungen zu Ressourcen aktivieren

Ermöglicht es Ihnen, einen Schwellenwert für CPU-Auslastung, Speicherverwendung, Datenträgerdurchsatz, Netzwerk-E/A anzugeben. Sie können den Wert in Prozent angeben. Sie erhalten eine E-Mail, wenn der Wert "Warnmeldung zum Schwellenwert" überschritten ist.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Knoten installiert ist und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agenten oder kein Agent installiert ist. Um den Agent auf diesen Knoten zu installieren bzw. um ein Upgrade der Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus und klicken auf Speichern.

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie eine andere Task hinzufügen müssen, müssen Sie den Plan aus der Registerkarte **Ressourcen** auswählen und den Plan ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern.

Der Sicherungsplan wird erstellt und automatisch für den Quellknoten bereitgestellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

(Optional) Ausführen einer manuellen Sicherung

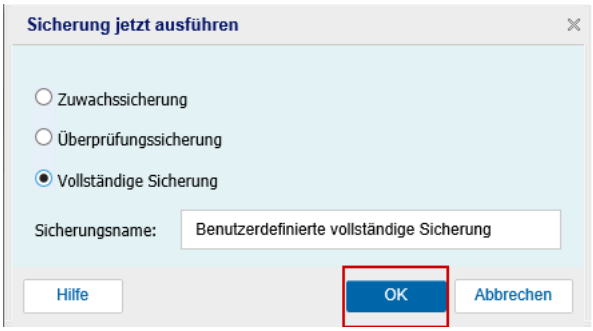
Normalerweise werden Ihre Sicherungen automatisch durchgeführt und von den Ablaufplan-Einstellungen gesteuert. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern. Wenn Sie z. B. einen Wiederholungsplan für vollständige Sicherungen, Zuwachssicherungen und Überprüfungssicherungen festgelegt haben und größere Veränderungen an Ihrem Rechner vornehmen möchten, müssen Sie sofort eine manuelle Sicherung durchführen, ohne auf die nächste geplante Sicherung zu warten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Navigieren Sie zu **Ressourcen** > **Plan** > **Alle Pläne**.

   Die Liste aller Pläne wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Plan, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
4. Wählen Sie im Dialogfeld "Sicherung jetzt ausführen" den gewünschten Sicherungstyp aus, und geben Sie dann gegebenenfalls den Sicherungsnamen an.



Es sind folgende Optionen verfügbar:

Zuwachssicherung

Startet eine Zuwachssicherung Ihres Rechners. Eine Zuwachssicherung sichert nur jene Blöcke, die seit der vorherigen Sicherung geändert wurden.

Hinweis: Wenn Sie eine Sicherung zum ersten Mal ausführen, wird automatisch die vollständige Sicherung initiiert, auch wenn Sie die Option "Zuwachssicherung" ausgewählt haben.

Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

Überprüfungssicherung

Startet eine Überprüfungssicherung Ihres Rechners, indem die aktuellste Sicherung von jedem einzelnen Block überprüft und der Inhalt und die Informationen mit der ursprünglichen Quelle verglichen wird. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht, aktualisiert Arcserve UDP Agent (Windows) die Sicherung dieses Blocks (Neusynchronisierung).

Vorteil: Im Vergleich zu einer vollständigen Sicherung wird nur ein sehr kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteil: Die Sicherung benötigt viel Zeit, da alle Blöcke des Quelldatenträgers mit den Blöcken der letzten Sicherung verglichen werden.

Vollständige Sicherung

Startet eine vollständige Sicherung Ihres gesamten Rechners oder der ausgewählten Volumes.

Hinweise:

- Wenn Sie der Sicherungsquelle ein neues Volume hinzufügen, wird das neue Volume vollständig gesichert, unabhängig davon, welche allgemeine Sicherungsmethode ausgewählt wurde.
- Wenn Sie keinen Sicherungsnamen angeben, wird automatisch der Name "Benutzerdefinierte vollständige Sicherung/Zuwachssicherung/Überprüfungssicherung" vergeben.

5. Klicken Sie auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.

6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.

7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Hinweis: Nur ein Job kann gleichzeitig ausgeführt werden. Wenn Sie versuchen, einen Sicherungsjob manuell zu starten, während gerade ein anderer Job ausgeführt wird, werden Sie in einer Warnmeldung darüber informiert, dass ein anderer Job ausgeführt wird, und aufgefordert, es später erneut zu versuchen.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Andere Aufgaben im UNC/NFS-Plan

Sie können den UNC/NFS-Pfad-Plantask zusammen mit anderen Tasks verfolgen. Sie können Folgeaufgaben erstellen, wie z.B. Wiederherstellungspunkt kopieren, auf Band kopieren, auf Arcserve Cloud replizieren, replizieren und auf fern-verwalteten RPS replizieren.

Task für das Kopieren von Wiederherstellungspunkten

Ermöglicht es Ihnen, die Wiederherstellungspunkte in einen lokalen oder freigegebenen Ordner sowie in eine Cloud zu kopieren.

Auf Band kopieren

Ermöglicht es Ihnen, durch die Integration mit Arcserve Backup den Wiederherstellungspunkt auf Band zu speichern.

Replikationstask

Ermöglicht es Ihnen, einen Task erstellen, um Sicherungsdaten von einem Recovery Point Server auf einem anderen Recovery Point Server zu replizieren.

Zu einem remote verwalteten RPS replizieren

Ermöglicht es Ihnen, einen Task zum Replizieren oder Senden von Daten zu einem Remote-Recovery Point Server zu erstellen.

Replizieren auf Arcserve Cloud

Ermöglicht es Ihnen, eine Aufgabe zu erstellen, um Daten zu replizieren oder an einen Cloud Wiederherstellungspunkt-Server zu senden.

Assured Recovery-Test

Ermöglicht es Ihnen zu überprüfen, ob auf die Daten zugegriffen werden kann und sie auf jeden Fall wiederhergestellt werden können.

Überprüfen der Sicherung

Zur Überprüfung Ihres Sicherungsjobs bestätigen Sie, dass Sie den Sicherungsplan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Sie können den Status von Sicherungsjobs auf der Registerkarte **Jobs** überprüfen.

Gehen Sie wie folgt vor, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Wenden Sie zur Überprüfung von Sicherungsjobs eine der folgenden Methoden an:

Methode 1

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs vollständig**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Methode 2

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Jobs erfolgreich abgeschlossen**.

   Die Liste der abgeschlossenen Sicherungsjobs wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf den Job, den Sie überprüfen möchten.

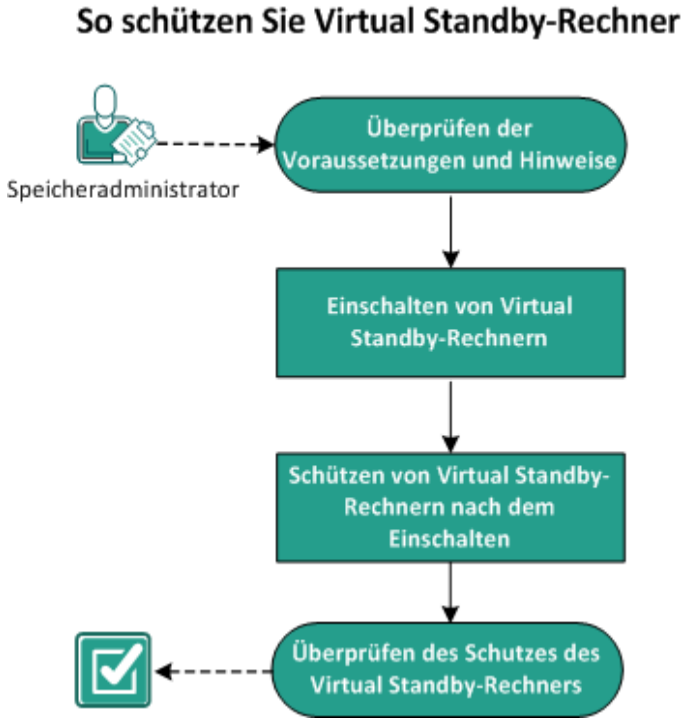
   Der rechte Fensterbereich wird aktualisiert.
4. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
5. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Schützen von Virtual Standby-Rechnern

Sie können Virtual Standby-Rechner sichern und die Daten vor Beschädigungen schützen. Bevor Sie einen Rechner schützen, müssen Sie ihn einschalten.

Die folgende Abbildung veranschaulicht den Prozess zum Schützen von Virtual Standby-Rechnern:



Der nächste Schritt?

- Überprüfen der Voraussetzungen und Hinweise
- Einschalten von Virtual Standby-Rechnern
- Schützen von Virtual Standby-Rechner nach dem Einschalten
- Überprüfen des Schutzes des Virtual Standby-Rechners

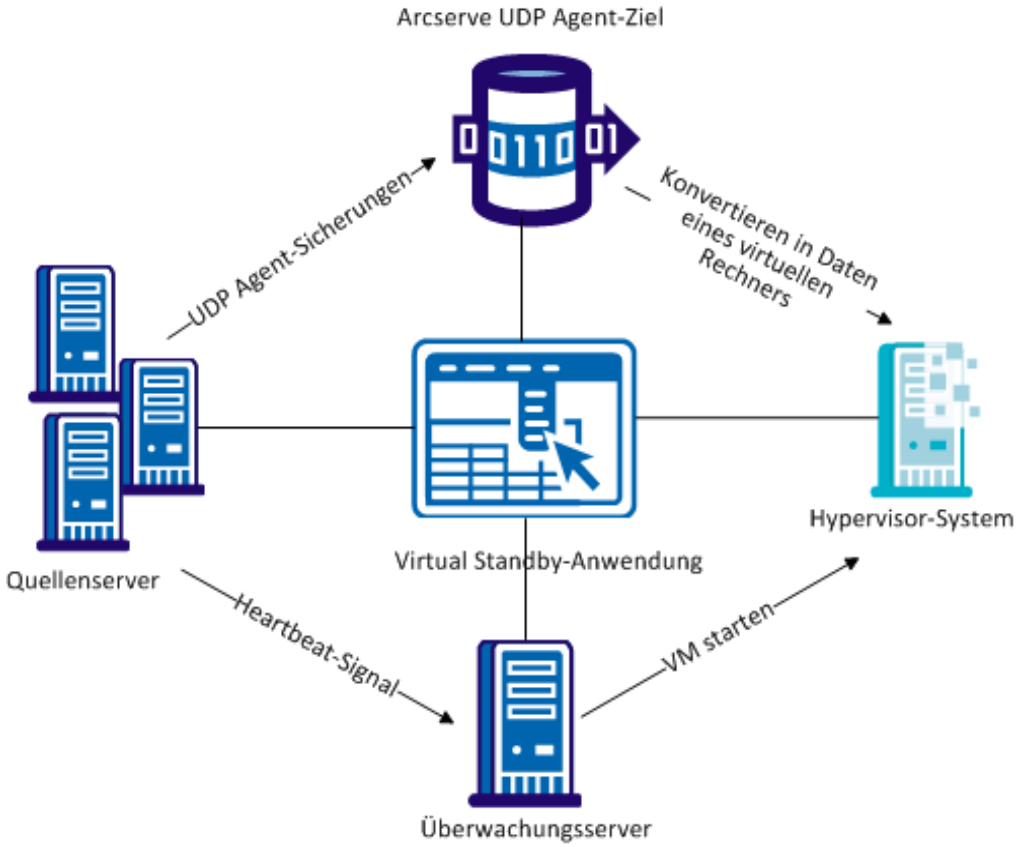
Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie die folgenden erforderlichen Aufgaben durchgeführt haben:

- Sie sind bei der Konsole angemeldet
- Ein Virtual Standby-Rechner ist bereit.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Einschalten von Virtual Standby-Rechnern

Sie können Virtual Standby-Rechner einschalten und die virtuellen Rechner schützen, nachdem die Rechner eingeschaltet wurden. Folgendes Diagramm beschreibt den Prozessablauf, um die virtuellen Rechner einzuschalten:



Einschalten von Virtual Standby-Rechnern aus Wiederherstellungspunkt-Snapshots

Virtual Standby kann so konfiguriert werden, dass Virtual Standby-Rechner aus Wiederherstellungspunkt-Snapshots automatisch in Betrieb genommen werden, wenn der Überwachungsserver kein Heartbeat-Signal vom Quellserver entdeckt. Optional können Sie Virtual Standby-Rechner aus Wiederherstellungspunkt-Snapshots manuell in Betrieb nehmen, falls ein Quellserver fehlschlägt, ein Notfall eintritt oder Sie einen Quellserver zur Wartung offline schalten wollen.

Hinweis: Die folgenden Schritte beschreiben, wie Sie Virtual Standby-Rechner manuell aus Wiederherstellungspunkt-Snapshots einschalten. Weitere Informationen zum automatischen Einschalten von Virtual Standby-Rechnern aus Wiederherstellungspunkt-Snapshots finden Sie unter Hinzufügen eines Virtual Standby zu EC2-Task zum Plan.

Gehen Sie wie folgt vor:

1. Navigieren Sie auf der Registerkarte **Ressourcen** zur Knotengruppe **Virtual Standby**.

   Die Virtual Standby-Knoten werden im mittleren Fensterbereich angezeigt.

2. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf "**Standby-VM**".

   Das Dialogfeld "**Standby-VM**" wird geöffnet.

3. Führen Sie im Dialogfeld **Standby-VM** folgende Tasks aus:

   - Wählen Sie einen Datums-und Zeitbereich des Wiederherstellungspunkt-Snapshots aus, um den virtuellen Rechner einzuschalten.

     Hinweis: Wenn der virtuelle Standby-Rechner noch nicht konfiguriert wurde, wird der Link "Das Netzwerk des virtuellen Standby-Rechners ist nicht konfiguriert." angezeigt.

     a. Klicken Sie auf diesen Link, um das Netzwerk zu konfigurieren.

     b. Klicken Sie auf "**Speichern**". Die Einstellungen für den virtuellen Virtual Standby-Rechner werden gespeichert.

     c. Klicken Sie auf **Schließen**. Das Dialogfeld **Wiederherstellungspunkt-Snapshot** wird angezeigt.

   - Klicken Sie auf **VM starten**.

     Der virtuelle Rechner wird unter Verwendung der im Wiederherstellungspunkt-Snapshot enthaltenen Daten eingeschaltet.

Hinweis: Nachdem der virtuelle Rechner eingeschaltet wurde, werden Sie möglicherweise aufgefordert, den Computer einmal oder mehrmals neu zu starten. Dieses Verhalten tritt auf, weil ein Amazon PV-Treiber auf dem virtuellen Rechner installiert ist.

Nachdem Sie Virtual Standby-Rechner von Wiederherstellungspunkt-Snapshots eingeschaltet haben, müssen Sie möglicherweise folgende Tasks ausführen:

- Aktivieren Sie das Windows-Betriebssystem, das auf dem virtuellen Rechner ausgeführt wird.
- Starten Sie Arcserve Unified Data Protection Agent für Windows auf dem virtuellen Rechner.
- Aktualisieren Sie Arcserve UDP mit dem Hostnamen, der IP-Adresse und den Anmeldeinformationen für den virtuellen Rechner.
- Weisen Sie den Knoten eines Plans zu.

Hinweis: Dieser Task ist nur erforderlich, wenn Sie Wiederherstellungspunkt-Snapshots für den eingeschalteten virtuellen Rechner erstellen möchten.

Einschalten von Virtual Standby-Rechner über den Hyper-V-Manager

Wenn Sie virtuelle Virtual Standby-Rechner manuell einschalten möchten, sollten Sie die virtuellen Rechner als Best Practice über das Fenster "Standby-VM" auf dem Arcserve Unified Data Protection-Server einschalten. Weitere Informationen finden Sie unter Einschalten von virtuellen Virtual Standby-Rechnern aus Wiederherstellungspunkt-Snapshots. Wenn Sie virtuelle Virtual Standby-Rechner über den Hyper-V-Server starten möchten, können Sie dies allerdings mithilfe von Hyper-V-Manager tun.

Hinweis: Der Hyper-V-Manager ermöglicht Ihnen den Zugriff auf die Wiederherstellungspunkt-Snapshots, die Virtual Standby erstellt hat, um den Knoten zu schützen. Sie sollten diese Snapshots nicht löschen. Wenn Sie die Snapshots löschen, wird die Beziehung zwischen den in den Snapshots enthaltenen Daten bei der nächsten Ausführung eines Virtual Standby-Jobs inkonsistent. Mit inkonsistenten Daten können Sie virtuelle Virtual Standby-Rechner nicht korrekt einschalten.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Hyper-V-Server an, der die Knoten überwacht, die Sie schützen.
2. Starten Sie Hyper-V-Manager folgendermaßen:
   a. Klicken Sie auf "Start", dann auf "Programme" und anschließend auf "Hyper-V-Manager.

      Hyper-V-Manager wird geöffnet.

   b. Blenden Sie in der Verzeichnisstruktur des Hyper-V-Managers "Hyper-V Manager" ein, und klicken Sie auf den Hyper-V-Server, der den virtuellen Rechner enthält, den Sie einschalten möchten.

      Die virtuellen Rechner, die mit dem angegebenen Hyper-V-Server verbunden sind, werden in der Liste "Virtual Machines" im Hauptfenster angezeigt.
3. Führen Sie eine der folgenden Aufgaben durch:
   - **Um den virtuellen Rechner unter Verwendung des neuesten Snapshot einzuschalten**: Klicken Sie in der Liste "Virtuelle Computer" mit der rechten Maustaste auf den virtuellen Rechner, den Sie einschalten möchten, und anschließend im Pop-up-Menü auf "Start".
   - **Um den virtuellen Rechner mithilfe eines älteren Snapshot einzuschalten:**

a. Klicken Sie in der Liste "Virtuelle Machines" mit der rechten Maustaste auf den virtuellen Rechner, den Sie einschalten möchten.

   Die Snapshots, die mit dem virtuellen Rechner verbunden sind, werden in der Liste "Snapshots" angezeigt.

b. Klicken Sie mit der rechten Maustaste auf den Snapshot, den Sie verwenden möchten, um den virtuellen Rechner einzuschalten, und klicken Sie im Pop-up-Menü auf "Anwenden".

   Der Dialogfeld "Snapshot anwenden" wird geöffnet.

c. Klicken Sie auf "Apply".

d. Klicken Sie in der Liste "Virtual Machines " mit der rechten Maustaste auf den virtuellen Rechner, den Sie einschalten möchten, und anschließend im Pop-up-Menü auf "Start".

   Der Virtual Standby-Rechner ist eingeschaltet.

Wenn nötig, können Sie die virtuellen Rechner sichern und Wiederherstellungspunkt-Snapshots erstellen, nachdem Sie den virtuellen Rechner eingeschaltet haben.

Einschalten von Virtual Standby-Rechnern über VMware vSphere Client

Wenn Sie Virtual Standby-Rechner manuell einschalten möchten, sollten Sie als Best Practice die virtuellen Rechner über das Fenster "Standby-VM" von Arcserve UDP einschalten. Weitere Informationen finden Sie unter Einschalten von virtuellen Virtual Standby-Rechnern aus Wiederherstellungspunkt-Snapshots. Wenn Sie die Virtual Standby-Rechner über das ESX Server- oder vCenter Server-System starten möchten, können Sie dies allerdings über VMware vSphere Client tun.

Hinweis: Der VMware vSphere Client ermöglicht Ihnen den Zugriff auf die Wiederherstellungspunkt-Snapshots, die Virtual Standby erstellt hat, um den Knoten zu schützen. Sie sollten diese Snapshots nicht löschen. Wenn Sie die Snapshots löschen, wird die Beziehung zwischen den in den Snapshots enthaltenen Daten bei der nächsten Ausführung von Virtual Standby inkonsistent. Mit inkonsistenten Daten können Sie Virtual Standby-Rechner nicht korrekt einschalten.

Gehen Sie wie folgt vor:

1. Öffnen Sie VMware vSphere Client, und melden Sie sich beim ESX Server- oder vCenter Server-System an, das die Knoten überwacht, die Sie schützen.
2. Blenden Sie in der Verzeichnisstruktur das ESX Server-System oder vCenter Server-System ein, durchsuchen Sie es, und klicken Sie auf den virtuellen Rechner, den Sie einschalten möchten
3. Führen Sie eine der folgenden Aufgaben durch:

   Um den virtuellen Rechner mithilfe des aktuellsten Snapshots einzuschalten: Klicken Sie auf die Registerkarte "Erste Schritte" und anschließend unten im Fenster auf "Virtuellen Rechner einschalten".

   Um den virtuellen Rechner mithilfe eines älteren Snapshot einzuschalten:

   a. Klicken Sie in der Symbolleiste auf die Schaltfläche "Snapshot Manager" .

      Das Dialogfeld "Snapshots for (Name des virtuellen Rechners) wird geöffnet, um eine Liste der Snapshots anzuzeigen, die für den virtuellen Rechner zur Verfügung stehen.

   b. Klicken Sie in der Snapshot-Liste auf den Snapshot, den Sie verwenden möchten, um den virtuellen Rechner einzuschalten, und anschließend auf "Go".

      Der Virtual Standby-Rechner ist eingeschaltet.

   Wenn nötig, können Sie die virtuellen Rechner sichern und Wiederherstellungspunkt-Snapshots erstellen, nachdem Sie den virtuellen Rechner eingeschaltet haben.

Schützen von Virtual Standby-Rechnern nach dem Einschalten

Nachdem ein Virtual Standby-Rechner eingeschaltet wurde (entweder manuell oder automatisch), werden der Arcserve Unified Data Protection Agent für Windows-Sicherungsjob und der Virtual Standby-Job nicht wie geplant ausgeführt. Sie müssen den Virtual Standby-Rechner manuell konfigurieren, um ihn zu schützen.

Gehen Sie wie folgt vor:

1. Ändern Sie das **Präfix des Namens des virtuellen Rechners** im Virtual Standby-Task.

   Wenn Sie Virtual Standby-Rechner einschalten, definiert die Anwendung die Namen der virtuellen Rechner auf den eingeschalteten virtuellen Rechnern als Verknüpfung aus der Option **Präfix des Namens des virtuellen Rechners**, die im Virtual Standby-Task angegeben ist, und dem Hostnamen des Quellknotens.

   Beispiel:

   - VM-Namenspräfix: AA_
   - Hostname des Quellknotens: Server1
   - Virtueller Rechnername des Virtual Standby-Rechners: AA_Server1

   Wenn Sie das **Präfix des Namens des virtuellen Rechners** im Virtual Standby-Task nicht ändern, können nach dem Einschalten der Virtual Standby-Rechner Namenskonflikte bei virtuellen Rechnern auftreten. Probleme dieser Art treten auf, wenn sich die Quellknoten und die Virtual Standby-Rechner auf dem gleichen Hypervisor befinden.

   Im Bedarfsfall können Sie andere Einstellungen des Virtual Standby-Tasks aktualisieren. Optional können Sie eine neue Virtual Standby-Richtlinie erstellen, um den Virtual Standby-Rechner zu schützen.

2. Nachdem Sie den Plan für den Virtual Standby-Rechner bereitgestellt haben, nehmen Sie den Virtual Standby-Job wieder auf.

   Weitere Informationen finden Sie unter Aussetzen und Wiederaufnehmen von Virtual Standby-Jobs.

3. Nachdem Sie den Plan bereitgestellt haben, melden Sie sich bei Arcserve Unified Data Protection Agent für Windows auf dem Virtual Standby-Rechner an, und planen Sie eine Wiederholungsmethode für den Arcserve Unified Data Protection Agent für Windows-Sicherungsjob.

Weitere Informationen finden Sie im *Arcserve Unified Data Protection Agent für Windows-Benutzerhandbuch*.

Hinweis: Aussetzen und Wiederaufnehmen von Virtual Standby-Jobs

Überprüfen des Schutzes von Virtual Standby-Rechnern

Überprüfen Sie, ob die Virtual Standby-Rechner geschützt sind, indem Sie prüfen, ob die gültigen Wiederherstellungspunkte am Sicherungsziel verfügbar sind.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Sicherungsziel an, und navigieren Sie zum Ordner des Sicherungsziels.
2. Überprüfen Sie, ob die Sicherung des Virtual Standby-Rechners erfolgreich war und Wiederherstellungspunkte verfügbar sind.

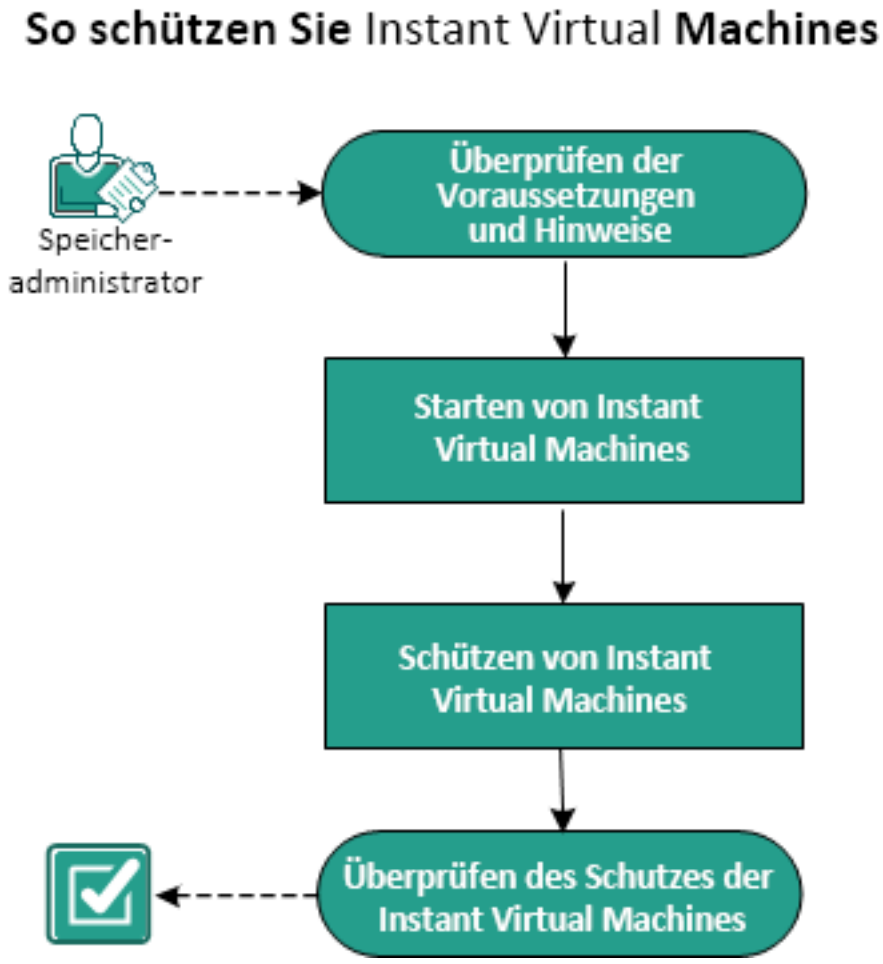
   Der Virtual Standby-Rechner wurde überprüft.

   Die Virtual Standby-Rechner werden erfolgreich geschützt.

Schützen von Instant VMs

Sie können Instant VMs sichern und die Daten vor Beschädigungen schützen. Bevor Sie einen Rechner schützen, müssen Sie ihn einschalten.

Die folgende Abbildung veranschaulicht den Prozess zum Schützen von Instant VMs:



Der nächste Schritt?

- Überprüfen der Voraussetzungen und Hinweise
- Starten von Instant VMs
- Schützen von Instant VMs
- Überprüfen des Schutzes von Instant VMs

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie die folgenden erforderlichen Aufgaben durchgeführt haben:

- Sie sind bei der Konsole angemeldet.
- Sorgen Sie dafür, dass eine Instant VM betriebsbereit ist.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Einschalten von Instant VMs aus Wiederherstellungspunkten

Sie können Instant VMs erstellen und die virtuellen Rechner manuell vom Wiederherstellungspunkt schützen, nachdem die Rechner eingeschaltet wurden.

Sie können "Jetzt starten" oder "Später starten" auswählen, wenn Sie eine Instant VM erstellen. Wenn Sie die Option "Jetzt booten" auswählen, wird die Instant VM sofort nach der erfolgreichen Erstellung gestartet, andernfalls müssen Sie die Instant VM manuell einschalten.

Sie können Instant VMs nur dann vom Wiederherstellungspunkt einschalten, wenn Sie einen Wiederherstellungspunkt für den virtuellen Rechner erstellen möchten, der eingeschaltet wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie über die Registerkarte **Ressourcen** zur Knotengruppe **Infrastruktur: Instant VMs**.

   Die Instant VM-Knoten werden im mittleren Fensterbereich angezeigt.

2. Wählen Sie im mittleren Fensterbereich den Knoten aus, klicken Sie auf **Aktionen**, und klicken Sie dann in der Drop-Down-Liste auf **Einschalten**.

   Der virtuelle Rechner wird unter Verwendung der im Wiederherstellungspunkt-Snapshot enthaltenen Daten eingeschaltet.

   Hinweis: Nachdem der virtuelle Rechner eingeschaltet wurde, werden Sie möglicherweise aufgefordert, den Computer einmal oder mehrmals neu zu starten. Dieses Verhalten tritt auf, da auf dem virtuellen Rechner VMware Tools durch VMware und Hyper-V-Integrationsdienste durch Windows installiert werden.

   Nachdem Sie Instant VMs von Wiederherstellungspunkt-Snapshots eingeschaltet haben, müssen Sie möglicherweise folgende Tasks ausführen:

   - Aktivieren Sie das Windows-Betriebssystem, das auf dem virtuellen Rechner ausgeführt wird.
   - Starten Sie Arcserve Unified Data Protection Agent für Windows auf dem virtuellen Rechner.
   - Aktualisieren Sie Arcserve UDP mit dem Hostnamen, der IP-Adresse und den Anmeldeinformationen für den virtuellen Rechner.

Schützen einer eingeschalteten Instant VM

Nachdem eine Instant VM eingeschaltet wurde (entweder manuell oder automatisch), werden der Arcserve Unified Data Protection Agent für Windows-Sicherungsjob und der Virtual Standby-Job nicht wie geplant ausgeführt. Sie müssen die Instant VM manuell konfigurieren, um sie zu schützen.

Gehen Sie wie folgt vor:

1. Fügen Sie eine Instant VM zur Konsole hinzu.

   Hinweis: Sie können einen Knoten hinzufügen, indem Sie die Knotendetails manuell angeben oder virtuelle Rechner von ESX/vCenter- und Hyper-V-Servern importieren.

   Weitere Informationen finden Sie unter Hinzufügen von Knoten.

2. Fügen Sie ein Ziel hinzu.

   Bei einem Ziel kann es sich um einen Recovery Point Server, lokalen Ordner oder freigegebenen Remote-Ordner handeln.

3. Erstellen Sie einen Plan, um den Instant VM-Knoten zu schützen.

   Ein Plan ist eine Gruppe von Tasks zum Verwalten der Sicherung, Replikation und Erstellung von Virtual Standby-Rechnern.

   Hinweis: Sie können einen Plan mit dem agentenbasierten Windows-Sicherungstask oder dem hostbasierten agentenlosen Sicherungstask erstellen.

4. Führen Sie Jobs wie Sicherung, Erstellen von Virtual Standby und Replikation aus.

   Weitere Informationen finden Sie im *Arcserve UDP Agent (Windows)-Benutzerhandbuch.*

Überprüfen des Schutzes von Instant VMs

Überprüfen Sie, ob der Instant VM-Rechner geschützt sind, indem Sie prüfen, ob die gültigen Wiederherstellungspunkte am Sicherungsziel verfügbar sind.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Sicherungsziel an, und navigieren Sie zum Ordner des Sicherungsziels.
2. Überprüfen Sie, ob die Sicherung des Instant VM-Rechners erfolgreich war und Wiederherstellungspunkte verfügbar sind.

   Der Instant VM-Rechner wurde überprüft.

   Der Instant VM-Rechner wird erfolgreich geschützt.

Replizieren von Daten zwischen Datenspeichern, die von einer UDP-Konsole verwaltet werden

Mit Arcserve UDP können Sie Ihre Sicherungsdaten von einem Datenspeicher auf einen anderen replizieren. Diese Datenspeicher werden von der gleichen UDP-Konsole verwaltet, jedoch befinden sie sich auf verschiedenen Recovery Point Servern. Sie müssen einen Plan mit zwei Tasks erstellen: Sicherung und Replikation. Der Sicherungstask sichert Daten gemäß Ablaufplan, und der Replikationstask repliziert die gesicherten Daten auf dem angegebenen Recovery Point Server. Die Ausführung des Replikationsjobs richtet sich nach dem Ablaufplan, den Sie im Replikationstask angeben. Sie können mehrere Replikationstasks in einem Plan erstellen.

Wenn der Replikationsjob fehlschlägt (beispielsweise aufgrund von Netzwerkproblemen), wird der fehlgeschlagene Replikationsjob wiederaufgenommen, bevor eine neue Sitzung übertragen wird. Der Replikationsjob wird ab dem Zeitpunkt der Unterbrechung des letzten fehlgeschlagenen Replikationsjobs wiederaufgenommen.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen eines Plans mit einem Sicherungstask
3. Hinzufügen eines Replikationstasks zum Plan
4. (Optional) Ausführen einer manuellen Replikation
5. Überprüfen des Plans

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich bei der Konsole an.
- Installieren Sie die Server-Komponente, und erstellen Sie Datenspeicher.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Erstellen eines Sicherungstasks

Ein Plan umfasst verschiedene Arten von Tasks, die Sie ausführen möchten. Ein Plan beinhaltet normalerweise einen primären Task, gefolgt von einem sekundären Task. In der Regel ist der primäre Task ein Sicherungstask oder das Replikat eines Remote-Konsolen-Tasks. Die Funktion eines Sicherungstasks besteht darin, eine Sicherung der Quellknoten zu erstellen, die Sie schützen möchten. Sie können Daten von physischen und virtuellen Windows- und Linux-Rechnern sichern. Danach können Sie die gesicherten Daten als zusätzliche Vorsichtsmaßnahme an einem anderen Speicherort speichern.

Weitere Informationen:

- Weitere Informationen zur Sicherung eines Windows-Knotens finden Sie unter Erstellen eines Sicherungsplans für Windows.
- Weitere Informationen zur Sicherung virtueller Rechner finden Sie unter Erstellen eines Sicherungsplans für hostbasierte virtuelle Rechner.
- Weitere Informationen zur Sicherung von Linux-Knoten finden Sie unter Erstellen eines Sicherungsplans für Linux.

Hinzufügen eines Replikationstasks zum Plan

Erstellen Sie einen Replikationstask, der Ihre Sicherungsdaten von einem Recovery Point Server zu einem anderen Recovery Point Server kopiert, um Ihre Daten besser zu schützen. Sie können Ihre Sicherungsdaten auch von einem Datenspeicher in einen anderen Datenspeicher auf demselben Recovery Point Server kopieren. Das Replikationsziel muss ein Datenspeicher auf dem Recovery Point Server sein. Sie können mehrere Replikationstasks erstellen, um mehrere Replikationen durchzuführen.

Hinweise:

- **Bei einem Zusammenführungsjob:** Wenn ein Replikationstask konfiguriert ist und Sie einen On-Demand-Zusammenführungsjob über den Quelldatenspeicher ausführen, überprüft der Job nicht, ob die Sitzungen repliziert werden. Als Folge können die zusammengeführten Sitzungen nicht auf den Zieldatenspeicher repliziert werden, und Sie replizieren am Ende mehr Daten. Angenommen beispielsweise, es gibt fünf Sitzungen, s1, s2, s3, s4 und s5. s1 und s2 werden repliziert. Nun führen Sie einen On-Demand-Zusammenführungsjob auf der Quellseite aus und behalten zwei Sitzungen bei. s4 und s5 werden beibehalten. s4 ist eine vollständige Sitzung. Wenn also der nächste Replikationsjob gestartet wird, muss der Job eine vollständige Sitzung replizieren.
- **Bei einem Bereinigungsjob:**Wenn ein Replikationstask konfiguriert ist und Sie einen Bereinigungsjob auf dem Zieldatenspeicher ausführen, repliziert der nächste Replikationsjob alle Sitzungen auf den Zieldatenspeicher.
- Das Replizieren von einem Datenspeicher mit Deduplizierung zu einem Datenspeicher ohne Deduplizierung ist nicht möglich.
- Auch das Replizieren von einem Datenspeicher mit aktivierter Verschlüsselung zu einem Datenspeicher ohne Verschlüsselung wird nicht unterstützt.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Fensterbereich auf **Task hinzufügen**.

   Ein neuer Task wird im linken Fensterbereich hinzugefügt.

2. Wählen Sie im Drop-down-Menü **Tasktyp** die Option **Replizieren** aus.

   Der Replikationstask wird hinzugefügt. Sie müssen die Registerkarte **Quelle** im Replikationstask nicht konfigurieren. Sie enthält automatisch das Sicherungsziel des Sicherungstasks.

   Hinweis: Sie können einen Task nicht ohne den primären Task wie Sicherung auf Recovery Point Server replizieren.

3. Klicken Sie auf die Registerkarte **Ziel**, und geben Sie die Details für Recovery Point Server und Wiederholungsablaufplan ein.

Recovery Point Server

Wählen Sie den Recovery Point Server aus der Liste aus.

Datenspeicher

Wählen Sie den Datenspeicher aus der Liste aus.

Startwiederholung

Geben Sie die Zeit nach dem Fehlschlagen des Replikationsjobs (in Minuten) an, nach deren Ablauf der Job neu gestartet werden soll. Wenn Sie beispielsweise 10 Minuten angeben, wird der Replikationsjob 10 Minuten, nachdem er fehlgeschlagen ist, neu gestartet.

Beschränkung: 1 bis 60

Wiederholen

Geben Sie an, wie oft der Replikationsjob bei einem Fehlschlag neu gestartet werden soll. Der Replikationsjob wird so oft ausgeführt, bis der Job erfolgreich ist oder die Beschränkung erreicht ist.

Beschränkung: 1 bis 99

4. Klicken Sie auf die Registerkarte **Ablaufplan**, und fügen Sie **Ablaufplan des Replikationsjobs**, **Ablaufplan der Replikationsdrosselung**, **Zusammenführungsplan** und **Aufbewahrungseinstellungen** hinzu.

Hinweis: Das Kontingent der Replikationsdrosselung wird durchschnittlich von allen Replikationsjobs, die aus allen Knoten eines aktuellen Planes gestartet wurden, gemeinsam genutzt.

5. Klicken Sie auf die Registerkarte **Erweitert**, und geben Sie die Details ein.
6. Klicken Sie auf **Änderungen speichern** oder **Task hinzufügen**.

   Wenn Sie einen Task hinzugefügt haben, können Sie einen weiteren Replikationstask erstellen, um Replikationen auf mehreren Ebenen auszuführen. Sie können mehrere Replikationstasks zum Plan hinzufügen.

   Wenn Sie die Änderungen speichern, wird der Plan gespeichert, und der Replikationstask wird am Replikationsziel bereitgestellt.

   Der Replikationstask wurde erstellt.

   Sie haben einen Replikationsplan erfolgreich erstellt und automatisch bereitgestellt.

(Optional) Ausführen einer manuellen Replikation

Um einen Replikationsjob manuell auszuführen, müssen Sie mindestens eine erfolgreiche Sicherung von Daten durchgeführt haben. Wenn Sie keinen Ablaufplan für die Replikation festgelegt haben, wird der Replikationsjob nach dem Sicherungsjob sofort ausgeführt. Anderenfalls hängt dies von Ihren Einstellungen für den Ablaufplan für die Replikation ab.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Wenn Sie Pläne hinzugefügt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Wählen Sie die Knoten aus, die Sie sichern möchten und für die ein zugewiesener Plan vorliegt.
4. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Jetzt replizieren**.

   Das Dialogfeld "**Knoten replizieren**" wird geöffnet.
5. Wählen Sie den Quell-RPS und den Ziel-RPS für den Job aus.
6. Klicken Sie auf **OK**.

   Der Replikationsjob wird ausgeführt.

   Die manuelle Replikation wurde erfolgreich ausgeführt.

Überprüfen des Plans

Um die Replikationsfunktion zu überprüfen, stellen Sie sicher, dass Sie den Replikationsplan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Nachdem der Sicherungsjob erfolgreich abgeschlossen wurde, wird der Replikationsjob ausgeführt. Sie können den Status des Sicherungsjobs und des Replikationsjobs in der Registerkarte **Jobs** überprüfen.

Gehen Sie wie folgt vor: Zum Überprüfen von Plänen

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Gehen Sie wie folgt vor: Zum Überprüfen von Replikationsjobs

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf "**Alle Jobs**".

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob und der Replikationsjob erfolgreich ausgeführt werden.

Replizieren von Daten zwischen Datenspeichern, die von unterschiedlichen UDP-Konsolen verwaltet werden

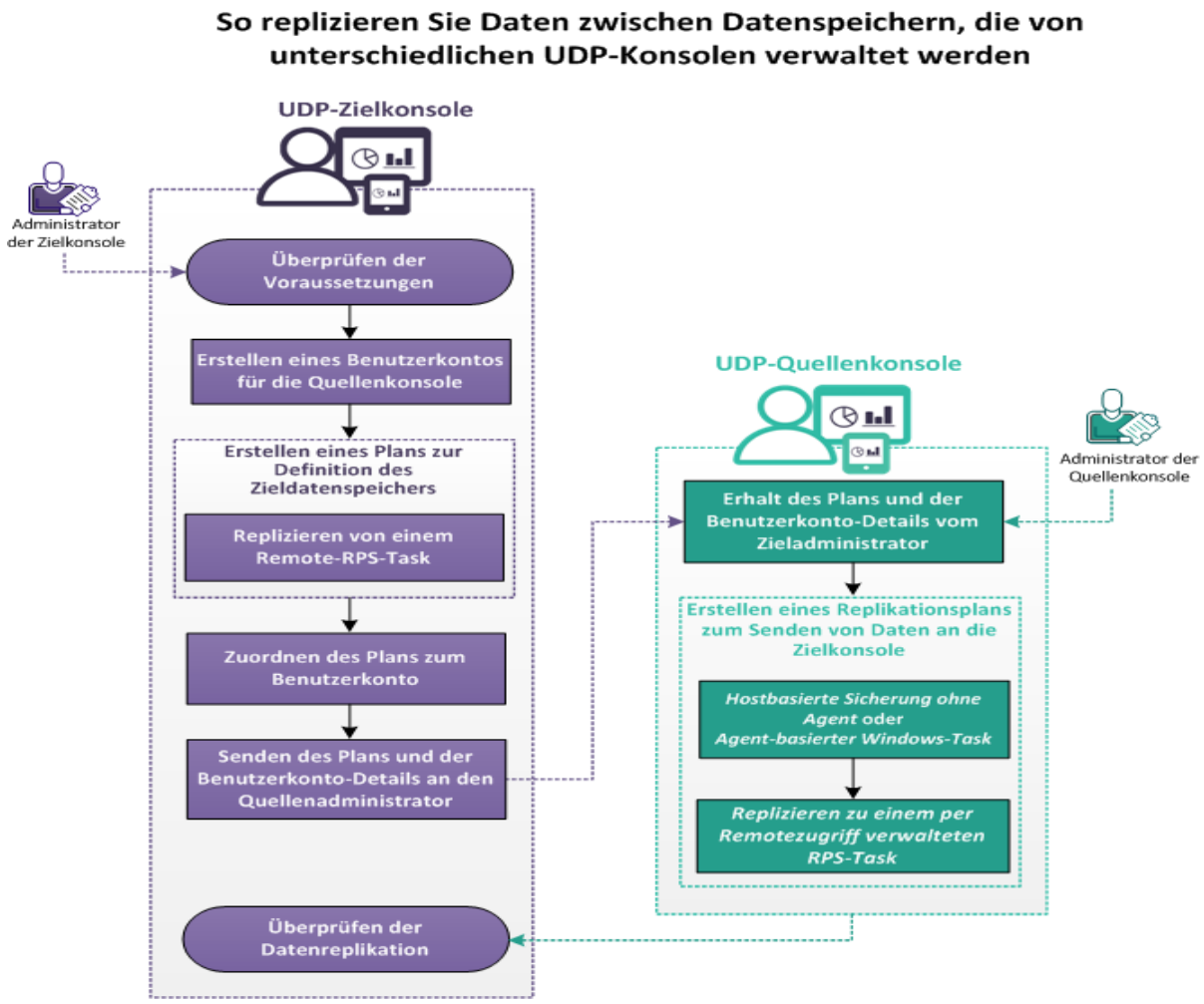
Um Ihre Daten zu schützen, müssen Sie Ihre Sicherungsdaten evtl. zu einem anderen Recovery Point Server replizieren, der von einer anderen Arcserve UDP-Konsole verwaltet wird. Zum Beispiel können Sie Ihre Daten zu einem Dienstanbieter replizieren, der seine Replikationsdienste mehreren Kunden anbietet. In diesem Beispiel werden die Daten von einem Quelldatenspeicher (auf der Quellenkonsole) zu einem Zieldatenspeicher (auf der Zielkonsole) repliziert.

Erstellen Sie als Administrator der Zielkonsole einen Benutzernamen, ein Kennwort und einen Plan für die Quellenkonsole.Diese müssen eindeutig sein. Der Plan definiert den Zieldatenspeicher.Mit dem Benutzernamen und Kennwort kann der Quellenadministrator eine Verbindung zu Ihrem Server herstellen und Daten replizieren.

Erstellen Sie als Administrator der Quellenkonsole einen Plan, um Daten zum Zieldatenspeicher zu replizieren. Während Sie den Plan erstellen, stellen Sie eine Verbindung zum Zielserver her, und wählen Sie den Plan aus, der Ihnen vom Zieladministrator zugewiesen wird.

Hinweis: Als Best Practice wird empfohlen, Multistreaming-Parameter zu konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von Multistreaming-Parametern.

Das folgende Diagramm veranschaulicht die Replikation von Daten zu einem anderen Datenspeicher, der von einer anderen Konsole verwaltet wird:



Der nächste Schritt?

1. Überprüfen der Voraussetzungen
2. Erstellen eines Benutzerkontos für die Quellenkonsole
3. Erstellen eines Plans zur Definition des Zieldatenspeichers
4. Zuordnen des Plans zum Benutzerkonto
5. Senden des Plans und der Benutzerkonto-Details an den Quellenadministrator

6. Erhalt des Plans und der Benutzerkonto-Details vom Zieladministrator
7. Erstellen eines Replikationsplans zum Senden von Daten an die Zielkonsole
8. Überprüfen der Datenreplikation

Überprüfen der Voraussetzungen

Überprüfen Sie folgende Voraussetzungen, bevor Sie Daten replizieren:

- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Administratoren – Zielkonsole

- Stellen Sie sicher, dass Arcserve UDP auf dem Zielserver installiert ist.
- Stellen Sie sicher, dass Sie über alle Berechtigungen verfügen, um Windows-Benutzerkonten auf dem Zielserver zu erstellen.
- Überprüfen Sie, ob Sie während der Erstellung eines Plans zur Replikation von einem remote verwalteten RPS das Kontrollkästchen **Abrufen von Wiederherstellungspunkten zulassen** in den erweiterten Einstellungen aktiviert haben.

  Hinweis: Wenn Sie das Kontrollkästchen **Abrufen von Wiederherstellungspunkten zulassen** nicht aktivieren und den umgekehrten Replikationsjob für die Remote-Konsole starten, werden Sie aufgefordert, das Flag für das Zulassen des Remote-Abrufs für die umgekehrte Replikation zu aktivieren.

Administrator – UDP-Quellenkonsole

- Stellen Sie sicher, dass Arcserve UDP auf dem Quellserver installiert ist.
- Stellen Sie sicher, dass Sie mindestens eine vollständige Sicherung eines Datenspeichers durchgeführt haben.

Erstellen eines Benutzerkontos für die Quellenkonsole

Zieladministrator

Um die replizierten Daten auf dem Zielserver zu identifizieren und zu verwalten, erstellen Sie ein Windows-Benutzerkonto. Wenn Sie mehr als eine Quellenkonsole verwalten, dann erstellen Sie ein Benutzerkonto für jede Quellenkonsole.

Der Administrator der Quellenkonsole verwendet diese Kontodetails, um eine Verbindung zum Zielserver herzustellen.

Um ein Benutzerkonto auf einem Windows-Betriebssystem zu erstellen, verwenden Sie den Bereich "Benutzerkonten" in der Windows-Systemsteuerung. Weitere Informationen zur Erstellung von Benutzerkonten unter Microsoft Windows finden Sie in der Microsoft-Dokumentation.

Erstellen eines Plans zur Definition des Zieldatenspeichers

Zieladministrator

Die Quelldaten werden zu diesem Zieldatenspeicher repliziert. Um diesen Zieldatenspeicher zu definieren, erstellen Sie einen Plan. Mit dem Plan können Sie den Zieldatenspeicher und den Ablaufplan für die Zusammenführung definieren.

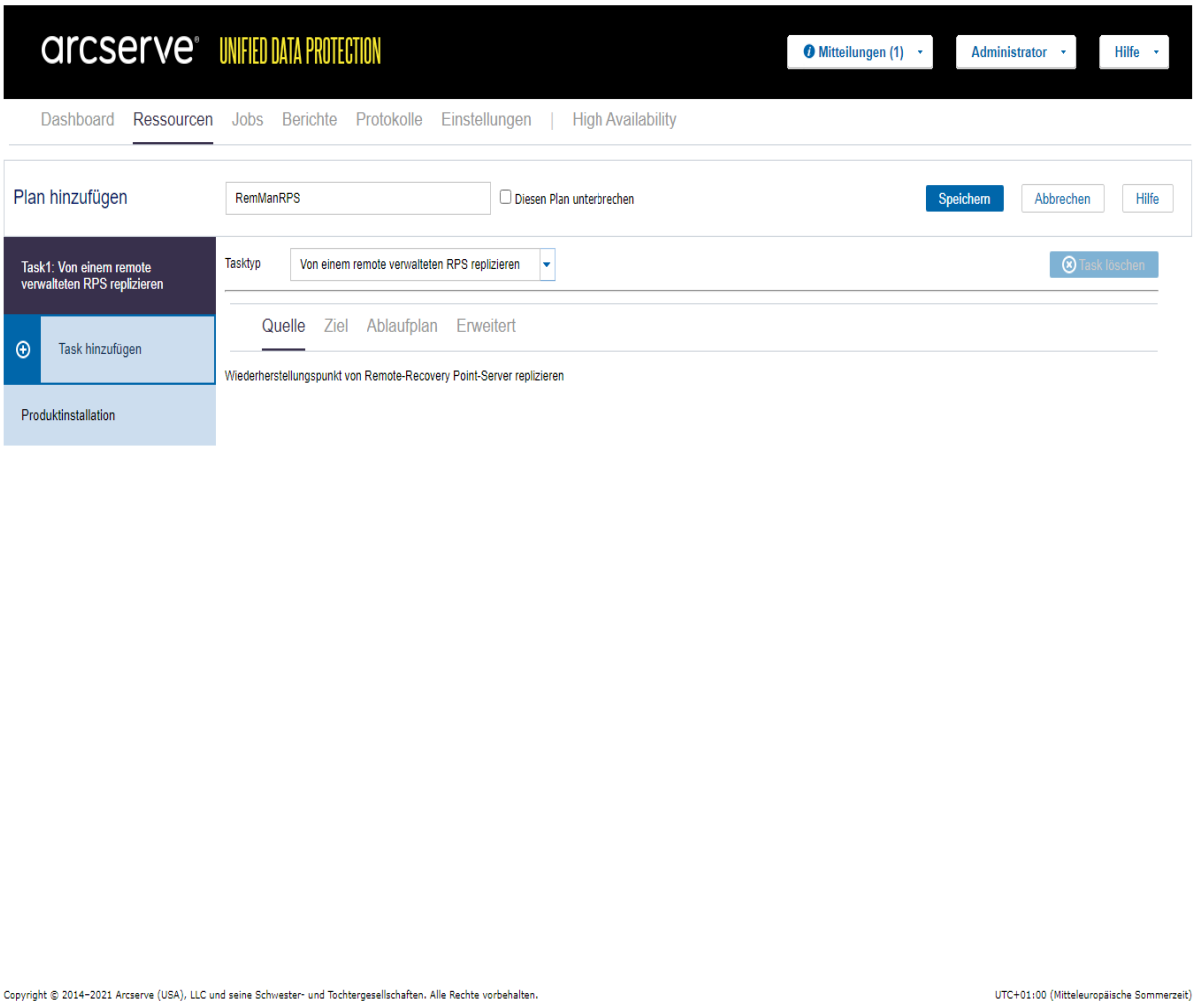
Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

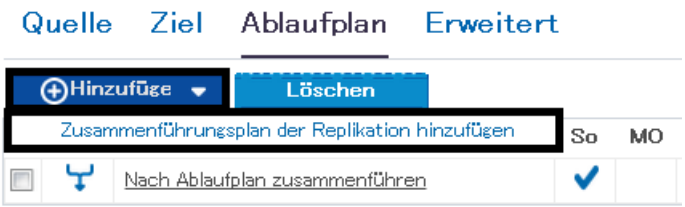
   Wenn Sie Pläne hinzugefügt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Die Seite **Plan hinzufügen** wird geöffnet.
4. Geben Sie im Feld **Neuer Plan** einen Plannamen ein.
5. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Von einem remote verwalteten RPS replizieren** aus.

   Die Registerkarte **Quelle** wird angezeigt. Sie können keine Details auf der Registerkarte "Quelle" angeben. Der Quellenadministrator der Quellenkonsole stellt die Quellendetails bereit.



6. Klicken Sie auf die Registerkarte **Ziel**, und geben Sie den Recovery Point Server und den Datenspeicher an.
7. (Optional) Aktivieren Sie das Kontrollkästchen **Server hinter NAT-Router**, und geben Sie die Serveradresse sowie die Portnummer an.
8. Klicken Sie auf die Registerkarte **Ablaufplan**.



9. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zusammenführungsplan der Replikation hinzufügen** aus.

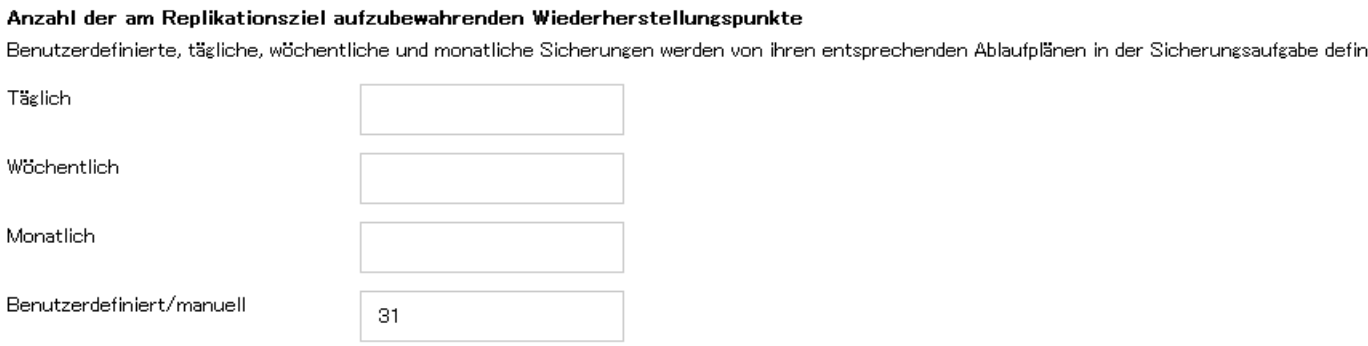
   Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.
10. Geben Sie den Ablaufplan für die Zusammenführung ein.

Hinweis: Weitere Informationen zu Ablaufplänen finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

11. Klicken Sie auf **Speichern**.

    Das Dialogfeld **Neuen Zusammenführungsplan hinzufügen** wird geschlossen.

12. Geben Sie die Details für die Aufbewahrung der Wiederherstellungspunkte ein.



13. Klicken Sie auf die Registerkarte **Erweitert**, und geben Sie folgende Details an.

    Konfigurationsabfrage

    Ermöglicht Ihnen das Abrufen von Wiederherstellungspunkten. Zum Aktivieren der Funktion markieren Sie das Kontrollkästchen **Abrufen von Wiederherstellungspunkten zulassen**.

    E-Mail-Alerts aktivieren

    Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Arten der Alerts angeben, die Sie in Form von E-Mails empfangen möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

    E-Mail-Einstellungen

    Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers.

    Job-Alerts

    Ermöglicht es Ihnen, die Arten von Job-Alerts auszuwählen, die Sie erhalten möchten.

14. Klicken Sie auf **Speichern**.

    Die Änderungen werden gespeichert, und der Plan ist erstellt.

    Der Replikationsplan wurde erfolgreich erstellt. Sie können auch Replizieren-Tasks, Replizieren zu einem Remote-RPS-Task und Virtual Standby-Tasks zu einem Plan hinzufügen.

Zuordnen des Plans zum Benutzerkonto

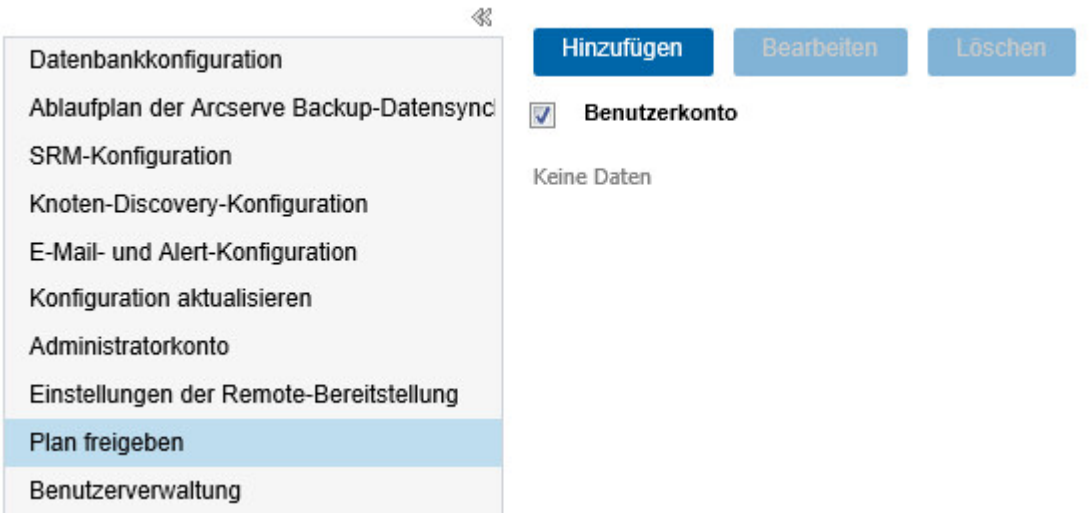
Zieladministrator

Sie haben bereits ein Benutzerkonto und einen Plan für eine Quellkonsole erstellt. Um replizierte Daten zu identifizieren und zu verwalten, weisen Sie den Plan dem Benutzerkonto zu.

Hinweis: Sie können einem Benutzerkonto mehrere Pläne zuweisen, doch ein Plan kann nicht von zwei verschiedenen Konten gemeinsam verwendet werden. Es wird jedoch empfohlen, einem Benutzerkonto jeweils nur einen Plan zuzuweisen, damit Sie die replizierten Daten einfach identifizieren und verwalten können.

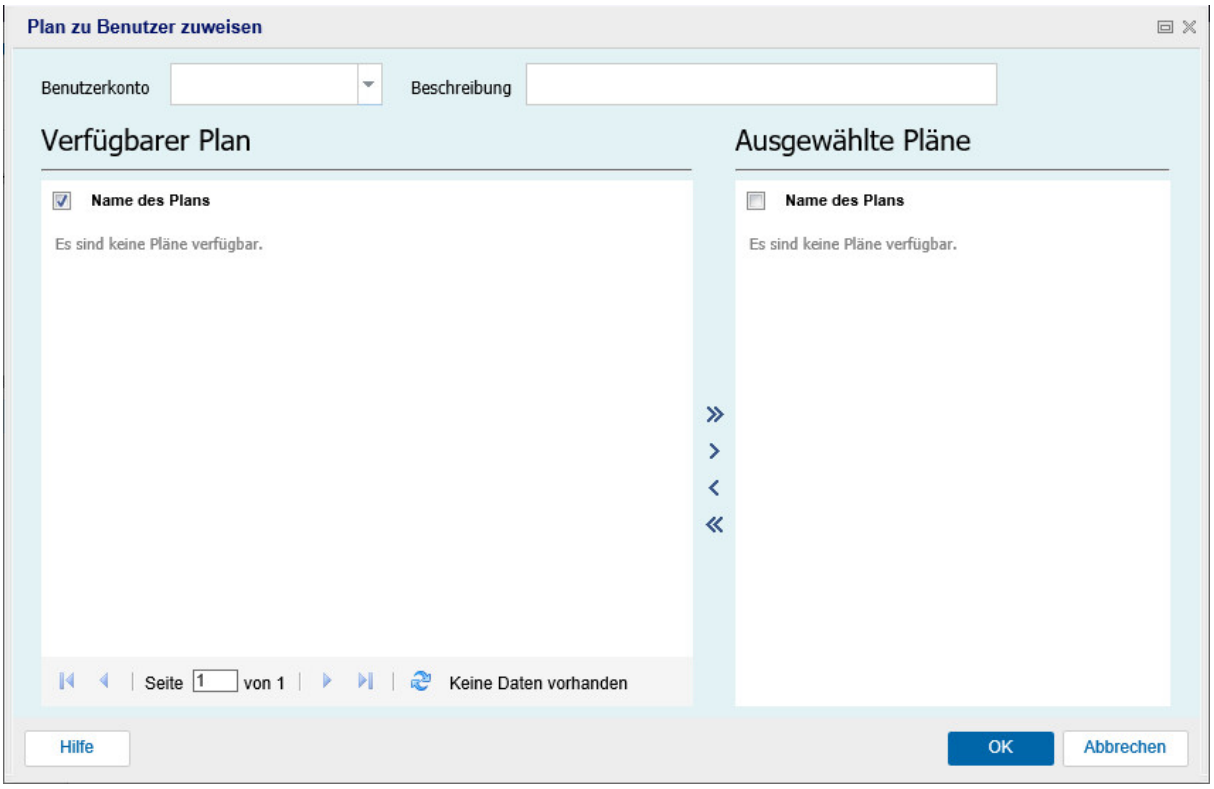
Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Plan freigeben**.



3. Klicken Sie im mittleren Fensterbereich auf **Hinzufügen**.

   Das Dialogfeld **Plan zu Benutzer zuweisen** wird geöffnet.



4. Wählen Sie das **Benutzerkonto** aus.
5. Wählen Sie einen Plan aus der Spalte **Verfügbarer Plan** aus.

   Hinweis: Wenn ein Plan bereits zu einem Benutzernamen hinzugefügt ist, wird dieser Plan nicht in der Spalte "**Verfügbarer Plan**" angezeigt.
6. Klicken Sie auf **Alle Pläne hinzufügen** oder **Ausgewählte Pläne hinzufügen**, um die Pläne in der Spalte **Ausgewählte Pläne** hinzuzufügen.
7. Klicken Sie auf **"OK**".

   Das Dialogfeld **Plan zu Benutzer zuweisen** wird geschlossen. Der Benutzername und die zugeordneten Pläne werden auf der Seite **Plan freigeben** angezeigt.

   Das Benutzerkonto wird dem Plan zugeordnet, der für die Quellkonsole erstellt wurde.

   Sie können **Bearbeiten** verwenden, um die Benutzerkonfiguration zu ändern, oder **Löschen**, um das Benutzerkonto aus der Liste zu entfernen.

Senden des Plans und der Benutzerkonto-Details an den Quellenadministrator

Zieladministrator

Nachdem der Plan mit dem Benutzerkonto verknüpft worden ist, senden Sie dem Quellenadministrator den Plan und die Benutzerkonto-Details. Der Quellenadministrator verwendet diese Details, um eine Verbindung zur Zielkonsole herzustellen.

Als Zieladministrator haben Sie alle Aufgaben abgeschlossen.

Erhalt des Plans und der Benutzerkonto-Details vom Zieladministrator

Quellenadministrator

Um Daten zur Quellenkonsole zu replizieren, benötigen Sie den Zielserver, den Plan und die Benutzerkonto-Details vom Zieladministrator. Sie erhalten die Details vom Zieladministrator. Gehen Sie die Details durch, und klären Sie Fragen mit dem Zieladministrator, bevor Sie mit der Erstellung der Replikationspläne beginnen.

Erstellen eines Replikationsplans zum Senden von Daten an die Zielkonsole

Quellenadministrator

Um Ihre Sicherungsdaten zu dem Ziel-Recovery Point Server zu replizieren, der von einer anderen Konsole verwaltet wird, erstellen Sie einen Replikationsplan. Dieser Replikationsplan schließt einen Sicherungstask und einen per Remote-Zugriff verwalteten Replikationstask ein. Geben Sie im Replikationstask den Remote-Server und Plandetails an, und stellen Sie eine Verbindung mit dem Remote-Server her. Wenn die Verbindung erfolgreich ist, wählen Sie den Plan, den der Zieladministrator für Sie erstellt hat.

Gehen Sie wie folgt vor:

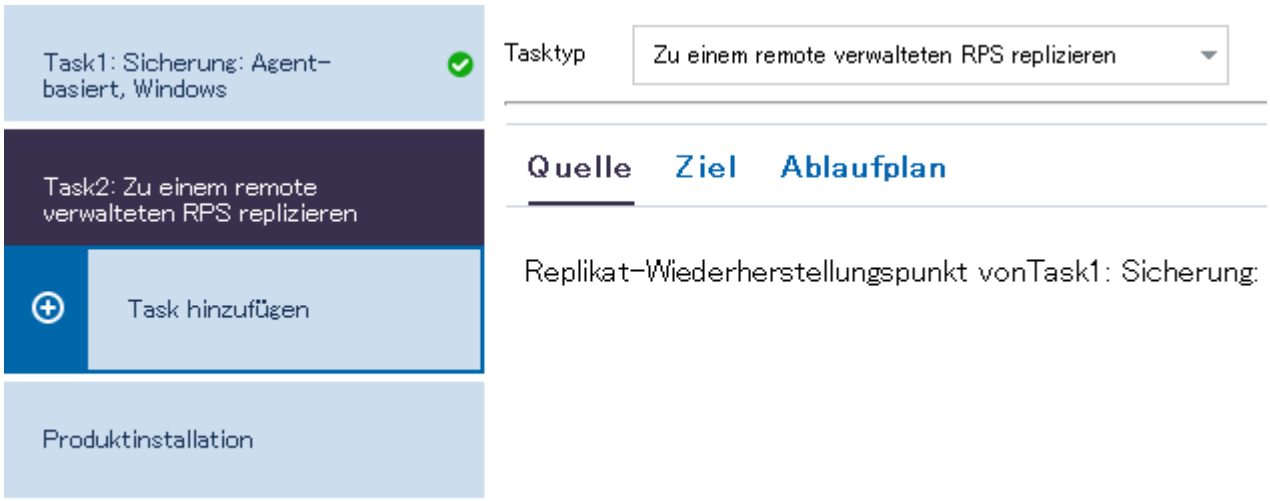
1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.
3. Klicken Sie auf **Plan hinzufügen**.

   Die Seite **Plan hinzufügen** wird geöffnet.
4. Geben Sie einen Plannamen ein, wählen Sie einen der folgenden Sicherungstasks aus, und erstellen Sie den Task:
   - **Sicherung: Agent-basiert, Windows**
   - **Sicherung: Hostbasiert und ohne Agent**
   - **Sicherung: Agent-basiert, Linux**

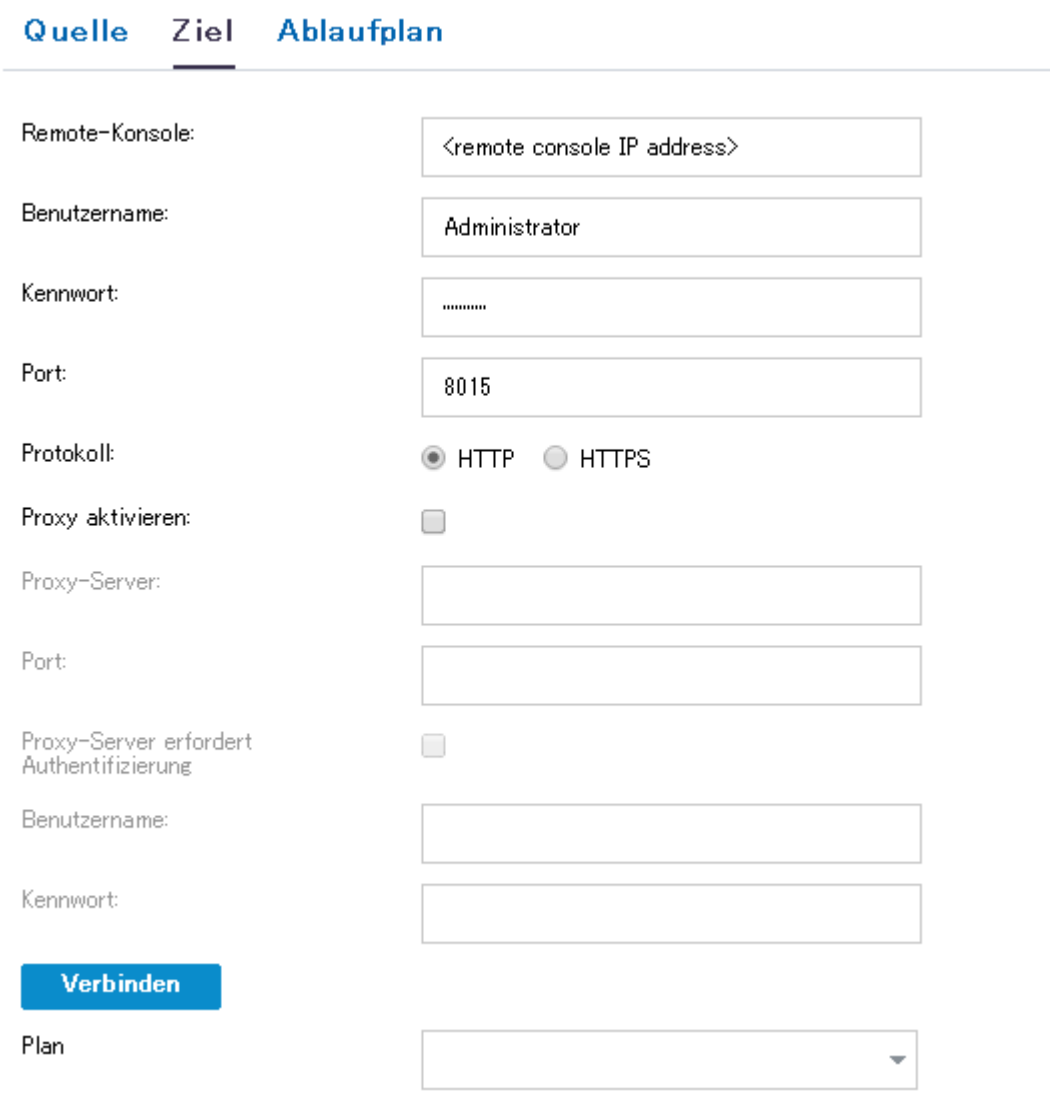
     Hinweis: Weitere Informationen über das Erstellen von Sicherungsaufgaben finden Sie in folgenden Themen:
     - Erstellen eines Sicherungsplans für Windows
     - Erstellen eines Sicherungsplans für hostbasierte virtuelle Rechner
     - Erstellen eines Sicherungsplans für Linux
5. Klicken Sie im mittleren Fensterbereich auf **Task hinzufügen**.

   Ein neuer Task wird im linken Fensterbereich hinzugefügt.
6. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Zu einem remote verwalteten RPS replizieren** aus.

   Der Replikationstask wird hinzugefügt, und die Seite **Quelle** wird geöffnet. Für die Registerkarte **Quelle** ist das Ziel der Sicherungsaufgabe (beispielsweise Sicherung: Agent-basiertes Windows) die Quelle für die Aufgabe **Zu einem remote verwalteten RPS replizieren**.



7. Klicken Sie auf die Registerkarte **Ziel**, und geben Sie folgende Details an.



Remote-Konsole

Wählen Sie ein Konto für die Remote-Konsole aus der Dropdown-Liste aus oder fügen Sie ein neues Konto für die Remote-Konsole hinzu, indem Sie auf **Hinzufügen** klicken.

Weitere Informationen finden Sie unter Remote-Konsole hinzufügen.

Benutzername

Geben Sie den vom Zieladministrator erstellten Benutzernamen an. Der Zieladministrator stellt Ihnen den Benutzernamen bereit.

Kennwort

Geben Sie das Kennwort an, das vom Zieladministrator erstellt wurde. Der Zieladministrator stellt Ihnen das Kennwort bereit.

Port

Geben Sie die Portnummer der Zielkonsole an. Der Zieladministrator stellt Ihnen die Portnummer der Zielkonsole bereit.

Protokoll

Geben Sie das Protokoll an, das der Zieladministrator für die Verbindung mit der Zielkonsole verwendet.

Proxy aktivieren

Aktivieren Sie das Kontrollkästchen, um die Proxy-Server-Auswahl zu aktivieren.

Proxy-Server

Geben Sie die Adresse des Proxy-Servers an.

Port

Geben Sie die Portnummer des Proxy-Servers an.

Proxy-Server erfordert Authentifizierung

Aktivieren Sie das Kontrollkästchen, um die Authentifizierungsfelder für den Proxy-Server zu aktivieren.

Benutzername

Geben Sie den Benutzernamen an, der mit dem Proxy-Server verbunden werden soll.

Kennwort

Geben Sie das Kennwort an, um die Verbindung des Proxy-Servers zu authentifizieren.

Verbinden

Überprüft die Verbindung zwischen der Quellkonsole und der Zielkonsole. Wenn die Verbindung erfolgreich ist, wird der Planname im Feld **Plan** angezeigt. Dieser Planname wird dieser Konsole vom Zieladministrator zugewiesen.

Plan

Geben Sie den Plan an, den der Zieladministrator für Sie erstellt hat. Wenn mehrere Pläne in der Liste vorhanden sind, fragen Sie den Zieladministrator nach dem korrekten Plan.

Startwiederholung

Wiederholt den Replikationsjob nach der angegebenen Zeit, wenn ein Fehler auftritt. Geben Sie einen Wert von 1 bis 60 ein. Die Zeit wird in Minuten angegeben.

Wiederholen

Geben Sie die Anzahl der Wiederholungen an, die ausgeführt werden sollen, wenn ein Jobfehler auftritt. Nach der Anzahl der Wiederholung wird der Replikationsjob nur zum nächsten geplanten Zeitpunkt ausgeführt. Geben Sie einen Wert von 1 bis 99 ein.

8. Klicken Sie auf die Registerkarte **Ablaufplan** und geben Sie den Ablaufplan des Replikationsjobs und den Ablaufplan der Replikationsdrosselung an.

   Ablaufplan des Replikationsjobs

   Geben Sie das Datum und die Uhrzeit für den Start der Replikationsjobs an. Sie können einen Plan für den Replikationsjob bearbeiten oder löschen.

   Ablaufplan der Replikationsdrosselung

   Geben Sie die Höchstgeschwindigkeit (Mbit/s) an, mit der die Replikation durchgeführt wird. Sie können die Replikationsgeschwindigkeit drosseln, um die CPU- oder Netzwerkauslastung zu reduzieren. Für einen Replikationsjob zeigt die Registerkarte **Jobs** die durchschnittliche Lese- und Schreibgeschwindigkeit des Jobs an, der ausgeführt wird. Außerdem wird die Begrenzung angezeigt, die für die Drosselung der Geschwindigkeit konfiguriert ist.

   Sie können einen Ablaufplan der Replikationsdrosselung bearbeiten oder löschen.

9. Klicken Sie auf **Speichern**.

   Der Plan wird gespeichert und gemäß Ablaufplan ausgeführt.

   Sie haben einen Replikationsplan erfolgreich erstellt und automatisch bereitgestellt. Bei Ausführung des Plans werden die Daten vom Quellspeicherort zum Zieldatenspeicherort über ein Netzwerk repliziert.

Hinweis: Nach der Replikation werden die replizierten Knotendetails automatisch der Zielkonsole hinzugefügt.

Sie haben erfolgreich Daten zwischen zwei Datenspeichern repliziert, die von unterschiedlichen UDP-Konsolen verwaltet werden.

Überprüfen der Datenreplikation

Zieladministrator

Nachdem Daten repliziert worden sind, können Sie überprüfen, ob die Replikation erfolgreich war.

Gehen Sie wie folgt vor:

1. Navigieren Sie auf der Zielkonsole zum Zieldatenspeicher auf dem Recovery Point Server.
2. Überprüfen Sie, ob die Größe der replizierten Daten mit der Größe der Quelldaten übereinstimmt.

   Sie haben erfolgreich Daten zwischen zwei Datenspeichern repliziert, die von unterschiedlichen UDP-Konsolen verwaltet werden.

So führen Sie eine Offline-Datenreplikation mithilfe von RPS Jumpstart aus

Die Replikation eines großen Datenspeichers zu einem anderen Recovery Point Server (verwaltet von einer anderen UDP-Konsole) ist über ein Netzwerk (LAN, WAN, Internet) zeitaufwändig. Um einen großen Datenspeicher schnell zu replizieren, stellt Arcserve UDP eine Offline-Datenreplikationsmethode bereit. Diese Methode wird RPS-Jumpstart genannt.

RPS-Jumpstart ist eine Offline-Replikationsmethode, die ein externes Speichergerät wie ein USB-Flash-Laufwerk verwendet, um einen Datenspeicher zu replizieren. Diese Replikation erfolgt zwischen zwei Datenspeichern, die von unterschiedlichen UDP-Konsolen verwaltet werden. Ziehen Sie zum Beispiel einen Dienstanbieter in Betracht, der seine Replikationsdienste mehreren Kunden anbietet. Der Kunde repliziert die Daten zu einem Speichergerät und sendet das Speichergerät an den Dienstanbieter. Der Dienstanbieter repliziert Daten vom Speichergerät zum Zielserver. Sowohl beim Dienstanbieter als auch beim Kunden muss Arcserve UDP installiert sein.

Die Offline-Replikation erfordert, dass beide Administratoren (Quellen- und Zieladministrator) jeweils die folgenden Schritte durchführen.

Wichtig! Hinweise zur Replikation aus einem freigegebenen Ordner zu einem auf einem Recovery Point Server ausgewählten Datenspeicher finden Sie unter So migrieren Sie r16.5-Wiederherstellungspunkte auf Arcserve UDP.

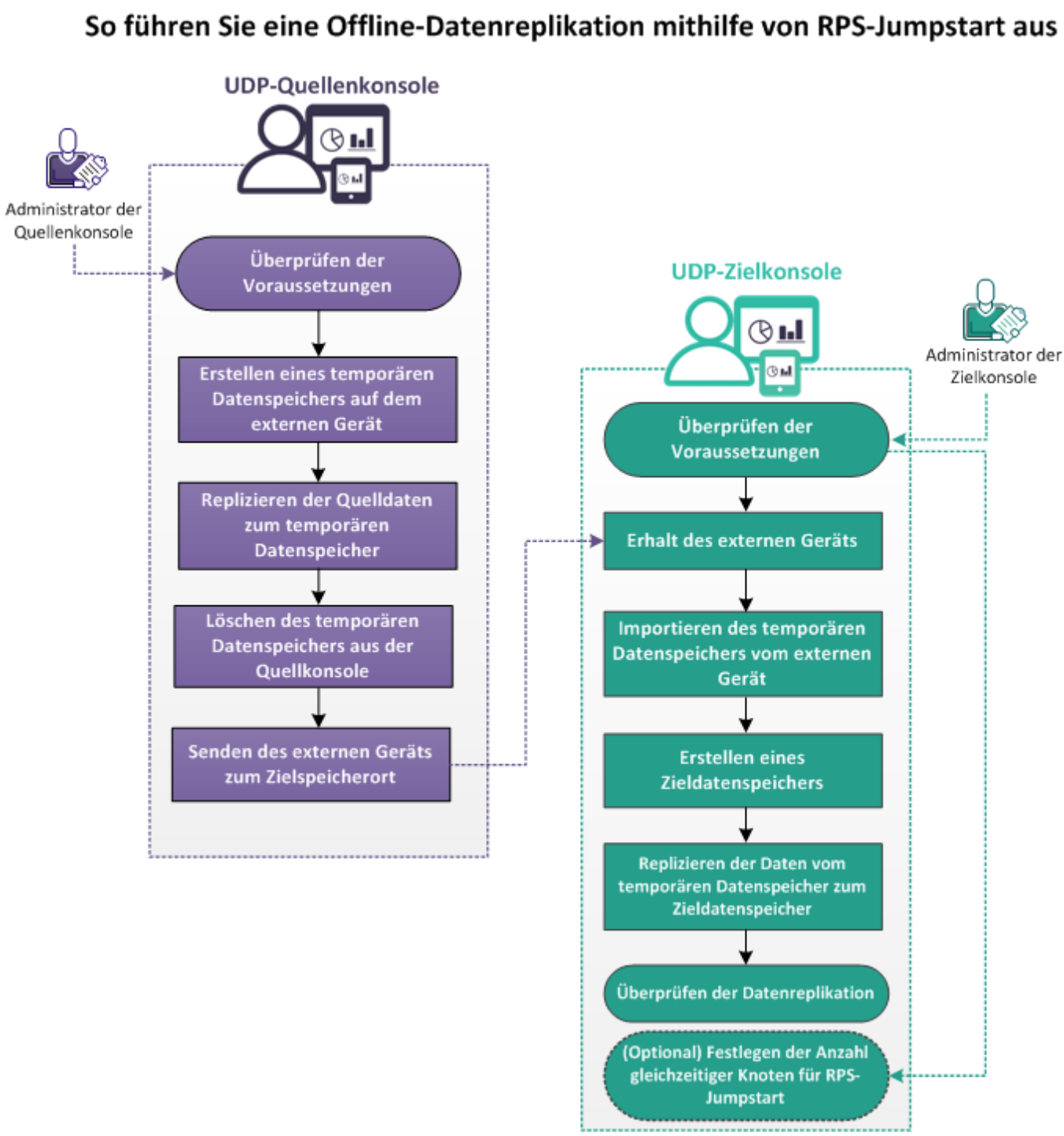
Quellenadministrator

1. Replizieren des Quelldatenspeichers zu einem externen Gerät.
2. Senden des externen Geräts zum Zielspeicherort.

Zieladministrator

1. Erhalt des externen Geräts.
2. Replizieren des Quelldatenspeichers vom externen Gerät zum Ziel-Recovery Point Server.

Das folgende Diagramm veranschaulicht die Durchführung einer Offline-Datenreplikation mithilfe von RPS-Jumpstart.



Der nächste Schritt?

- Überprüfen der Voraussetzungen
- Erstellen eines temporären Datenspeichers auf einem externen Gerät
- Replizieren der Quelldaten zum temporären Datenspeicher
- Löschen des temporären Datenspeichers aus der Quellkonsole

- Senden des externen Geräts zum Zielspeicherort
- Erhalt des externen Geräts
- Importieren der temporären Daten aus dem externen Gerät
- Erstellen eines Zieldatenspeichers
- Replizieren der Daten vom temporären Datenspeicher zum Zieldatenspeicher
- Überprüfen der Datenreplikation
- (Optional) Festlegen der Anzahl gleichzeitiger Knoten für RPS-Jumpstart

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie eine Offline-Datenreplikation ausführen:

- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.
- Wenn die Quelle ein Datenspeicher mit aktivierter Deduplizierung ist, muss das Ziel ebenfalls ein Datenspeicher mit aktivierter Deduplizierung sein.
- Wenn die Quelle ein Datenspeicher mit aktivierter Verschlüsselung ist, muss das Ziel auch ein Datenspeicher mit aktivierter Verschlüsselung sein.

Administrator – Quellkonsole

- Stellen Sie sicher, dass Sie den Quelldatenspeicher erstellt haben.
- Stellen Sie sicher, dass Sie mindestens eine Sicherung eines Datenspeichers durchgeführt haben.
- (Optional) Stellen Sie sicher, dass Sie die Anzahl gleichzeitiger Knoten für RPS-Jumpstart konfiguriert haben. Weitere Informationen zum Konfigurieren der Anzahl gleichzeitiger Knoten finden Sie unter Festlegen der Anzahl gleichzeitiger Knoten für RPS-Jumpstart.

Administratoren – Zielkonsole

- Stellen Sie sicher, dass Sie über ausreichend Speicherplatz für die Replikation verfügen.
- Stellen Sie sicher, dass Sie die erforderlichen Berechtigungen für das externe Gerät haben.

Erstellen eines temporären Datenspeichers auf einem externen Gerät

Quellenadministrator

Um Daten von einem vorhandenen Datenspeicher auf einem externen Gerät zu importieren, erstellen Sie zuerst einen temporären Datenspeicher auf dem externen Gerät. Um den temporären Datenspeicher zu erstellen, schließen Sie das externe Gerät am Computer an.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der UDP-Konsole an.
2. Navigieren Sie zu **Ziele**, **Recovery Point Server**.
3. Wählen Sie den Recovery Point Server aus.
4. Klicken Sie mit der rechten Maustaste, und wählen Sie **Einen Datenspeicher hinzufügen** aus.
5. Geben Sie die Details auf der Seite **Einen Datenspeicher hinzufügen** ein.

   Hinweis: Stellen Sie sicher, dass sich die Sicherungszielordner auf dem externen Gerät befinden.
6. Speichern Sie den Datenspeicher.

   Der temporäre Datenspeicher wird auf dem externen Gerät erstellt.

Replizieren der Quelldaten zum temporären Datenspeicher

Quellenadministrator

Nachdem Sie den temporären Datenspeicher auf dem externen Gerät erstellt haben, können Sie die Quelldaten mithilfe von RPS-Jumpstart zum externen Gerät replizieren.

Hinweis: Bevor Sie den RPS-Jumpstart-Prozess starten, unterbrechen Sie den verknüpften Plan. Dadurch wird sichergestellt, dass ein geplanter Replikationsjob nicht während des Jumpstart-Prozesses gestartet wird.

Gehen Sie wie folgt vor:

1. Klicken Sie auf "**Aktionen**", und klicken Sie dann auf "**RPS-Jumpstart**".

   Der **Assistent für RPS-Jumpstart** wird geöffnet.

2. Wählen Sie aus, ob Sie vom gleichen Datenspeicher oder von einem freigegebenen Speicherort migrieren möchten.

3. Wählen Sie den Recovery Point-Server der Quelle, den Quelldatenspeicher und den Plan aus.

   Die Knoten, die zum Plan gehören, werden angezeigt.

4. Wählen Sie die Knoten aus, die migriert werden sollen.

5. Klicken Sie auf **Weiter**.

   Die Seite **Zieldatenspeicher auswählen** wird geöffnet. Wenn der Quelldatenspeicher verschlüsselt ist, werden nur die verschlüsselten Datenspeicher in der Drop-down-Liste angezeigt.

6. Wählen Sie die Zieldatenspeicher. Der Zieldatenspeicher sollte auf dem externen Gerät sein.

7. Klicken Sie auf **Fertig stellen**.

   Der Bereich **Letzte Ereignisse** rechts zeigt den Replikationsfortschritt an.

   Nach dem Abschluss des Replikationsprozesses werden die Daten zum temporären Datenspeicher repliziert. Sie können die Größe beider Datenspeicher auf der Seite **Ziele: Recovery Point Server** prüfen.

Löschen des temporären Datenspeichers aus der Quellkonsole

Quellenadministrator

Um die Datenintegrität auf dem externen Gerät zu wahren, löschen Sie den temporären Datenspeicher aus der UDP-Konsole, bevor Sie das externe Gerät entfernen.

Hinweis: Beim Löschen des temporären Datenspeichers aus der UDP-Quellenkonsole werden die Datenspeicherdateien auf dem externen Gerät nicht gelöscht.

Gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf den temporären Datenspeicher, und klicken Sie auf **Stoppen**.

   Der Datenspeicher wird gestoppt.

2. Klicken Sie mit der rechten Maustaste auf den temporären Datenspeicher, und wählen Sie **Löschen**.

   Ein Bestätigungsdialogfeld wird geöffnet.

3. Klicken Sie auf **Ja**.

   Der Datenspeicher ist nun gelöscht.

   Jetzt können Sie das externe Gerät vom Computer entfernen.

Senden des externen Geräts zum Zielspeicherort

Quellenadministrator

Nachdem Sie das externe Gerät entfernt haben, senden Sie das Gerät zum Zielspeicherort.

Erhalt des externen Geräts

Zieladministrator

Sie erhalten das externe Gerät, das Quelldaten umfasst. Verbinden Sie jetzt dieses externe Gerät mit dem Zielserver.

Importieren des temporären Datenspeichers vom externen Gerät

Zieladministrator

Bevor Sie die Quelldaten zum Zieldatenspeicher replizieren können, importieren Sie den temporären Datenspeicher zum Ziel-Recovery Point Server.

Gehen Sie wie folgt vor:

1. Navigieren Sie zur Registerkarte **Ressourcen**, und wählen Sie den Recovery Point Server aus, in den Sie den Datenspeicher importieren möchten.
2. Klicken Sie mit der rechten Maustaste auf den Recovery Point Server, und wählen Sie **Datenspeicher importieren** aus.

   Das Dialogfeld **Datenspeicher importieren** wird geöffnet.
3. Wählen Sie den Sicherungszielordner auf dem externen Gerät aus.
4. Klicken Sie auf **Weiter**.

   Die temporären Datenspeicherdetails werden angezeigt. Falls erforderlich, ändern Sie anschließend Daten-, Index- und Hash-Pfad.
5. Klicken Sie auf "**Speichern**".

   Der Datenspeicher wird importiert und in der Zielkonsole angezeigt.

Erstellen eines Zieldatenspeichers

Zieladministrator

Um Daten vom temporären Datenspeicher zu replizieren, erstellen Sie zuerst einen Zieldatenspeicher. Weitere Informationen finden Sie unter So fügen Sie einen Datenspeicher hinzu.

Hinweis: Sie können auch einen vorhandenen Datenspeicher als Zieldatenspeicher verwenden.

Replizieren der Daten vom temporären Datenspeicher zum Zieldatenspeicher

Nachdem Sie den Zieldatenspeicher erstellt haben, replizieren Sie die Daten vom temporären Datenspeicher zum Zieldatenspeicher. Nachdem die Daten zum Zieldatenspeicher repliziert worden sind, können Sie den temporären Datenspeicher löschen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf "**Aktionen**", und klicken Sie dann auf "**RPS-Jumpstart**".

   Der **Assistent für RPS-Jumpstart** wird geöffnet.

2. Wählen Sie den Recovery Point-Server der Quelle und den Quelldatenspeicher aus. Der Plan muss hier ausgewählt werden.

   Die Knoten werden angezeigt.

3. Wählen Sie die Knoten aus, die migriert werden sollen.

4. Klicken Sie auf **Weiter**.

   Die Seite **Zieldatenspeicher auswählen** wird geöffnet. Wenn der Quelldatenspeicher verschlüsselt ist, werden nur die verschlüsselten Datenspeicher in der Drop-down-Liste angezeigt.

5. Wählen Sie den Zieldatenspeicher. Der Zieldatenspeicher sollte auf dem externen Gerät sein.

6. Klicken Sie auf **Fertig stellen**.

   Der Bereich **Letzte Ereignisse** rechts zeigt den Replikationsfortschritt an.

   Nach dem Abschluss des Replikationsprozesses werden die Daten zum temporären Datenspeicher repliziert. Sie können die Größe beider Datenspeicher auf der Seite **Ziele: Recovery Point Server** prüfen.

   Die Daten werden zum Zieldatenspeicher repliziert.

Überprüfen der Datenreplikation

Zieladministrator

Nachdem Daten repliziert worden sind, können Sie überprüfen, ob die Replikation erfolgreich war.

Gehen Sie wie folgt vor:

1. Navigieren Sie auf der Zielkonsole zum Zieldatenspeicher auf dem Recovery Point Server.
2. Überprüfen Sie, ob die Größe der replizierten Daten mit der Größe der Quelldaten übereinstimmt.

   Sie haben erfolgreich Daten zwischen zwei Datenspeichern repliziert, die von unterschiedlichen UDP-Konsolen verwaltet werden.

(Optional) Festlegen der Anzahl gleichzeitiger Knoten für RPS-Jumpstart

Quellenadministrator

Wenn Sie einen RPS Jumpstart-Job starten, beträgt die Anzahl gleichzeitiger Knoten für den Datenspeicher standardmäßig 4. Um die Anzahl gleichzeitiger Knoten anzugeben, müssen Sie einen Schlüssel erstellen und manuell ein DWORD hinzufügen.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Recovery Point Server an.
2. Navigieren Sie zu folgendem Speicherort:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
3. Erstellen Sie einen Schlüssel im Verzeichnis "Engine", und nennen Sie ihn *RPS Jumpstart*.
4. Fügen Sie im Schlüssel "RPS Jumpstart" folgendes DWORD hinzu:

   JumpStartConCurrencyCount
5. Geben Sie einen Wert für das DWORD an.

   Beispiel: Wenn Sie die Knoten pro RPS Jumpstart-Job auf 10 Knoten beschränken möchten, fügen Sie folgendes DWORD hinzu:

   JumpStartConCurrencyCount=10

   Die Anzahl gleichzeitiger Knoten für RPS Jumpstart ist nun festgelegt.

Ausführen einer umgekehrten Replikation

Mit dieser Funktion können Sie Daten (Wiederherstellungspunkt) aus der Cloud, vom MSP oder von einem remote verwalteten RPS zu einem lokalen UDP-Rechner oder einem RPS-Server vor Ort replizieren. Um Ihre replizierten Daten von einem Recovery Point Server, der von einer anderen Arcserve UDP-Konsole wie Cloud, MSP oder remote verwaltetem RPS verwaltet wird, wieder auf den lokalen UDP-Rechner oder den Server vor Ort abzurufen, müssen Sie eine umgekehrte Replikation durchführen. Bei der umgekehrten Replikation werden die Daten von einem Zieldatenspeicher (auf der Zielkonsole) zu einem Quelldatenspeicher (auf der Quellkonsole) repliziert.

In diesem Abschnitt werden die folgenden Themen behandelt:

Überprüfen der Voraussetzungen

Überprüfen Sie folgende Voraussetzungen, bevor Sie Daten replizieren:

- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Administratoren – Zielkonsole

- Stellen Sie sicher, dass Arcserve UDP auf dem Zielserver installiert ist.
- Stellen Sie sicher, dass Sie über alle Berechtigungen verfügen, um Windows-Benutzerkonten auf dem Zielserver zu erstellen.
- Überprüfen Sie, ob Sie während der Erstellung eines Plans zur Replikation von einem remote verwalteten RPS das Kontrollkästchen **Abrufen von Wiederherstellungspunkten zulassen** in den erweiterten Einstellungen aktiviert haben.

  Hinweis: Wenn Sie das Kontrollkästchen **Abrufen von Wiederherstellungspunkten zulassen** nicht aktivieren und den umgekehrten Replikationsjob für die Remote-Konsole starten, werden Sie aufgefordert, das Flag für das Zulassen des Remote-Abrufs für die umgekehrte Replikation zu aktivieren.

Administrator – UDP-Quellenkonsole

- Stellen Sie sicher, dass Arcserve UDP auf dem Quellserver installiert ist.
- Stellen Sie sicher, dass Sie mindestens eine vollständige Sicherung eines Datenspeichers durchgeführt haben.

Durchführen einer Ad-hoc-Replikation

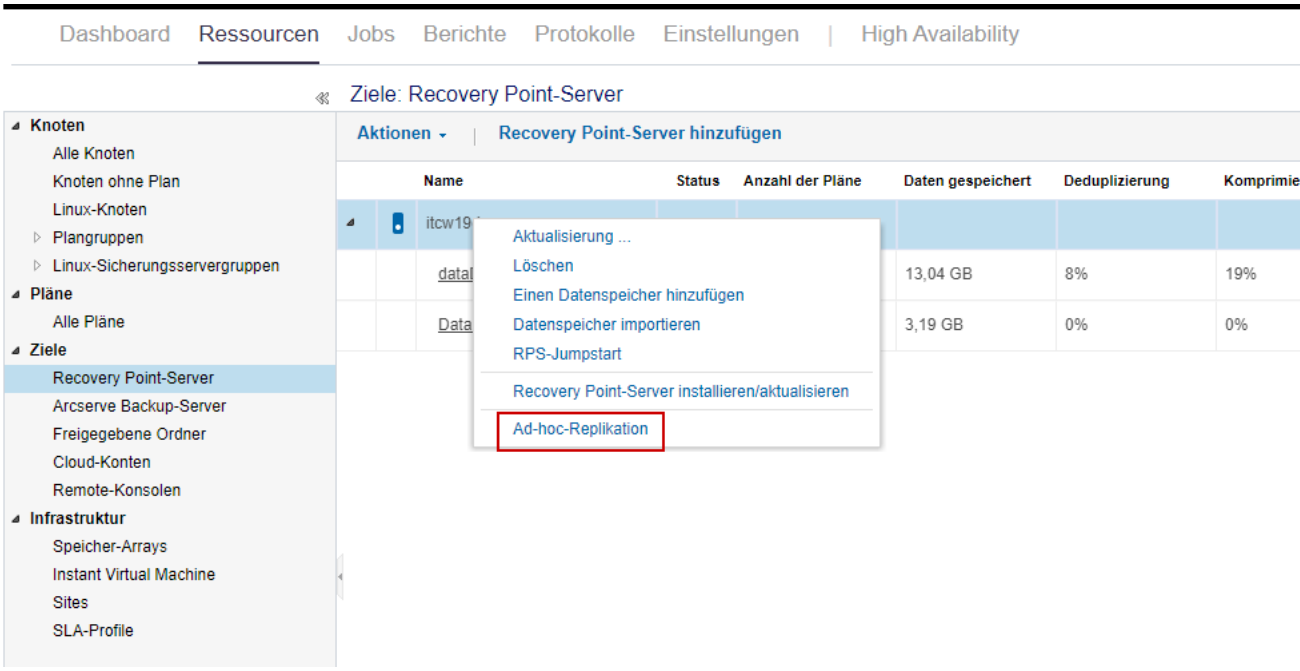
In diesem Abschnitt wird erläutert, wie Sie eine Ad-hoc-Replikation initiieren.

Hinweis: Stellen Sie vor dem Starten der Ad-hoc-Replikation sicher, dass die Weiterleiten-Replikation erfolgreich ausgeführt wird. Unter Überprüfen der Datenreplikation erfahren Sie, wie Sie überprüfen, ob die Weiterleiten-Replikation erfolgreich war.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele** > **Recovery Point Server**.

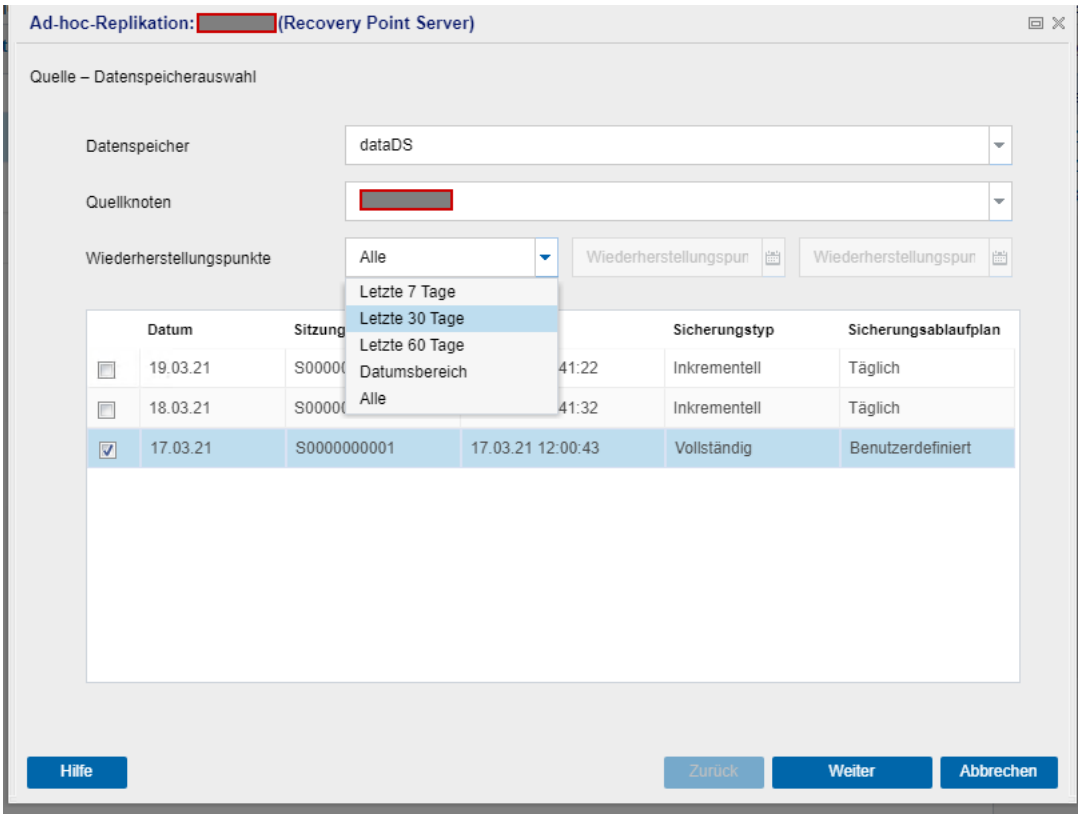
   Die Liste der Recovery Point Server wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Recovery Point Server, und wählen Sie dann **Ad-hoc-Replikation** aus.



Warten Sie, bis eine Verbindung zum Recovery Point Server hergestellt wurde.

Das Dialogfeld "Ad-hoc-Replikation: xx-xx-xx (Recovery Point Server)" wird geöffnet.

4. Gehen Sie auf der Seite "Quelle – Datenspeicherauswahl" wie folgt vor:

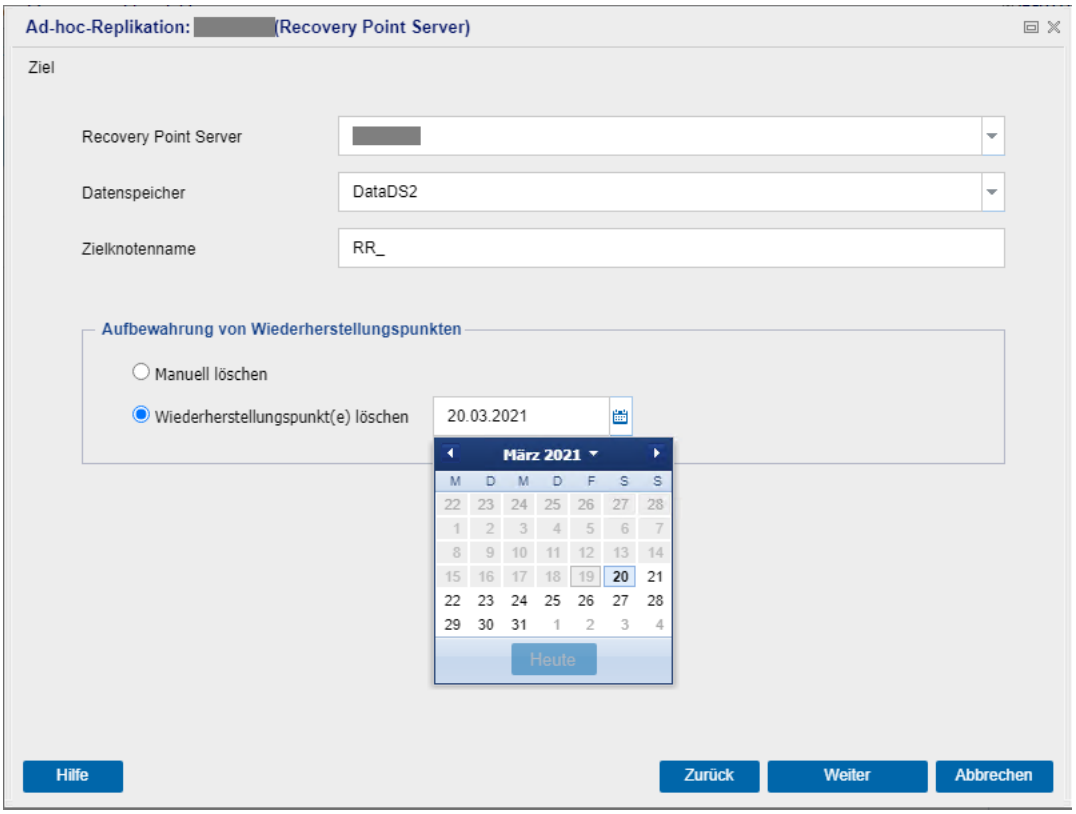


- Datenspeicher: Wählen Sie den Quelldatenspeicher in der Drop-down-Liste aus.
- Quellknoten: Wählen Sie den Quellknoten in der Drop-down-Liste aus.
- Wiederherstellungspunkte: Führen Sie einen der folgenden Schritte aus:
  - Wenn alle gesicherten Wiederherstellungspunkte angezeigt werden sollen, wählen Sie in der Drop-down-Liste die Option **Alle** aus.
  - Wenn die Wiederherstellungspunkte für einen bestimmten Zeitraum angezeigt werden sollen, wählen Sie in der Drop-down-Liste eine der folgenden Optionen aus:
    - Letzte 7 Tage
    - Letzte 30 Tage
    - Letzte 60 Tage
    - Datumsbereich

    Hinweis: Wenn Sie die Option **Datumsbereich** ausgewählt haben, legen Sie das Datum in den Feldern **Wiederherstellungspunkte von** und **Wiederherstellungspunkte bis** fest.

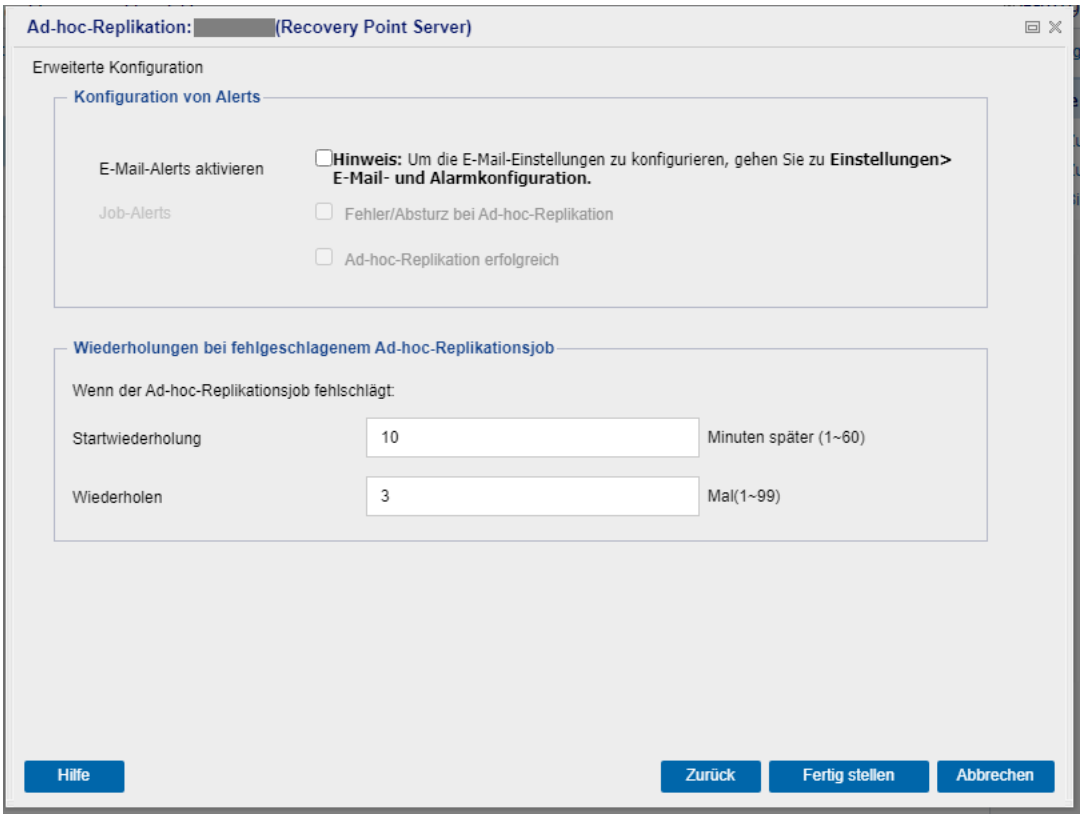
  Alle zugeordneten Wiederherstellungspunkte im angegebenen Zeitraum werden angezeigt.
- Wählen Sie einen oder mehrere Wiederherstellungspunkte aus, indem Sie die entsprechenden Kontrollkästchen in der Tabelle aktivieren.

5. Klicken Sie auf **Weiter**.
6. Gehen Sie auf der Seite "Ziel" wie folgt vor:



- Recovery Point Server: Wählen Sie den Ziel-Recovery Point Server in der Drop-down-Liste aus.
- Datenspeicher: Wählen Sie den Zieldatenspeicher in der Drop-down-Liste aus.
- Zielknotenname: Geben Sie einen Zielknotennamen Ihrer Wahl ein.
- Aufbewahrung von Wiederherstellungspunkten: Löschen Sie die Wiederherstellungspunkte mit einer der folgenden Methoden:
  - Wählen Sie die Option **Manuell löschen** aus, um Wiederherstellungspunkte manuell zu löschen.
  - Wenn die Wiederherstellungspunkte automatisch gelöscht werden sollen, wählen Sie die Option **Wiederherstellungspunkt(e) löschen** aus und geben dann das Datum an. Alle Wiederherstellungspunkte mit diesem Datum werden automatisch gelöscht.

7. Klicken Sie auf **Weiter**.
8. Gehen Sie auf der Seite "Erweiterte Konfiguration" wie folgt vor:



- Für "Konfiguration von Alerts"

  E-Mail-Alerts aktivieren

  Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Typen der Warnmeldungen angeben, die Sie in einer E-Mail erhalten möchten. Wenn Sie das Kontrollkästchen **Hinweis: Stellen Sie sicher, dass Sie die E-Mail-Einstellungen auf der Registerkarte "E-Mail- und Alarm-konfiguration" konfigurieren.** aktivieren, wird die folgende Option zur Auswahl verfügbar:

  Job-Alerts

  Ermöglicht es Ihnen, die Art von Job-Alerts auszuwählen, die Sie per E-Mail empfangen möchten.

  - Wenn Sie E-Mail-Alerts für fehlgeschlagene oder abgestürzte Ad-hoc-Replikationen erhalten möchten, aktivieren Sie das Kontrollkästchen **Fehler/Absturz bei Ad-hoc-Replikation**.

    Hinweis: Dieser E-Mail-Alert wird mit hoher Wichtigkeit gesendet. E-Mail-Alerts mit festgelegter hoher Wichtigkeit werden in Ihrem

Posteingang mit einem Ausrufezeichen als visueller Indikator angezeigt.

- Wenn Sie E-Mail-Alerts für erfolgreiche Ad-hoc-Replikationen erhalten möchten, aktivieren Sie das Kontrollkästchen **Ad-hoc-Replikation erfolgreich**.

- Für "Wiederholungen bei fehlgeschlagenem Ad-hoc-Replikationsjob"

  Wenn der Ad-hoc-Replikationsjob fehlschlägt, gehen Sie folgendermaßen vor:

  Startwiederholung

  Ermöglicht es Ihnen anzugeben, nach wie vielen Minuten ein fehlgeschlagener Replikationsjobs neu gestartet werden soll. Wenn Sie beispielsweise 10 Minuten angeben, wird der Replikationsjob 10 Minuten, nachdem er fehlgeschlagen ist, neu gestartet.

  Beschränkung: 1 bis 60

  Wiederholen

  Ermöglicht es Ihnen, die Anzahl der Wiederholungen anzugeben, die Sie ausführen möchten, wenn der Replikationsjob fehlschlägt. Der Replikationsjob wird so oft ausgeführt, bis der Job erfolgreich ist oder die Beschränkung erreicht ist. Nach Durchführung der angegebenen Anzahl von Wiederholungen wird der Replikationsjob erst wieder zum nächsten geplanten Zeitpunkt ausgeführt.

  Beschränkung: 1 bis 99

9. Klicken Sie auf **Finish**.

   Hinweis: Wenn Sie die Einstellungen in den vorherigen Bildschirmen ändern möchten, klicken Sie auf **Zurück**, und ändern Sie dann die Einstellung nach Bedarf.

   Ein Informationsdialogfeld mit der Meldung *Ad-hoc-Replikationsjob wurde erfolgreich übergeben* wird angezeigt.

10. Klicken Sie auf **OK**, um das Informationsdialogfeld zu schließen.

    Die Ad-Hoc-Replikation wird erfolgreich ausgeführt.

Überwachen des Status der Ad-hoc-Replikation

Quellenadministrator

Wenn die Ad-hoc-Replikation erfolgreich ist, können Sie den Status des Ad-hoc-Replikationsjobs überwachen.

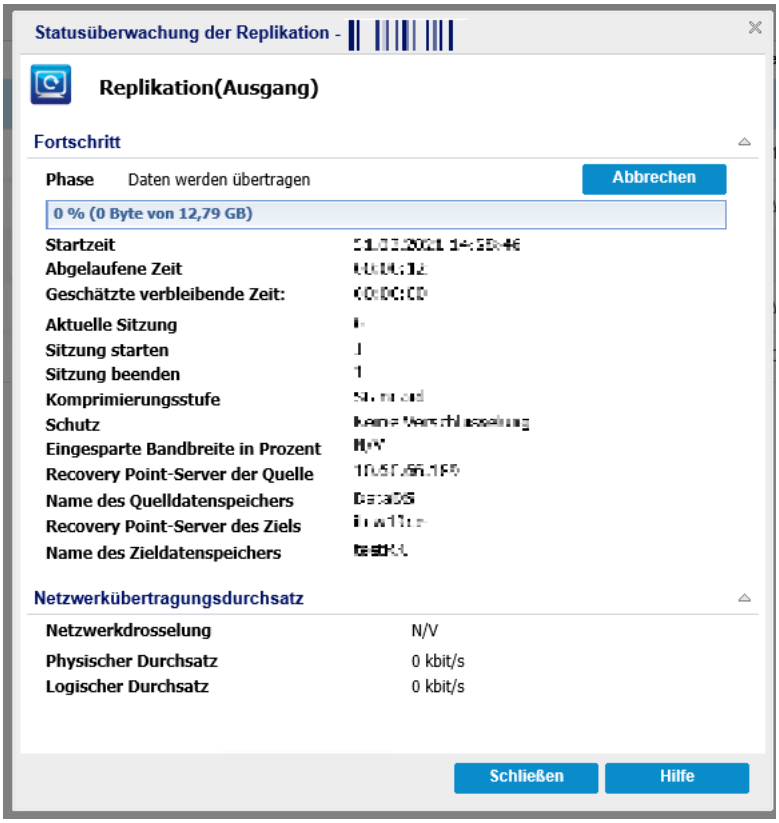
Gehen Sie wie folgt vor:

1. Navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Die in Bearbeitung befindlichen Jobs vom Typ "Replikation (Ausgang)" und "Replikation (Eingang)" werden im mittleren Fensterbereich angezeigt.

2. Um den Status eines bestimmten Jobs zu überwachen, klicken Sie neben der Fortschrittsleiste des betreffenden Jobs auf **Details**.

   Das Dialogfeld "Statusüberwachung der Replikation - xx.xx.xx.xx" wird angezeigt.



3. Warten Sie, bis die Datenübertragung zu 100 % abgeschlossen ist, und klicken Sie auf **Schließen**.

Sie haben den Status der Ad-hoc-Replikation erfolgreich überwacht.

Überprüfen der erfolgreichen Durchführung der Ad-hoc-Replikation

Quellenadministrator

Nachdem Daten repliziert wurden, können Sie überprüfen, ob die Ad-hoc-Replikation erfolgreich war.

Gehen Sie wie folgt vor:

1. Navigieren Sie in der Quellkonsole zu **Jobs** > **Jobs erfolgreich abgeschlossen**.

   Im mittleren Fensterbereich wird eine Liste der abgeschlossenen Jobs angezeigt.
2. Klicken Sie auf den abgeschlossenen umgekehrten Replikationsjob. Der rechte Fensterbereich wird aktualisiert.
3. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
4. Überprüfen Sie, ob die Datenreplikation erfolgreich war.

Sie haben die Ad-hoc-Replikation erfolgreich überprüft.

Durchführen einer umgekehrten Replikation von der Remote-Konsole zum RPS-Server vor Ort

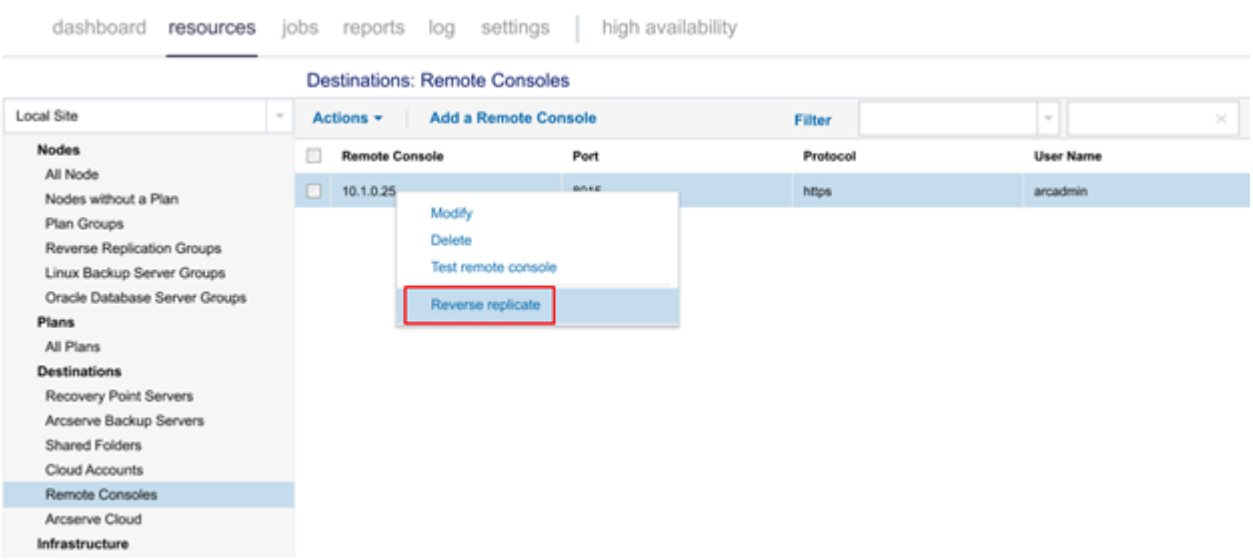
In diesem Abschnitt wird erläutert, wie Sie eine umgekehrte Replikation von der Remote-Konsole zu einem lokalen UDP-Rechner oder einem RPS-Server vor Ort durchführen.

Hinweis: Stellen Sie vor dem Starten der umgekehrten Replikation sicher, dass die Weiterleiten-Replikation erfolgreich ausgeführt wird. Unter Überprüfen der Datenreplikation erfahren Sie, wie Sie überprüfen, ob die Weiterleiten-Replikation erfolgreich war.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele** > **Remote-Konsolen**.

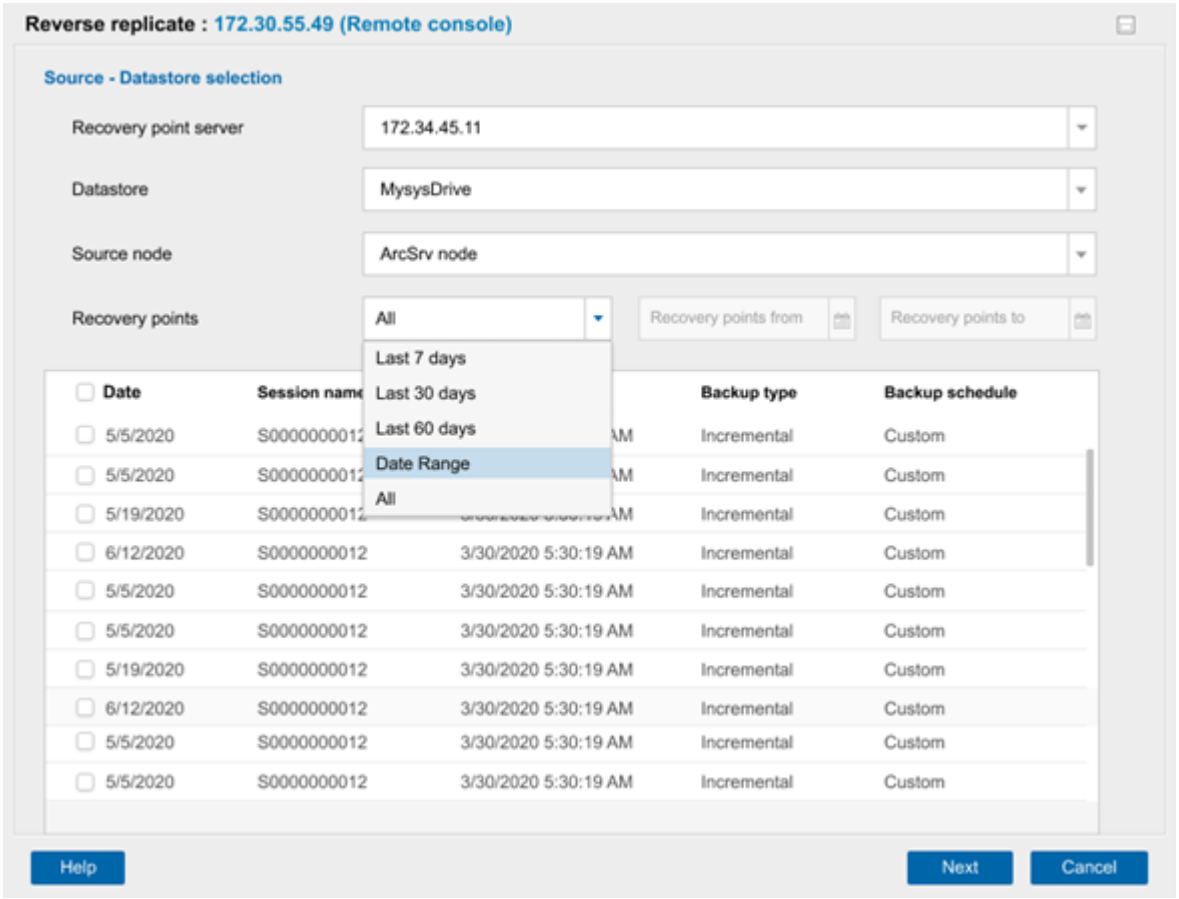
   Die Liste der Remote-Konsolen wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie mit der rechten Maustaste auf die Remote-Konsole, und wählen Sie dann **Umgekehrte Replikation** aus.



Warten Sie, bis die Verbindung zur Remote-Konsole hergestellt wurde.

Das Dialogfeld "Umgekehrte Replikation: xxx.xx.xx.xxx (Remote Console)" wird geöffnet.

4. Gehen Sie auf der Seite "Quelle – Datenspeicherauswahl" wie folgt vor:

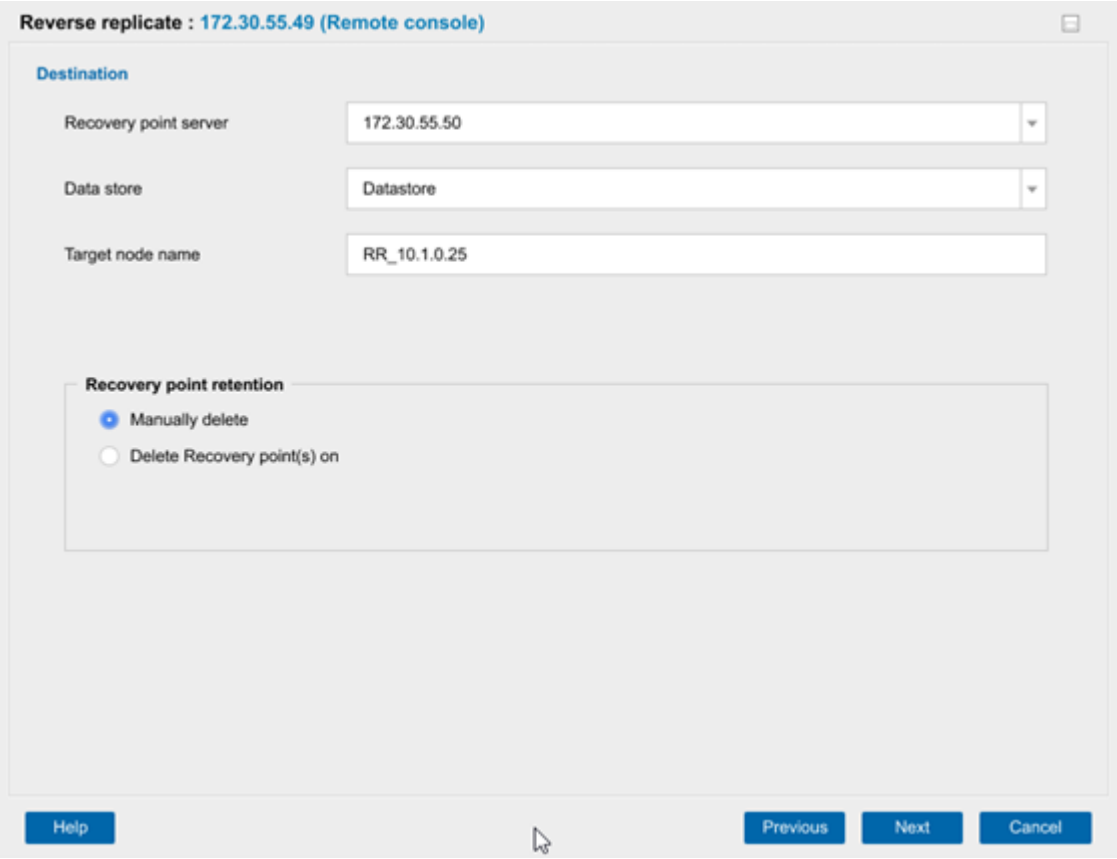


- Recovery Point Server: Wählen Sie den Quell-Recovery Point Server in der Drop-down-Liste aus.
- Datenspeicher: Wählen Sie den Quelldatenspeicher in der Drop-down-Liste aus.
- Quellknoten: Wählen Sie den Quellknoten in der Drop-down-Liste aus.
- Wiederherstellungspunkte: Führen Sie einen der folgenden Schritte aus:
  - Wenn alle gesicherten Wiederherstellungspunkte angezeigt werden sollen, wählen Sie in der Drop-down-Liste die Option **Alle** aus.
  - Wenn die Wiederherstellungspunkte für einen bestimmten Zeitraum angezeigt werden sollen, wählen Sie in der Drop-down-Liste eine der folgenden Optionen aus:
    - Letzte 7 Tage
    - Letzte 30 Tage
    - Letzte 60 Tage
    - Datumsbereich

    Hinweis: Wenn Sie die Option **Datumsbereich** ausgewählt haben, legen Sie das Datum in den Feldern **Wiederherstellungspunkte von** und **Wiederherstellungspunkte bis** fest.

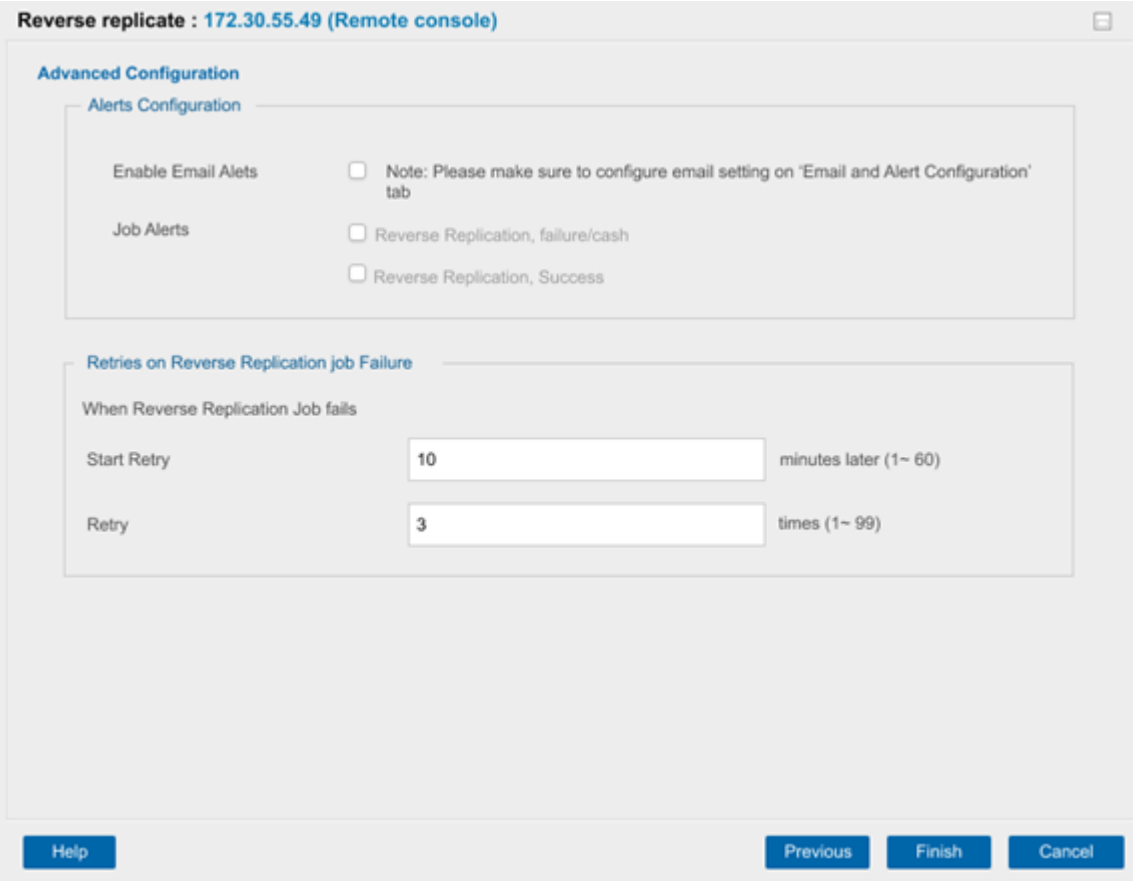
  Alle zugeordneten Wiederherstellungspunkte im angegebenen Zeitraum werden angezeigt.
- Wählen Sie einen oder mehrere Wiederherstellungspunkte aus, indem Sie die entsprechenden Kontrollkästchen in der Tabelle aktivieren.

5. Klicken Sie auf **Weiter**.
6. Gehen Sie auf der Seite "Ziel" wie folgt vor:



- Recovery Point Server: Wählen Sie den Ziel-Recovery Point Server in der Drop-down-Liste aus.
- Datenspeicher: Wählen Sie den Zieldatenspeicher in der Drop-down-Liste aus.
- Zielknotenname: Geben Sie einen Zielknotennamen Ihrer Wahl ein.
- Aufbewahrung von Wiederherstellungspunkten: Löschen Sie die Wiederherstellungspunkte mit einer der folgenden Methoden:
  - Wählen Sie die Option **Manuell löschen** aus, um Wiederherstellungspunkte manuell zu löschen.
  - Wenn die Wiederherstellungspunkte automatisch gelöscht werden sollen, wählen Sie die Option **Wiederherstellungspunkt(e) löschen** aus und geben dann das Datum an. Alle Wiederherstellungspunkte mit diesem Datum werden automatisch gelöscht.

7. Klicken Sie auf **Weiter**.
8. Gehen Sie auf der Seite "Erweiterte Konfiguration" wie folgt vor:



- Für "Konfiguration von Alerts"

  E-Mail-Alerts aktivieren

  Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Typen der Warnmeldungen angeben, die Sie in einer E-Mail erhalten möchten. Wenn Sie das Kontrollkästchen **Hinweis: Stellen Sie sicher, dass Sie die E-Mail-Einstellungen auf der Registerkarte "E-Mail- und Alarm-konfiguration" konfigurieren.** aktivieren, wird die folgende Option zur Auswahl verfügbar:

  Job-Alerts

  Ermöglicht es Ihnen, die Art von Job-Alerts auszuwählen, die Sie per E-Mail empfangen möchten.

  - Wenn Sie E-Mail-Alerts für fehlgeschlagene oder abgestürzte umgekehrte Replikationen erhalten möchten, aktivieren Sie das Kontrollkästchen **Fehler/Absturz bei umgekehrter Replikation**.

    Hinweis: Dieser E-Mail-Alert wird mit hoher Wichtigkeit gesendet. E-Mail-Alerts mit festgelegter hoher Wichtigkeit werden in Ihrem

Posteingang mit einem Ausrufezeichen als visueller Indikator angezeigt.

- Wenn Sie E-Mail-Alerts für erfolgreiche umgekehrte Replikationen erhalten möchten, aktivieren Sie das Kontrollkästchen **Umgekehrte Replikation erfolgreich**.

- Für "Wiederholungen bei fehlgeschlagenem Replikationsjob"

  Wenn der umgekehrte Replikationsjob fehlschlägt, gehen Sie folgendermaßen vor:

  Startwiederholung

  Ermöglicht es Ihnen anzugeben, nach wie vielen Minuten ein fehlgeschlagener Replikationsjobs neu gestartet werden soll. Wenn Sie beispielsweise 10 Minuten angeben, wird der Replikationsjob 10 Minuten, nachdem er fehlgeschlagen ist, neu gestartet.

  Beschränkung: 1 bis 60

  Wiederholen

  Ermöglicht es Ihnen, die Anzahl der Wiederholungen anzugeben, die Sie ausführen möchten, wenn der Replikationsjob fehlschlägt. Der Replikationsjob wird so oft ausgeführt, bis der Job erfolgreich ist oder die Beschränkung erreicht ist. Nach Durchführung der angegebenen Anzahl von Wiederholungen wird der Replikationsjob erst wieder zum nächsten geplanten Zeitpunkt ausgeführt.

  Beschränkung: 1 bis 99

9. Klicken Sie auf **Fertig stellen**.

   Hinweis: Wenn Sie die Einstellungen in den vorherigen Bildschirmen ändern möchten, klicken Sie auf **Zurück**, und ändern Sie dann die Einstellung nach Bedarf.

   Ein Informationsdialogfeld mit der Meldung *Umgekehrter Replikations-Job wurde erfolgreich übergeben* wird angezeigt.

10. Klicken Sie auf **OK**, um das Informationsdialogfeld zu schließen.

    Die umgekehrte Replikation von der Remote-Konsole zum lokalen UDP-Rechner oder Server vor Ort wurde erfolgreich abgeschlossen.

Überwachen des Status der umgekehrten Replikation

Quellenadministrator

Wenn die umgekehrte Replikation erfolgreich ist, können Sie den Status des umgekehrten Replikationsjobs überwachen.

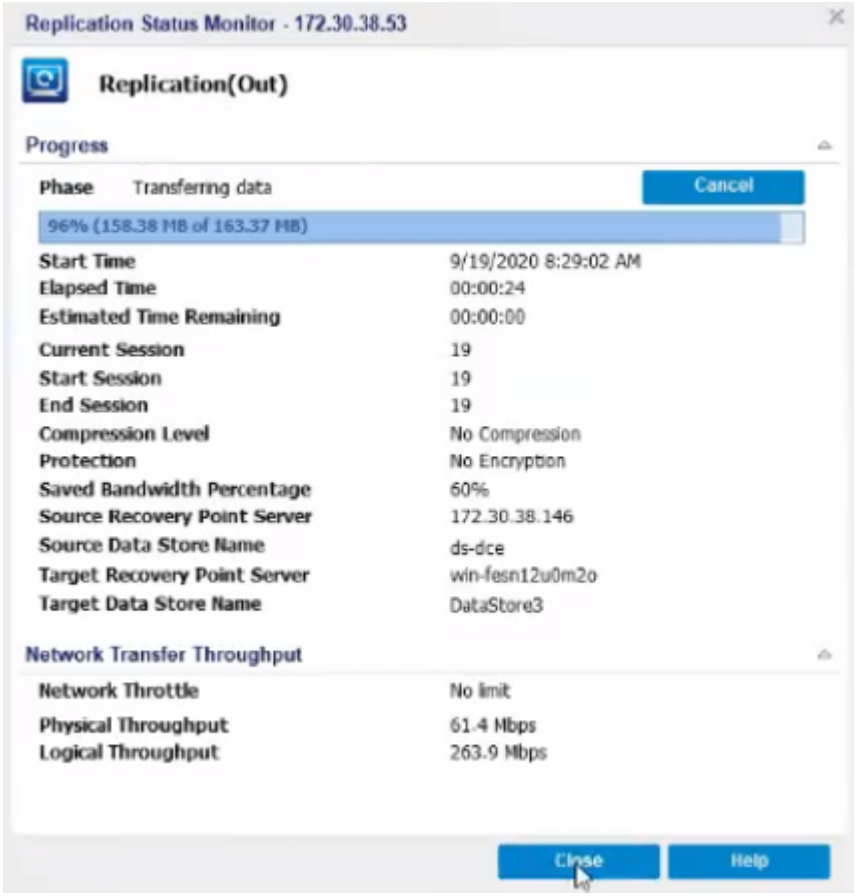
Gehen Sie wie folgt vor:

1. Navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Die in Bearbeitung befindlichen Jobs vom Typ "Replikation (Ausgang)" und "Replikation (Eingang)" werden im mittleren Fensterbereich angezeigt.

2. Um den Status eines bestimmten Jobs zu überwachen, klicken Sie neben der Fortschrittsleiste des betreffenden Jobs auf **Details**.

   Das Dialogfeld "Statusüberwachung der Replikation - xx.xx.xx.xx" wird angezeigt.



3. Warten Sie, bis die Datenübertragung zu 100 % abgeschlossen ist, und klicken Sie auf **Schließen**.

Sie haben den Status der umgekehrten Replikation erfolgreich überwacht.

Überprüfen der erfolgreichen Durchführung der umgekehrten Replikation

Quellenadministrator

Nachdem Daten repliziert wurden, können Sie überprüfen, ob die umgekehrte Replikation erfolgreich war.

Gehen Sie wie folgt vor:

1. Navigieren Sie in der Quellkonsole zu **Jobs** > **Jobs erfolgreich abgeschlossen**.

   Im mittleren Fensterbereich wird eine Liste der abgeschlossenen Jobs angezeigt.

2. Klicken Sie auf den abgeschlossenen umgekehrten Replikationsjob. Der rechte Fensterbereich wird aktualisiert.
3. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
4. Überprüfen Sie, ob die Datenreplikation erfolgreich war.

Sie haben die umgekehrte Replikation von Daten von der Remote-Konsole zum lokalen UDP-Rechner oder RPS-Server vor Ort erfolgreich überprüft.

Erstellen eines Ablaufplans für das Kopieren von Wiederherstellungspunkten

Mit Arcserve Unified Data Protection können Sie die Wiederherstellungspunkte in die Cloud, in einen freigegebenen Ordner oder in ein lokales Volume kopieren, um die Wiederherstellungspunkte zu schützen. Durch diesen Vorgang wird sichergestellt, dass Sie über eine zusätzliche Kopie der Wiederherstellungspunkte verfügen, falls Ihre ursprünglichen Wiederherstellungspunkte versehentlich gelöscht werden. Der Task zum Kopieren von Wiederherstellungspunkten kopiert die Wiederherstellungspunkte nur vom Sicherungsziel in eine Cloud, einen freigegebenen Ordner oder ein lokales Volume. Sie können den Wiederherstellungspunkt nicht auf einen Recovery Point Server kopieren.

Sie können in einem Plan nur einen einzigen Task zum Kopieren von Wiederherstellungspunkten hinzufügen.

Hinweise:

- In der aktuellen Version werden CRP-Jobs nicht unterstützt, wenn **Sicherung: Agent-basiertes Linux** als Task1 erstellt wird.
- CRP-Jobs werden immer auf dem Agent ausgeführt, auch wenn die Sicherung auf RPS konfiguriert ist.

  Für die agentenlose VM-Sicherung verarbeitet der in Task1 verwendete UDP-Agent-Proxy den CRP-Job.

Problembehandlung: Bandbreiten-Überlastung bei der Kopie von Wiederherstellungspunkten zu Cloud-Aufträgen

Der nächste Schritt?

- Überprüfen der Voraussetzungen und Hinweise
- Erstellen eines Plans mit einem Sicherungstask
- Hinzufügen eines Tasks für das Kopieren von Wiederherstellungspunkten zum Plan
- Überprüfen des Plans

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich bei der Konsole an.
- Wenn Sie die Sicherungsdaten auf Recovery Point-Servern speichern möchten, installieren Sie die Serverkomponente, und erstellen Sie Datenspeicher.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Erstellen eines Plans mit einem Sicherungstask

Ein Plan umfasst verschiedene Arten von Tasks, die Sie ausführen möchten. Um einen Task zum Kopieren von Wiederherstellungspunkten zu erstellen, müssen Sie zuerst einen gültigen Wiederherstellungspunkt haben. Um einen gültigen Wiederherstellungspunkt zu erhalten, müssen Sie einen Sicherungstask erstellen.

Ein Sicherungstask führt eine Sicherung der Quellknoten aus und speichert die Daten am angegebenen Ziel. Das Kopieren von Wiederherstellungspunkten wird sowohl für agentenbasierte Windows-Sicherungen als auch für hostbasierte agentenlose Sicherungen unterstützt. Der folgende Vorgang beschreibt die Schritte zur Erstellung des agentenbasierten Windows-Sicherungstasks. Sie können für Linux-Agent-basierte Sicherungspläne keine Wiederherstellungspunkte kopieren.

Hinweis: Weitere Informationen über hostbasierte agentenlose Sicherungen finden Sie unter So erstellen Sie einen Sicherungsplan für hostbasierte virtuelle Rechner.

Weitere Informationen zur UNC- Pfad-Sicherung finden Sie unter Erstellen eines UNC- Pfad-Sicherungsplans.

Weitere Informationen zur Sicherung von Exchange Online finden Sie unter So erstellen Sie einen Sicherungsplan für Exchange Online.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

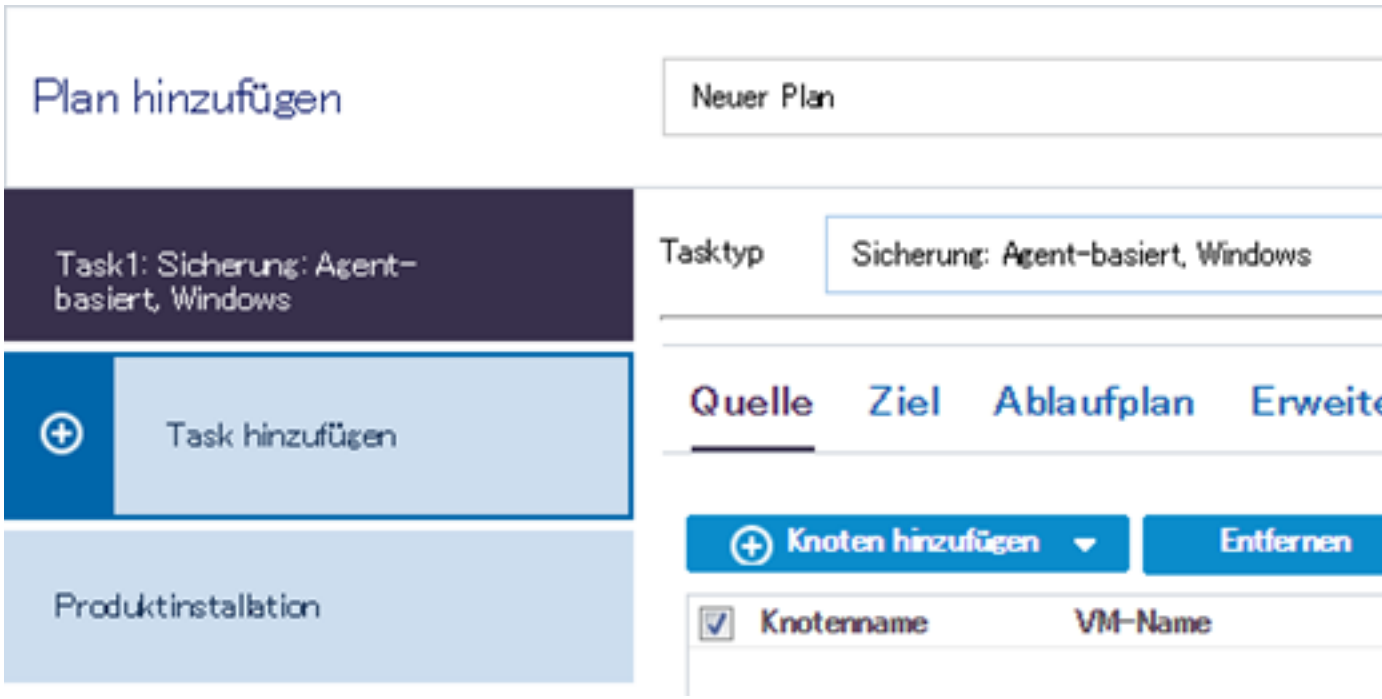
   Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**, um den Plan zu unterbrechen.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan

unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.

6. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Sicherung, Agent-basiertes Windows** aus.



Geben Sie nun Quelle, Ziel, Zeitplan und Erweitert-Details an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die Quellknoten angeben, die Sie schützen möchten. Sie können mehrere Knoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Knoten hinzufügen, wenn Sie einen Plan auf der Quellenseite erstellen oder ändern. Sie können einen Plan auch speichern, ohne Quellknoten hinzuzufügen. Der Plan wird erst bereitgestellt, wenn Sie Quellknoten hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Quelle" auf **Hinzufügen**.
2. Wählen Sie eine der folgenden Optionen:

   Wählen Sie zu sichernden Knoten in Arcserve UDP aus

   Öffnet das Dialogfeld "Wählen Sie zu sichernden Knoten in Arcserve UDP aus". Wählen Sie die Knoten in der angezeigten Liste aus. Wählen Sie diese Option aus, wenn Sie die Knoten bereits zu der Konsole hinzugefügt haben.

   Windows-Knoten hinzufügen

   Öffnet das Dialogfeld "Knoten zu Plan hinzufügen". Wählen Sie diese Option aus, wenn Sie die Knoten nicht hinzugefügt haben und Sie die zu schützenden Knoten manuell hinzufügen möchten.

   Knoten aus Active Directory erkennen

   Öffnet das Dialogfeld Knoten zu Arcserve UDP-Konsole hinzufügen. Wählen Sie diese Option, wenn Sie Knoten aus Active Directory erkennen und hinzufügen möchten.
3. Wenn Sie die Option **Wählen Sie zu sichernden Knoten in Arcserve UDP aus** ausgewählt haben, gehen Sie im Dialogfeld "Zu schützende Knoten auswählen" folgendermaßen vor:

   a. (Optional) Wählen Sie einen Filter aus der Dropdown-Liste "Gruppen" aus, um nach Knoten zu filtern. Sie können Schlüsselwörter eingeben, um den Knotenfilter weiter einzuschränken.

      Die Knoten werden in der Spalte "Verfügbare Knoten" angezeigt.

   b. Wählen Sie die Knoten aus der Spalte "Verfügbare Knoten" aus, und klicken Sie dann auf den einfachen Nach-rechts-Pfeil (>) oder den doppelten Nach-rechts-Pfeil (>>), um die ausgewählten Knoten bzw. alle Knoten in die Spalte "Ausgewählte Knoten" zu verschieben.

Die Knoten werden in der Spalte "Ausgewählte Knoten" angezeigt.

c. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

4. Wählen Sie zum Festlegen des Schutztyps eine der folgenden Optionen aus:

Alle Volumes sichern

Bereitet einen Sicherungs-Snapshot aller Volumes vor.

Ausgewählte Volumes sichern

Bereitet einen Sicherungs-Snapshot des ausgewählten Volumes vor.

Die Sicherungsquelle ist nun angegeben.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Wählen Sie einen der folgenden **Zieltypen** aus:

   Lokaler Datenträger oder freigegebener Ordner

   Gibt an, dass das Sicherungsziel ein lokales Ziel oder ein freigegebener Ordner ist. Wenn Sie diese Option auswählen, können Sie Daten als Wiederherstellungspunkte oder Wiederherstellungssätze speichern. Die Optionen für Wiederherstellungspunkte und Wiederherstellungssätze sind auf der Registerkarte **Ablaufplan** verfügbar.

   Arcserve UDP-Recovery Point Server

   Gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.

2. Wenn Sie **Arcserve UDP-Recovery Point Server** ausgewählt haben, geben Sie folgende Details an:
   a. Wählen Sie einen Recovery Point Server aus
   b. Wählen Sie einen Datenspeicher aus. Die Liste enthält alle Datenspeicher, die am angegebenen Recovery Point Server erstellt wurden.
   c. Geben Sie ein Sitzungskennwort ein.
   d. Bestätigen Sie das Sitzungskennwort.
3. Wenn Sie **Lokaler Datenträger oder freigegebener Ordner** ausgewählt haben, geben Sie folgende Details an:
   a. Geben Sie den vollständigen Pfad des lokalen Ziels oder Netzwerkziels an. Geben Sie für das Netzwerkziel Anmeldeinformationen für ein Konto mit Schreibzugriff an.
   b. Wählen Sie den Verschlüsselungsalgorithmus aus. Weitere Informationen finden Sie unter Verschlüsselungseinstellungen.
   c. Geben Sie optional ein Verschlüsselungskennwort an.
   d. Bestätigen Sie das Verschlüsselungskennwort.
   e. Wählen Sie einen Komprimierungstyp aus. Weitere Informationen finden Sie unter "Komprimierungstyp".

Hinweise:

- Der Task "Wiederherstellungspunkt kopieren" (Copy Recovery Point, CRP) unterstützt keine benutzerdefinierten Sicherungen, auch wenn der CRP-Ablaufplan hinzugefügt wird. Außerdem unterstützt der CRP-Task den benutzerdefinierten Sicherungsablaufplan nicht.
- Das Kopieren eines Wiederherstellungspunkts in die Cloud wird nur von einer Konsole aus unterstützt. Ein eigenständiger Agent wird nicht unterstützt.
- Sowohl Sicherungen mit dem Ziel *Lokaler Datenträger oder freigegebener Ordner* als auch *auf RPS gespeicherte Sicherungen* unterstützen die CRP-Tasks.

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Zeitplan für die Sicherung festlegen. Das Kopieren von Wiederherstellungspunkten unterstützt Backups von der Konsole täglich, wöchentlich und monatlich. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können tägliche, wöchentliche und monatliche Ablaufpläne sowie Beibehaltungseinstellungen anlegen.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

Gehen Sie wie folgt vor:

1. (Optional) Wählen Sie die Option für die Verwaltung von Wiederherstellungspunkten aus. Diese Option ist nur sichtbar, wenn Sie als Sicherungsziel "Lokaler oder freigegebener Ordner" ausgewählt haben.

   Nach Wiederherstellungspunkten aufbewahren

   Die Sicherungsdaten werden als Wiederherstellungspunkte gespeichert.

   Nach Wiederherstellungssätzen aufbewahren

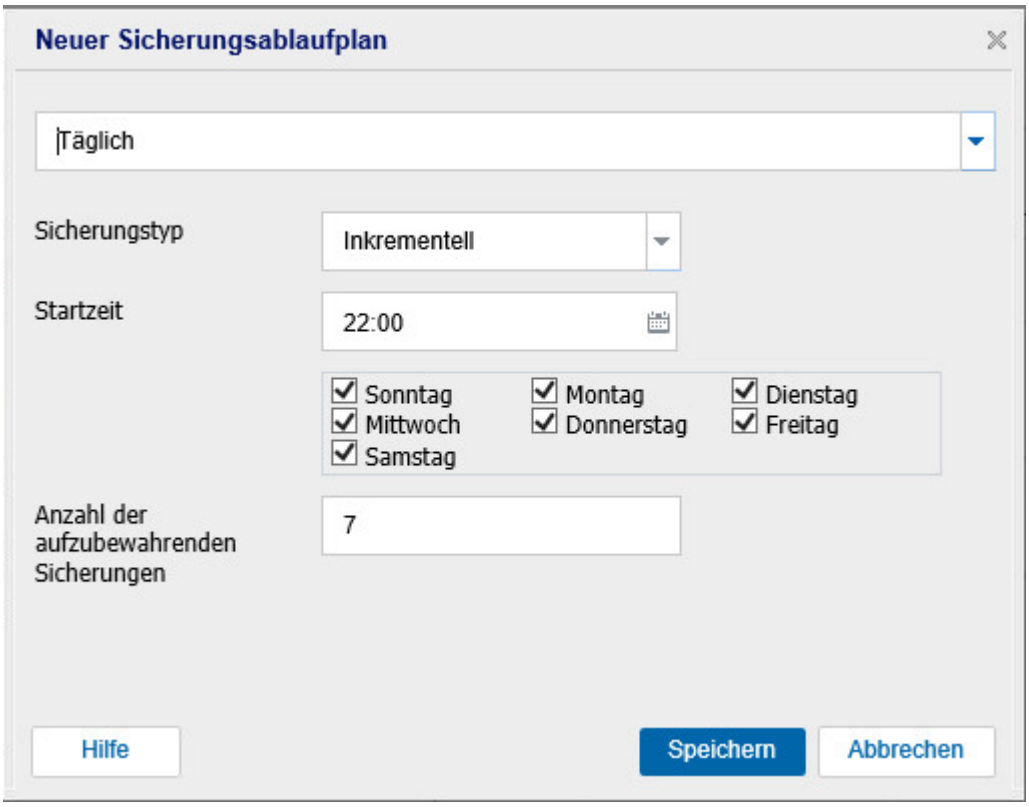
   Die Sicherungsdaten werden als Wiederherstellungssätze gespeichert.

   Hinweis: Das Aufbewahren von Wiederherstellungssätzen wird für das Kopieren von Wiederherstellungspunkten nicht unterstützt.

2. Sicherungsablaufplan hinzufügen.

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

Gemäß Ablaufplan erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die seit der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

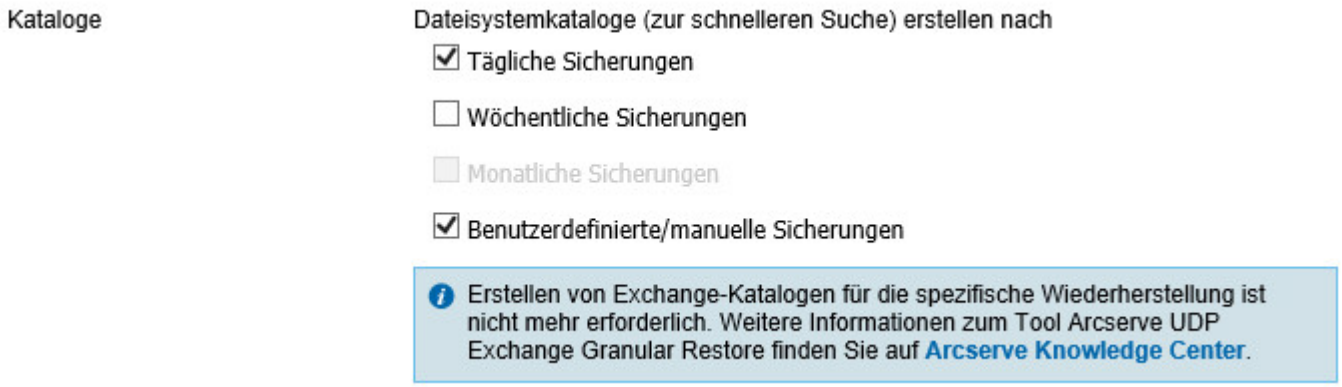
Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

3. Geben Sie die Startzeit für die geplante Sicherung an.

4. Legen Sie die Einstellungen für die tägliche, wöchentliche und monatliche Beibehaltung von Wiederherstellungspunkten fest.

   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld "Sicherungsablaufplan" übernommen.

5. Geben Sie die Katalogdetails an.



Mit Katalogen können Sie den Dateisystemkatalog generieren. Der Dateisystemkatalog ist erforderlich, um schnellere und bessere Suchvorgänge auszuführen. Wenn Sie die Kontrollkästchen für den Katalog aktivieren, werden die Kataloge je nach der Sicherungsart, die Sie angegeben haben, aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Kataloggenerierung zu deaktivieren.

Der Ablaufplan ist nun angegeben.

Funktionsweise der erweiterten Planung und Aufbewahrung

Mit der Ablaufplanoption können Sie einen benutzerdefinierten Ablaufplan, einen Ablaufplan für tägliche/wöchentliche/monatliche Sicherungen oder beides festlegen. Im benutzerdefinierten Ablaufplan können Sie den Sicherungsablaufplan für jeden Tag der Woche konfigurieren und bis zu vier Sicherungsablaufpläne für jeden Tag hinzufügen. Sie können einen bestimmten Wochentag auswählen und ein Zeitfenster erstellen, um anzugeben, wann und wie oft die Sicherung durchgeführt werden soll.

Ablaufplan	Unterstützter Job	Kommentare
Sichern	Sicherungsjob	Gibt Zeitfenster für die Ausführung von Sicherungsjobs an.
Sicherungsdrosselung	Sicherungsjob	Gibt die Zeitfenster an, um die Sicherungsgeschwindigkeit zu steuern.
Zusammenführen	Zusammenführungsjob	Gibt an, wann Zusammenführungsjobs ausgeführt werden sollen.
Täglicher Ablaufplan	Sicherungsjob	Gibt an, wann tägliche Sicherungsjobs ausgeführt werden sollen.
Wöchentlicher Ablaufplan	Sicherungsjob	Gibt an, wann wöchentliche Sicherungsjobs ausgeführt werden sollen.
Monatlicher Ablaufplan	Sicherungsjob	Gibt an, wann monatliche Sicherungsjobs ausgeführt werden sollen.

Sie können auch die Aufbewahrungseinstellungen für die Wiederherstellungspunkte angeben.

Hinweis: Legen Sie innerhalb der einzelnen Pläne Einstellungen für die Aufbewahrungszeit fest, um zu steuern, wie die Daten für die Knoten des entsprechenden Plans im Zieldatenspeicher aufbewahrt werden.

Ablaufpläne für tägliche/wöchentliche/monatliche Sicherungen sind vom benutzerdefinierten Ablaufplan und voneinander unabhängig. Sie können die Ausführung einer täglichen, wöchentlichen oder monatlichen Sicherung konfigurieren, ohne einen benutzerdefinierten Ablaufplan zu konfigurieren.

Jobplan der Sicherung

Sie können vier Zeitfenster pro Tag in Ihrem Sicherungsablaufplan hinzufügen. Ein gültiges Zeitfenster liegt im Bereich 12:00 Uhr bis 23:59 Uhr. Sie können kein Zeitfenster wie z. B. 18:00 Uhr bis 06:00 Uhr angeben. In solchen Fällen müssen Sie manuell zwei verschiedene Zeitfenster angeben.

Für jedes Zeitfenster wird die Startzeit einbezogen, und die Endzeit wird nicht einbezogen. Zum Beispiel haben Sie das Ausführen einer Zuwachssicherung konfiguriert, die stündlich zwischen 06:00 Uhr und 09:00 Uhr stattfinden soll, und die Sicherung wird um 06:00 Uhr gestartet. Das bedeutet, dass die Sicherung um 06:00 Uhr, 07:00 Uhr und 08:00 Uhr ausgeführt wird, NICHT aber um 09:00 Uhr.

Hinweis: Wenn Sie die Sicherung bis zum Ende des Tages wiederholt ausführen möchten, legen Sie den Ablaufplan bis 12:00 Uhr fest. Um den Sicherungsjob beispielsweise alle 15 Minuten während des gesamten Tages auszuführen, legen Sie den Ablaufplan von 00:00 Uhr bis 00:00 Uhr alle 15 Minuten fest.

Drosselungsplan der Sicherung

Mit dem Drosselungsplan der Sicherung können Sie die Geschwindigkeit des Sicherungsdurchsatzes steuern, die wiederum die Ressourcenverwendung (Datenträger-E/A, CPU, Netzwerkbandbreite) des Servers, der gesichert wird, steuert. Dies ist hilfreich, wenn die Serverleistung während der Geschäftszeiten nicht beeinträchtigt werden soll. Sie können vier Zeitfenster pro Tag in Ihrem Drosselungsplan der Sicherung hinzufügen. Für jedes Zeitfenster können Sie einen Wert in MB pro Minute angeben. Dieser Wert wird verwendet, um den Sicherungsdurchsatz zu steuern. Gültige Werte liegen im Bereich zwischen 1 MB/Minute bis 99.999 MB/Minute.

Wenn ein Sicherungsjob die angegebene Zeit überschreitet, dann wird das Drosselungslimit entsprechend dem angegebenen Zeitfenster angepasst. Zum Beispiel haben Sie als Drosselungslimit der Sicherung den Wert 500 MB/Minute von 08:00 Uhr bis 20:00 Uhr und 2500 MB/Minute von 20:00 Uhr bis 22:00 Uhr angegeben. Wenn ein Sicherungsjob um 19:00 Uhr startet und drei Stunden ausgeführt wird, dann hat das Drosselungslimit von 19:00 Uhr bis 20:00 Uhr den Wert 500 MB/Minute. Von 20:00 Uhr bis 22:00 Uhr hat das Drosselungslimit den Wert 2.500 MB/Minute.

Wenn Sie keinen Sicherungsablaufplan und keinen Ablaufplan für den Sicherungsdurchsatz angeben, dann wird die Sicherung so schnell wie möglich ausgeführt.

Ablaufplan für Zusammenführung

Ermöglicht es Ihnen, Wiederherstellungspunkte basierend auf dem angegebenen Ablaufplan zusammenzuführen.

Beachten Sie folgende Punkte für den Zusammenführungsjob:

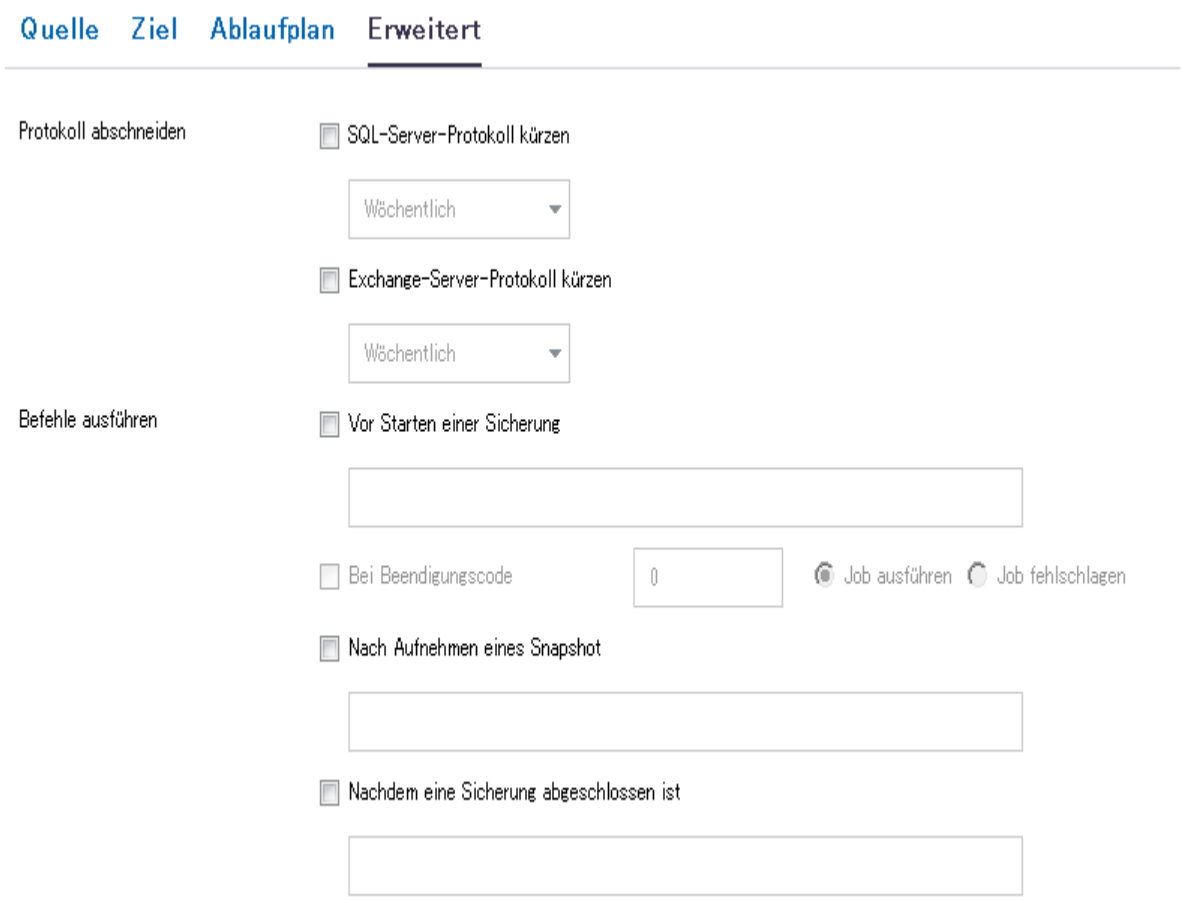
- Es kann immer nur ein Zusammenführungsjob für einen Knoten ausgeführt werden.

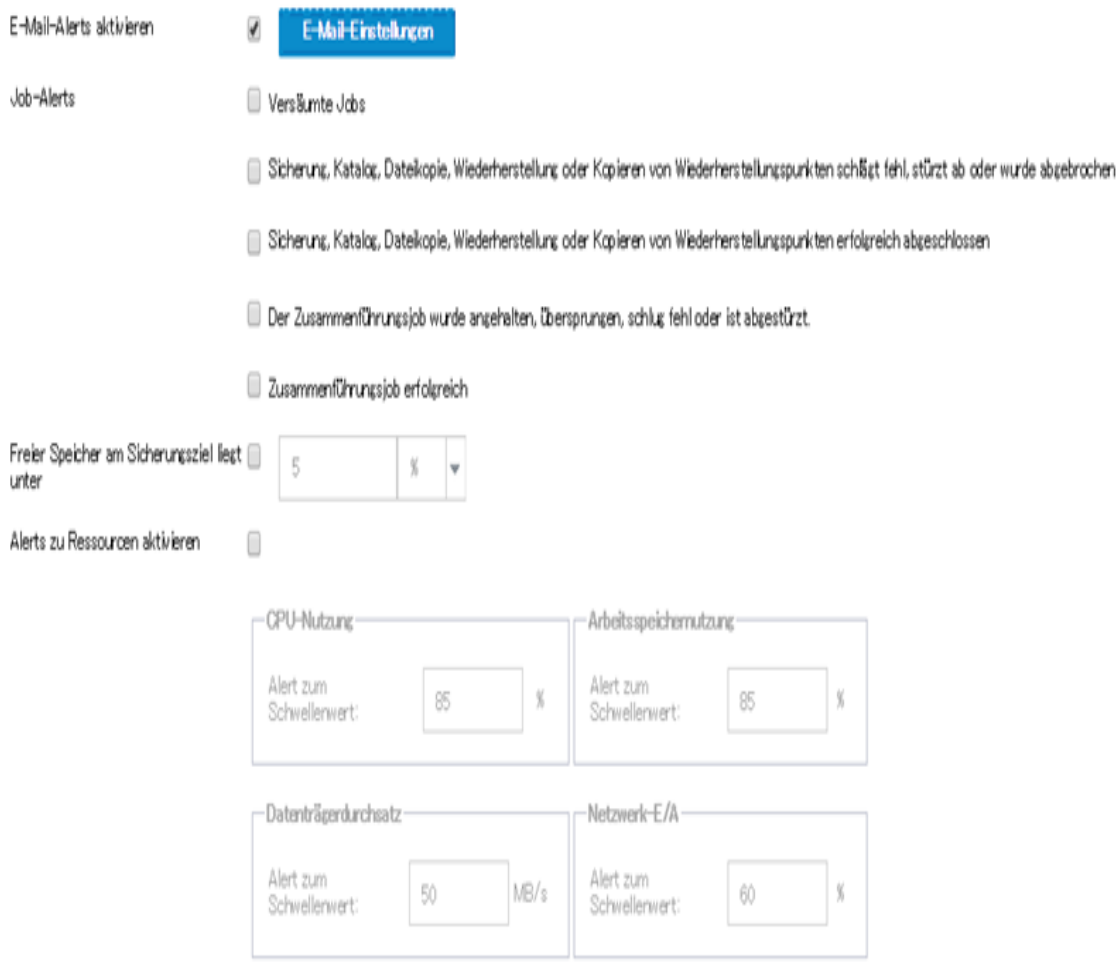
- Wenn ein Zusammenführungsjob gestartet wird, muss er abgeschlossen werden, bevor der nächste Zusammenführungsjob gestartet werden kann. Das bedeutet: Wenn ein oder mehrere Sätze an Wiederherstellungspunkten zusammengeführt werden, dann kann der neue Wiederherstellungspunkt nicht zu diesem Zusammenführungsprozess hinzugefügt werden, bis der Zusammenführungsprozess für den aktuellen Satz an Wiederherstellungspunkten abgeschlossen ist.
- Wenn ein Zusammenführungsjob mehr als einen Satz an Wiederherstellungspunkten bearbeitet (zum Beispiel Satz [1~4], Satz [5~11] und Satz [12~14], also drei Sätze), dann werden diese Sätze nacheinander vom Recovery Point Server bearbeitet.
- Wenn ein Zusammenführungsjob nach einer Pause fortgesetzt wird, erkennt der Job an welchem Punkt er unterbrochen wurde, und die Zusammenführung wird ab der Abbruchstelle fortgesetzt.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen die Einstellungen zum Abschneiden von Protokollen, das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte "Erweitert":





Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

   Protokoll abschneiden

   Ermöglicht es Ihnen, den Ablaufplan anzugeben, um Protokolle für SQL Server und Exchange Server zu kürzen. Sie können den Ablaufplan als **Täglich**, **Wöchentlich** oder **Monatlich** angeben.

   Benutzername

   Ermöglicht es Ihnen, den Benutzer anzugeben, der zur Ausführung eines Skripts autorisiert ist.

   Kennwort

   Ermöglicht es Ihnen, das Kennwort des Benutzers anzugeben, der zur Ausführung des Skripts autorisiert ist.

   Befehl ausführen, bevor eine Sicherung gestartet wird

Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, in dem das Skript gespeichert wird. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem ein Snapshot aufgenommen wurde

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungs-Snapshot aufgenommen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Arten der Alerts angeben, die Sie in Form von E-Mails empfangen möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers.

Job-Alerts

Ermöglicht es Ihnen, die Typen der Job-E-Mails auszuwählen, die Sie erhalten möchten.

Warnmeldungen zu Ressourcen aktivieren

Ermöglicht es Ihnen, einen Schwellenwert für CPU-Auslastung, Speicherverwendung, Datenträgerdurchsatz, Netzwerk-E/A anzugeben. Sie können den Wert in Prozent angeben. Sie erhalten eine E-Mail, wenn der Wert "Warnmeldung zum Schwellenwert" überschritten ist.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Knoten installiert ist und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung

an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agenten oder kein Agent installiert ist. Um den Agenten auf diesen Knoten zu installieren bzw. um ein Upgrade des Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus, und klicken Sie auf "Speichern".

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie eine andere Task hinzufügen müssen, müssen Sie den Plan aus der Registerkarte **Ressourcen** auswählen und den Plan ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern.

Der Sicherungsplan wird erstellt und automatisch für den Quellknoten bereitgestellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

Hinzufügen eines Tasks für das Kopieren von Wiederherstellungspunkten zum Plan

Der Task zum Kopieren von Wiederherstellungspunkten kopiert die Wiederherstellungspunkte vom Sicherungsziel in die Cloud, einen freigegebenen Ordner oder ein lokales Volume.

Hinweis: Wenn ein Sicherungsjob ausgeführt wird und Sie den Plan unterbrechen, hat der Sicherungsjob Vorrang, und der Job zum Kopieren von Wiederherstellungspunkten startet nicht. Wenn Sie den Plan wieder aufnehmen, wird der Job für die Wiederherstellungspunkt-Kopie nicht automatisch fortgesetzt. Sie müssen einen anderen Sicherungsjob manuell ausführen, um den Job zum Kopieren von Wiederherstellungspunkten zu starten.

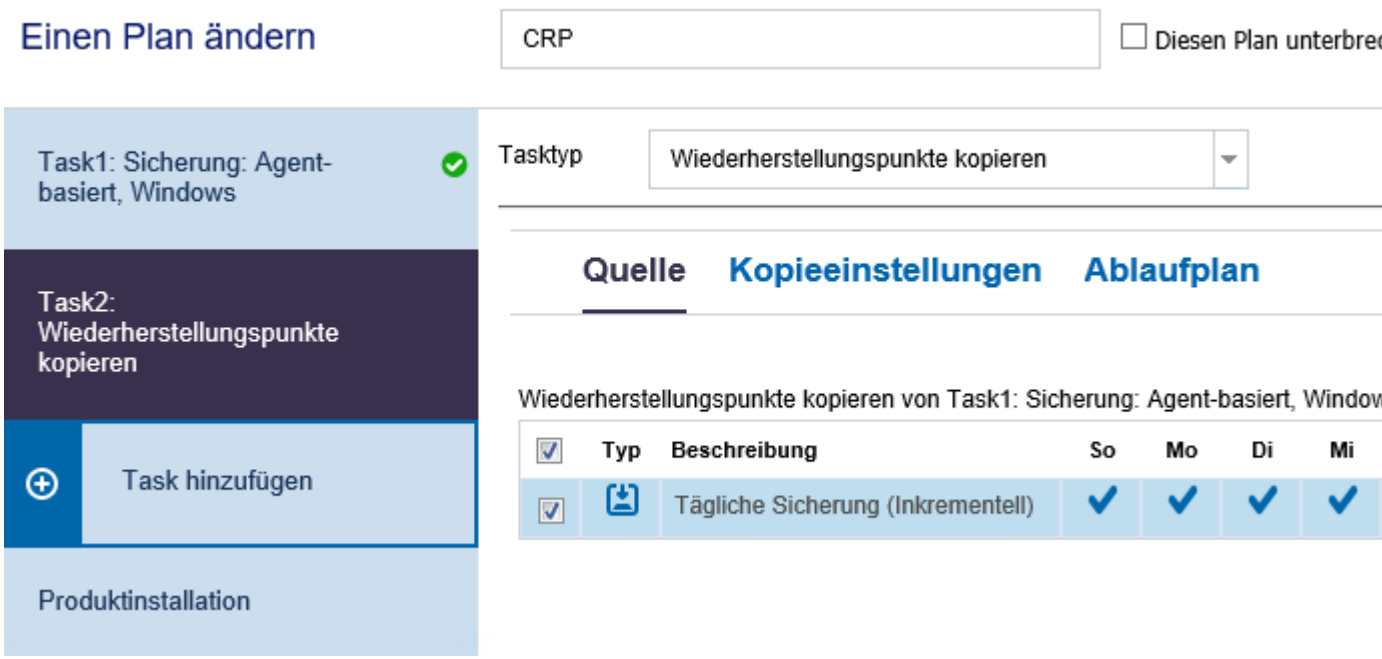
Gehen Sie wie folgt vor:

1. Klicken Sie im linken Fensterbereich auf **Task hinzufügen**.

   Ein neuer Task wird im linken Fensterbereich hinzugefügt.

2. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Wiederherstellungspunkte kopieren** aus.

   Der Task zum Kopieren von Wiederherstellungspunkten wird hinzugefügt. Sie müssen die Registerkarte **Quelle** im CRP-Task (Copy Recovery Points, Wiederherstellungspunkte kopieren) nicht konfigurieren. Außerdem können Sie das Sicherungsziel im Sicherungstask anzeigen.



Hinweis: Mithilfe des Registrierungsschlüssels unten können Sie einen benutzerdefinierten Speicherort als Pfad zum Kopieren von Wiederherstellungspunkten festlegen.

Pfad: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession*

Schlüsselname: *LocalTempPath*

Schlüsseltyp: *REG_SZ (Zeichenfolge)*

Schlüsselwert: *"Local_disk_path"*

3. Wählen Sie auf der Registerkarte "Quelle" einen Ablaufplan aus.
4. Geben Sie auf der Registerkarte "Kopieeinstellungen" die folgenden Details ein:

Zieltyp

Gibt den Typ des Ziels an. Sie können eine der verfügbaren Optionen wählen, z. B. Cloud-Speicher, lokale Festplatte oder freigegebener Ordner. Recovery Point Server lassen sich nicht als Zieltyp festlegen.

Lokaler Datenträger oder freigegebener Ordner

Sie müssen die Details für das Ziel eingeben.

Ziel

Gibt das Ziel an, auf dem Sie die Wiederherstellungspunkt-Kopien aufbewahren möchten.

Hinweis: Klicken Sie auf den Pfeil, um das angegebene Ziel zu validieren. Der Pfeil wird angezeigt, wenn Sie ein Ziel eingeben.

Cloud-Speicher

Sie müssen den Cloud-Dienst auswählen und einen Cloud-Speicher hinzufügen.

Ausführliche Informationen über die Verzeichnisstruktur finden Sie unter Wiederherstellungspunkt-Verzeichnisstruktur im S3-Cloud-Bucket.

Cloud-Dienst

Hier können Sie aus zahlreichen verfügbaren Speicherdiensten die gewünschte Option auswählen.

Cloud-Speicher

Hier können Sie das Cloud-Konto im ausgewählten Speicherdienst auswählen. Falls in der Drop-down-Liste kein Konto angezeigt wird, klicken Sie auf **Hinzufügen**, um ein Konto hinzuzufügen.

Aktivieren der Objektsperre

Hiermit können Sie den Cloud-Speicher mithilfe der Objektsperrfunktion schützen. Wenn Sie Folgendes als Cloud-Dienst auswählen, wird das Kontrollkästchen "Objektsperre aktivieren" angezeigt.

- Amazon S3
- Wasabi Hot Cloud-Speicher
- Nutanix Objects

Wenn Sie das Kontrollkästchen **Objektsperre aktivieren** aktivieren, wird die Schaltfläche "Einstellungen der Objektsperre" aktiviert. Sie müssen die Einstellungen für die Objektsperre konfigurieren, nachdem Sie das Kontrollkästchen "Objektsperre" aktiviert haben. Weitere Informationen zum Konfigurieren der Einstellungen der Objektsperre finden Sie unter Konfigurieren der Einstellungen der Objektsperre für einen Cloud-Dienst.

Hinweise:

- Für Amazon S3 und Wasabi Hot Cloud Storage:
  - Sie können die Objektsperroption nur für neue Buckets aktivieren.
  - Beachten Sie beim Ändern eines Plans Folgendes:
    - Wenn ein Plan mit aktivierter Objektsperre erstellt wird, ist das Kontrollkästchen *Objektsperre aktivieren* deaktiviert und die Schaltfläche *Einstellungen für die Objektsperre* aktiviert. Sie können den Aufbewahrungsmodus und den Aufbewahrungszeitraum über die Schaltfläche *Einstellungen der Objektsperre* ändern.
    - Wenn ein Plan mit deaktivierter Objektsperre erstellt wird, werden das Kontrollkästchen *Objektsperre aktivieren* und die Schaltfläche *Einstellungen für die Objektsperre* deaktiviert.
- Für Nutanix-Objekte:
  - Sie können die Objektsperroption für alte und neue Buckets aktivieren.
  - Beachten Sie beim Ändern eines Plans Folgendes:

- Wenn ein Plan mit aktivierter Objektsperre erstellt wird, können Sie das Kontrollkästchen *Objektsperre aktivieren* nicht deaktivieren. Sie können den Aufbewahrungszeitraum nur über die Schaltfläche *Einstellungen der Objektsperre* erhöhen.
- Wenn ein Plan mit deaktivierter Objektsperre erstellt wird, können Sie das Kontrollkästchen *Objektsperre aktivieren* aktivieren und die Einstellungen für die Objektsperre konfigurieren.

- Wenn Sie die Option "Objektsperre" aktivieren, gelten die Aufbewahrungseinstellungen auf der Registerkarte "Ablaufplan" nicht.

Komprimierung

Legt fest, dass eine Komprimierungsebene für die Kopien der Wiederherstellungspunkte ausgewählt wird. Eine Komprimierung wird normalerweise durchgeführt, um den verwendeten Speicherplatz zu verringern, hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit der Sicherung. Es sind folgende Optionen verfügbar:

Keine Komprimierung: Es wird keine Komprimierung durchgeführt. Die Dateien haben reines VHD-Format. Diese Option bedeutet niedrigste CPU-Auslastung (höchste Geschwindigkeit), aber auch höchste Speicherplatzverwendung für Ihr Sicherungs-Image.

Keine Komprimierung – VHD: Es wird keine Komprimierung durchgeführt. Die Dateien werden direkt in das VHD-Format konvertiert, ohne dass manuelle Schritte ausgeführt werden müssen. Diese Option bedeutet niedrigste CPU-Auslastung (höchste Geschwindigkeit), aber auch höchste Speicherplatzverwendung für Ihr Sicherungs-Image.

Standard-Komprimierung: Komprimierung wird bis zu einem gewissen Grad durchgeführt. Diese Option bietet ein Gleichgewicht zwischen CPU-Auslastung und verwendetem Speicherplatz. Diese Einstellung ist die Standardeinstellung.

Maximale Komprimierung: Es wird eine maximale Komprimierung durchgeführt. Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigste Speicherplatzverwendung für Ihr Sicherungs-Image.

Hinweis: Wenn Ihr Sicherungs-Image unkomprimierbare Daten enthält (wie JPG-Bilder oder ZIP-Dateien), kann zusätzlicher Speicherplatz für diese Daten zugewiesen werden. Die Aktivierung einer Komprimierungsoption kann in solchen Fällen eine erhöhte Speicherplatzverwendung zur Folge haben.

Verschlüsselungsalgorithmus

Legt den Typ des für das Kopieren der Wiederherstellungspunkte zu verwendenden Verschlüsselungsalgorithmus fest. Die verfügbaren Formatoptionen sind "Keine Verschlüsselung", "AES-128", "AES-192" und "AES-256".

Verschlüsselungskennwort

Legt fest, dass ein Verschlüsselungskennwort bereitgestellt wird, das verwendet wird, um die Zielsitzung zu verschlüsseln. Wenn Sie eine Wiederherstellung von den Wiederherstellungspunkt-Kopien durchführen, müssen Sie dieses Kennwort angeben, um Ihre Authentifizierung zu bestätigen.

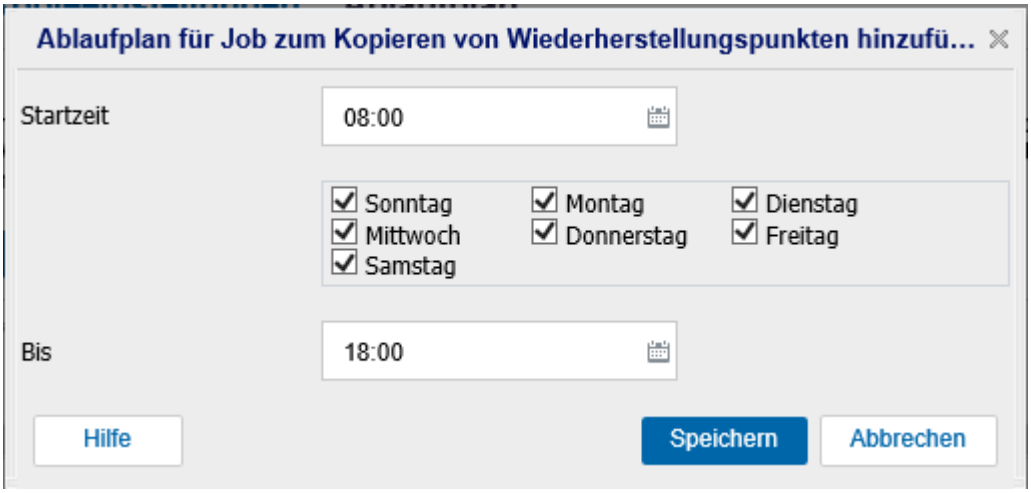
Verschlüsselungskennwort bestätigen

Legt fest, dass das Kennwort erneut eingegeben werden muss.

5. Klicken Sie auf die Registerkarte **Ablaufplan**, und geben Sie einen Jobablaufplan an.

   Mithilfe der Ablaufplanoption können Sie mehrere Ablaufpläne für einen Wiederherstellungspunkt hinzufügen. Beachten Sie auch die folgenden Details:

   - Wenn kein Ablaufplan konfiguriert wird, wird der Job zum Kopieren von Wiederherstellungspunkten sofort nach Abschluss des Sicherungsjobs ausgeführt.
   - Jetzt können Sie den Job zum Kopieren von Wiederherstellungspunkten für eine Start- und Endzeit konfigurieren.



   - Der CRP-Job versucht stets, die Sitzung in der vorgegebenen Zeit zu überprüfen.

- Wenn im angegebenen Zeitraum eine auf der Registerkarte "Quelle" konfigurierte Sicherungssitzung verfügbar ist, kopiert der CRP-Job die Sitzung an das jeweilige Ziel.
- Sie können auch die tägliche, wöchentliche und monatliche Aufbewahrung von Wiederherstellungspunkten konfigurieren.

Hinweis: Die Anzahl der erfolgreichen Sicherungen wird für alle konfigurierten täglichen, wöchentlichen und monatlichen Sicherungen gezählt.

6. Klicken Sie auf **Änderungen speichern**.

   Die Änderungen werden gespeichert, und der Task zum Kopieren von Wiederherstellungspunkten wird automatisch auf dem Knoten bereitgestellt.

   Sie haben den Plan zum Kopieren von Wiederherstellungspunkten erfolgreich erstellt und bereitgestellt.

Konfigurieren der Einstellungen der Objektsperre für einen Cloud-Dienst

Dieser Abschnitt enthält Informationen zum Konfigurieren der Einstellungen für die Objektsperre für einen Cloud-Dienst:

Befolgen Sie diese Schritte:

1. Aktivieren Sie das Kontrollkästchen "Objektsperre aktivieren".

   Die Schaltfläche "Einstellungen für die Objektsperre" wird aktiviert.

2. Klicken Sie auf die Schaltfläche "Einstellungen für die Objektsperre".

   Das Dialogfeld "Einstellungen für die Objektsperre" wird angezeigt.

3. Führen Sie im Dialogfeld "Einstellungen für die Objektsperre" die folgenden Schritte aus:

   Hinweis: Die Optionen im Dialogfeld "Einstellungen der Objektsperre" können je nach Cloud-Dienst, den Sie beim Erstellen eines Plans ausgewählt haben, variieren.

   Amazon S3

   Standard-Aufbewahrungsmodus

   Ermöglicht es Ihnen, verschiedene Schutzstufen für Objektversionen zu aktivieren. Wählen Sie zum Aktivieren eine der folgenden Optionen aus:

- **Governance:** Wenn Sie während des Aufbewahrungszeitraums über bestimmte IAM-Berechtigungen verfügen, können Sie die geschützten Objektversionen überschreiben, löschen oder die Sperreinstellungen ändern.
- **Compliance:** Sie können geschützte Objektversionen nicht überschreiben oder löschen, auch wenn Sie ein Stammbenutzer im AWS-Konto sind.

Standard-Aufbewahrungszeitraum

Ermöglicht Ihnen die Angabe eines festen Zeitraums, in dem Objektversionen geschützt sein sollen. Sie können den Aufbewahrungszeitraum in Tagen oder Jahren angeben.

Wasabi Hot Cloud-Speicher

Standard-Aufbewahrungsmodus

Ermöglicht es Ihnen, verschiedene Schutzstufen für Objektversionen zu aktivieren. Wählen Sie zum Aktivieren eine der folgenden Optionen aus:

- **Governance:** Wenn Sie während des Aufbewahrungszeitraums über bestimmte IAM-Berechtigungen verfügen, können Sie die geschützten Objektversionen überschreiben, löschen oder die Sperreinstellungen ändern.
- **Compliance:** Sie können geschützte Objektversionen nicht überschreiben oder löschen, auch wenn Sie ein Stammbenutzer im AWS-Konto sind.

Standard-Aufbewahrungszeitraum

Ermöglicht Ihnen die Angabe eines festen Zeitraums, in dem Objektversionen geschützt sein sollen. Sie können den Aufbewahrungszeitraum in Tagen oder Jahren angeben.

Nutanix Objects

Standard-Aufbewahrungszeitraum

Ermöglicht Ihnen die Angabe eines festen Zeitraums, in dem Objektversionen geschützt sein sollen. Sie können den Aufbewahrungszeitraum in Tagen oder Jahren angeben.

Hinweis: Wenn die Objektsperre aktiviert wird, während ein Plan für Nutanix-Objekte erstellt wird, wird auch Folgendes aktiviert:

- **WORM (Write-Once-Read-Many):** Sie können die vorhandenen Objekte während einer angegebenen Verweildauer nicht überschreiben oder löschen.
- **Versionierung:** Sie können mehrere Versionen von Nutanix Objects in einem Bucket speichern.

4. Klicken Sie auf **OK**.

Wiederherstellungspunkt-Verzeichnisstruktur im Cloud-Bucket/Container

Alle Wiederherstellungspunkte von Knoten mit einem einzigen CRP-Plan und einem (in der Arcserve-Verwaltungskonsole erstellten) Cloud-Konto als Ziel werden in einem einzigen Cloud-Bucket gespeichert.

Die Wiederherstellungspunkt-Verzeichnisstruktur im Cloud-Bucket/Container ist wie folgt:

arcserve-{nach-dem-Zufallsprinzip-generierte-ID}-<BucketName>

ca_root_arcserve-recovery-points_<NodeName1>

Set0

<YYYY-MM-DD_HH-MM-SS_<ScheduleType>>

<NodeName1>

<YYYY-MM-DD_HH-MM-SS_<ScheduleType>>

<NodeName1>

.....

<YYYY-MM-DD_HH-MM-SS_<ScheduleType>>

<NodeName1>

ca_root_arcserve-recovery-points_<NodeName2>

.....

ca_root_arcserve-recovery-points_<NodeNameN>

Hinweise:

- Die Änderungen des neuen Präfix "arcserve-{nach-dem-Zufallsprinzip-generierte-ID}" haben keine Auswirkungen auf vorhandene Pläne.
- Das Präfix "arcserve-{nach-dem-Zufallsprinzip-generierte-ID}" wird zu dem im Cloud-Konto konfigurierten Bucket-Namen hinzugefügt.
- Der Knotenname stimmt mit der Anzeige auf dem Sicherungsziel überein.
- YYYY-MM-DD: Datumsformat (Y – Jahr, M – Monat, D – Tag)
- HH-MM-SS: Zeitformat (H – Stunde, M – Minute, S – Sekunde)
- <ScheduleType> ist der Ablaufplan für Sicherungen und bezieht sich auf eine der folgenden Optionen:

- Täglich: Tägliche Sicherung des Wiederherstellungspunkts
- Wöchentlich: Wöchentliche Sicherung des Wiederherstellungspunkts
- Monatlich: Monatliche Sicherung des Wiederherstellungspunkts
- Benutzerdefiniert: Der Wiederherstellungspunkt wird mit der Option "Hochladen von Wiederherstellungspunkten in die Cloud" (Ad-hoc-Kopie des Wiederherstellungspunkts) hochgeladen

- Wiederherstellungspunkte von Knoten mit dem gleichen Namen den im selben Verzeichnis gespeichert, wenn sie für das gleiche Cloud-Konto bestimmt sind. Als Folge empfehlen wir, verschiedene Cloud-Konten für Knotenmit demselben Namen zu verwenden, um die Speicherung in anderen Buckets zu ermöglichen.

Überprüfen des Plans

Um die Funktion für das Kopieren von Wiederherstellungspunkten zu überprüfen, stellen Sie sicher, dass Sie den Plan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Nachdem der Sicherungsjob erfolgreich abgeschlossen wurde, wird der Job zum Kopieren von Wiederherstellungspunkten ausgeführt. Sie können den Status des Sicherungsjobs und des Jobs zum Kopieren von Wiederherstellungspunkten auf der Registerkarte **Jobs** überprüfen.

Folgen Sie diesen Schritten, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Führen Sie diese Schritte durch, um die Jobs zum Kopieren von Wiederherstellungspunkten zu überprüfen:

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf "**Alle Jobs**".

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Stellen Sie sicher, dass der Sicherungsjob und der Job zum Kopieren von Wiederherstellungspunkten erfolgreich ausgeführt wurden.

Erstellen eines Ablaufplans für Dateikopie

Mit Arcserve Unified Data Protection können Sie ausgewählte Quelldateien in ein Ziel kopieren oder verschieben. Bei dem Ziel kann es sich um einen Cloud-Speicher oder ein freigegebenes Netzwerk handeln. Die Quelldatei muss zum selben Volume gehören, das Sie bereits gesichert haben. Beispielsweise haben Sie Volume D:\ Ihres Quellknotens vollständig gesichert. Nun möchten Sie eine bestimmte Datei aus Volume D:\ des Quellknotens kopieren. Sie können einen Task für eine Dateikopie erstellen, um diesen Vorgang auszuführen.

Die Dateikopieoption kann für das Kopieren kritischer Daten an sekundäre Speicherorte sowie als Archivierungslösung verwendet werden.

Die Vorteile des Kopierens von Daten sind:

- Verbesserung der Leistungsfähigkeit - Hilft Ihnen, durch Kopieren und Verschieben unveränderter Daten Sicherungs- und Wiederherstellungsvorgänge zu beschleunigen und dadurch die Menge der wirklich zu sichernden und auf Band oder einem Datenträger zu speichernden Daten zu reduzieren.
- Einhaltung zwingender Compliance - Hilft Ihnen, wichtige Dokumente, E-Mails und andere entscheidende Daten je nach Notwendigkeit aufzubewahren, um den internen Richtlinien und externen Regelungen zu entsprechen.
- Reduzierung der Speicherkosten - Hilft Ihnen dabei, Speicherplatz zurückzugewinnen, indem Sie ältere oder weniger häufig verwendete Daten von Ihren Primärsystemen an kostengünstigere Archivspeicherorte migrieren können.
- Verwaltung mehrerer Dateiversionen - Hilft Ihnen, (im Bedarfsfall) auf vorherige Versionen gesicherter Dateien zurückzugreifen oder mehrere Versionen der gleichen Dateien an unterschiedlichen Zielen zu verwalten.

Der nächste Schritt?

- Überprüfen der Voraussetzungen
- Erstellen eines Plans mit einem Sicherungstask
- Hinzufügen eines Dateikopietasks zum Plan
- Ausführen einer manuellen Dateikopie (optional)
- Überprüfen des Plans

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich bei der Konsole an.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Besondere Aspekte:

- Die folgende Tabelle enthält die Längenbeschränkung des Dateinamens für Dateikopiejobs. Die Dateien, die die entsprechende Länge überschreiten, werden übersprungen.

Ziel	Beschränkung
Netzwerkfreigabe	240
Cloud	245

- Wenn die Dateikopie über eine replizierte Sitzung ausgeführt wird und die Replikations-*Quelle* mehrere Sicherungssitzungen hat, wird der Dateikopiejob für jede Sitzung einzeln ausgeführt. Wenn beispielsweise **fünf** *Sicherungssitzungen* im Sicherungsziel vorhanden sind und Sie einen Replizierungs-Task hinzufügen, werden mit dem Replizierungs-Task alle Sicherungen in *einem einzigen Job* repliziert. Wenn Sie jetzt einen Dateikopie-Task hinzufügen und die Quelle der Dateikopie das Replizierungsziel ist, dann erfolgen **fünf** *Dateikopiejob*-Durchläufe zur Replizierung der jeweiligen Sitzungen.

Erstellen eines Plans mit einem Sicherungstask

Ein Plan umfasst verschiedene Arten von Tasks, die Sie ausführen möchten. Um einen Dateikopietask zu erstellen, müssen Sie zuerst einen gültigen Wiederherstellungspunkt haben. Um einen gültigen Wiederherstellungspunkt zu erhalten, müssen Sie einen Sicherungstask erstellen.

Ein Sicherungstask führt eine Sicherung der Quellknoten aus und speichert die Daten am angegebenen Ziel. Dateikopie wird nur für agentenbasierte Windows-Sicherung unterstützt. Der folgende Vorgang beschreibt die Schritte zur Erstellung des agentenbasierten Windows-Sicherungstasks.

Gehen Sie wie folgt vor:

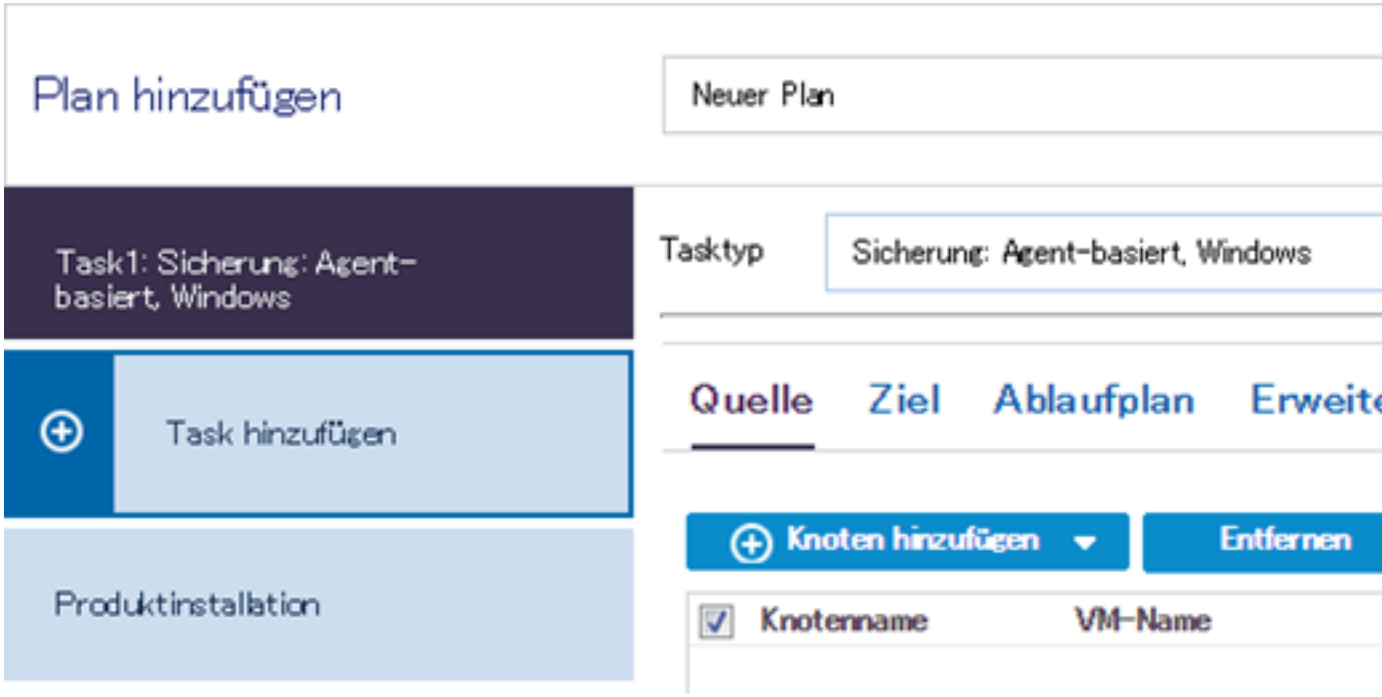
1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Sicherung, Agent-basiertes Windows** aus.



Geben Sie nun Einstellungen für "Quelle", "Ziel", "Ablaufplan" und "Erweitert" an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die Quellknoten angeben, die Sie schützen möchten. Sie können mehrere Knoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Knoten hinzufügen, wenn Sie einen Plan auf der Quellenseite erstellen oder ändern. Sie können einen Plan auch speichern, ohne Quellknoten hinzuzufügen. Der Plan wird erst bereitgestellt, wenn Sie Quellknoten hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Quelle" auf **Hinzufügen**.
2. Wählen Sie eine der folgenden Optionen:

   Wählen Sie zu sichernden Knoten in Arcserve UDP aus

   Öffnet das Dialogfeld "Wählen Sie zu sichernden Knoten in Arcserve UDP aus". Wählen Sie die Knoten in der angezeigten Liste aus. Wählen Sie diese Option aus, wenn Sie die Knoten bereits zu der Konsole hinzugefügt haben.

   Windows-Knoten hinzufügen

   Öffnet das Dialogfeld "Knoten zu Plan hinzufügen". Wählen Sie diese Option aus, wenn Sie die Knoten nicht hinzugefügt haben und Sie die zu schützenden Knoten manuell hinzufügen möchten.

   Knoten aus Active Directory erkennen

   Öffnet das Dialogfeld Knoten zu Arcserve UDP-Konsole hinzufügen. Wählen Sie diese Option, wenn Sie Knoten aus Active Directory erkennen und hinzufügen möchten.
3. Wenn Sie die Option **Wählen Sie zu sichernden Knoten in Arcserve UDP aus** ausgewählt haben, gehen Sie im Dialogfeld "Zu schützende Knoten auswählen" folgendermaßen vor:

   a. (Optional) Wählen Sie einen Filter aus der Dropdown-Liste "Gruppen" aus, um nach Knoten zu filtern. Sie können Schlüsselwörter eingeben, um den Knotenfilter weiter einzuschränken.

      Die Knoten werden in der Spalte "Verfügbare Knoten" angezeigt.

   b. Wählen Sie die Knoten aus der Spalte "Verfügbare Knoten" aus, und klicken Sie dann auf den einfachen Nach-rechts-Pfeil (>) oder den doppelten Nach-rechts-Pfeil (>>), um die ausgewählten Knoten bzw. alle Knoten in die Spalte "Ausgewählte Knoten" zu verschieben.

Die Knoten werden in der Spalte "Ausgewählte Knoten" angezeigt.

c. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

4. Wählen Sie zum Festlegen des Schutztyps eine der folgenden Optionen aus:

Alle Volumes sichern

Bereitet einen Sicherungs-Snapshot aller Volumes vor.

Ausgewählte Volumes sichern

Bereitet einen Sicherungs-Snapshot des ausgewählten Volumes vor.

Die Sicherungsquelle ist nun angegeben.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Wählen Sie einen der folgenden **Zieltypen** aus:

   Lokaler Datenträger oder freigegebener Ordner

   Gibt an, dass das Sicherungsziel ein lokales Ziel oder ein freigegebener Ordner ist. Wenn Sie diese Option auswählen, können Sie Daten als Wiederherstellungspunkte oder Wiederherstellungssätze speichern. Die Optionen für Wiederherstellungspunkte und Wiederherstellungssätze sind auf der Registerkarte **Ablaufplan** verfügbar.

   Arcserve UDP-Recovery Point Server

   Gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.

2. Wenn Sie **Arcserve UDP-Recovery Point Server** ausgewählt haben, geben Sie folgende Details an:
   a. Wählen Sie einen Recovery Point Server aus.
   b. Wählen Sie einen Datenspeicher aus. Die Liste enthält alle Datenspeicher, die am angegebenen Recovery Point Server erstellt wurden.
   c. Geben Sie ein Sitzungskennwort ein.
   d. Bestätigen Sie das Sitzungskennwort.
3. Wenn Sie **Lokaler Datenträger oder freigegebener Ordner** ausgewählt haben, geben Sie folgende Details an:
   a. Geben Sie den vollständigen Pfad des lokalen Ziels oder Netzwerkziels an. Geben Sie für das Netzwerkziel Anmeldeinformationen für ein Konto mit Schreibzugriff an.
   b. Wählen Sie den Verschlüsselungsalgorithmus aus. Weitere Informationen finden Sie unter Verschlüsselungseinstellungen.
   c. Geben Sie optional ein Verschlüsselungskennwort an.
   d. Bestätigen Sie das Verschlüsselungskennwort.

e. Wählen Sie einen Komprimierungstyp aus. Weitere Informationen finden Sie unter "Komprimierungstyp".

Hinweis: Wenn Sie die Daten auf einem lokalen Datenträger oder in einem freigegebenen Ordner speichern, können Sie die Daten nicht auf einem anderen Recovery Point Server replizieren. Die Replikation wird nur unterstützt, wenn Sie die Daten auf einem Recovery Point Server speichern.

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

Gehen Sie wie folgt vor:

1. (Optional) Wählen Sie die Option für die Verwaltung von Wiederherstellungspunkten aus. Diese Option ist nur sichtbar, wenn Sie als Sicherungsziel "Lokaler oder freigegebener Ordner" ausgewählt haben.

   Nach Wiederherstellungspunkten aufbewahren

   Die Sicherungsdaten werden als Wiederherstellungspunkte gespeichert.

   Nach Wiederherstellungssätzen aufbewahren

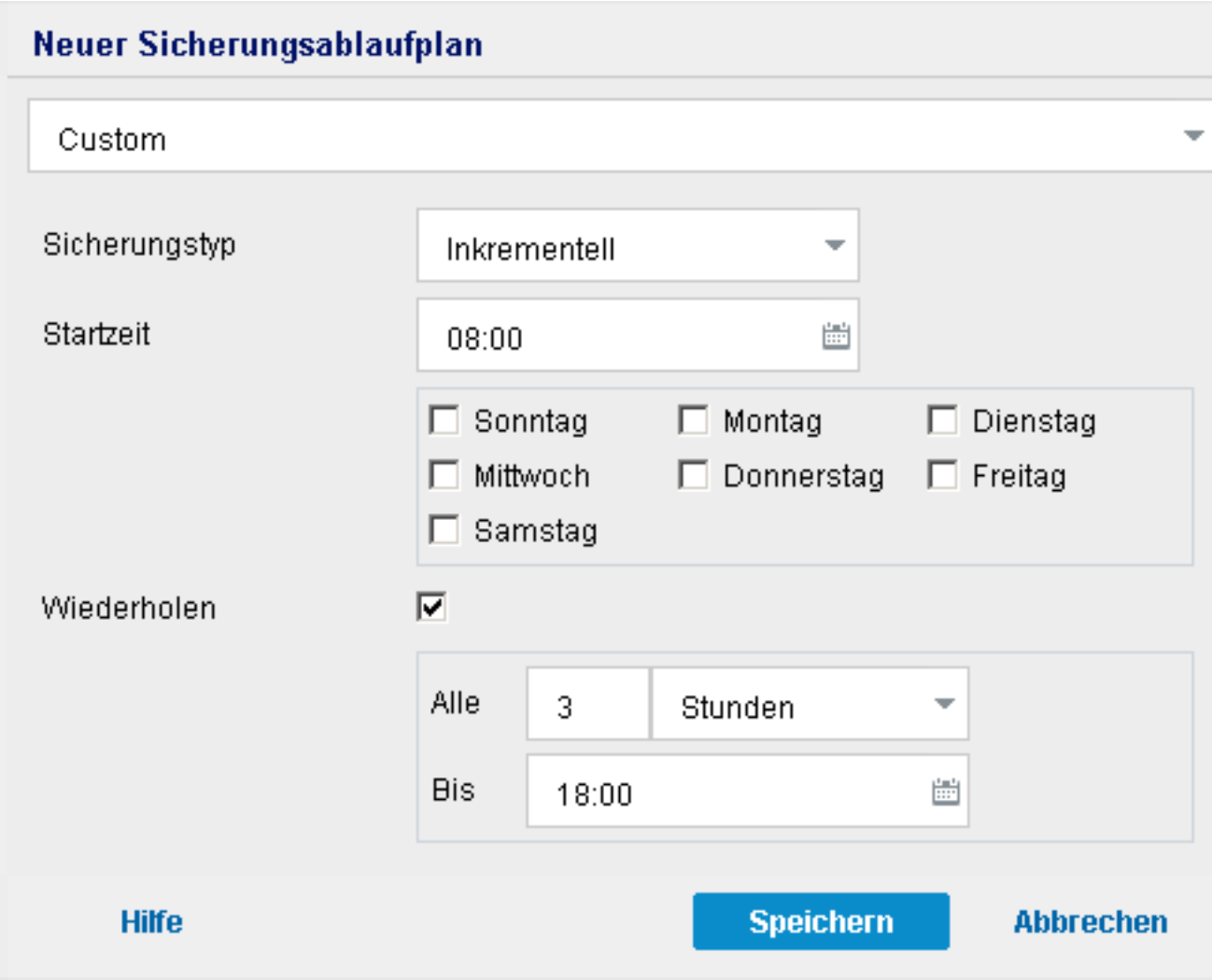
   Die Sicherungsdaten werden als Wiederherstellungssätze gespeichert.

2. Fügen Sie Ablaufpläne für Sicherungen, Zusammenführungen und Drosselungsvorgänge hinzu.

   Hinzufügen eines Sicherungsablaufplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Überprüfen

Legt den Ablaufplan für Überprüfungssicherungen fest.

Arcserve UDP überprüft die Gültigkeit und Vollständigkeit der geschützten Daten durch einen Vergleich des gespeicherten Sicherungs-Images mit der Sicherungsquelle. Im Bedarfsfall wird das Image neu synchronisiert. Bei einer Überprüfungssicherung wird die letzte Sicherung jedes einzelnen Blocks mit den Inhalten und Informationen der Quelle verglichen. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht (zumeist aufgrund von Änderungen seit der letzten Sicherung), aktualisiert Arcserve UDP die Sicherung dieses Blocks (Neusynchronisierung). In seltenen Fällen kann eine Überprüfungssicherung auch durchgeführt werden, um eine vollständige Sicherung zu erhalten, ohne den erforderlichen Speicherplatz einer vollständigen Sicherung zu verwenden.

Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteile: Die Sicherung benötigt viel Zeit, da alle Quellenblöcke mit den Blöcken der letzten Sicherung verglichen werden.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die seit der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf Hinzufügen, und wählen Sie Zusammenführungsplan hinzufügen aus.

Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

b. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

d. Klicken Sie auf **Speichern**.

Der Zusammenführungsablaufplan ist auf der Seite **Ablaufplan** angegeben und wird dort angezeigt.

Hinzufügen eines Drosselungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

Das Dialogfeld Drosselungsplan hinzufügen wird geöffnet.

b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

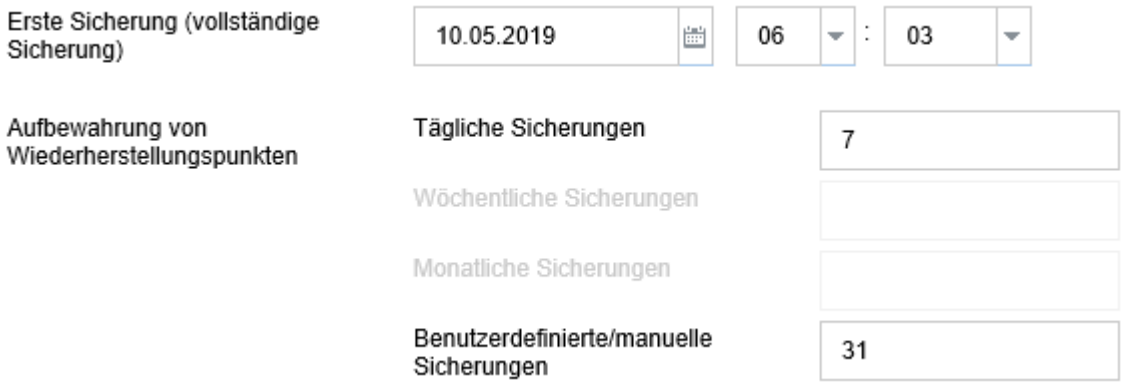
c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Drosselungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

3. Geben Sie die Startzeit für die geplante Sicherung an.



4. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld "Sicherungsablaufplan" übernommen.

5. Geben Sie die Katalogdetails an.

   Mit Katalogen können Sie den Dateisystemkatalog generieren. Der Dateisystemkatalog ist erforderlich, um schnellere und bessere Suchvorgänge auszuführen. Wenn Sie die Kontrollkästchen für den Katalog aktivieren, werden die Kataloge je nach der Sicherungsart, die Sie angegeben haben, aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Kataloggenerierung zu deaktivieren.

   Der Ablaufplan ist nun angegeben.

Funktionsweise der erweiterten Planung und Aufbewahrung

Mit der Ablaufplanoption können Sie einen benutzerdefinierten Ablaufplan, einen Ablaufplan für tägliche/wöchentliche/monatliche Sicherungen oder beides festlegen. Im benutzerdefinierten Ablaufplan können Sie den Sicherungsablaufplan für jeden Tag der Woche konfigurieren und bis zu vier Sicherungsablaufpläne für jeden Tag hinzufügen. Sie können einen bestimmten Wochentag auswählen und ein Zeitfenster erstellen, um anzugeben, wann und wie oft die Sicherung durchgeführt werden soll.

Ablaufplan	Unterstützter Job	Kommentare
Sichern	Sicherungsjob	Gibt Zeitfenster für die Ausführung von Sicherungsjobs an.
Sicherungsdrosselung	Sicherungsjob	Gibt die Zeitfenster an, um die Sicherungsgeschwindigkeit zu steuern.
Zusammenführen	Zusammenführungsjob	Gibt an, wann Zusammenführungsjobs ausgeführt werden sollen.
Täglicher Ablaufplan	Sicherungsjob	Gibt an, wann tägliche Sicherungsjobs ausgeführt werden sollen.
Wöchentlicher Ablaufplan	Sicherungsjob	Gibt an, wann wöchentliche Sicherungsjobs ausgeführt werden sollen.
Monatlicher Ablaufplan	Sicherungsjob	Gibt an, wann monatliche Sicherungsjobs ausgeführt werden sollen.

Sie können auch die Aufbewahrungseinstellungen für die Wiederherstellungspunkte angeben.

Hinweis: Legen Sie innerhalb der einzelnen Pläne Einstellungen für die Aufbewahrungszeit fest, um zu steuern, wie die Daten für die Knoten des entsprechenden Plans im Zieldatenspeicher aufbewahrt werden.

Ablaufpläne für tägliche/wöchentliche/monatliche Sicherungen sind vom benutzerdefinierten Ablaufplan und voneinander unabhängig. Sie können die Ausführung einer täglichen, wöchentlichen oder monatlichen Sicherung konfigurieren, ohne einen benutzerdefinierten Ablaufplan zu konfigurieren.

Jobplan der Sicherung

Sie können vier Zeitfenster pro Tag in Ihrem Sicherungsablaufplan hinzufügen. Ein gültiges Zeitfenster liegt im Bereich 12:00 Uhr bis 23:59 Uhr. Sie können kein Zeitfenster wie z. B. 18:00 Uhr bis 06:00 Uhr angeben. In solchen Fällen müssen Sie manuell zwei verschiedene Zeitfenster angeben.

Für jedes Zeitfenster wird die Startzeit einbezogen, und die Endzeit wird nicht einbezogen. Zum Beispiel haben Sie das Ausführen einer Zuwachssicherung konfiguriert, die stündlich zwischen 06:00 Uhr und 09:00 Uhr stattfinden soll, und die Sicherung wird um 06:00 Uhr gestartet. Das bedeutet, dass die Sicherung um 06:00 Uhr, 07:00 Uhr und 08:00 Uhr ausgeführt wird, NICHT aber um 09:00 Uhr.

Hinweis: Wenn Sie die Sicherung bis zum Ende des Tages wiederholt ausführen möchten, legen Sie den Ablaufplan bis 12:00 Uhr fest. Um den Sicherungsjob beispielsweise alle 15 Minuten während des gesamten Tages auszuführen, legen Sie den Ablaufplan von 00:00 Uhr bis 00:00 Uhr alle 15 Minuten fest.

Drosselungsplan der Sicherung

Mit dem Drosselungsplan der Sicherung können Sie die Geschwindigkeit des Sicherungsdurchsatzes steuern, die wiederum die Ressourcenverwendung (Datenträger-E/A, CPU, Netzwerkbandbreite) des Servers, der gesichert wird, steuert. Dies ist hilfreich, wenn die Serverleistung während der Geschäftszeiten nicht beeinträchtigt werden soll. Sie können vier Zeitfenster pro Tag in Ihrem Drosselungsplan der Sicherung hinzufügen. Für jedes Zeitfenster können Sie einen Wert in MB pro Minute angeben. Dieser Wert wird verwendet, um den Sicherungsdurchsatz zu steuern. Gültige Werte liegen im Bereich zwischen 1 MB/Minute bis 99.999 MB/Minute.

Wenn ein Sicherungsjob die angegebene Zeit überschreitet, dann wird das Drosselungslimit entsprechend dem angegebenen Zeitfenster angepasst. Zum Beispiel haben Sie als Drosselungslimit der Sicherung den Wert 500 MB/Minute von 08:00 Uhr bis 20:00 Uhr und 2500 MB/Minute von 20:00 Uhr bis 22:00 Uhr angegeben. Wenn ein Sicherungsjob um 19:00 Uhr startet und drei Stunden ausgeführt wird, dann hat das Drosselungslimit von 19:00 Uhr bis 20:00 Uhr den Wert 500 MB/Minute. Von 20:00 Uhr bis 22:00 Uhr hat das Drosselungslimit den Wert 2.500 MB/Minute.

Wenn Sie keinen Sicherungsablaufplan und keinen Ablaufplan für den Sicherungsdurchsatz angeben, dann wird die Sicherung so schnell wie möglich ausgeführt.

Ablaufplan für Zusammenführung

Ermöglicht es Ihnen, Wiederherstellungspunkte basierend auf dem angegebenen Ablaufplan zusammenzuführen.

Beachten Sie folgende Punkte für den Zusammenführungsjob:

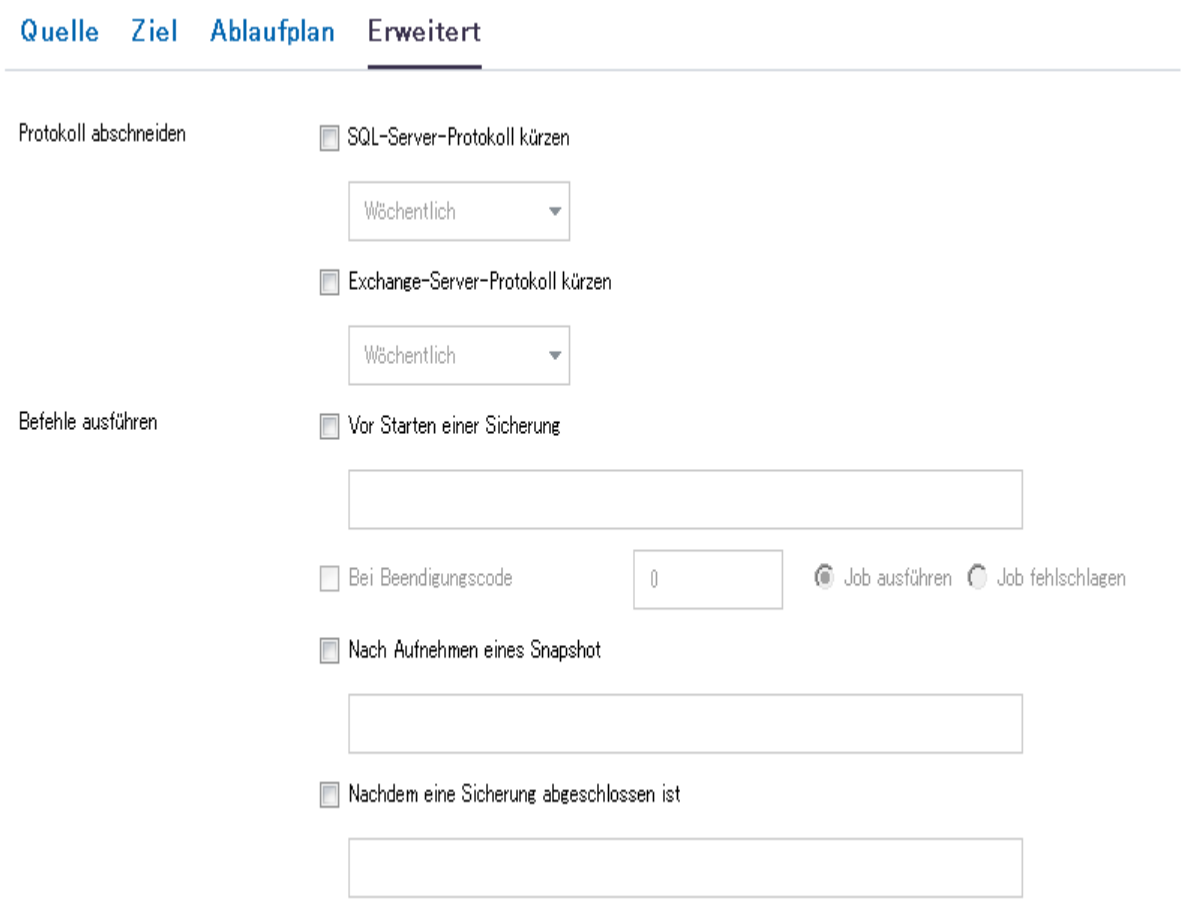
- Es kann immer nur ein Zusammenführungsjob für einen Knoten ausgeführt werden.

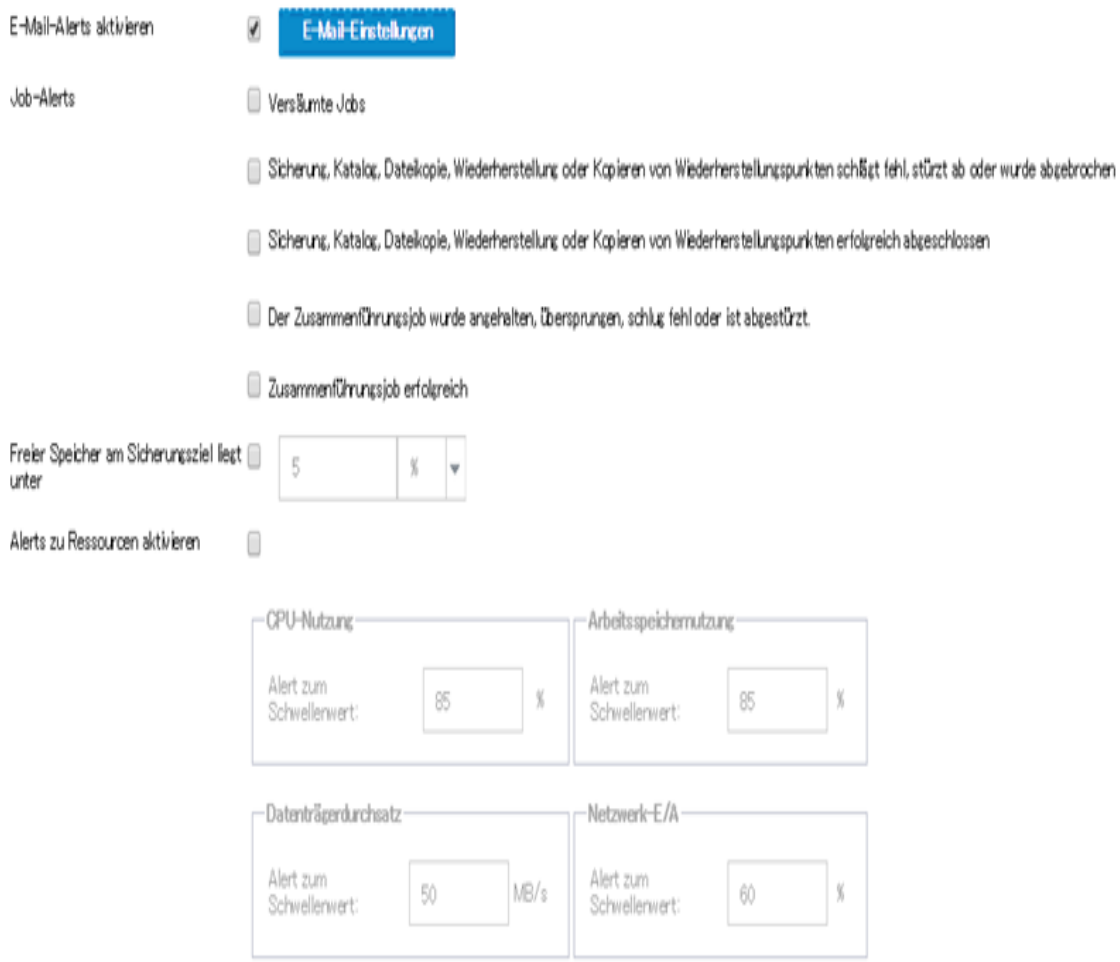
- Wenn ein Zusammenführungsjob gestartet wird, muss er abgeschlossen werden, bevor der nächste Zusammenführungsjob gestartet werden kann. Das bedeutet: Wenn ein oder mehrere Sätze an Wiederherstellungspunkten zusammengeführt werden, dann kann der neue Wiederherstellungspunkt nicht zu diesem Zusammenführungsprozess hinzugefügt werden, bis der Zusammenführungsprozess für den aktuellen Satz an Wiederherstellungspunkten abgeschlossen ist.
- Wenn ein Zusammenführungsjob mehr als einen Satz an Wiederherstellungspunkten bearbeitet (zum Beispiel Satz [1~4], Satz [5~11] und Satz [12~14], also drei Sätze), dann werden diese Sätze nacheinander vom Recovery Point Server bearbeitet.
- Wenn ein Zusammenführungsjob nach einer Pause fortgesetzt wird, erkennt der Job an welchem Punkt er unterbrochen wurde, und die Zusammenführung wird ab der Abbruchstelle fortgesetzt.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen die Einstellungen zum Abschneiden von Protokollen, das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte "Erweitert":





Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

Protokoll abschneiden

Ermöglicht es Ihnen, den Ablaufplan anzugeben, um Protokolle für SQL Server und Exchange Server zu kürzen. Sie können den Ablaufplan als **Täglich**, **Wöchentlich** oder **Monatlich** angeben.

Benutzername

Ermöglicht es Ihnen, den Benutzer anzugeben, der zur Ausführung eines Skripts autorisiert ist.

Kennwort

Ermöglicht es Ihnen, das Kennwort des Benutzers anzugeben, der zur Ausführung des Skripts autorisiert ist.

Befehl ausführen, bevor eine Sicherung gestartet wird

Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, in dem das Skript gespeichert wird. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem ein Snapshot aufgenommen wurde

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungs-Snapshot aufgenommen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Arten der Alerts angeben, die Sie in Form von E-Mails empfangen möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers.

Job-Alerts

Ermöglicht es Ihnen, die Typen der Job-E-Mails auszuwählen, die Sie erhalten möchten.

Warnmeldungen zu Ressourcen aktivieren

Ermöglicht es Ihnen, einen Schwellenwert für CPU-Auslastung, Speicherverwendung, Datenträgerdurchsatz, Netzwerk-E/A anzugeben. Sie können den Wert in Prozent angeben. Sie erhalten eine E-Mail, wenn der Wert "Warnmeldung zum Schwellenwert" überschritten ist.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Knoten installiert ist und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung

an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agenten oder kein Agent installiert ist. Um den Agenten auf diesen Knoten zu installieren bzw. um ein Upgrade des Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus, und klicken Sie auf "Speichern".

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie eine andere Task hinzufügen müssen, müssen Sie den Plan aus der Registerkarte **Ressourcen** auswählen und den Plan ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern.

Der Sicherungsplan wird erstellt und automatisch für den Quellknoten bereitgestellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

Hinzufügen eines Dateikopietasks zum Plan

Der Dateikopietask ermöglicht es Ihnen, individuelle Dateien in das angegebene Ziel zu kopieren. Nachdem Sie die Dateien in das angegebene Ziel kopiert haben, wird die ursprüngliche Kopie aufbewahrt. "Dateikopie" ist von keinem Katalogjob abhängig. Wenn das Sicherungsziel ein Datenspeicher mit Deduplizierung oder ohne Deduplizierung ist, wird der Katalogordner zum Sicherungsziel verschoben. Der Katalogjob ist Teil des Dateikopiejobs. Der Dateikopiejob wird auf dem Recovery Point Server ausgeführt. Dadurch nimmt Arcserve UDP den Agenten den Task ab.

Arcserve UDP unterstützt das Kopieren von Dateien aus einem Replikationsdatenspeicher. ;

Preflight-Check für die Dateikopieknoten: Sie können auch einen Pre-Flight Check (PFC) für Dateikopien durchführen. Nur die Knoten, die für die Dateikopie hinzugefügt werden, kommen für den PFC in Frage. Für die Ausführung des PFC für Dateikopien klicken Sie unter "Alle Knoten" mit der rechten Maustaste auf den Knoten und wählen "Preflight-Check für Dateikopie" aus.

Hinweis: Wenn ein Sicherungsjob ausgeführt wird und Sie den Plan unterbrechen, hat der Sicherungsjob Vorrang, und der Dateikopiejob startet nicht. Wenn Sie den Plan erneut wieder aufnehmen, wird der Dateikopiejob nicht automatisch fortgesetzt. Sie müssen einen anderen Sicherungsjob manuell ausführen, um den Dateikopiejob zu starten.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Fensterbereich auf **Task hinzufügen**.

   Ein neuer Task wird im linken Fensterbereich hinzugefügt.

2. Wählen Sie im Drop-down-Menü **Tasktyp** die Option **Dateikopie** aus.

   Der Dateikopietask wird hinzugefügt.

3. Klicken Sie auf die Registerkarte **Quelle**, und geben Sie die Details ein.

   Wiederherstellungspunktquelle für die Dateikopie

   Ermöglicht es Ihnen, die Quelle von Wiederherstellungspunkten auszuwählen. Wenn nur eine Quelle vorhanden ist, wird die Quelle automatisch angezeigt. Wenn mehr als eine Quelle vorhanden ist, müssen Sie die richtige Quelle aus der Drop-down-Liste auswählen.

   Typen von Wiederherstellungspunkten

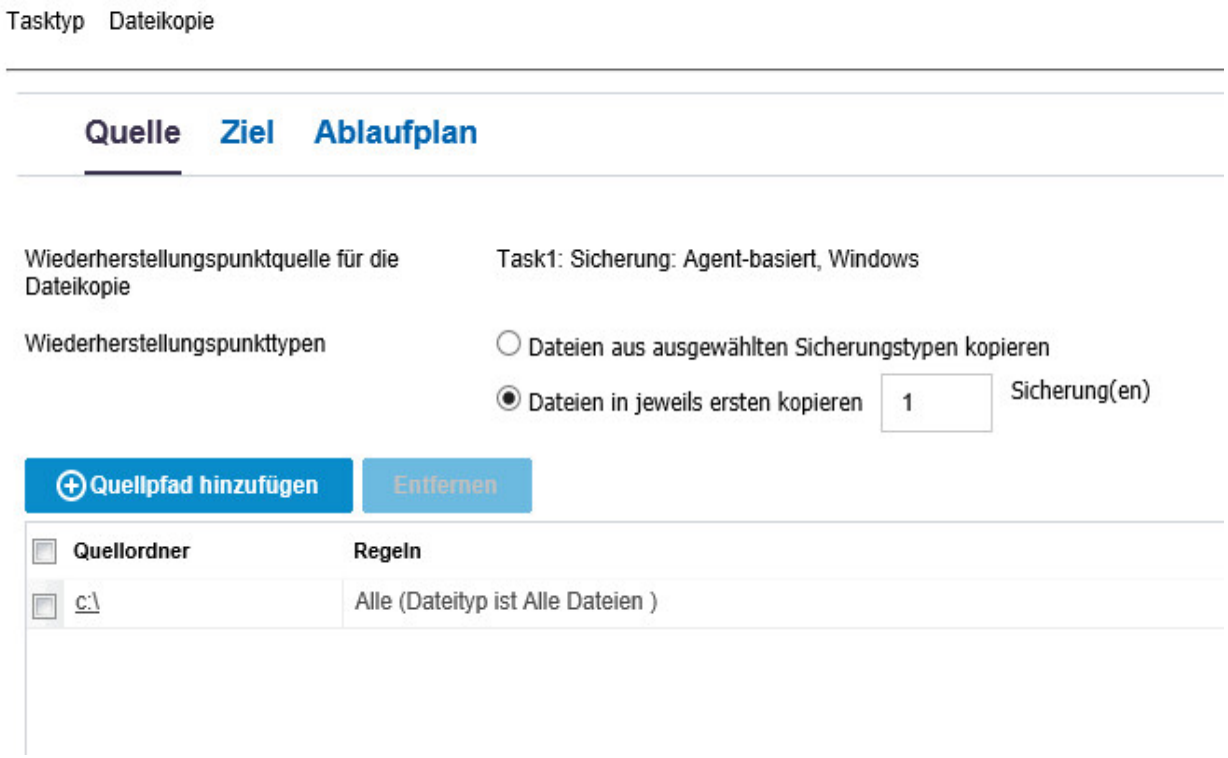
   Ermöglicht es Ihnen, die Wiederherstellungspunkte für Dateikopien auszuwählen. Folgende zwei Optionen stehen zur Auswahl:

   Kopieren von Dateien aus ausgewählten Sicherungstypen

Sie können **Tägliche Sicherungen**, **Wöchentliche Sicherungen** und **Monatliche Sicherungen** wählen. Die Optionen für tägliche, wöchentliche oder monatliche Sicherungen werden in Abhängigkeit vom Ablaufplan der Quellsicherung aktiviert. Wenn für die Quellsicherung beispielsweise nur eine monatliche Sicherung geplant ist, ist bei der Option **Kopieren von Dateien aus ausgewählten Sicherungstypen** nur **Monatliche Sicherungen** aktiviert.

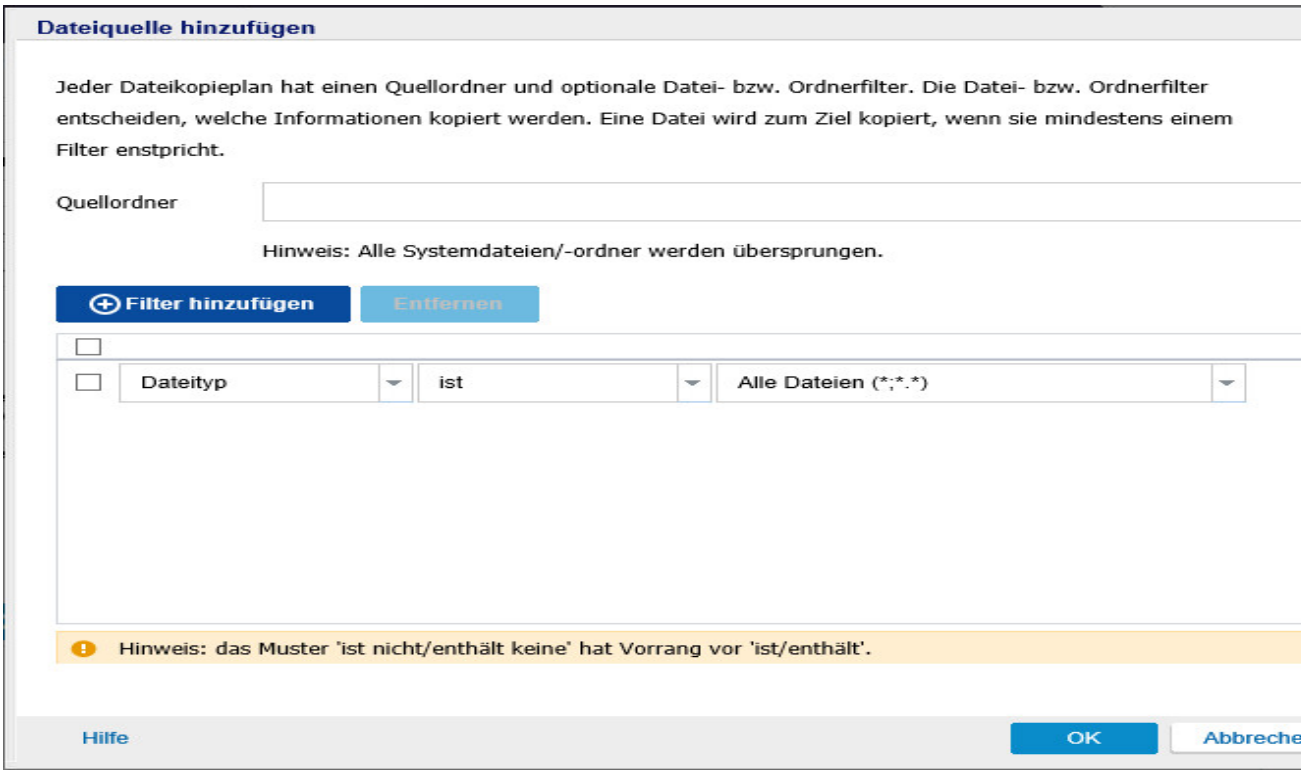
Kopieren der Datei aus jeder ersten Sicherung

Sie können die Sicherungsnummer angeben, die Sie kopieren möchten. Wenn Sie beispielsweise "3" angeben, wird die dritte Sicherung kopiert. "Dateikopie" unterstützt bis zu 700 Wiederherstellungspunkte, von denen aus Kopien erstellt werden können.



4. Klicken Sie auf **Quellpfad hinzufügen**.

   Das Dialogfeld **Dateiquelle hinzufügen** wird geöffnet.



Verwenden Sie die folgende Konfiguration, um das Überspringen der Verzeichnisse des Windows-Systems (C:\\Windows) und der Programmdateien (C:\\Programme, C:\\Programme (x86)) zu vermeiden:

Fügen Sie den folgenden XML-Tag hinzu, falls nicht bereits vorhanden, oder aktualisieren Sie die Datei "FileCopyDebugSetting.xml" im Ordner "$UDPHome\Engine\Configuration":

<SkipWindowsFolders>0</SkipWindowsFolders>

Die XML-Datei wird wie folgt angezeigt:

<?xml version="1.0" encoding="UTF-8"?>

<HKLM>

<AFArchiveDLL>

.....

<SkipWindowsFolders>0</SkipWindowsFolders>

</AFArchiveDLL>

</HKLM>

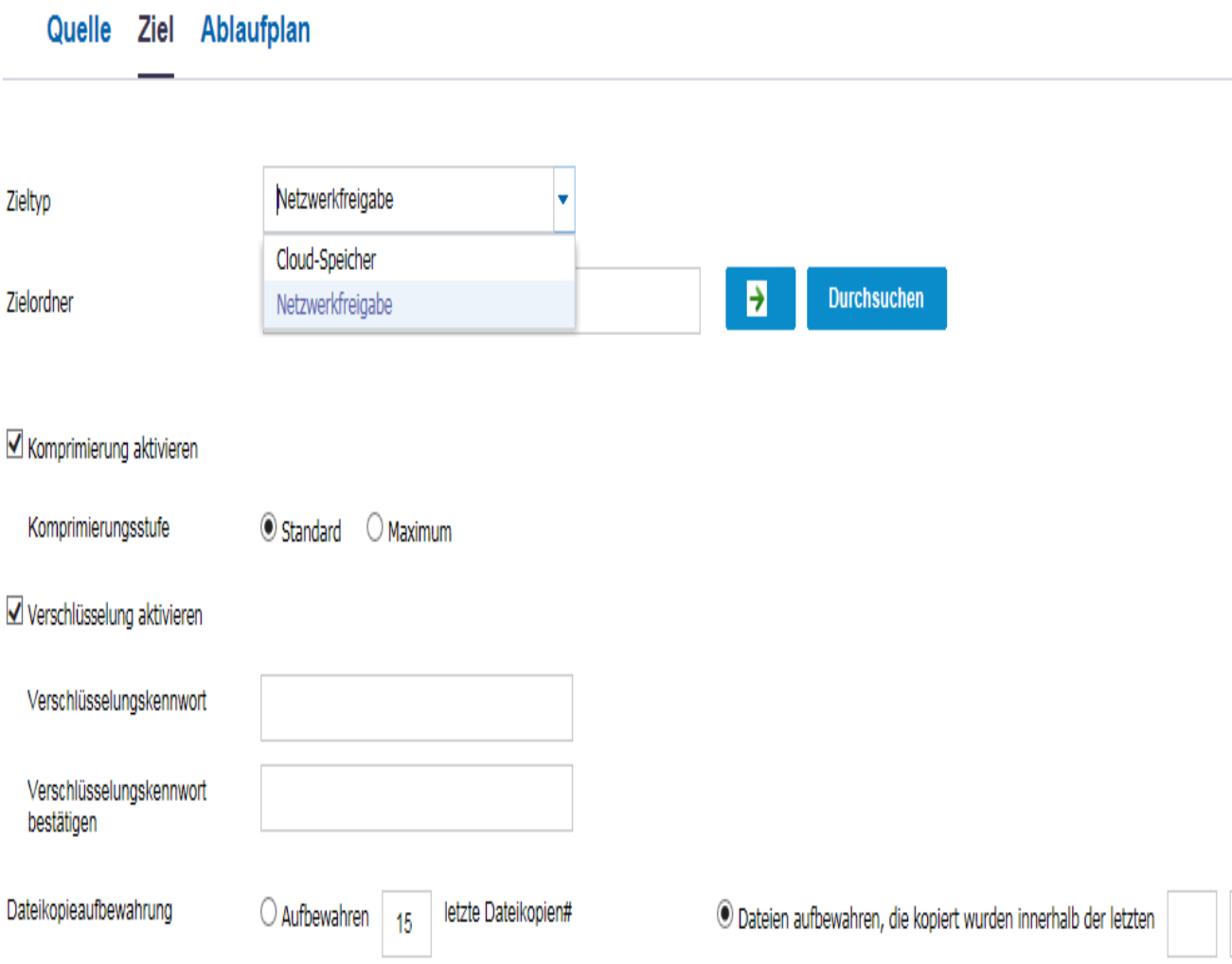
5. Geben Sie den Pfad des Quellordners ein, den Sie kopieren möchten.
6. Klicken Sie auf **Filter hinzufügen**.

Der Filter wird unter der Schaltfläche **Filter hinzufügen** hinzugefügt. Sie können mehrere Filter hinzufügen und diese auch wieder entfernen. Weitere Informationen finden Sie unter Hinzufügen von Dateikopiefiltern.

7. Wählen Sie den Filter aus der Liste aus, und klicken Sie auf **OK**.

   Das Dialogfeld **Dateiquelle hinzufügen** wird geschlossen.

8. Klicken Sie auf die Registerkarte **Ziele**, und geben Sie die Zieldetails an.



Zieltyp

Gibt an, dass der Zieltyp eine Netzwerkfreigabe oder ein Cloud-Speicher ist. Falls die Verbindung zum angegebenen Ziel verloren ging oder unterbrochen wurde, versucht Arcserve UDP für jede Zieloption einige Male, mit dem Dateiarchivjob fortzufahren. Falls diese Neuversuche nicht erfolgreich sind, wird ein Ergänzungsjob von dem Punkt aus ausgeführt werden, an dem der Fehler auftrat. Zusätzlich wird das Aktivitätsprotokoll mit einer entsprechenden Fehlermeldung aktualisiert, und es wird eine E-Mail-Benachrichtigung gesendet (falls konfiguriert).

Netzwerkfreigabe

Gibt an, dass das Ziel ein freigegebener Ordner ist. Wenn diese Option ausgewählt ist, können Sie den vollständigen Pfad des Speicherorts angeben, auf den Sie Ihre Quelldateien/-ordner kopieren oder verschieben wollen.

Zielordner

Gibt das Ziel an, an dem die kopierten Dateien gespeichert sind. Ziele können lokale Volumes, Ordner oder Dateifreigaben sein, auf die über einen UNC-Pfad (Uniform Naming Convention) zugegriffen werden kann. Dieses Feld ist verfügbar, wenn Sie eine Netzwerkfreigabe als Zieltyp auswählen. Sie können auch den Zielordner durchsuchen.

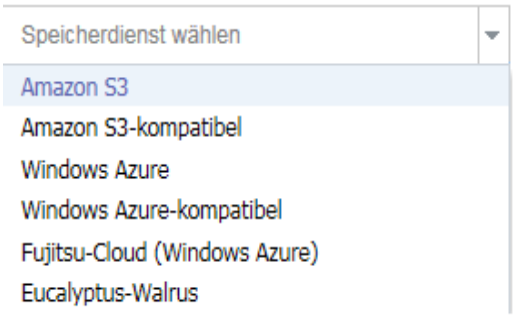
Cloud-Speicher

Gibt an, dass die kopierten Dateien in einer Cloud-Umgebung gespeichert werden. Arcserve UDP unterstützt derzeit das Kopieren von Dateien an mehrere Cloud-Anbieter, wie Amazon S3 (Simple Storage Service), Amazon S3-kompatibel, Windows Azure, Windows Azure-kompatibel, Eucalyptus-Walrus und FUJITSU Hybrid IT Service FJcloud-O. Diese Cloud-Anbieter sind öffentlich verfügbare Webdienste, mit denen Sie jederzeit und von überall im Internet eine beliebige Datenmenge in einer sicheren Umgebung speichern und abrufen können.

Hinweis: Um einen potenziellen Uhrabweichungsfehler zu beheben, wenn Sie versuchen, eine Verbindung zur Cloud herzustellen, sollten Sie sicherstellen, dass bei Ihrem Rechner die richtige Zeitzone eingestellt ist und die Uhr synchron zur globalen Zeit ist. Sie sollten die Zeit Ihres Rechners immer mit der GMT-Zeit abgleichen. Wenn die Uhrzeit Ihres Rechners nicht mit der korrekten globalen Uhrzeit (auf 5 bis 10 Minuten) synchronisiert ist, wird Ihre Cloud-Verbindung möglicherweise nicht funktionieren. Stellen Sie gegebenenfalls die richtige Zeit für Ihren Rechner ein, und wiederholen Sie Ihren Dateikopierjob.

Speichergeräte

Wählen Sie den Gerätetyp aus der Drop-down-Liste aus.



Cloud-Speicher

Wählen Sie den Pfad des Cloud-Speichers aus der Drop-down-Liste aus. Die Drop-down-Liste ist verfügbar, wenn Sie die Details Ihres Cloud-Speichers angegeben haben. Wenn Sie zum ersten Mal das Cloud-Speicherkonto angeben, klicken Sie auf "Hinzufügen", um Ihr Cloud-Konto hinzuzufügen. Wenn Sie das nächste Mal Cloud-Speicher auswählen, wird das Konto in der Cloud-Speicher-Drop-down-Liste angezeigt.

Hinweis: Weitere Informationen zum Hinzufügen eines Cloud-Kontos finden Sie unter Hinzufügen eines Cloud-Kontos.

Komprimierung

Legt den Komprimierungstyp für die Dateikopiejobs fest.

Eine Komprimierung wird normalerweise durchgeführt, um den Speicherplatz am Dateikopierziel zu verringern, hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit Ihrer Dateikopie.

Hinweis: Bei komprimierten Dateikopiejobs zeigt das Aktivitätsprotokoll nur die unkomprimierte Größe an.

Es sind folgende Optionen verfügbar:

Standard-Komprimierung

Es wird eine Komprimierung bis zu einem gewissen Grad ausgeführt. Diese Option bietet ein Gleichgewicht zwischen CPU-Auslastung und erforderlichem Speicherplatz. Dies ist die Standardeinstellung.

Maximale Komprimierung

Es wird eine maximale Komprimierung durchgeführt. Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigsten Speicherplatzbedarf für Ihre Dateikopie.

Verschlüsselung aktivieren

Legt die Verschlüsselung für Dateikopie fest.

Bei der Datenverschlüsselung werden Daten in ein Format umgewandelt, das ohne den entsprechenden Entschlüsselungsmechanismus nicht verständlich ist. Arcserve UDP verwendet für den Datenschutz sichere AES-256-Verschlüsselungsalgorithmen (Advanced Encryption Standard), um größtmögliche Sicherheit und Datenschutz für Ihre angegebenen Daten zu erreichen. Wenn eine Verschlüsselung ausgewählt wird, müssen Sie ein Verschlüsselungskennwort angeben (und es bestätigen).

Hinweis: Wenn Sie ein Dateikopietask ändern, kann die Verschlüsselung oder Komprimierung nicht geändert werden.

Datei-Aufbewahrungszeit

Bewahrt die Dateien im Dateikopieziel auf, wenn die angegebenen Kriterien erfüllt sind.

Datei, erstellt innerhalb der letzten

Gibt die Länge der Zeit (Jahre, Monate, Tage) an, während der die gespeicherten Daten am Zielspeicherort aufbewahrt werden. Nach Ablauf der angegebenen Aufbewahrungszeit werden die gespeicherten Daten vom Ziel entfernt.

Wichtig! Nachdem die Daten am Ende der angegebenen Verweildauer vom Ziel gelöscht wurden, werden diese verschobenen Daten nicht weiter gespeichert.

Hinweis: Der Entfernungsvorgang der Aufbewahrungszeit wird nur ausgelöst, wenn die Option für den Dateikopieablaufplan aktiviert ist.

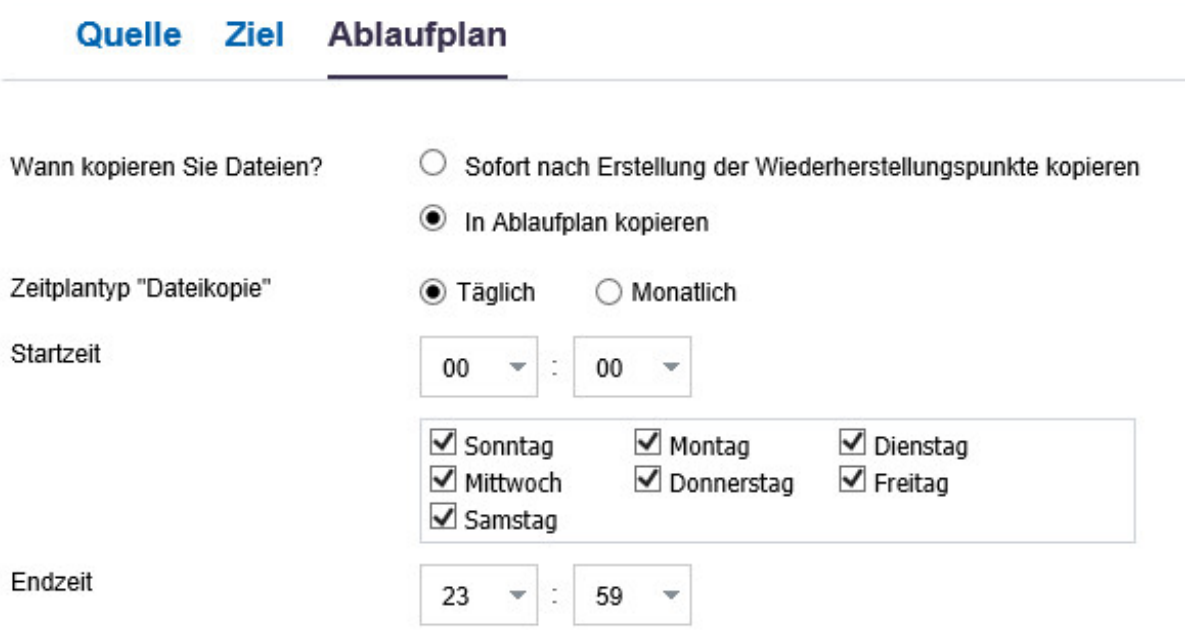
Dateiversion niedriger als

Gibt die Zahl der Kopien an, die am Zielspeicherort (Cloud oder Datenträger) aufbewahrt und gespeichert werden. Wenn diese Zahl überschritten wurde, wird die früheste (älteste) Version verworfen. Dieser Zyklus des Verwerfens der ältesten gespeicherten Version wiederholt sich jedes Mal, wenn neuere Versionen dem Ziel hinzugefügt werden, wodurch Sie immer die festgelegte Anzahl von gespeicherten Versionen aufbewahren können.

Wenn Ihre festgelegte Anzahl an aufzubewahrenden Dateiversionen beispielsweise auf 5 festgelegt ist und Sie zu den Zeiten t1, t2, t3, t4 und t5 fünf Dateikopien ausführen, werden diese fünf Kopien die aufbewahrten und zur Wiederherstellung verfügbaren Dateikopieversionen. Nachdem die sechste Dateikopie ausgeführt wurde (neue Version wird gespeichert), entfernt Arcserve UDP die t1-Kopie und die fünf zur Wiederherstellung verfügbaren Versionen werden zu t2, t3, t4, t5 und t6.

Standardmäßig beläuft sich die Zahl der vor der Beseitigung am Zielspeicherort aufbewahrten Dateien auf 15.

9. Klicken Sie auf die Registerkarte **Ablaufplan**, und geben Sie den Dateikopieablaufplan an.



Wenn nach dem Zeitpunkt für das Ende ein Kopiejob ausgeführt wird, wird der Job fortgesetzt, bis er abgeschlossen ist. Der nächste Dateikopiejob wird nicht ausgeführt, bis der vorherige Dateikopiejob abgeschlossen ist, auch wenn sich ein geplanter Job mit dem ausgeführten Job überschneidet.

Der Dateikopiejob wird gemäß dem Ablaufplan ausgeführt.

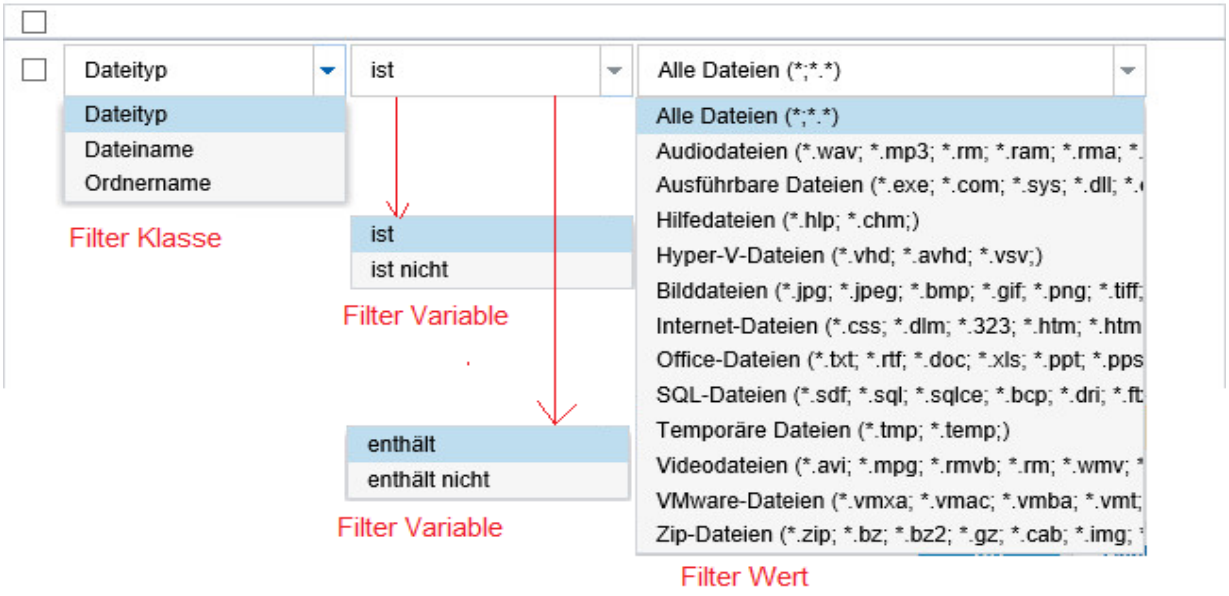
10. Klicken Sie auf **Speichern**.

    Die Änderungen werden gespeichert, und der Task zum Kopieren von Dateien wird automatisch auf dem Knoten bereitgestellt.

Hinzufügen von Dateikopiefiltern

Filter hinzufügen

Ermöglicht Ihnen das Hinzufügen eines Filters. Mit Filtern können Sie die zu kopierenden Objekte anhand bestimmter festgelegter Typen und Werte einschränken.



Filterkategorie

Es stehen drei Filterkategorien zur Verfügung: **Dateityp**, **Dateiname** und **Ordnername**. Die Felder "Filtervariable" und "Filterwert" ändern sich je nach Filterkategorie.

Filtervariable

Wird als Filterkategorie **Dateityp** ausgewählt, sind die Optionen für Filtervariablen **ist** und **ist nicht**. Wird als Filterkategorie **Dateiname oder Ordnername** ausgewählt, sind die Optionen für Filtervariablen **enthält** und **enthält nicht**.

Sie können mehrere Filter innerhalb der gleichen Dateikopieanforderung festlegen. Sie können auch die gleiche Filterkategorie aber eine andere Filtervariable angeben.

Hinweis: Wenn für die Filtervariable ein Konflikt im Hinblick auf die gleiche Filterkategorie besteht, haben die Variablen **ist nicht** oder **enthält nicht** immer eine höhere Priorität und werden durchgesetzt.

Filterwert

Der Filterwert lässt Sie die Informationen eingrenzen, die kopiert werden, dadurch dass nur die Parameterinformationen ausgewählt werden, die Sie festlegen, wie beispielsweise .txt-Dateien.

Arcserve UDP unterstützt die Verwendung von Platzhalterzeichen, die dabei helfen, mehrere Objekte auszuwählen, die mit einer einzelnen Anfrage kopiert werden. Ein Platzhalterzeichen ist ein Sonderzeichen, das als Ersatz benutzt werden kann, um entweder ein alleinstehendes Zeichen oder eine Zeichenfolge eines Textes darzustellen.

Die Platzhalterzeichen Sternchen (*) und Fragezeichen (?) werden im Wertefeld unterstützt. Wenn Ihnen der vollständige Datei- oder Ordnermustername nicht bekannt ist, können Sie die Ergebnisse des Filters vereinfachen, indem Sie ein Platzhalterzeichen angeben.

"*": Verwenden Sie das Sternchen, um null oder mehr Zeichen in dem Wert zu ersetzen.

"?" Verwenden Sie das Fragezeichen, um ein einzelnes Zeichen in dem Wert zu ersetzen.

Sie können beispielsweise "*.txt" eingeben, um alle Dateien auszuschließen, die eine ".txt" -Erweiterung haben, falls Sie den genauen Dateinamen nicht kennen. Sie können so viele Zeichen des Dateinamens angeben, wie Sie kennen, und die Platzhalter verwenden, um Leerstellen auszufüllen.

Hinweis: Wenn Sie **Dateityp** als Filtertyp auswählen, ist eine Drop-down-Liste mit vordefinierten Filtern für viele üblicherweise verwendete Dateien verfügbar (MS Office-Dateien, Bilddateien, ausführbare Dateien, temporäre Dateien usw.). Nachdem Sie einen der vordefinierten Filter ausgewählt haben, können Sie die entsprechenden Werte noch anhängen oder ändern.

Systemordner vor dem Überspringen schützen

Der Dateikopierauftrag überspringt standardmäßig die Systemordner, wenn der Auftrag auf den Volumes ausgeführt wird, die Systemordner enthalten. Um diese Ordner zu schützen und im Ziel zu kopieren, können Sie den Standardtext ändern, indem Sie einen Konfigurationseintrag hinzufügen.

Fügen Sie den folgenden XML-Tag-Eintrag zur Datei "FileCopyDebugSetting.xml" im Verzeichnis "$UDPHome\Engine\Configuration" hinzu:

Dateiname: FileCopyDebugSetting.xml

TagName: SkipWindowsFolders

Standardwert: 1

Um zu schützen, ändern Sie den Wert auf: 0

Hinweis: Diese Option ist nur auf den Dateikopierauftrag beschränkt. Dateiarchiv überspringt alle Systemordner, unabhängig vom konfigurierten TagValue.

Ausführen einer manuellen Dateikopie (optional)

In der Regel wird eine Dateikopie automatisch ausgeführt und durch die Dateikopie-Ablaufplan-Einstellungen gesteuert. Als Ergänzung zur geplanten Dateikopie können Sie wichtige Dateien durch manuelle Dateikopien bedarfsgerecht sichern.

Wenn Sie eine manuelle Dateikopie ausführen, wird der Dateikopiejob nur für die erste Sicherungssitzung ausgeführt, die für einen Dateikopiejob qualifiziert ist. (Sicherungssitzungen sind für eine Dateikopie nach Ablaufplan geeignet, und dann, wenn sich die Sitzungen in einer Warteschlange befinden. Wenn Sie beispielsweise festlegen, dass die Dateikopie für jede zweite Sicherung ausgeführt werden soll, ist nur jede zweite Sicherung für die Dateikopie qualifiziert und es sind nicht alle Sicherungen für die Dateikopie qualifiziert.) Nach Abschluss der Dateikopie wird die erste Sitzung entfernt, und die zweite Sitzung in der Reihe wird zur ersten Sitzung. Wenn es beispielsweise nur drei Sicherungssitzungen (S1, S2, S3) gibt und Sie eine manuelle Dateikopie ausführen, wird der Dateikopiejob nur für S1 ausgeführt. Der Dateikopiejob wird nicht für S2 und S3 ausgeführt. Wenn Sie den manuelle Dateikopiejob erneut ausführen, wird S2 kopiert.

Die Dateikopie kann in der Ansicht "Knoten" und der Ansicht "Pläne" per Klick auf das Menü **Aktionen** oder das Kontextmenü manuell ausgeführt werden.

Folgen Sie diesen Schritten, um die Dateikopie manuell in der Ansicht "Knoten" auszuführen:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Knoten werden im Hauptfenster angezeigt.
3. Wählen Sie die Knoten für einen Dateikopiejob aus. Den Knoten muss ein Dateikopieplan zugewiesen sein.
4. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Dateikopie jetzt**.

   Das Dialogfeld **Dateikopie jetzt ausführen** wird geöffnet.
5. Klicken Sie auf **OK**.

   Der Dateikopiejob wird ausgeführt.

   Die manuelle Dateikopie wurde erfolgreich ausgeführt.

Überprüfen des Plans

Um den Plan für die Dateikopie zu überprüfen, stellen Sie sicher, dass Sie den Plan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Nachdem der Sicherungsjob erfolgreich abgeschlossen wurde, wird der Dateikopiejob planmäßig ausgeführt. Sie können den Status des Sicherungsjobs und des Dateikopierjobs auf der Registerkarte **Jobs** überprüfen.

Folgen Sie diesen Schritten, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Führen Sie diese Schritte durch, um die Dateikopiejobs zu überprüfen:

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs vollständig**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Stellen Sie sicher, dass der Sicherungsjob und der Dateikopiejob erfolgreich ausgeführt wurden.

Erstellen eines Dateiarchivierungsplans

Mit Arcserve Unified Data Protection können Sie ausgewählte Quelldateien in einem Ziel archivieren. Bei dem Ziel kann es sich um ein Cloud-Konto oder ein freigegebenes Netzwerk handeln. Die Quelldatei muss zum selben Volume gehören, das Sie bereits gesichert haben. Beispielsweise haben Sie Volume D:\ Ihres Quellknotens vollständig gesichert. Jetzt kopieren Sie eine bestimmte Dateityp (z. B. .htm) aus Volume D:\ des Quellknotens. Nachdem Sie die Datei kopiert haben, löschen Sie diese Datei aus dem Quellknoten. Sie können einen Dateiarchivierungsplan erstellen, um diesen Vorgang auszuführen.

Ein Dateiarchiv ermöglicht es Ihnen, die Quelldaten sicher zu löschen, nachdem sie in ein Repository außerhalb des Standorts oder in ein sekundäres Speicher-Repository kopiert wurden.

Die Vorteile des Archivierens von Daten sind:

- Verbesserung der Leistungsfähigkeit: Hilft Ihnen, durch Archivieren unveränderter Daten Sicherungs- und Wiederherstellungsvorgänge zu beschleunigen und dadurch die Menge der wirklich zu sichernden und auf Band oder einem Datenträger zu speichernden Daten zu reduzieren.
- Einhaltung zwingender Compliance - Hilft Ihnen, wichtige Dokumente, E-Mails und andere entscheidende Daten je nach Notwendigkeit aufzubewahren, um den internen Richtlinien und externen Regelungen zu entsprechen.
- Reduzierung der Speicherkosten - Hilft Ihnen dabei, Speicherplatz zurückzugewinnen, indem Sie ältere oder weniger häufig verwendete Daten von Ihren Primärsystemen an kostengünstigere Archivspeicherorte migrieren können.
- Verwaltung mehrerer Dateiversionen - Hilft Ihnen, (im Bedarfsfall) auf vorherige Versionen gesicherter Dateien zurückzugreifen oder mehrere Versionen der gleichen Dateien an unterschiedlichen Zielen zu verwalten.

Der nächste Schritt?

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich bei der Konsole an.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Beachten Sie Folgendes:

- Der Dateiarchivierungsjob wird von der neuesten verfügbaren Sicherungssitzung ausgeführt.
- Der Dateiarchivierungsjob wird nur einmal pro Tag gemäß dem Ablaufplan ausgeführt.
- Der Job "Dateiarchiv löschen" wird als neuer Job zum Löschen der Quelldateien ausgeführt.
- Die folgende Tabelle enthält die Längenbeschränkung des Dateinamens für Dateiarchivierungsjobs. Die Dateien, die die entsprechende Länge überschreiten, werden übersprungen.

Ziel	Beschränkung
Netzwerkfreigabe	240
Cloud	245

Erstellen eines Plans mit einem Sicherungstask

Ein Plan umfasst verschiedene Arten von Tasks, die Sie ausführen möchten. Um einen Dateiarchivierungstask zu erstellen, müssen Sie zuerst einen gültigen Wiederherstellungspunkt haben. Um einen gültigen Wiederherstellungspunkt zu erhalten, müssen Sie einen Sicherungstask erstellen.

Ein Sicherungstask führt eine Sicherung der Quellknoten aus und speichert die Daten am angegebenen Ziel. Dateiarchiv wird nur für agentenbasierte Windows-Sicherungen unterstützt. Der folgende Vorgang beschreibt die Schritte zur Erstellung des agentenbasierten Windows-Sicherungstasks.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

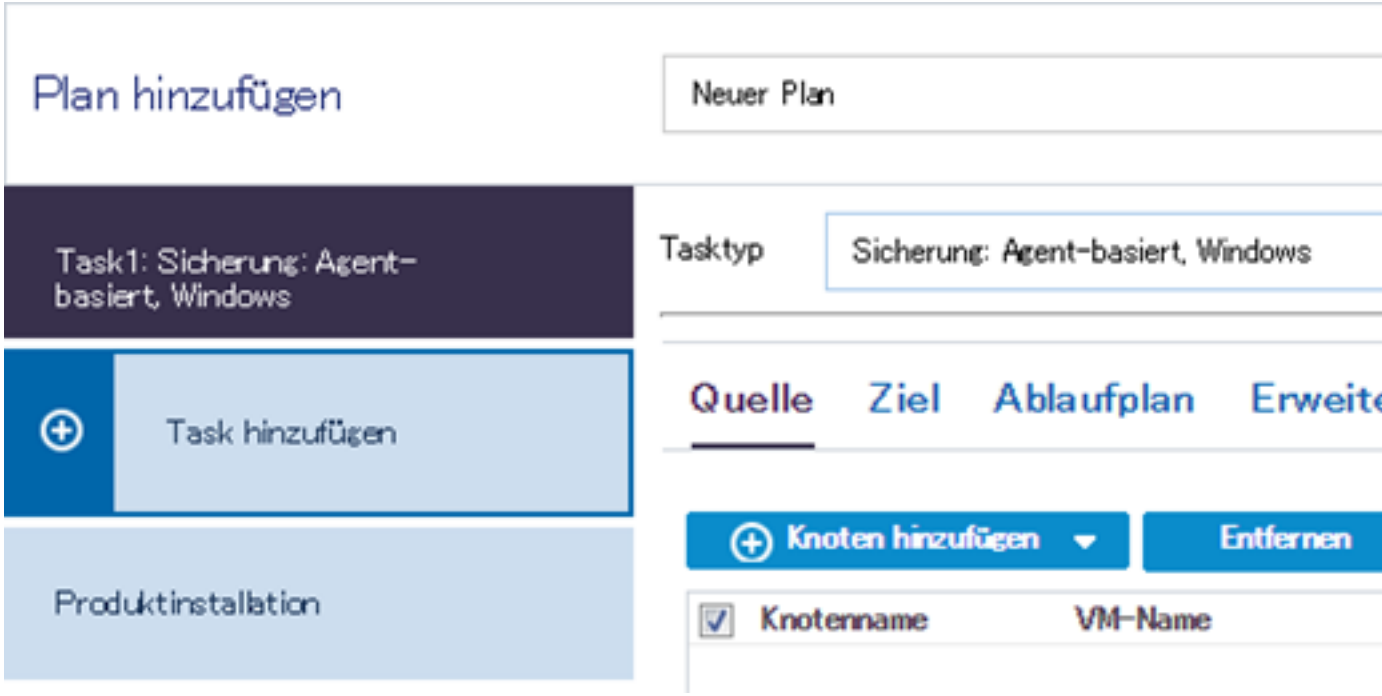
   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Sicherung, Agent-basiertes**

Windows aus.



Geben Sie nun Einstellungen für "Quelle", "Ziel", "Ablaufplan" und "Erweitert" an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die Quellknoten angeben, die Sie schützen möchten. Sie können mehrere Knoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Knoten hinzufügen, wenn Sie einen Plan auf der Quellenseite erstellen oder ändern. Sie können einen Plan auch speichern, ohne Quellknoten hinzuzufügen. Der Plan wird erst bereitgestellt, wenn Sie Quellknoten hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Quelle" auf **Hinzufügen**.
2. Wählen Sie eine der folgenden Optionen:

   Wählen Sie zu sichernden Knoten in Arcserve UDP aus

   Öffnet das Dialogfeld "Wählen Sie zu sichernden Knoten in Arcserve UDP aus". Wählen Sie die Knoten in der angezeigten Liste aus. Wählen Sie diese Option aus, wenn Sie die Knoten bereits zu der Konsole hinzugefügt haben.

   Windows-Knoten hinzufügen

   Öffnet das Dialogfeld "Knoten zu Plan hinzufügen". Wählen Sie diese Option aus, wenn Sie die Knoten nicht hinzugefügt haben und Sie die zu schützenden Knoten manuell hinzufügen möchten.

   Knoten aus Active Directory erkennen

   Öffnet das Dialogfeld Knoten zu Arcserve UDP-Konsole hinzufügen. Wählen Sie diese Option, wenn Sie Knoten aus Active Directory erkennen und hinzufügen möchten.

3. Wenn Sie die Option **Wählen Sie zu sichernden Knoten in Arcserve UDP aus** ausgewählt haben, gehen Sie im Dialogfeld "Zu schützende Knoten auswählen" folgendermaßen vor:

   a. (Optional) Wählen Sie einen Filter aus der Dropdown-Liste "Gruppen" aus, um nach Knoten zu filtern. Sie können Schlüsselwörter eingeben, um den Knotenfilter weiter einzuschränken.

      Die Knoten werden in der Spalte "Verfügbare Knoten" angezeigt.

   b. Wählen Sie die Knoten aus der Spalte "Verfügbare Knoten" aus, und klicken Sie dann auf den einfachen Nach-rechts-Pfeil (>) oder den doppelten Nach-rechts-Pfeil (>>), um die ausgewählten Knoten bzw. alle Knoten in die Spalte "Ausgewählte Knoten" zu verschieben.

Die Knoten werden in der Spalte "Ausgewählte Knoten" angezeigt.

c. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

4. Wählen Sie zum Festlegen des Schutztyps eine der folgenden Optionen aus:

Alle Volumes sichern

Bereitet einen Sicherungs-Snapshot aller Volumes vor.

Ausgewählte Volumes sichern

Bereitet einen Sicherungs-Snapshot des ausgewählten Volumes vor.

Die Sicherungsquelle ist nun angegeben.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Wählen Sie einen der folgenden **Zieltypen** aus:

   Lokaler Datenträger oder freigegebener Ordner

   Gibt an, dass das Sicherungsziel ein lokales Ziel oder ein freigegebener Ordner ist. Wenn Sie diese Option auswählen, können Sie Daten als Wiederherstellungspunkte oder Wiederherstellungssätze speichern. Die Optionen für Wiederherstellungspunkte und Wiederherstellungssätze sind auf der Registerkarte **Ablaufplan** verfügbar.

   Arcserve UDP-Recovery Point Server

   Gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.

2. Wenn Sie **Arcserve UDP-Recovery Point Server** ausgewählt haben, geben Sie folgende Details an:
   a. Wählen Sie einen Recovery Point Server aus.
   b. Wählen Sie einen Datenspeicher aus. Die Liste enthält alle Datenspeicher, die am angegebenen Recovery Point Server erstellt wurden.
   c. Geben Sie ein Sitzungskennwort ein.
   d. Bestätigen Sie das Sitzungskennwort.
3. Wenn Sie **Lokaler Datenträger oder freigegebener Ordner** ausgewählt haben, geben Sie folgende Details an:
   a. Geben Sie den vollständigen Pfad des lokalen Ziels oder Netzwerkziels an. Geben Sie für das Netzwerkziel Anmeldeinformationen für ein Konto mit Schreibzugriff an.
   b. Wählen Sie den Verschlüsselungsalgorithmus aus. Weitere Informationen finden Sie unter Verschlüsselungseinstellungen.
   c. Geben Sie optional ein Verschlüsselungskennwort an.
   d. Bestätigen Sie das Verschlüsselungskennwort.

e. Wählen Sie einen Komprimierungstyp aus. Weitere Informationen finden Sie unter "Komprimierungstyp".

Hinweis: Wenn Sie die Daten auf einem lokalen Datenträger oder in einem freigegebenen Ordner speichern, können Sie die Daten nicht auf einem anderen Recovery Point Server replizieren. Die Replikation wird nur unterstützt, wenn Sie die Daten auf einem Recovery Point Server speichern.

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

Gehen Sie wie folgt vor:

1. (Optional) Wählen Sie die Option für die Verwaltung von Wiederherstellungspunkten aus. Diese Option ist nur sichtbar, wenn Sie als Sicherungsziel "Lokaler oder freigegebener Ordner" ausgewählt haben.

   Nach Wiederherstellungspunkten aufbewahren

   Die Sicherungsdaten werden als Wiederherstellungspunkte gespeichert.

   Nach Wiederherstellungssätzen aufbewahren

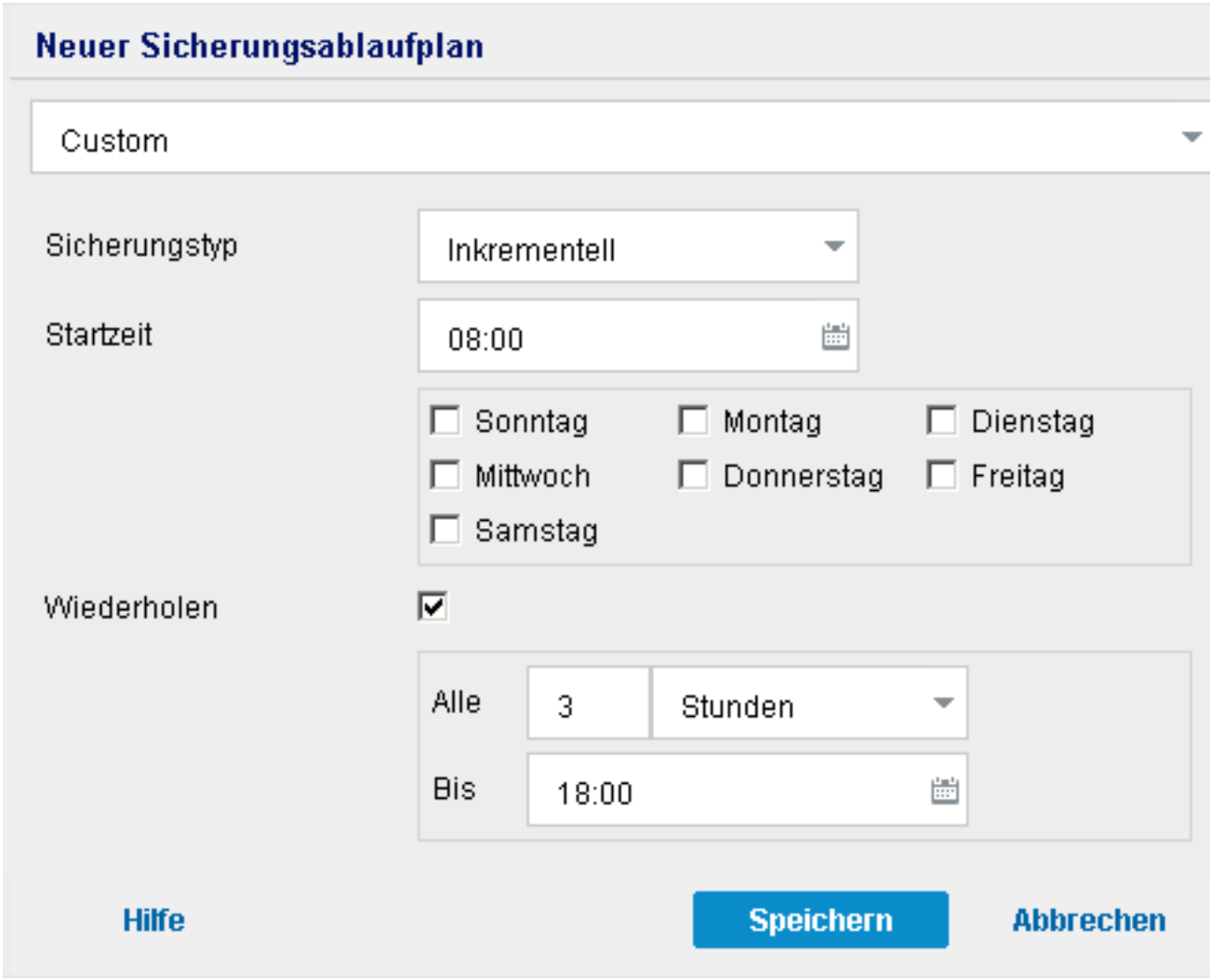
   Die Sicherungsdaten werden als Wiederherstellungssätze gespeichert.

2. Fügen Sie Ablaufpläne für Sicherungen, Zusammenführungen und Drosselungsvorgänge hinzu.

   Hinzufügen eines Sicherungsablaufplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Überprüfen

Legt den Ablaufplan für Überprüfungssicherungen fest.

Arcserve UDP überprüft die Gültigkeit und Vollständigkeit der geschützten Daten durch einen Vergleich des gespeicherten Sicherungs-Images mit der Sicherungsquelle. Im Bedarfsfall wird das Image neu synchronisiert. Bei einer Überprüfungssicherung wird die letzte Sicherung jedes einzelnen Blocks mit den Inhalten und Informationen der Quelle verglichen. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht (zumeist aufgrund von Änderungen seit der letzten Sicherung), aktualisiert Arcserve UDP die Sicherung dieses Blocks (Neusynchronisierung). In seltenen Fällen kann eine Überprüfungssicherung auch durchgeführt werden, um eine vollständige Sicherung zu erhalten, ohne den erforderlichen Speicherplatz einer vollständigen Sicherung zu verwenden.

Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.

Nachteile: Die Sicherung benötigt viel Zeit, da alle Quellenblöcke mit den Blöcken der letzten Sicherung verglichen werden.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die seit der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf Hinzufügen, und wählen Sie Zusammenführungsplan hinzufügen aus.

Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

b. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

d. Klicken Sie auf **Speichern**.

Der Zusammenführungsablaufplan ist auf der Seite **Ablaufplan** angegeben und wird dort angezeigt.

Hinzufügen eines Drosselungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

Das Dialogfeld Drosselungsplan hinzufügen wird geöffnet.

b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

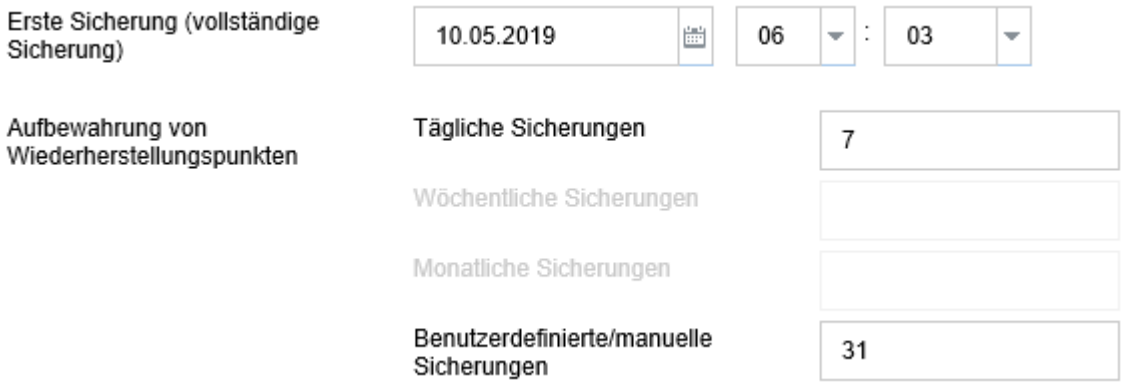
c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Drosselungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

3. Geben Sie die Startzeit für die geplante Sicherung an.



4. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld "Sicherungsablaufplan" übernommen.

5. Geben Sie die Katalogdetails an.

   Mit Katalogen können Sie den Dateisystemkatalog generieren. Der Dateisystemkatalog ist erforderlich, um schnellere und bessere Suchvorgänge auszuführen. Wenn Sie die Kontrollkästchen für den Katalog aktivieren, werden die Kataloge je nach der Sicherungsart, die Sie angegeben haben, aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Kataloggenerierung zu deaktivieren.

   Der Ablaufplan ist nun angegeben.

Funktionsweise der erweiterten Planung und Aufbewahrung

Mit der Ablaufplanoption können Sie einen benutzerdefinierten Ablaufplan, einen Ablaufplan für tägliche/wöchentliche/monatliche Sicherungen oder beides festlegen. Im benutzerdefinierten Ablaufplan können Sie den Sicherungsablaufplan für jeden Tag der Woche konfigurieren und bis zu vier Sicherungsablaufpläne für jeden Tag hinzufügen. Sie können einen bestimmten Wochentag auswählen und ein Zeitfenster erstellen, um anzugeben, wann und wie oft die Sicherung durchgeführt werden soll.

Ablaufplan	Unterstützter Job	Kommentare
Sichern	Sicherungsjob	Gibt Zeitfenster für die Ausführung von Sicherungsjobs an.
Sicherungsdrosselung	Sicherungsjob	Gibt die Zeitfenster an, um die Sicherungsgeschwindigkeit zu steuern.
Zusammenführen	Zusammenführungsjob	Gibt an, wann Zusammenführungsjobs ausgeführt werden sollen.
Täglicher Ablaufplan	Sicherungsjob	Gibt an, wann tägliche Sicherungsjobs ausgeführt werden sollen.
Wöchentlicher Ablaufplan	Sicherungsjob	Gibt an, wann wöchentliche Sicherungsjobs ausgeführt werden sollen.
Monatlicher Ablaufplan	Sicherungsjob	Gibt an, wann monatliche Sicherungsjobs ausgeführt werden sollen.

Sie können auch die Aufbewahrungseinstellungen für die Wiederherstellungspunkte angeben.

Hinweis: Legen Sie innerhalb der einzelnen Pläne Einstellungen für die Aufbewahrungszeit fest, um zu steuern, wie die Daten für die Knoten des entsprechenden Plans im Zieldatenspeicher aufbewahrt werden.

Ablaufpläne für tägliche/wöchentliche/monatliche Sicherungen sind vom benutzerdefinierten Ablaufplan und voneinander unabhängig. Sie können die Ausführung einer täglichen, wöchentlichen oder monatlichen Sicherung konfigurieren, ohne einen benutzerdefinierten Ablaufplan zu konfigurieren.

Jobplan der Sicherung

Sie können vier Zeitfenster pro Tag in Ihrem Sicherungsablaufplan hinzufügen. Ein gültiges Zeitfenster liegt im Bereich 12:00 Uhr bis 23:59 Uhr. Sie können kein Zeitfenster wie z. B. 18:00 Uhr bis 06:00 Uhr angeben. In solchen Fällen müssen Sie manuell zwei verschiedene Zeitfenster angeben.

Für jedes Zeitfenster wird die Startzeit einbezogen, und die Endzeit wird nicht einbezogen. Zum Beispiel haben Sie das Ausführen einer Zuwachssicherung konfiguriert, die stündlich zwischen 06:00 Uhr und 09:00 Uhr stattfinden soll, und die Sicherung wird um 06:00 Uhr gestartet. Das bedeutet, dass die Sicherung um 06:00 Uhr, 07:00 Uhr und 08:00 Uhr ausgeführt wird, NICHT aber um 09:00 Uhr.

Hinweis: Wenn Sie die Sicherung bis zum Ende des Tages wiederholt ausführen möchten, legen Sie den Ablaufplan bis 12:00 Uhr fest. Um den Sicherungsjob beispielsweise alle 15 Minuten während des gesamten Tages auszuführen, legen Sie den Ablaufplan von 00:00 Uhr bis 00:00 Uhr alle 15 Minuten fest.

Drosselungsplan der Sicherung

Mit dem Drosselungsplan der Sicherung können Sie die Geschwindigkeit des Sicherungsdurchsatzes steuern, die wiederum die Ressourcenverwendung (Datenträger-E/A, CPU, Netzwerkbandbreite) des Servers, der gesichert wird, steuert. Dies ist hilfreich, wenn die Serverleistung während der Geschäftszeiten nicht beeinträchtigt werden soll. Sie können vier Zeitfenster pro Tag in Ihrem Drosselungsplan der Sicherung hinzufügen. Für jedes Zeitfenster können Sie einen Wert in MB pro Minute angeben. Dieser Wert wird verwendet, um den Sicherungsdurchsatz zu steuern. Gültige Werte liegen im Bereich zwischen 1 MB/Minute bis 99.999 MB/Minute.

Wenn ein Sicherungsjob die angegebene Zeit überschreitet, dann wird das Drosselungslimit entsprechend dem angegebenen Zeitfenster angepasst. Zum Beispiel haben Sie als Drosselungslimit der Sicherung den Wert 500 MB/Minute von 08:00 Uhr bis 20:00 Uhr und 2500 MB/Minute von 20:00 Uhr bis 22:00 Uhr angegeben. Wenn ein Sicherungsjob um 19:00 Uhr startet und drei Stunden ausgeführt wird, dann hat das Drosselungslimit von 19:00 Uhr bis 20:00 Uhr den Wert 500 MB/Minute. Von 20:00 Uhr bis 22:00 Uhr hat das Drosselungslimit den Wert 2.500 MB/Minute.

Wenn Sie keinen Sicherungsablaufplan und keinen Ablaufplan für den Sicherungsdurchsatz angeben, dann wird die Sicherung so schnell wie möglich ausgeführt.

Ablaufplan für Zusammenführung

Ermöglicht es Ihnen, Wiederherstellungspunkte basierend auf dem angegebenen Ablaufplan zusammenzuführen.

Beachten Sie folgende Punkte für den Zusammenführungsjob:

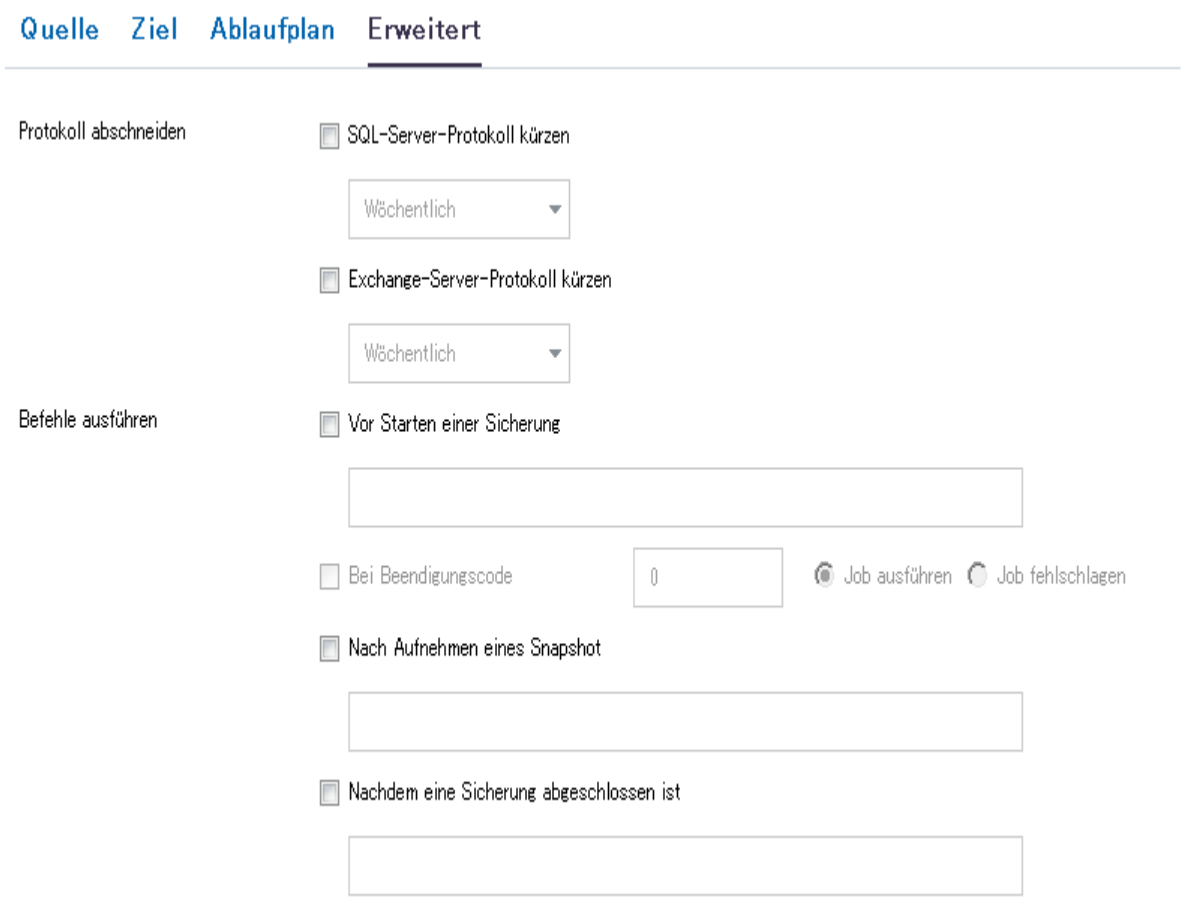
- Es kann immer nur ein Zusammenführungsjob für einen Knoten ausgeführt werden.

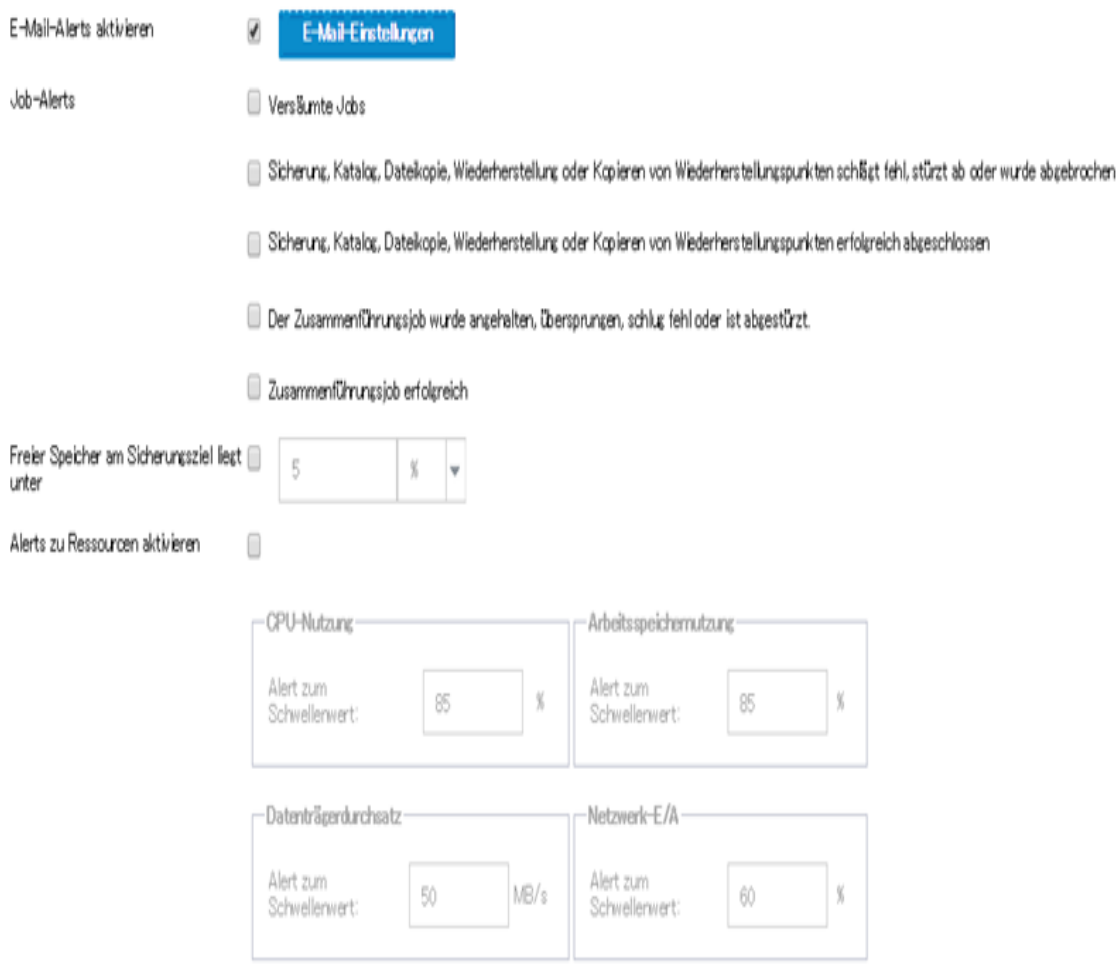
- Wenn ein Zusammenführungsjob gestartet wird, muss er abgeschlossen werden, bevor der nächste Zusammenführungsjob gestartet werden kann. Das bedeutet: Wenn ein oder mehrere Sätze an Wiederherstellungspunkten zusammengeführt werden, dann kann der neue Wiederherstellungspunkt nicht zu diesem Zusammenführungsprozess hinzugefügt werden, bis der Zusammenführungsprozess für den aktuellen Satz an Wiederherstellungspunkten abgeschlossen ist.
- Wenn ein Zusammenführungsjob mehr als einen Satz an Wiederherstellungspunkten bearbeitet (zum Beispiel Satz [1~4], Satz [5~11] und Satz [12~14], also drei Sätze), dann werden diese Sätze nacheinander vom Recovery Point Server bearbeitet.
- Wenn ein Zusammenführungsjob nach einer Pause fortgesetzt wird, erkennt der Job an welchem Punkt er unterbrochen wurde, und die Zusammenführung wird ab der Abbruchstelle fortgesetzt.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen die Einstellungen zum Abschneiden von Protokollen, das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte "Erweitert":





Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

Protokoll abschneiden

Ermöglicht es Ihnen, den Ablaufplan anzugeben, um Protokolle für SQL Server und Exchange Server zu kürzen. Sie können den Ablaufplan als **Täglich**, **Wöchentlich** oder **Monatlich** angeben.

Benutzername

Ermöglicht es Ihnen, den Benutzer anzugeben, der zur Ausführung eines Skripts autorisiert ist.

Kennwort

Ermöglicht es Ihnen, das Kennwort des Benutzers anzugeben, der zur Ausführung des Skripts autorisiert ist.

Befehl ausführen, bevor eine Sicherung gestartet wird

Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, in dem das Skript gespeichert wird. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem ein Snapshot aufgenommen wurde

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungs-Snapshot aufgenommen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Arten der Alerts angeben, die Sie in Form von E-Mails empfangen möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers.

Job-Alerts

Ermöglicht es Ihnen, die Typen der Job-E-Mails auszuwählen, die Sie erhalten möchten.

Warnmeldungen zu Ressourcen aktivieren

Ermöglicht es Ihnen, einen Schwellenwert für CPU-Auslastung, Speicherverwendung, Datenträgerdurchsatz, Netzwerk-E/A anzugeben. Sie können den Wert in Prozent angeben. Sie erhalten eine E-Mail, wenn der Wert "Warnmeldung zum Schwellenwert" überschritten ist.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Knoten installiert ist und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung

an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agenten oder kein Agent installiert ist. Um den Agenten auf diesen Knoten zu installieren bzw. um ein Upgrade des Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus, und klicken Sie auf "Speichern".

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie eine andere Task hinzufügen müssen, müssen Sie den Plan aus der Registerkarte **Ressourcen** auswählen und den Plan ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern.

Der Sicherungsplan wird erstellt und automatisch für den Quellknoten bereitgestellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

Hinzufügen eines Dateiarchivierungstasks zum Plan

Der Dateiarchivierungstask ermöglicht es Ihnen, individuelle Dateien am angegebenen Ziel zu archivieren. Die ursprünglichen Dateien werden aus der Quelle gelöscht, nachdem Sie die Dateien in das angegebene Ziel kopiert haben, wodurch mehr freier Speicherplatz auf der Quelle verfügbar wird. Der Dateiarchivjob ist von keinem Katalogjob abhängig.

Hinweis: Wenn ein Sicherungsjob ausgeführt wird und Sie den Plan unterbrechen, wird der Sicherungsjob abgebrochen, und der Dateiarchivierungsjob wird nicht gestartet. Wenn Sie den Plan wieder aufnehmen, wird der Dateiarchivjob nicht automatisch fortgesetzt. Sie müssen einen anderen Sicherungsjob manuell ausführen, um den Dateiarchivjob zu starten.

Für Dateien, die unter Verwendung von "Dateiarchiv" kopiert werden, hinterlässt Arcserve UDP eine Stub-Datei mit der Erweiterung "UDP.txt". Weitere Informationen zum Aktualisieren der Stub-Datei finden Sie im Abschnitt Aktualisieren von Stub-Dateien.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Fensterbereich auf **Task hinzufügen**.

   Ein neuer Task wird im linken Fensterbereich hinzugefügt.

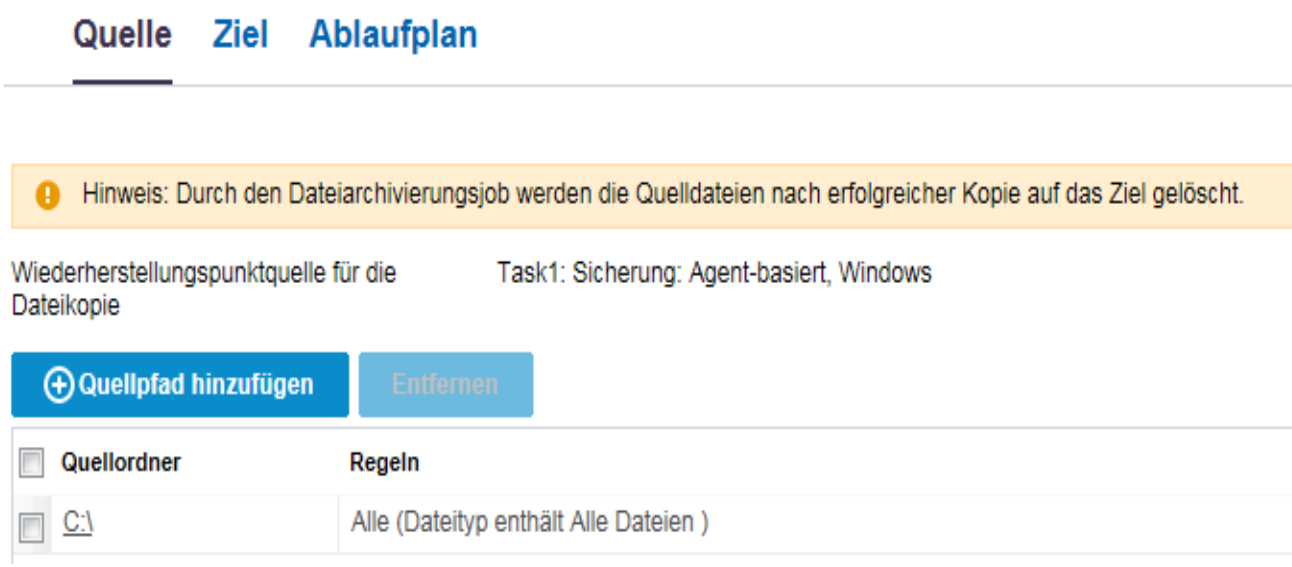
2. Wählen Sie im Drop-down-Menü **Tasktyp** die Option **Dateiarchivierung** aus.

   Der Dateiarchivierungstask wird hinzugefügt.

3. Klicken Sie auf die Registerkarte **Quelle**, und geben Sie die Details ein.

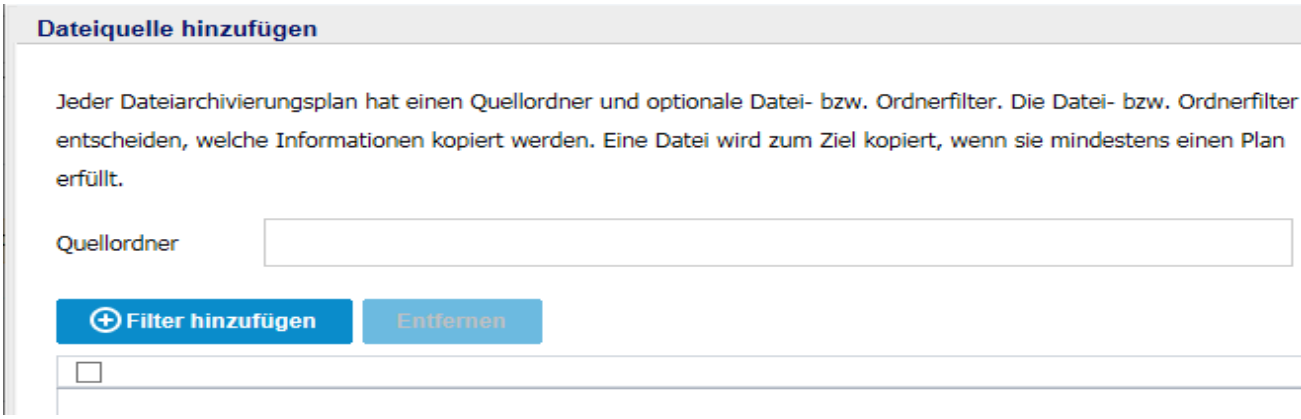
   Speicherort des Wiederherstellungspunkts

   Gibt den Speicherort der Wiederherstellungspunkte an, die archiviert werden. Dieses Feld ist vorab ausgewählt.

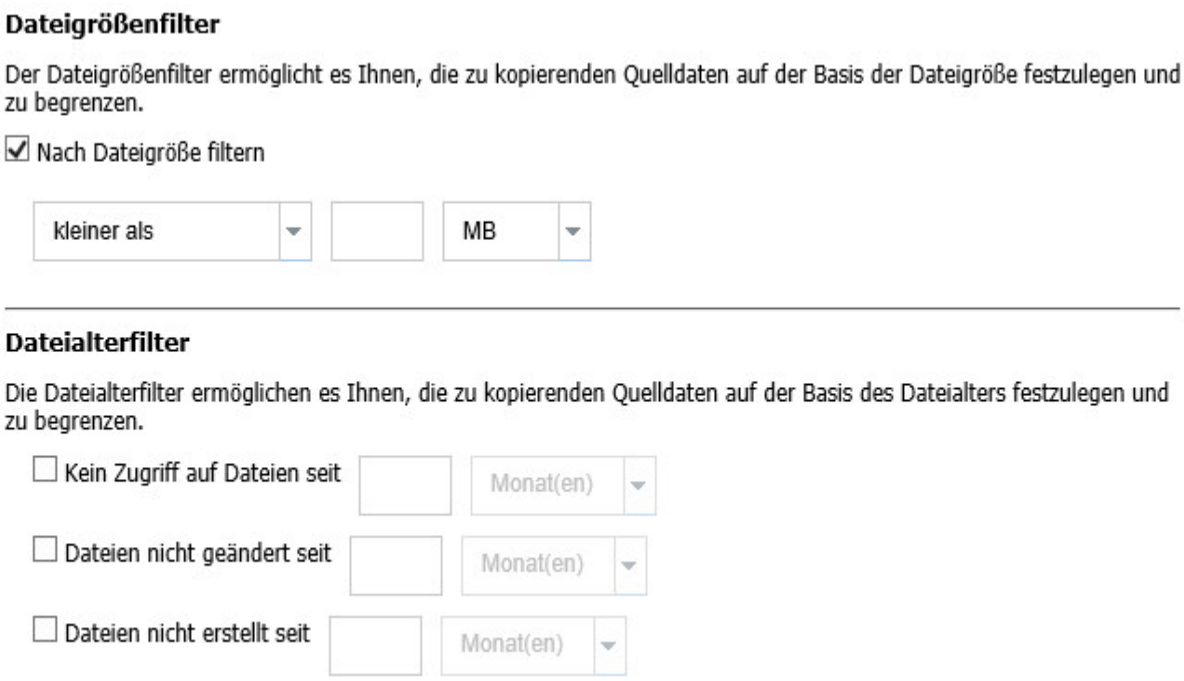


4. Klicken Sie auf **Quelle hinzufügen**.

   Das Dialogfeld **Dateiquelle hinzufügen** wird geöffnet.

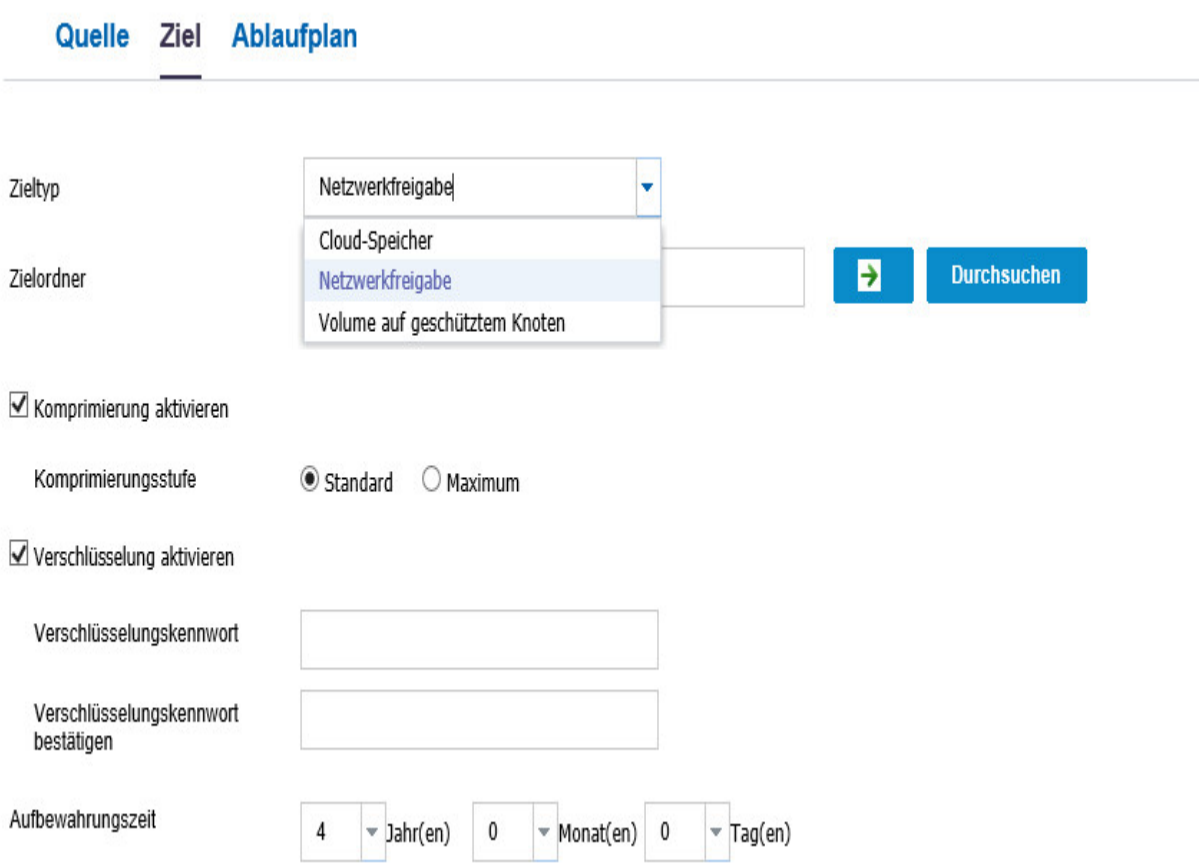


5. Geben Sie den Dateipfad des Quellpfads ein, den Sie kopieren möchten.
6. Geben Sie den **Dateigrößenfilter** und den **Dateialterfilter** an.



7. Klicken Sie auf **Filter hinzufügen**.
8. Wählen Sie den Filter aus der Liste aus, und klicken Sie auf **Anwenden**.
9. Klicken Sie auf **OK**.

   Das Dialogfeld **Dateiquelle hinzufügen** wird geschlossen.
10. Klicken Sie auf die Registerkarte **Ziele**, und geben Sie die Zieldetails an.



Zieltyp

Gibt an, dass die Zieltypen eine Netzwerkfreigabe oder ein Cloud-Speicher sind. Falls die Verbindung zum angegebenen Ziel verloren ging oder unterbrochen wurde, versucht Arcserve UDP für jede Zieloption einige Male, mit dem Dateikopiejob fortzufahren. Falls diese Neuversuche nicht erfolgreich sind, wird ein Ergänzungsjob von dem Punkt aus ausgeführt werden, an dem der Fehler auftrat. Zusätzlich wird das Aktivitätsprotokoll mit einer entsprechenden Fehlermeldung aktualisiert, und es wird eine E-Mail-Benachrichtigung gesendet (falls konfiguriert).

Netzwerkfreigabe

Gibt an, dass das Ziel ein freigegebener Ordner ist. Wenn diese Option ausgewählt ist, können Sie den vollständigen Pfad des Speicherorts angeben, an den Sie Ihre Quelldateien/-ordner verschieben wollen.

Zielordner

Gibt das Ziel an, an dem die archivierten Dateien gespeichert werden. Ziele können lokale Volumes, Ordner oder Dateifreigaben sein, auf die über einen UNC-Pfad (Uniform Naming Convention) zugegriffen werden kann. Dieses Feld ist ver-

fügbar, wenn Sie als Zieltyp "Netzwerkfreigabe" oder "Volume" auf einem geschützten Knoten auswählen. Sie können auch den Zielordner durchsuchen.

Cloud-Speicher

Gibt an, dass die kopierten Dateien in einer Cloud-Umgebung gespeichert werden. Arcserve UDP unterstützt derzeit das Kopieren von Dateien an mehrere Cloud-Anbieter, wie Amazon S3 (Simple Storage Service), Amazon S3-kompatibel, Windows Azure, Windows Azure-kompatibel, Eucalyptus-Walrus und FUJITSU Hybrid IT Service FJcloud-O. Diese Cloud-Anbieter sind öffentlich verfügbare Webdienste, mit denen Sie jederzeit und von überall im Internet eine beliebige Datenmenge in einer sicheren Umgebung speichern und abrufen können.

Hinweis: Um einen potenziellen Uhrabweichungsfehler zu beheben, wenn Sie versuchen, eine Verbindung zur Cloud herzustellen, sollten Sie sicherstellen, dass bei Ihrem Rechner die richtige Zeitzone eingestellt ist und die Uhr synchron zur globalen Zeit ist. Sie sollten die Zeit Ihres Rechners immer mit der GMT-Zeit abgleichen. Wenn die Uhrzeit Ihres Rechners nicht mit der korrekten globalen Uhrzeit (auf 5 bis 10 Minuten) synchronisiert ist, wird Ihre Cloud-Verbindung möglicherweise nicht funktionieren. Stellen Sie gegebenenfalls die richtige Zeit für Ihren Rechner ein, und wiederholen Sie Ihren Dateikopierjob.

Speichergeräte

Wählen Sie den Gerätetyp aus der Drop-down-Liste aus.

Cloud-Speicher

Wählen Sie den Pfad des Cloud-Speichers aus der Drop-down-Liste aus. Die Drop-down-Liste ist verfügbar, wenn Sie die Details Ihres Cloud-Speichers angegeben haben. Wenn Sie zum ersten Mal das Cloud-Speicherkonto angeben, klicken Sie auf "Hinzufügen", um Ihr Cloud-Konto hinzuzufügen. Wenn Sie das nächste Mal Cloud-Speicher auswählen, wird das Konto in der Cloud-Speicher-Drop-down-Liste angezeigt.

Hinweis: Weitere Informationen zum Hinzufügen eines Cloud-Kontos finden Sie unter Hinzufügen eines Cloud-Kontos.

Komprimierung

Legt den Komprimierungstyp für die Dateiarchivierungsjobs fest.

Eine Komprimierung wird normalerweise durchgeführt, um den Speicherplatz am Dateiarchivierungsziel zu verringern, hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit Ihrer Dateiarchivierung.

Hinweis: Bei einem komprimierten Dateiarchivierungsjob zeigt das Aktivitätsprotokoll nur die unkomprimierte Größe an.

Es sind folgende Optionen verfügbar:

Standard-Komprimierung

Es wird eine Komprimierung bis zu einem gewissen Grad ausgeführt. Diese Option bietet ein Gleichgewicht zwischen CPU-Auslastung und erforderlichem Speicherplatz. Dies ist die Standardeinstellung.

Maximale Komprimierung

Es wird eine maximale Komprimierung durchgeführt. Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigsten Speicherplatzbedarf für Ihre Dateikopie.

Verschlüsselung aktivieren

Legt die Verschlüsselung für Dateiarchivierung fest.

Bei der Datenverschlüsselung werden Daten in ein Format umgewandelt, das ohne den entsprechenden Entschlüsselungsmechanismus nicht verständlich ist. Arcserve UDP verwendet für den Datenschutz sichere AES-256-Verschlüsselungsalgorithmen (Advanced Encryption Standard), um größtmögliche Sicherheit und Datenschutz für Ihre angegebenen Daten zu erreichen. Wenn eine Verschlüsselung ausgewählt wird, müssen Sie ein Verschlüsselungskennwort angeben (und es bestätigen).

Aufbewahrungszeit

Gibt die Länge der Zeit (Jahre, Monate, Tage) an, während der die gespeicherten Daten am Zielspeicherort aufbewahrt werden. Nach Ablauf der angegebenen Aufbewahrungszeit werden die gespeicherten Daten vom Ziel entfernt.

Bei den Berechnungen der Aufbewahrungszeit wird davon ausgegangen, dass ein Monat 30 Tage und ein Jahr 365 Tage hat. Beispiel: Wenn Sie eine Aufbewahrungszeit von 2 Jahren, 2 Monaten und 5 Tagen festlegen, beläuft sich die gesamte Aufbewahrungszeit für Ihre kopierten Daten auf 795 Tage (365 + 365 + 30 + 30 + 5).

Wichtig! Nachdem die Daten am Ende der angegebenen Verweildauer vom Ziel gelöscht werden, werden diese verschobenen Daten nicht weiter gespeichert.

Hinweis: Der Entfernungsvorgang der Aufbewahrungszeit wird nur ausgelöst, wenn die Option für den Dateikopieablaufplan aktiviert ist.

Dateiversion niedriger als

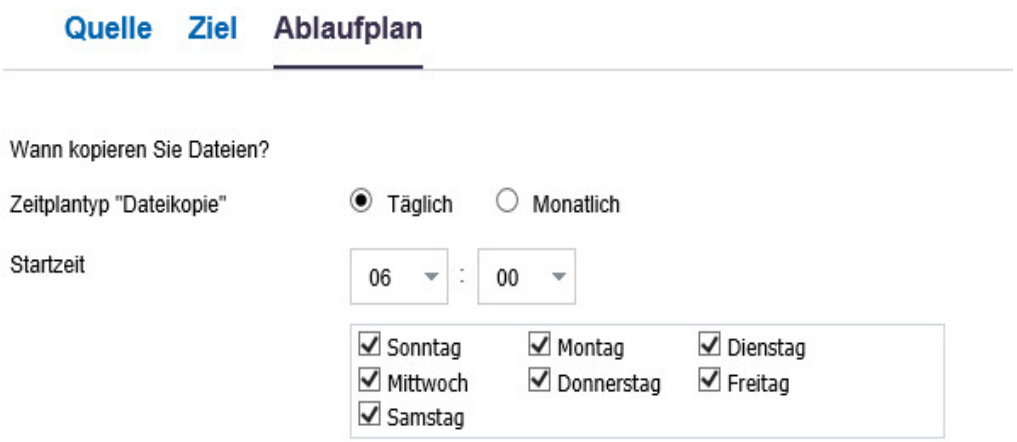
Diese Einstellung bezieht sich nur auf kopierte Daten, die aufbewahrt werden (nicht auf kopierte Daten, die verschoben werden).

Sie gibt die Zahl der Kopien an, die aufbewahrt und am Zielspeicherort (Cloud oder Datenträger) gespeichert werden. Wenn diese Zahl überschritten wurde, wird die früheste (älteste) Version verworfen. Dieser Zyklus des Verwerfens der ältesten gespeicherten Version wiederholt sich jedes Mal, wenn neuere Versionen dem Ziel hinzugefügt werden, wodurch Sie immer die festgelegte Anzahl von gespeicherten Versionen aufbewahren können.

Wenn Ihre festgelegte Anzahl an aufzubewahrenden Dateiversionen beispielsweise auf 5 festgelegt ist und Sie zu den Zeiten t1, t2, t3, t4 und t5 fünf Dateikopien ausführen, werden diese fünf Kopien die aufbewahrten und zur Wiederherstellung verfügbaren Dateikopieversionen. Nachdem die sechste Dateikopie durchgeführt wurde (die neue Version wurde gespeichert), entfernt Arcserve UDP die t1-Kopie und die fünf verfügbaren Versionen für die Wiederherstellung sind nun t2, t3, t4, t5 und t6.

Standardmäßig beläuft sich die Zahl der vor der Beseitigung am Zielspeicherort aufbewahrten Dateien auf 15.

11. Klicken Sie auf die Registerkarte **Ablaufplan**, und legen Sie den benötigten Ablaufplan für den Job fest.



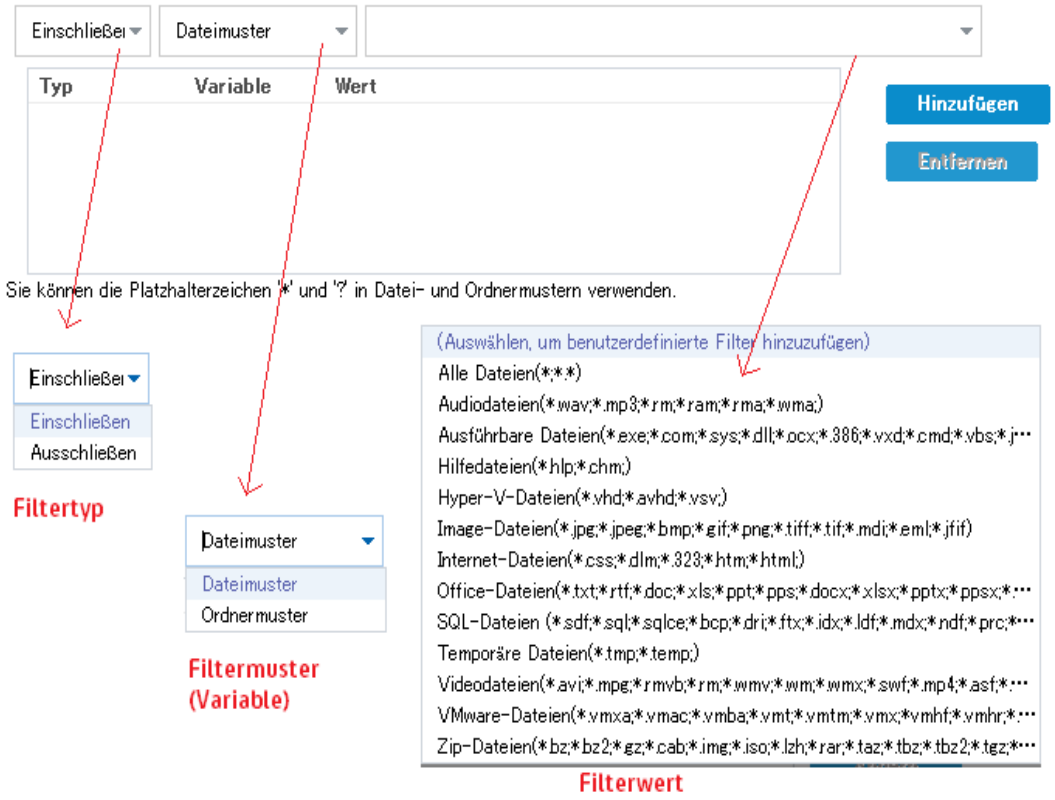
12. Klicken Sie auf **Speichern**.

Die Änderungen werden gespeichert, und der Task zum Archivieren von Dateien wird automatisch auf dem Knoten bereitgestellt.

Hinzufügen von Dateiarchivfiltern

Filter hinzufügen

Ermöglicht Ihnen das Hinzufügen eines Filters. Mit Filtern können Sie die zu kopierenden Objekte anhand bestimmter festgelegter Typen und Werte einschränken.



Filtertyp

Es gibt zwei Arten von Filtern: Einschließfilter und Ausschließfilter.

Ein Einschließfilter kopiert nur diejenigen Objekte der Dateikopiequelle, die mit den angegebenen Werten übereinstimmen.

Ein Ausschlussfilter kopiert alle Objekte der Dateikopiequelle, außer denen, die mit den angegebenen Werten übereinstimmen.

Sie können innerhalb einer Dateikopieanforderung mehrere Filter festlegen, indem Sie jeden Filterwert mit einem Komma abtrennen.

- Wenn Sie mehrere Einschließfilter festlegen, werden die Daten in die Dateikopie aufgenommen, wenn einer dieser Einschließfilter eine Übereinstimmung erzeugt.

- Wenn Sie mehrere Ausschlussfilter festlegen, werden die Daten von der Dateikopie ausgeschlossen, wenn einer dieser Ausschlussfilter eine Übereinstimmung erzeugt.
- Sie können Einschließfilter und Ausschlussfilter in einer Dateikopieanforderung auch zusammen verwenden.

  Hinweis: Wenn die angegebenen Parameter von Einschließfilter und Ausschlussfilter in Konflikt stehen, stellt der Ausschlussfilter immer die höhere Priorität dar und wird erzwungen. Ein Einschließfilter kann niemals ein Objekt kopieren, das auch ausgeschlossen wurde.

Filtervariable (Muster)

Es gibt zwei Arten von Mustern für variable Filter: Dateimuster und Ordnermuster.

Sie können einen Dateimusterfilter oder Ordnermusterfilter verwenden, um bestimmte Objekte in die Dateikopie einzuschließen oder davon auszuschließen.

Filterwert

Der Filterwert lässt Sie die Informationen eingrenzen, die kopiert werden, dadurch dass nur die Parameterinformationen ausgewählt werden, die Sie festlegen, wie beispielsweise .txt-Dateien.

Arcserve UDP unterstützt die Verwendung von Platzhalterzeichen, die dabei helfen, mehrere Objekte auszuwählen, die mit einer einzelnen Anfrage kopiert werden. Ein Platzhalterzeichen ist ein Sonderzeichen, das als Ersatz benutzt werden kann, um entweder ein alleinstehendes Zeichen oder eine Zeichenfolge eines Textes darzustellen.

Die Platzhalterzeichen Sternchen (*) und Fragezeichen (?) werden im Wertefeld unterstützt. Wenn Ihnen der vollständige Datei- oder Ordnermustername nicht bekannt ist, können Sie die Ergebnisse des Filters vereinfachen, indem Sie ein Platzhalterzeichen angeben.

"*": Verwenden Sie das Sternchen, um null oder mehr Zeichen in dem Wert zu ersetzen.

"?" Verwenden Sie das Fragezeichen, um ein einzelnes Zeichen in dem Wert zu ersetzen.

Sie können beispielsweise "*.txt" eingeben, um alle Dateien auszuschließen, die eine ".txt" -Erweiterung haben, falls Sie den genauen Dateinamen nicht

kennen. Sie können so viele Zeichen des Dateinamens angeben, wie Sie kennen, und die Platzhalter verwenden, um Leerstellen auszufüllen.

Hinweis: Wenn Sie "Dateimuster" als Filtertyp auswählen, ist eine Dropdown-Liste mit vordefinierten Filtern für viele üblicherweise verwendete Dateien verfügbar (MS Office-Dateien, Bilddateien, ausführbare Dateien, temporäre Dateien etc.). Nachdem Sie einen der vordefinierten Filter ausgewählt haben, können Sie die entsprechenden Werte noch anhängen oder ändern.

Dateigrößenfilter

Dateigrößenfilter ermöglichen es Ihnen, die zu kopierenden Quellobjekte auf Basis der Dateigröße einzuschränken. Wenn Sie den Dateigrößenfilter aktivieren, werden die von Ihnen angegebenen Parameter zu dem Filter, von dem abhängt, welche Objekte in die Dateikopie eingeschlossen werden und welche nicht. Sie können den Bereich auswählen ("Gleich oder größer als", "Gleich oder kleiner als" oder "Zwischen") und dann einen Wert für die Größe eingeben.

Wenn Sie beispielsweise "Gleich oder größer als 10 MB" angeben, kopiert Arcserve UDP nur Objekte, die diesen Kriterien entsprechen. Alle anderen Objekte, die diesen Dateigrößenkriterien nicht entsprechen, werden nicht kopiert.

Dateialterfilter

Dateialterfilter ermöglichen es Ihnen, zu kopierende Quellobjekte auf der Basis bestimmter Daten der Datei automatisch einzuschließen. Sie können einen Parameter auswählen ("Kein Zugriff auf Dateien in", "Dateien nicht geändert in", und/oder "Dateien nicht erstellt in") und dann einen Wert für die Anzahl an Tagen, Monaten oder Jahren für den Dateialterfilter eingeben. Sie können mehrere Dateialterfilter für automatische Dateikopie auswählen.

Wenn Sie beispielsweise "Dateien nicht geändert seit 180 Tagen" angeben, wird Arcserve UDP automatisch alle Dateien kopieren, die diesen Kriterien entsprechen, d. h. die während der letzten 180 Tage nicht geändert worden sind.

Wichtig! Wenn Sie sowohl Dateigrößen- als auch Dateialterfilter festlegen (oder mehrere Dateialterfilter), werden nur die Dateien kopiert, die allen angegebenen Filterparametern entsprechen. Dateien, die keinem dieser angegebenen Parameter entsprechen, werden nicht kopiert.

Aktualisieren von Stub-Dateien

Für Dateien, die mithilfe des Dateiarchivs kopiert wurden, hinterlässt Arcserve UDP eine Stub-Datei mit der Erweiterung "UDP.txt". Die Stub-Datei enthält Informationen über das Ziel, an das die Dateien verschoben wurden, sowie einige weitere Informationen. Wenn eine Datei am ursprünglichen Speicherort wiederhergestellt und anschließend erneut zum angegebenen Ziel verschoben wird, wird die Stub-Datei mit diesen Verschiebungsinformationen aktualisiert. Im Bedarfsfall können diese Stub-Dateien der Dateikopie ohne negative Auswirkungen sicher deaktiviert oder gelöscht werden. (Vorhandene Stub-Dateien werden nicht gelöscht, wenn der Registrierungsschlüssel so geändert wird, dass keine weiteren Stub-Dateien erstellt werden).

Die folgenden Informationen sind in der Stub-Datei standardmäßig vorhanden:

Wenden Sie sich an Ihre IT-Abteilung, um diese Datei wiederherzustellen.

Sie können den Standardtext ändern, indem Sie einen Konfigurationseintrag hinzufügen. Fügen Sie den folgenden XML-Tag-Eintrag zur Datei "FileCopyDebugSetting.xml" im Verzeichnis "$UDPHome\Engine\Configuration" hinzu:

<ArchiveStubFileText> Neuer Text kann hier hinzugefügt werden, damit er in der Stub-Datei angezeigt wird.

</ArchiveStubFileText>

Beispiel: Die Datei "FileCopyDebugSetting.xml" würde wie folgt aussehen.

```
<?xml version="1.0" encoding="UTF-8"?>
<HKLM>
<AFArchiveDLL>
<ArchiveStubFileText> Neuer Text kann hier hinzugefügt werden, damit er in der Stub-Datei angezeigt wird.</ArchiveStubFileText>.
</AFArchiveDLL>
</HKLM>
```

Wenn die Datei "FileCopyDebugSetting.xml" nicht im Verzeichnis "$UDPHome\Engine\Configuration" vorhanden ist, erstellen Sie die XML-Datei.

Wenn Sie die Erstellung von Stub-Datei deaktivieren möchten, fügen Sie den folgenden XML-Tag-Eintrag zur Datei "FileCopyDebugSetting.xml" im Verzeichnis "$UDPHome\Engine\Configuration" hinzu:

<CreateStubFile>0</CreateStubFile>

Beispiel: Die Datei "FileCopyDebugSetting.xml" würde wie folgt aussehen.

```
<?xml version="1.0" encoding="UTF-8"?>
<HKLM>

<AFArchiveDLL>
<CreateStubFile>0</CreateStubFile>
</AFArchiveDLL>
</HKLM>
```

Hinweis: Wenn Sie die Stub-Dateien der Dateikopie deaktivieren oder löschen, können Sie den Status und Speicherort der verschobenen Dateien nicht mehr verfolgen.

Ausführen einer manuellen Dateiarchivierung (optional)

In der Regel wird eine Dateiarchivierung automatisch ausgeführt und über die Dateiarchivierungs-Ablaufplan-Einstellungen gesteuert. Als Ergänzung zur geplanten Dateiarchivierung können Sie wichtige Dateien durch manuelle Dateikopien bedarfsgerecht sichern. Wenn Sie eine manuelle Dateiarchivierung ausführen, werden durch den Job alle Sitzungen in der Dateiarchivierungsquelle archiviert.

Die Dateiarchivierung kann in der Ansicht "Knoten" und der Ansicht "Pläne" per Klick auf das Menü **Aktionen** oder das Kontextmenü manuell ausgeführt werden.

Folgen Sie diesen Schritten, um die Dateiarchivierung manuell in der Ansicht "Knoten" auszuführen:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Knoten werden im Hauptfenster angezeigt.
3. Wählen Sie die Knoten für einen Dateiarchivierungsjob aus. Den Knoten muss ein Dateiarchivierungsplan zugewiesen sein.
4. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Dateiarchivierung jetzt**.

   Das Dialogfeld **Archivierung jetzt ausführen** wird geöffnet.
5. Klicken Sie auf **OK**.

   Der Dateiarchivierungsjob wird ausgeführt.

   Die manuelle Dateiarchivierung wurde erfolgreich ausgeführt.

Überprüfen des Plans

Um den Plan für die Dateikopie zu überprüfen, stellen Sie sicher, dass Sie den Plan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Nachdem der Sicherungsjob erfolgreich abgeschlossen wurde, wird der Dateikopiejob planmäßig ausgeführt. Sie können den Status des Sicherungsjobs und des Dateikopierjobs auf der Registerkarte **Jobs** überprüfen.

Folgen Sie diesen Schritten, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Führen Sie diese Schritte durch, um die Dateikopiejobs zu überprüfen:

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs vollständig**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Stellen Sie sicher, dass der Sicherungsjob und der Dateikopiejob erfolgreich ausgeführt wurden.

Erstellen eines Zeitplans für das Kopieren auf Band

Arcserve UDP ist in Arcserve Backup integriert, um Sicherungsdaten in einen Bandsicherungs-Speicherort kopieren zu können. Sie können einen Zeitplan für die Sicherung von Quelldaten und das Kopieren der gesicherten Daten auf Band erstellen. Sie können den Plan in der Konsole erstellen und verwalten.

Nachfolgend sind die Vorteile der Archivierung von Wiederherstellungspunkten auf Band aufgeführt:

- Einhaltung zwingender Compliance - Hilft Ihnen, wichtige Dokumente, E-Mails und andere entscheidende Daten je nach Notwendigkeit aufzubewahren, um den internen Richtlinien und externen Regelungen zu entsprechen.
- Reduzierung der Speicherkosten - Hilft Ihnen dabei, Speicherplatz zurückzugewinnen, indem Sie ältere oder weniger häufig verwendete Daten von Ihren Primärsystemen an kostengünstigere Archivspeicherorte migrieren können.
- Verwaltung mehrerer Dateiversionen - Hilft Ihnen, (im Bedarfsfall) auf vorherige Versionen gesicherter Dateien zurückzugreifen oder mehrere Versionen der gleichen Dateien an unterschiedlichen Zielen zu verwalten.

Unterstützte Szenarien

- Wenn das Ziel von Task 1 der **Arcserve UDP-Recovery Point Server** ist, installieren Sie den Client-Agenten auf dem RPS-Knoten.
- Für einen agentenbasierten Zeitplan mit dem Ziel **Lokale/Remote-Freigabe** installieren Sie den Client-Agenten auf allen Arcserve UDP-Agentenknoten.
- Für einen hostbasierten, agentenlosen Plan installieren Sie den Client-Agenten auf dem Arcserve UDP-Proxy-Knoten.

Der nächste Schritt?

- Überprüfen der Voraussetzungen
- Erstellen eines Plans mit einem Sicherungstask
- Hinzufügen eines Zeitplans für das Kopieren auf Band
- Überprüfen des Plans

Überprüfen der Voraussetzungen und Hinweise

Stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich bei der Konsole an.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.
- Der Arcserve Backup-Server wurde zur Konsole hinzugefügt. Weitere Informationen zum Hinzufügen von Arcserve Backup-Server zur Konsole finden Sie unter Hinzufügen von Arcserve Backup-Servern.
- Auf dem Recovery Point-Server, den Sie im primären Task eines Plans angeben, muss der Arcserve Backup-Server-Agent installiert sein.

Erstellen eines Plans mit einem Sicherungstask

Ein Plan umfasst verschiedene Arten von Tasks, die Sie ausführen möchten. Ein Plan beinhaltet normalerweise einen primären Task, gefolgt von einem sekundären Task. In der Regel ist der primäre Task ein Sicherungstask oder das Replikat eines Remote-Konsolen-Tasks. Die Funktion eines Sicherungstasks besteht darin, eine Sicherung der Quellknoten zu erstellen, die Sie schützen möchten. Sie können Daten von physischen und virtuellen Windows- und Linux-Rechnern sichern. Danach können Sie die gesicherten Daten als zusätzliche Vorsichtsmaßnahme an einem anderen Speicherort speichern.

Weitere Informationen:

- Weitere Informationen zur Sicherung eines Windows-Knotens finden Sie unter Erstellen eines Sicherungsplans für Windows.
- Weitere Informationen zur Sicherung virtueller Rechner finden Sie unter Erstellen eines Sicherungsplans für hostbasierte virtuelle Rechner.
- Weitere Informationen zur Sicherung von Linux-Knoten finden Sie unter Erstellen eines Sicherungsplans für Linux.
- Weitere Informationen zum Replizieren von Sicherungsdaten an einem Remote-Ziel finden Sie unter Replizieren von Daten zwischen Datenspeichern, die von unterschiedlichen UDP-Konsolen verwaltet werden.

Hinzufügen eines Tasks "Auf Band kopieren" zum Plan

Mit dem Task "Auf Band kopieren" können Sie Ihre Daten auf ein Band kopieren. Der Banddatenträger wird von dem Arcserve Backup-Server identifiziert, den Sie hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Fensterbereich auf **Task hinzufügen**.

   Ein neuer Task wird im linken Fensterbereich hinzugefügt.

2. Wählen Sie im Dropdown-Menü **Tasktyp** die Option **Auf Band kopieren** aus.

   Der Task "Auf Band kopieren" wird hinzugefügt.

   Hinweis: Die benutzerdefinierten Sicherungen lösen keine Jobs vom Typ "Auf Band kopieren" aus.

   Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Angeben der Quelle

Die Quelldatei ist in der Regel ein Sicherungsziel oder ein Replikationsziel.

Gehen Sie wie folgt vor:

1. Geben Sie auf der Registerkarte **Quelle** die folgenden Details an.

   Auf Band zu kopierende Quelle

   Gibt den Speicherort der Wiederherstellungspunkte an, die kopiert werden. Wenn Sie nur eine Quelle haben, ist dieses Feld vorab ausgewählt. Wenn Ihr Plan z. B. nur einen Sicherungstask enthält und Sie dann den Task "Auf Band kopieren" hinzufügen, wird das Ziel der Sicherungsaufgabe zur Quelle von "Auf Band kopieren". Wenn Sie mehrere Quelle für "Auf Band kopieren" haben, können Sie für jede dieser Quellen einen Task "Auf Band kopieren" hinzufügen. Wenn der erste Task z. B. ein Sicherungstask ist und der zweite und dritte Task Replikationstasks sind, können Sie drei Tasks "Auf Band kopieren" zum Plan hinzufügen.

   Typen von Wiederherstellungspunkten

   Legt die Arten der Wiederherstellungspunkte fest. Die verfügbaren Optionen sind tägliche Sicherungen, wöchentliche Sicherungen und monatliche Sicherungen.

2. Klicken Sie auf die Registerkarte "**Ziel**".

   Die Seite "**Ziel**" wird geöffnet.

   Sie haben die Quelldetails erfolgreich angegeben.

Angeben des Ziels

Das Ziel ist eine Banddatenträgergruppe auf Ihrem Arcserve Backup-Server. Sie müssen den Arcserve Backup-Server zur Konsole hinzufügen, bevor Sie diesen Task erstellen.

Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details für das Sicherungsziel an.

Arcserve Backup-Server

Wählen Sie in der Dropdown-Liste den Arcserve Backup-Server aus.

Datenträgergruppe

Wählen Sie die Datenträgergruppe aus der Drop-down-Liste aus. Die Datenträgergruppe hängt vom Arcserve Backup-Server ab. Standardmäßig werden datenträgerbasierte <ASBU>-Geräte nicht in der Datenträgergruppe aufgelistet. Auch die Band-Raid-Gruppe wird nicht in der Datenträgergruppe aufgelistet.

Um Arcserve UDP-Wiederherstellungspunkte zu einem datenträgerbasierten Arcserve Backup-Gerät zu migrieren, müssen die inkrementellen Wiederherstellungspunkte zu vollständigen Wiederherstellungspunkten konvertiert werden. Die empfohlene Methode, um Arcserve UDP-Wiederherstellungspunkte zu einem datenträgerbasierten Gerät zu migrieren, ist die Replikation vom Arcserve Backup-Datenspeicher zu einem anderen Datenspeicher.

Nur Bandgruppen können als Ziel für Jobs zum Kopieren auf Band konfiguriert werden. Sie können einen Einstellungsschlüssel in der Datei "ConsoleConfiguration.xml" unter dem Pfad "UDP Management Configuration" bearbeiten, um die ASBU FSD-Gruppe als Ziel für den Kopiervorgang auf Band anzuzeigen:

C:\Programme\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml

<displayASBUFSDGroup>0</displayASBUFSDGroup>

Wenn der Wert 0 ist, wird die ASBU FSD-Gruppe nicht angezeigt.

<displayASBUFSDGroup>1</displayASBUFSDGroup>

Wenn der Wert 1 ist, wird die ASBU FSD-Gruppe angezeigt.

Starten Sie nach dem Ändern der Einstellungen Arcserve UDP Management Service neu, damit diese wirksam werden.

Die Liste der Datenträgergruppe wird vom Arcserve Backup-Server abgefragt. Sie entspricht der Geräteliste auf dem Arcserve Backup-Server.

Multiplexing

Aktivieren Sie das Kontrollkästchen, um Multiplexing zu aktivieren. Geben Sie die Höchstzahl an Streams ein, die gleichzeitig auf ein Band schreiben können. Die Standardeinstellung beträgt vier Streams. Es sind Einstellungen zwischen 2 und 32 Streams möglich.

Verschlüsselung

Legt die Verschlüsselung für Kopien auf Band fest.

Durch die Aktivierung der Verschlüsselung wird sichergestellt, dass Daten auf Band verschlüsselt werden. Wenn eine Verschlüsselung ausgewählt wird, müssen Sie ein Verschlüsselungskennwort angeben (und es bestätigen).

Komprimierung

Durch die Aktivierung der Komprimierung wird sichergestellt, dass Daten auf Band komprimiert werden.

2. Überprüfen Sie die Details der Datenträgergruppe für den ausgewählten Arcserve Backup-Server und die Datenträgergruppe.
3. Klicken Sie auf die Registerkarte **Ablaufplan**.

   Die Seite "Ablaufplan" wird geöffnet.

   Sie haben das Ziel angegeben.

Festlegen des Ablaufplans

Sie können den Zeitplan festlegen, um den Bandkopierjob zu starten. Sie können auch die Datenträger-Aufbewahrungsrichtlinie und den Bandnutzungsmodus festlegen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf **Hinzufügen**, **Zeitplans für "Auf Band kopieren" hinzufügen**.

   Das Dialogfeld **Neuen Zeitplan für "Auf Band kopieren" hinzufügen** wird geöffnet.

2. Geben Sie einen Bandzeitplan an.

   Ein Zeitplan definiert den Zeitraum eines Bandkopierjobs. Wenn Sie einen Zeitplan hinzufügen, wird der Bandkopierjob nur während des definierten Zeitplans ausgeführt. Wenn Sie keinen Zeitplan angeben, wird der Bandkopierjob innerhalb von 30 Minuten, nachdem ein qualifizierter Wiederherstellungspunkt auf einem Datenspeicher bereit ist, ausgeführt.

3. Klicken Sie auf **Speichern**.

   Das Dialogfeld **Neuen Zeitplan für "Auf Band kopieren" hinzufügen** wird geschlossen.

4. Wählen Sie den **Datenträgergruppennamen** aus der Drop-down-Liste aus.

   Ein Standardname für die Datenträgergruppe wird basierend auf dem Plannamen ausgewählt.

   Sie können auch einen vorhandenen Datenträgergruppennamen aus der Drop-down-Liste auswählen. In diesem Fall werden die Datenträger-Aufbewahrungsrichtlinie und der Bandnutzungsmodus, der dieser Datenträgergruppe zugeordnet ist, in diesen Task kopiert. Sie können die Bänder über mehrere Arcserve-UDP-Pläne gemeinsam verwenden, indem Sie dieselbe Datenträgergruppe in allen Arcserve UDP-Plänen angeben.

   Sie können auch einen anderen Gruppennamen angeben. Maximal 13 Zeichen werden für einen Datenträgergruppennamen akzeptiert.

5. Geben Sie eine Richtlinie für die **Aufbewahrung von Wiederherstellungspunkten** an.

   Anhand einer Richtlinie für die Aufbewahrung von Wiederherstellungspunkten können Sie Wiederherstellungspunkte auf täglicher, wöchentlicher oder monatlicher Basis aufbewahren. Sie können unterschiedliche Aufbewahrungszeiten für verschiedene Arten von Wiederherstellungspunkten angeben. Wenn Sie beispielsweise **Tägliche Sicherungen** und **Wöchentliche Sicherungen** auf der

Registerkarte **Quelle** auswählen, können Sie einen unterschiedlichen Wiederherstellungspunkt-Zeitraum für diese beiden Sicherungstypen festlegen.

6. Wählen Sie eine der Optionen für **Bandnutzung** aus.

An vorhandene Bänder anhängen

Gibt an, dass alle Wiederherstellungspunkte, die innerhalb der angegebenen Aufbewahrungszeit generiert werden, auf das gleiche Band kopiert werden. Wenn Sie beispielsweise die Aufbewahrungszeit für die tägliche Sicherung als 7 angegeben haben, dann werden alle Wiederherstellungspunkte von Tag 1 bis Tag 7 auf das gleiche Band kopiert. Danach werden alle Wiederherstellungspunkte der nächsten 7 Tage (Tag 8 bis Tag 14) auf ein anderes Band kopiert, usw.

Die Wiederherstellungspunkte der ersten Woche (Tag 1 bis Tag 7) werden für die nächsten 7 Tage (Tag 8 bis Tag 14) aufbewahrt. Ab Tag 15 werden die Wiederherstellungspunkte wieder auf Band 1 kopiert, weil die Aufbewahrungsrichtlinie für die Wiederherstellungspunkte der ersten Woche abgelaufen ist.

Die folgende Liste zeigt die Standard-Aufbewahrungszeit für "An vorhandene Bänder anhängen":

- Täglich: 7 Tage
- Wöchentlich: 5 Wochen
- Monatlich: 12 Monate

Sieben tägliche Wiederherstellungspunkte werden auf das gleiche Band kopiert, fünf wöchentliche Wiederherstellungspunkte werden auf das gleiche Band kopiert und 12 monatliche Wiederherstellungspunkte werden auf das gleiche Band kopiert.

Auf getrennte Bänder kopieren

Gibt an, dass die Wiederherstellungspunkte für jeden Tag auf ein getrenntes Band kopiert werden. Wenn Sie beispielsweise die Aufbewahrungszeit für tägliche Sicherung als 7 angegeben haben, dann werden die Wiederherstellungspunkte von Tag 1 auf Band 1 kopiert, die Wiederherstellungspunkte von Tag 2 auf Band 2, die Wiederherstellungspunkte von Tag 3 auf Band 3 usw.

Die Wiederherstellungspunkte für Tag 1 werden für 7 Tage aufbewahrt. An Tag 8 werden die Wiederherstellungspunkte auf Band 1 kopiert, da die Aufbewahrungsrichtlinie für Wiederherstellungspunkte von Tag 1 abgelaufen ist.

Die folgende Liste zeigt die Standard-Aufbewahrungszeit für "Auf getrennte Bänder kopieren".

- Täglich: 7 Tage
- Wöchentlich: 5 Wochen
- Monatlich: 12 Monate

Jeder der sieben täglichen Wiederherstellungspunkte wird auf getrennte Bänder kopiert, ebenso alle fünf wöchentlichen Wiederherstellungspunkte und alle 12 monatlichen Wiederherstellungspunkte.

7. Klicken Sie auf die Registerkarte **Erweitert**.

   Das Dialogfeld **"Erweitert"** wird geöffnet.

   Sie haben den Zeitplan angegeben.

Festlegen von erweiterten Einstellungen

Über die erweiterten Einstellungen können Sie weitere Einstellungen für den Task "Auf Band kopieren" festlegen.

1. Geben Sie die folgenden Details an.

Datenträger auswerfen

Gibt an, dass der Datenträger nach Abschließen des Jobs aus dem Laufwerk ausgeworfen wird. So wird verhindert, dass von anderen Jobs Daten auf diesem Datenträger überschrieben werden.

Sicherungsprüfung

Gibt an, dass Arcserve Backup die Zuverlässigkeit der Sicherung überprüft, indem der Header jeder einzelnen Dateien auf Lesbarkeit überprüft wird. Diese Option gilt nicht für Multiplex-Sicherungen.

Befehl ausführen, bevor ein "Auf Band kopieren"-Job gestartet wird

Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, in dem das Skript gespeichert wird. Klicken Sie auf "Bei Beendigungscode", und geben Sie den Beendigungscode für "Job ausführen" oder "Job fehlschlagen" an. "Job ausführen" gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den Beendigungscode zurückgibt. "Job fehlschlagen" gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem ein "Auf Band kopieren"-Job abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den Pfad an, in dem das Skript gespeichert wird.

Benutzername für Befehle

Ermöglicht die Angabe des Benutzernamens zum Ausführen des Skripts.

Kennwort für Befehle

Ermöglicht die Angabe des Kennworts zum Ausführen des Skripts.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Arten der Alerts angeben, die Sie in Form von E-Mails empfangen möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers.

Job-Alerts

Ermöglicht es Ihnen, die Typen der Job-E-Mails auszuwählen, die Sie erhalten möchten.

2. Klicken Sie auf **Speichern**.

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Der Task "Auf Band kopieren" ist erstellt und wird nach Plan ausgeführt.

Hinweis: Beim Ausführen der **Kopieren auf Band**-Jobs unterscheiden sich die Job-Monitor-Werte in der Arcserve UDP-Konsole von denen in Arcserve Backup.

Wichtig! Nachdem Sie die Wiederherstellungspunkte auf Band kopieren, können Sie die Daten auf Band nicht über die Arcserve UDP-Konsole wiederherstellen. Sie müssen die Daten mithilfe des Arcserve Backup-Managers wiederherstellen. Weitere Informationen zum Wiederherstellen der Daten auf Band finden Sie unter "Sichern und Wiederherstellen von D2D/UDP-Daten" im Arcserve Backup-Administratorhandbuch.

So erstellen und verwalten Sie eine Instant VM auf Microsoft Azure

Instant Virtual Machine (Instant VM) unterstützt das sofortige Erstellen eines virtuellen Rechners auf Microsoft Azure. Die IVM auf Microsoft Azure hat folgende Vorteile:

- Direkter Zugriff auf Daten und Programme im den Arcserve UDP Sicherungssitzungen.
- Sie eliminiert die mit einer herkömmlichen Wiederherstellung oder Konvertierung der Sicherungssitzung auf einen virtuellen Rechner einhergehende Ausfallzeit.
- Sie bietet die Alternative, einen virtuellen Rechner in der Cloud zu erstellen statt lokal.

Sie können eine Instant VM aus den folgenden Sicherungssitzungen erstellen:

- Agentenbasierte Linux-Sicherung
- Hostbasierte agentenlose Sicherung für Linux-VM

Hinweis: Informationen zu den Best Practices für einen Instant-Rechner unter Microsoft Azure finden Sie unter Best Practices.

Der nächste Schritt?

- Überprüfen der Voraussetzungen
- Erstellen einer Instant Virtual Machine auf Microsoft Azure
- Verwalten eines Instant Virtual Machine-Plans auf Microsoft Azure

Überprüfen der erforderlichen Komponenten für eine Instant VM auf Microsoft Azure

Stellen Sie die folgenden Voraussetzungen her, bevor Sie eine Instant VM erstellen:

- Aus der Kompatibilitätsmatrix überprüfen Sie, ob die VM von Microsoft Azure und UDP unterstützt wird.
- Microsoft Azure Cloud Konto hinzufügen
- Überprüfen Sie, dass Sie mindestens einen Wiederherstellungspunktserver auf dem lokalen Computer als Sicherungsziel haben.
- Überprüfen Sie, dass Sie mindestens einen Wiederherstellungspunktserver auf Microsoft Azure als Replikationssziel haben.
- Überprüfen Sie, dass Sie mindestens einen Linux-Sicherungsserver für den Sicherungsauftrag haben.
- Überprüfen Sie, dass Sie mindestens einen Linux-Sicherungsserver auf Microsoft Azure für den Instant VM-Auftrag haben.
- Stellen Sie sicher, dass ein Microsoft Azure-Konto hinzugefügt wurde.

Einschränkung

- Linux-Maschinen, die mit UEFI gestartet wurden, werden nicht unterstützt.
- Linux-Maschinen mit Btrfs-Dateisystem über mehrere Festplatten werden nicht unterstützt.

Instant Virtual Machine auf Microsoft Azure erstellen

Um eine IVM auf Microsoft Azure zu erstellen, empfehlen wir die Ausführung einer der folgenden Optionen:

- Sichern Sie den geschützten lokalen Knoten in lokalem Datenspeicher des Wiederherstellungspunktservers und replizieren Sie den Wiederherstellungspunktserver auf Microsoft Azure. Informationen zum Hinzufügen von Knoten finden Sie unter Hinzufügen von Knoten zur Konsole.
- Sichern Sie den geschützten lokalen Knoten im gemeinsamen Speicherort (CIFS, NFS) und kopieren Sie dann zum gemeinsamen Speicherort CIFS (NFS) auf Microsoft Azure. Weitere Informationen zur Sicherung von geschützten Knoten finden Sie unter Erstellen eines Sicherungsplans für Linux.

Die Erstellung einer Instant VM umfasst grob die folgenden fünf Schritte:

1. Öffnen des Instant VM-Assistenten
2. Den Wiederherstellungspunkt auswählen
3. Wählen Sie den Speicherort der VM
4. Wählen Sie den Wiederherstellungsserver
5. Festlegen der Instant VM-Details
6. Übermitteln des Instant VM-Jobs

Öffnen des Instant Virtual Machine-Assistenten

Über den Instant VM-Assistenten können Sie eine Instant VM konfigurieren und erstellen. Es gibt drei Möglichkeiten, den Instant VM-Assistenten zu öffnen:

- Mit der Knotenverwaltung
- Von der Zielverwaltung: Wiederherstellungspunktserver
- Von der Zielverwaltung: Freigegebene Ordner

Öffnen Sie den Assistenten über die Knotenverwaltungsansicht.

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.
3. Alle Knoten werden im mittleren Fensterbereich angezeigt.
4. Klicken Sie mit der rechten Maustaste auf einen Knoten, und wählen Sie **Instant VM erstellen**.

   Der Instant VM-Assistent wird geöffnet.

   Hinweis: Ist einem Knoten kein Plan zugeordnet, verfügt dieser Knoten nicht über die Option **Instant VM erstellen**.

Öffnen Sie den Assistenten über die Zielverwaltungsansicht.

Aus Zielen: Wiederherstellungspunktserver

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Wenn Sie keine Datenspeicher hinzugefügt haben, werden diese Datenspeicher im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf den Datenspeicher.

   Wenn Sie bereits Daten auf dem RPS gesichert haben, werden alle Quellknoten im Fensterbereich aufgelistet.
4. Klicken Sie mit der rechten Maustaste auf einen Knoten, und wählen Sie **Instant VM erstellen**.

   Der Instant VM-Assistent wird geöffnet.

Aus Zielen: Freigegebenen Ordner

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Freigegebene Ordner**.
3. Wenn Sie freigegebene Ordner hinzugefügt haben, werden diese im mittleren Fensterbereich angezeigt.
4. Klicken Sie auf einen freigegebenen Ordner, und wählen Sie **Wiederherstellungspunkt-Browser**.

   Wenn Sie bereits Daten im freigegebenen Ordner gesichert haben, werden alle Quellknoten im Fensterbereich aufgelistet.
5. Klicken Sie mit der rechten Maustaste auf einen Knoten, und wählen Sie **Instant VM erstellen**.

   Der Instant VM-Assistent wird geöffnet.

Auswählen eines Wiederherstellungspunkts

Die Seite "Wiederherstellungspunkt auswählen" zeigt den Speicherort des Wiederherstellungspunkts an und ermöglicht es Ihnen, einen Wiederherstellungspunkt auszuwählen. Der Wiederherstellungspunkt kann sich an einem freigegebenen Speicherort oder in einem Datenspeicher auf dem RPS befinden.

Die Konsole erkennt den Speicherort des Wiederherstellungspunkts und wählt die Felder **Lokationstyp**, **Recovery Point Server** und **Datenspeicher** oder **Netzwerkfreigabeordner** automatisch vorab aus.

Hinweis: Wählen Sie die Wiederherstellungspunktserver-Sitzung (freigegebener Ordner) als Replikationsziel zum Speichern von Netzwerkbandbreite und Zeit.

Erweitern Sie die Datumsliste, wählen Sie den erforderlichen Wiederherstellungspunkt aus der Liste aus, und klicken Sie auf **Weiter**.

Die Seite **VM-Ort** wird geöffnet.

Hinweis: Wenn Sie eine Instant Virtual Machine in der Knotenverwaltung-Ansicht erstellen, werden nur die Wiederherstellungspunktserver aufgelistet, die sich am selben Standort wie der Quellknoten befinden. Wenn Sie eine Instant VM über den Recovery Point Server erstellen möchten, die an einem anderen Standort verwaltet wird, navigieren Sie zu diesem Standort, und öffnen Sie den Assistenten in der Zielverwaltungsansicht.

Auswählen eines VM-Orts

Geben Sie den Speicherort des virtuellen Rechners an, auf dem Sie die Instant VM erstellen möchten.

Gehen Sie wie folgt vor:

1. Wählen Sie Microsoft Azure.
2. Wählen Sie einen Kontonamen aus.

   Hinweis: Wählen Sie das entsprechende Konto aus, wenn es nicht hinzugefügt ist, gehen Sie zu Microsoft Azure Cloud Konto hinzufügen.
3. Klicken Sie auf **Weiter**.

   Die Seite **Wiederherstellungsserver** wird geöffnet.

Auswählen eines Wiederherstellungsservers

Das Core-Modul der Instant VM wird auf dem Wiederherstellungsserver gehostet. Der Standardwiederherstellungsserver ist der Recovery Point Server. Sie können auch einen Knoten als Wiederherstellungsserver zuweisen.

Bei Linux-Sicherungssitzungen ist der Wiederherstellungsserver ein Linux-Sicherungsserver.

Gehen Sie wie folgt vor:

1. Wählen Sie einen Linux-Sicherungsserver aus der Knotenliste aus.

   Hinweis: Wählen Sie die Wiederherstellungspunktserver-Sitzung (freigegebener Ordner) als Replikationsziel zum Speichern von Netzwerkbandbreite und Zeit.

2. Klicken Sie auf **Weiter**.

   Die Seite "Instant VM-Details" wird geöffnet.

   Hinweis: Vergewissern Sie sich, dass Sie den Wiederherstellungspunktserver auf Microsoft Azure auswählen.

Angeben der Details zur Instant VM

Geben Sie die Details zur Instant VM an.

Gehen Sie wie folgt vor:

1. Geben Sie den Namen und eine Beschreibung der Instant VM an.

VM-Name

Gibt den Namen der Instant VM an. Der Name des Quellknotens ergänzt um das Präfix "UDPIVM_" wird der Standardname der Instant VM. Sie können den Namen ändern. Einige Sonderzeichen wie "@", "\" usw. dürfen in dem Namen nicht verwendet werden.

Beschreibung

(Optional) Gibt die Beschreibung für die Instant VM an.

Speicherort

Gibt den Speicherort der Microsoft Azure-Konto an.

Datenträgertyp

Gibt den Typ des Datenträgers an.

Azure VM-Größe

Gibt die unterstützte VM-Größe an.

Netzwerk

Gibt das Netzwerk auf dem Microsoft Azure-Konto an.

Subnetz

Gibt das Subnetz auf dem Microsoft Azure-Konto an.

Öffentliche IP-Adresse automatisch zuweisen

Gibt die öffentliche IP-Adresse an, die der VM zugewiesen ist. .

Primäre IP

Gibt die primäre IP-Adresse der VM an. Die Option wird automatisch gesetzt, wenn Sie sie nicht festlegen.

Sicherheitsgruppe auswählen

Gibt die Sicherheitsgruppe an. Sie können mehrere Gruppen auswählen. Wenn Sie keine Auswahl treffen, wird automatisch eine neue Sicherheitsgruppe erstellt.

Fortschritt: Hostnamen ändern

Gibt den Hostnamen der neuen VM an.

Fortschritt: Daten nach dem Start der Instant VM automatisch wiederherstellen

Legt fest, ob die Datenwiederherstellung automatisch nach Erstellung der Instant VM durchgeführt werden soll.

2. Klicken Sie auf **Fertig stellen**.

Jetzt können Sie den Job übergeben.

Übergeben des Instant VM-Jobs

Um die Instant VM zu erstellen, übergeben Sie den Instant VM-Job. Wenn der Job abgeschlossen ist, können Sie die Instant VM unter **Ressourcen**, **Infrastruktur**, **Instant VM** sehen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf **VM erstellen**.

   Das Dialogfeld **VM erstellen** wird geöffnet.

2. Wählen Sie eine der folgenden Optionen:

   Jetzt starten

   Übermittelt einen Job, um die Instant VM zu erstellen. Nachdem die VM erstellt wurde, wird sie automatisch gestartet.

   Später starten

   Erstellt eine Instant VM. Sie müssen die VM manuell starten. Wenn der Instant VM-Job abgeschlossen ist, können Sie die VM starten.

   Abbrechen

   Schließt das Dialogfeld "VM erstellen" ohne eine VM zu erstellen. Sie werden zur Seite "VM erstellen" zurückgeleitet.

   Der Instant VM-Job wurde erfolgreich erstellt.

Verwalten von Instant VMs

Sie können die Instant VM über die Konsole verwalten. Sie können eine Instant VM von der Konsole aus ein- und ausschalten. Außerdem können Sie alle Instant VMs löschen.

Hinweis: Die Konsole zeigt nur die Instant VMs an, die von den Wiederherstellungspunkten erstellt werden, die von der ausgewählten Seite verwaltet werden.

- Starten und Anhalten von Instant VMs
- Löschen von Instant VMs

Starten und Anhalten von Instant VMs

Sie können eine Instant VM nach der Erstellung starten oder anhalten. Je nach Status des virtuellen Rechners wird die Schaltfläche "Starten" oder "Anhalten" angezeigt.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie zu **Infrastrukturen**, und klicken Sie auf **Instant VM**.
3. Wählen Sie im mittleren Fensterbereich den virtuellen Rechner aus, und klicken Sie auf **Aktionen**.
4. Wählen Sie entsprechend dem Status des virtuellen Rechners **Einschalten** oder **Ausschalten** aus.

   Der virtuelle Rechner wird erfolgreich gestartet oder angehalten.

Löschen von Instant VMs

Sie können alle Instant VMs löschen, die Sie nicht mehr benötigen.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie zu **Infrastrukturen**, und klicken Sie auf **Instant VM**.
3. Wählen Sie im mittleren Fensterbereich den virtuellen Rechner aus, und klicken Sie auf **Aktionen**.
4. Klicken Sie auf **Löschen**.

   Ein Bestätigungsdialogfeld wird geöffnet.
5. Klicken Sie auf **"OK**".

   Der virtuelle Rechner wurde erfolgreich gelöscht.

Erstellen und Verwalten von Instant VMs auf Hyper-V- und VMware ESX-Servern

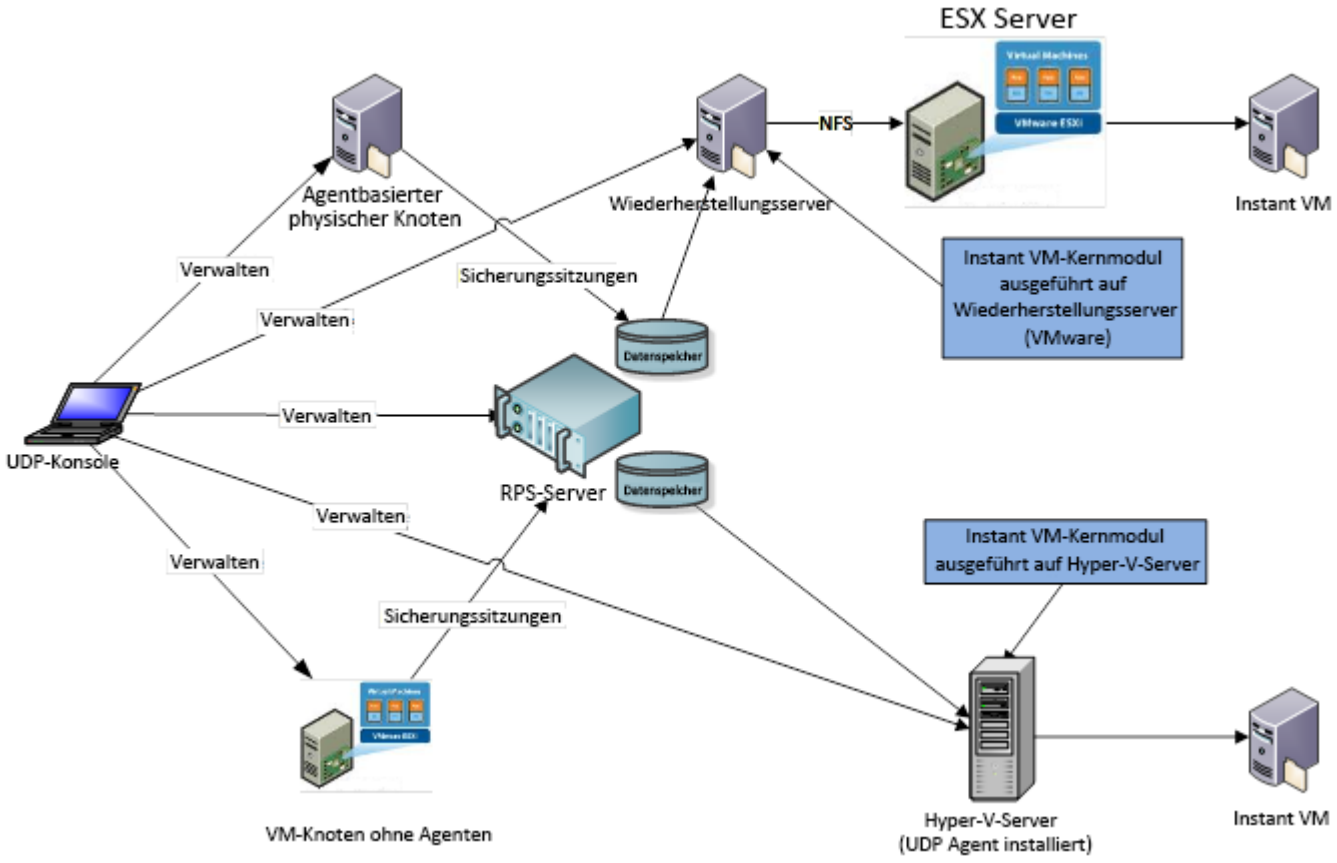
Die Instant VM erstellt im Hypervisor einen virtuellen Rechner und führt die Sicherungssitzung ohne vorherige Konvertierung im virtuellen Rechner aus. Der Vorteil einer Instant VM ist, dass sie einen sofortigen Zugriff auf Daten und Anwendungen in den Arcserve UDP-Sicherungssitzungen bietet. Eine Instant VM kommt ohne die mit einer herkömmlichen Wiederherstellung oder Konvertierung der Sicherungssitzung auf einem physischen oder virtuellen Rechner einhergehenden Ausfallzeit aus.

Sie können eine Instant VM aus den folgenden Sicherungssitzungen erstellen:

- Agentenbasierte Windows-Sicherung
- Agentenbasierte Linux-Sicherung
- Hostbasierte agentenlose Sicherung

Sie können einen VMware vCenter/ESX(i)-Server oder Windows Hyper-V-Server als Hypervisor auswählen.

Die folgende Abbildung erläutert die Architektur einer Instant VM:



Der nächste Schritt?

- Überprüfen der Voraussetzungen für eine Instant VM
- Erstellen einer neuen Instant VM
- Verwalten von Instant VMs

Überprüfen der Voraussetzungen für eine Instant VM

Stellen Sie die folgenden Voraussetzungen her, bevor Sie eine Instant VM erstellen:

- Stellen Sie sicher, dass Sie über mindestens eine Arcserve UDP-Sicherung verfügen.
- Stellen Sie sicher, dass die Arcserve UDP-Agenten bereits auf dem Wiederherstellungsserver installiert sind.
- Stellen Sie sicher, dass die NFS-Funktion auf dem Wiederherstellungsserver installiert ist, wenn der Ziel-Hypervisor ein VMware vCenter/ESX(i)-Server ist.
- Stellen Sie sicher, dass das Betriebssystem des Wiederherstellungsservers 64-Bit-Windows Server 2008 R2 oder höher ist.
- Stellen Sie sicher, dass auf dem Recovery-Server ausreichend Speicherplatz für die Instant VM vorhanden ist.
- Überprüfen Sie, ob Sie jeweils über die Mindestberechtigung zur Durchführung der erforderlichen IVM-Tasks verfügen. Weitere Informationen finden Sie unter Erforderliche VMware-Mindestberechtigungen für IVM-Tasks.

Hinweis: Der Rechner kann starten. Netzwerkkarten werden entsprechend der Eingaben in der Benutzeroberfläche konfiguriert.

Besondere Aspekte

- Die Funktion zur Migration von Instant VMs zwischen Knoten wird nicht unterstützt, wenn eine Instant VM in einem Hyper-V-Cluster gestartet wird.
- Wenn Sie eine Instant VM von einer Linux-Agent-Sicherung erstellen, können die von der Instant VM für einen virtuellen Rechner erstellten Einstellungen nicht mit einem vSphere-Client geändert werden. Sie müssen den vSphere Web-Client verwenden, um die Einstellungen des virtuellen Rechners zu ändern.
- Wenn die Anzahl der NFS-Datenspeicher die maximale Anzahl an NFS-Bereitstellungen auf einem ESXi/ESX-Host erreicht und Sie eine Instant VM erstellen, kann Arcserve UDP keinen NFS-Datenspeicher erstellen. Wie Sie die maximale Anzahl an NFS-Bereitstellungen auf dem ESXi/ESX-Host erhöhen können, erfahren Sie im entsprechenden VMware-KB-Artikel.
- Wenn ein Wiederherstellungspunkt aus einer agentenlosen Sicherung stammt und der Ziel-Hypervisor Vsphere ESX/VC ist, ist auf dem Linux-Sicherungsserver der NFS-Server erforderlich.

- Wenn der Ziel-Hypervisor MS Hyper-V ist, muss der Befehl "net" auf dem Linux-Sicherungsserver verfügbar sein. Dieser Befehl kann über Samba-Client-Pakete installiert werden.
- Der virtuelle Rechner funktioniert in den folgenden Situationen nicht:
  - Der Wiederherstellungsserver wird neu gestartet.
  - Der Wiederherstellungsserver stürzt ab.
  - Die Netzwerkverbindung zwischen Wiederherstellungsserver und Sicherungsziel (Datenspeicher oder Freigabeordner) wird getrennt.

Erforderliche VMware-Mindestberechtigungen für IVM-Tasks

In der Tabelle sind die für die einzelnen IVM-Tasks erforderlichen VMware-Mindestberechtigungen aufgeführt.

Hinweis: Berechtigungen des Typs "Global" werden auf vCenter-Ebene festgelegt.

Tasks	Berechtigung
Datenspeicher	Speicherplatz zuweisen
Global	Methoden deaktivieren
	Methoden aktivieren
	Lizenzen
Host > Konfiguration	Speicherpartitionen konfigurieren
Netzwerk	Netzwerk zuweisen
Resource	Ressourcenpool virtuellen Rechner zuweisen
Virtueller Rechner > Konfiguration	Vorhandenen Datenträger hinzufügen
	Erweitert
Virtueller Rechner > Interaktion	Ausschalten
	Einschalten
	Zurücksetzen
	Konsoleninteraktion
Virtueller Rechner > Bestand	Neu erstellen
	Entfernen
Virtueller Rechner > Bereitstellung	Festplattenzugriff erlauben
	Schreibgeschützten Datenträger-Zugriff erlauben
	Download durch virtuellen Rechner erlauben
Virtueller Rechner > Snapshot-Verwaltung	Snapshot erstellen
	Snapshot entfernen
	Auf Snapshot zurücksetzen
Virtueller Rechner > Gastvorgänge	Gastvorgang-Abfragen

Erstellen einer neuen Instant VM

Die Erstellung einer Instant VM umfasst grob die folgenden fünf Schritte:

1. Öffnen des Instant VM-Assistenten
2. Auswählen eines Wiederherstellungspunkts
3. Festlegen des VM-Ziels
4. Festlegen des Wiederherstellungsservers
5. Festlegen der Instant VM-Details
6. Übermitteln des Instant VM-Jobs

Bei erfolgreichem Abschluss des Jobs wird eine Instant VM erstellt.

Öffnen des Instant Virtual Machine-Assistenten

Über den Instant VM-Assistenten können Sie eine Instant VM konfigurieren und erstellen. Es gibt drei Möglichkeiten, den Instant VM-Assistenten zu öffnen:

- Mit der Knotenverwaltung
- Mit der Zielverwaltung: Recovery Point Server
- Mit der Zielverwaltung: Freigegebener Ordner

Öffnen Sie den Assistenten über die Knotenverwaltungsansicht.

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.
3. Alle Knoten werden im mittleren Fensterbereich angezeigt.
4. Klicken Sie mit der rechten Maustaste auf einen Knoten, und wählen Sie **Instant VM erstellen**.

   Der Instant VM-Assistent wird geöffnet.

   Hinweis: Wenn ein Knoten nicht mit einem Plan verknüpft ist, verfügt ein solcher Knoten nicht über die Option **Instant VM erstellen**.

Öffnen Sie den Assistenten über die Zielverwaltungsansicht.

Mit "Ziele": Recovery Point Server

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Wenn Sie keine Datenspeicher hinzugefügt haben, werden diese Datenspeicher im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf den Datenspeicher.

   Wenn Sie bereits Daten auf dem RPS gesichert haben, werden alle Quellknoten im Fensterbereich aufgelistet.
4. Klicken Sie mit der rechten Maustaste auf einen Knoten, und wählen Sie **Instant VM erstellen**.

   Der Instant VM-Assistent wird geöffnet.

Mit "Ziele": Freigegebener Ordner

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Freigegebene Ordner**.
3. Wenn Sie freigegebene Ordner hinzugefügt haben, werden diese im mittleren Fensterbereich angezeigt.
4. Klicken Sie auf einen freigegebenen Ordner, und wählen Sie **Wiederherstellungspunkt-Browser**.

   Wenn Sie bereits Daten im freigegebenen Ordner gesichert haben, werden alle Quellknoten im Fensterbereich aufgelistet.
5. Klicken Sie mit der rechten Maustaste auf einen Knoten, und wählen Sie **Instant VM erstellen**.

   Der Instant VM-Assistent wird geöffnet.

Auswählen eines Wiederherstellungspunkts

Die Seite "Wiederherstellungspunkt auswählen" zeigt den Speicherort des Wiederherstellungspunkts an und ermöglicht es Ihnen, einen Wiederherstellungspunkt auszuwählen. Der Wiederherstellungspunkt kann sich an einem freigegebenen Speicherort oder in einem Datenspeicher auf dem RPS befinden.

Die Konsole erkennt den Speicherort des Wiederherstellungspunkts und wählt die Felder **Lokationstyp**, **Recovery Point Server** und **Datenspeicher** oder **Netzwerkfreigabeordner** automatisch vorab aus.

Erweitern Sie die Datumsliste, wählen Sie den erforderlichen Wiederherstellungspunkt aus der Liste aus, und klicken Sie auf **Weiter**.

Die Seite **VM-Ort** wird geöffnet.

Hinweis: Wenn Sie eine Instant VM in der Knotenverwaltungsansicht erstellen, werden nur die Recovery Point Server aufgeführt, die sich am gleichen Standort wie der Quellknoten befinden. Wenn Sie eine Instant VM über den Recovery Point Server erstellen möchten, die an einem anderen Standort verwaltet wird, navigieren Sie zu diesem Standort, und öffnen Sie den Assistenten in der Zielverwaltungsansicht.

Auswählen eines VM-Orts

Geben Sie den Speicherort des virtuellen Rechners an, auf dem Sie die Instant VM erstellen möchten. Sie können entweder eine VMware- oder eine Microsoft Hyper-V-VM angeben.

Gehen Sie wie folgt vor:

1. Wählen Sie einen Hypervisor-Typ aus.

   VMware vSphere

   a. Wählen Sie **VMware vSphere**.

   b. Wenn Sie bereits einen VMware-Knoten zu dem ausgewählten Standort in der Konsole hinzugefügt haben, können Sie den Knoten in der Drop-down-Liste **Host** auswählen.

   c. Wenn Sie keine VMware-Knoten hinzugefügt haben, klicken Sie in der Drop-down-Liste "Host" auf **+Neuen Hypervisor hinzufügen**.

      Das Dialogfeld "Hypervisor hinzufügen" wird geöffnet.

   d. Geben Sie die Details zum VMware vCenter- oder ESX(i)-Server an, und klicken Sie auf **OK**.

      Das Dialogfeld "Hypervisor hinzufügen" wird geschlossen, und die Seite **VM-Ort** wird erneut angezeigt. Alle ESX(i)- oder Ressourcenpools werden im mittleren Fensterbereich angezeigt.

   e. Wählen Sie entweder "ESX(i)", "Cluster", "Ressourcenpool" oder "Virtuelle App" als Ort aus.

   Der VMware vSphere-Rechner ist nun angegeben.

   Microsoft Hyper-V

   a. Wählen Sie **Microsoft Hyper-V** aus.

   b. Wenn Sie bereits einen Hyper-V-Knoten zu dem ausgewählten Standort in der Konsole hinzugefügt haben, wählen Sie den Knoten in der Drop-down-Liste **Hyper-V Server/Cluster** aus.

   c. Wenn Sie noch keine Hyper-V-Knoten hinzugefügt haben, klicken Sie auf **Hinzufügen**.

      Das Dialogfeld **Geben Sie das VM-Ziel an** wird geöffnet.

      Hinweis: Wenn Sie eine Verbindung zu der Hyper-V-Instant VM mit einem nicht integrierten lokalen Administratorkonto herstellen, muss die Remote-UAC deaktiviert werden. Weitere Informationen zum Deaktivieren der

Remote-UAC bei nicht integrierten Administratoren finden Sie unter So deaktivieren Sie eine Remote-UAC bei nicht integrierten Administratoren.

d. Geben Sie die Details zum Hyper-V-Server an, und klicken Sie auf **OK**.

   Die Hyper-V-VM ist nun angegeben.

   Hinweis: Das Instant VM-Hilfsprogramm kann den Integrationsdienst nicht auf Instant VMs mit Microsoft Hyper-V 2016 installieren, wenn der Quellknoten Windows 2008 oder niedriger verwendet.

2. Klicken Sie auf **Weiter**.

   Die Seite **Wiederherstellungsserver** wird geöffnet.

Deaktivieren einer Remote-UAC für einen nicht integrierten Administrator

Zusätzliche Administratorkonten sind jene Konten, bei denen es sich nicht um Standardadministratoren handelt. Solche Konten werden auch als nicht integrierte Administratorkonten bezeichnet. Um einen virtuellen Rechner von einem Hyper-V-Host zu importieren, können Sie das integrierte Administratorkonto des Hyper-V-Hosts, ein Domänenkonto in der lokalen Administratorengruppe des Hyper-V-Hosts oder einen nicht integrierten Administratorbenutzer verwenden.

Der Benutzer des zusätzlichem Administratorkontos kann die Vorgänge zum Deaktivieren des Remote-Zugriffs auf UAC durchführen.

Hinweise:

- Dieser Vorgang weicht vom Deaktivieren von UAC grundsätzlich ab. Mit diesem Vorgang können Sie bestimmte Funktionen der UAC deaktivieren.
- Da für den Import die Technologie der Windows-Verwaltungsinstrumentation (WMI) eingesetzt wird, stellen Sie sicher, dass WMI nicht durch die Firewall blockiert ist.

Gehen Sie wie folgt vor:

1. Klicken Sie auf "Start", geben Sie *regedit* im Feld "Programme/Dateien durchsuchen" ein, und drücken Sie die Eingabetaste.

   Der Registrierungs-Editor von Windows wird geöffnet.

   Hinweis: Möglicherweise müssen Sie Administrator-Anmeldeinformationen angeben, um den Windows-Registrierungs-Editor zu öffnen.

2. Suchen Sie den folgenden Registrierungsschlüssel, und klicken Sie darauf:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. Klicken Sie im Menü "Bearbeiten" auf "Neu" und anschließend auf "DWORD-Wert (32-Bit)".
4. Geben Sie *LocalAccountTokenFilterPolicy* als Namen des neuen Eintrags ein, und drücken Sie die Eingabetaste.
5. Klicken Sie mit der rechten Maustaste auf *LocalAccountTokenFilterPolicy* und anschließend auf "Ändern".
6. Geben Sie im Datenfeld "Wert" "1" ein, und klicken Sie auf "OK".
7. Verlassen Sie den Registrierungseditor.

Weitere Informationen zum Verhalten von Windows finden Sie in der Microsoft-Dokumentation.

Auswählen eines Wiederherstellungsservers

Das Core-Modul der Instant VM wird auf dem Wiederherstellungsserver gehostet. Der Standardwiederherstellungsserver ist der Recovery Point Server. Sie können auch einen Knoten als Wiederherstellungsserver zuweisen.

Bei Linux-Sicherungssitzungen ist der Wiederherstellungsserver ein Linux-Sicherungsserver.

Gehen Sie wie folgt vor:

1. Wählen Sie eine der folgenden Optionen als Wiederherstellungsserver aus:

   Recovery Point Server verwenden

   Gibt an, dass der RPS als Wiederherstellungsserver verwendet wird.

   Windows-Knoten aus der Knotenliste auswählen

   Gibt an, dass der Wiederherstellungsserver ein Windows-Knoten ist. Sie können einen Knoten aus der Liste auswählen. Es werden nur die Knoten angezeigt, die durch den ausgewählten Standort verwaltet werden.

   Hinweise:

   - Sie müssen nur einen Wiederherstellungsserver auswählen, wenn der Hypervisor VMware vSphere ist.
   - Wenn der Hypervisor VMware vSphere ist, muss die Windows-Netzwerkdateisystemrolle (Network File System, NFS) auf dem Recovery Point Server installiert sein. Sie kann automatisch über den Instant VM-Prozess installiert werden. Informationen zur manuellen Installation des Netzwerkdateisystems finden Sie unter So installieren Sie das Netzwerkdateisystem manuell auf einem Windows-Server.
   - Wenn Arcserve Backup auf dem Wiederherstellungsserver installiert ist, kann der Start des Windows-NFS-Diensts fehlschlagen. Der Grund hierfür ist, dass die standardmäßige Portnummer des Windows-NFS-Dienstes 111 ist und sie vom Arcserve Backup-Dienst **Remoteprozeduraufruf-Server** verwendet wird. Informationen zur Änderung der standardmäßigen Portnummer vom Arcserve Backup-Dienst **Remote-Prozeduraufruf-Server** finden Sie unter Ändern der Portkonfigurationsdatei und Kommunikationsports von Primär- und Mitgliedsservern in der Arcserve Backup-Dokumentation.

2. Klicken Sie auf **Weiter**.

   Die Seite "Instant VM-Details" wird geöffnet.

Manuelles Installieren von Network File System auf einem Windows-Server

Mit dem Server-Manager können Sie Network File System (NFS) manuell auf einem Windows-Server installieren.

Gehen Sie wie folgt vor:

1. Öffnen Sie den Server-Manager, und klicken Sie auf "Verwalten", "Assistent zum Hinzufügen von Rollen und Features".

   Der Assistent zum Hinzufügen von Rollen und Features wird geöffnet.
2. Klicken Sie auf "Serverrollen", und wählen Sie *Datei- und Speicherdienste*.
3. Erweitern Sie *Datei- und iSCSI-Dienste*.
4. Wählen Sie *Dateiserver* und *Server für NFS*.
5. Klicken Sie auf "Features hinzufügen", um die ausgewählten NFS-Funktionen einzuschließen.
6. Klicken Sie auf "Installieren", um die NFS-Komponenten auf dem Server zu installieren.

   Sie haben Network File System manuell auf dem Windows-Server installiert.

Angeben der Details zur Instant VM

Geben Sie die Details zur Instant VM an. Die Optionen können je nach Hypervisor variieren.

Gehen Sie wie folgt vor:

1. Geben Sie den Namen und eine Beschreibung der Instant VM an.

   VM-Name

   Gibt den Namen der Instant VM an. Der Name des Quellknotens mit einem Präfix ist der Standardname der Instant VM. Einige Sonderzeichen dürfen nicht im Namen verwendet werden, z. B. "@", "\ " usw.

   Beschreibung

   (Optional) Gibt die Beschreibung für die Instant VM an.

2. Geben Sie den Speicherort der Instant VM auf dem Wiederherstellungsserver an.

   Sie können die Volume-Informationen des Wiederherstellungsservers durchsuchen.

   Hinweis Wenn Sie als VM-Speicherort **VMware vSphere** auswählen, wird der ausgewählte Ordner als VMware-NFS-Datenspeicher in VMware geladen. Ein Freigegeben-Symbol wird auf diesem Ordner im lokalen Rechner angezeigt. Standardmäßig wird der NFS-Datenspeicher am gleichen Ordnerspeicherort bereitgestellt, und Sie können ihn nur manuell vom VMware ESX(i)-Server entfernen.

3. Geben Sie die Instant VM-Einstellungen an.

   CPU-Zähler

   Gibt die Anzahl der CPUs an, die Sie in der Instant VM benötigen.

   Speichergröße

   Gibt die Größe des Arbeitsspeichers an, den Sie in der Instant VM benötigen.

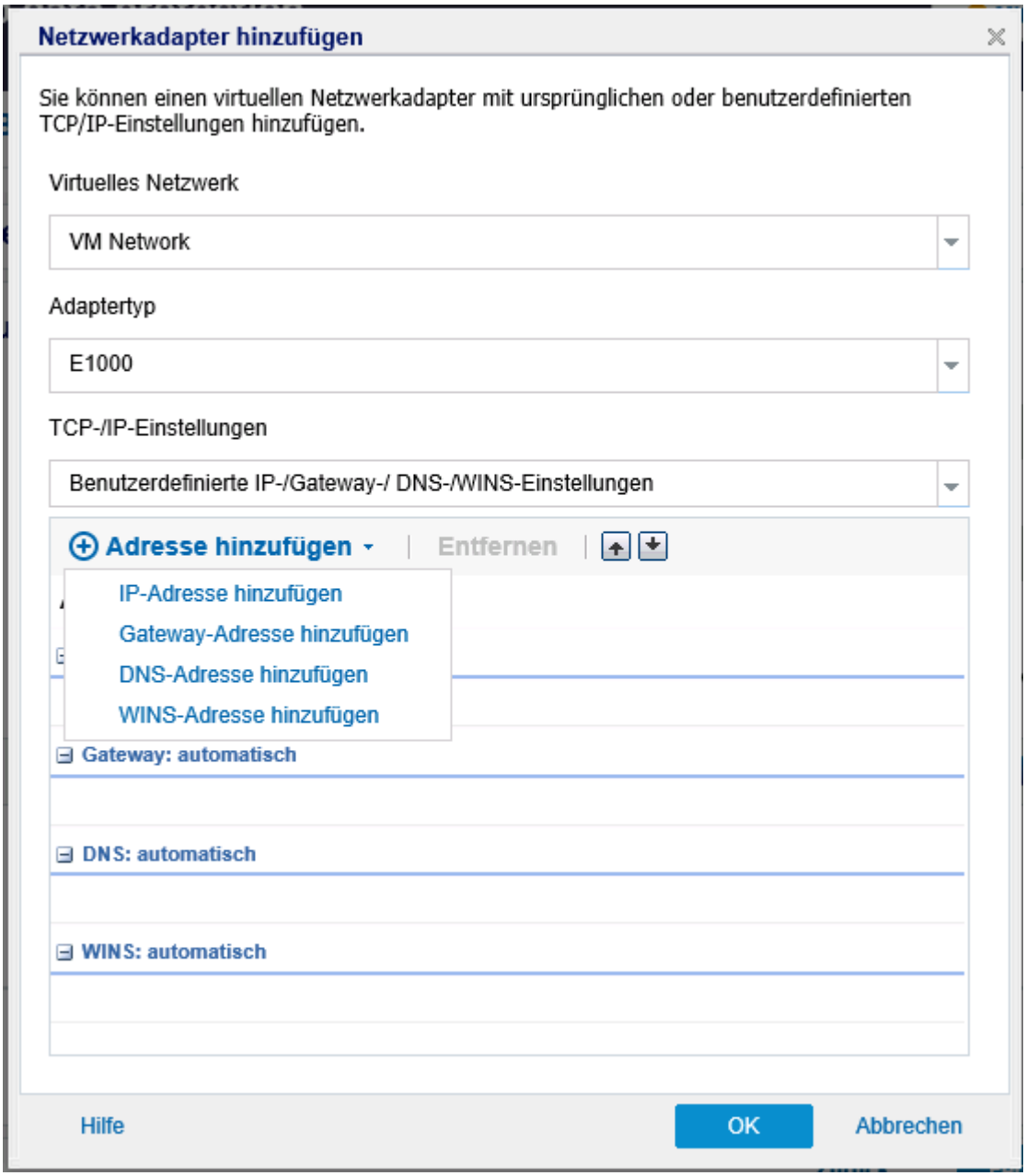
4. Fügt Netzwerkadapter hinzu.

   Hinweis: Für eine Linux-Instant VM kann mindestens eine virtuelle NIC für die Verbindung zum Linux-Sicherungsserver verwendet werden.

   a. Klicken Sie auf die Schaltfläche **Adapter hinzufügen**, und geben Sie die Details für das Netzwerk an.

Sie können mehrere Netzwerkadapter hinzufügen. Nach dem Hinzufügen eines Netzwerkadapters können Sie den Netzwerkadapter in der Spalte **Aktionen** bearbeiten und löschen.

b. Geben Sie das **virtuelle Netzwerk**, den **Adaptertyp** und die **TCP/IP-Einstellungen** an. Wenn Sie die IP-Adresse der Instant VM angeben möchten, klicken Sie auf **Adresse hinzufügen** und wählen die Adresse aus, die Sie konfigurieren möchten.



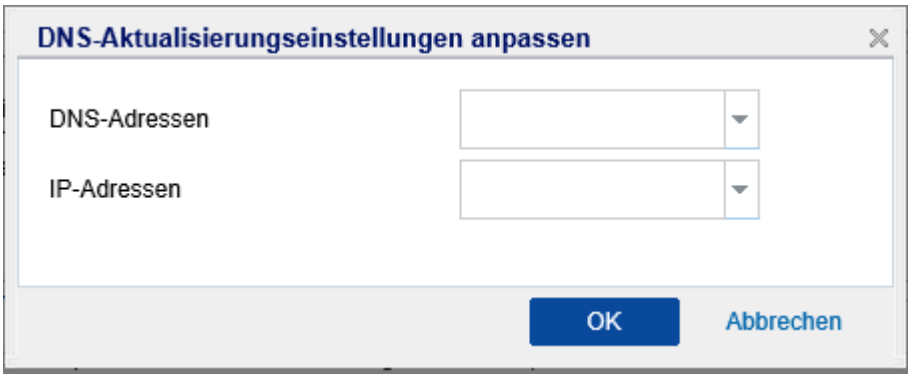
5. Aktualisieren Sie DNS.

   Hinweis: Diese Funktion steht nur für Windows-Instant VMs zur Verfügung.

   a. Klicken Sie auf die Schaltfläche **DNS aktualisieren**, um die DNS-Details anzugeben.

Hinweis: Sie können Detailinformationen zum Aktualisieren von DNS angeben, wenn Sie eine IP-Adresse und die DNS-Adresse im Netzwerkadapter angegeben haben und sich der Quellrechner in einer Domäne befindet.

b. Klicken Sie auf **DNS-Adresse hinzufügen**, um einen DNS-Aktualisierungsdatensatz hinzuzufügen. Klicken Sie auf **Entfernen**, um den DNS-Aktualisierungsdatensatz zu entfernen. Klicken Sie auf die Hoch- und Runter-Schaltfläche, um die Reihenfolge der Datensätze anzupassen.



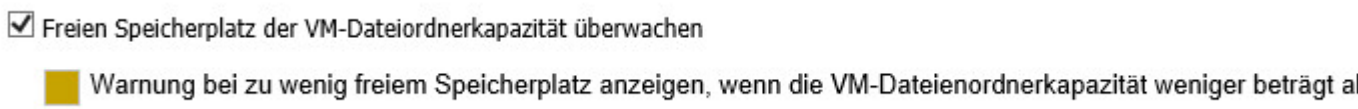
c. Wählen Sie in der Drop-down-Liste eine DNS-Adresse und eine IP-Adresse aus, und klicken Sie dann auf **OK**.

d. Geben Sie die **TTL (Zeit bis Ablauf)** an.

e. Geben Sie die DNS-Authentifizierung an.

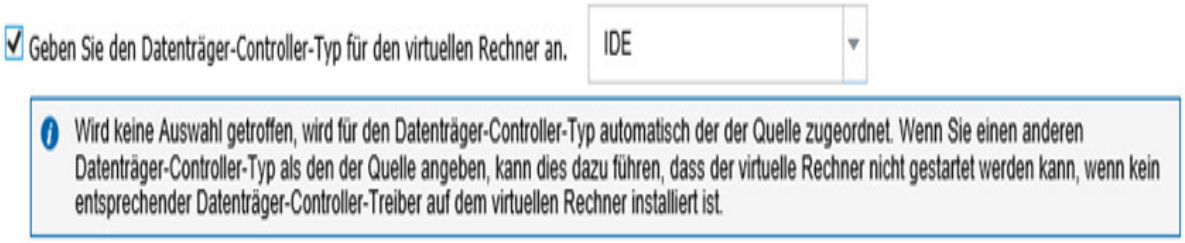
Geben Sie für den Microsoft-DNS-Server den Benutzernamen und das Kennwort ein. Für BIND-Server müssen Sie den vollständigen Pfadnamen, einschließlich des Dateinamens der Schlüsseldatei im Wiederherstellungsserver, angeben.

6. Überprüfen Sie den freien Speicherplatz der VM-Dateiordnerkapazität.



Hinweis: Das Kontrollkästchen **Freien Speicherplatz der VM-Dateiordnerkapazität überwachen** ist standardmäßig aktiviert. Die Kapazitätsleiste wird auf der Seite "Instant VMs" in gelb angezeigt, wenn der freie Speicherplatz der VM-Dateiordnerkapazität unter dem Schwellenwert liegt. Der Standardschwellenwert ist 3 %. Sie können den Wert ändern, wenn erforderlich.

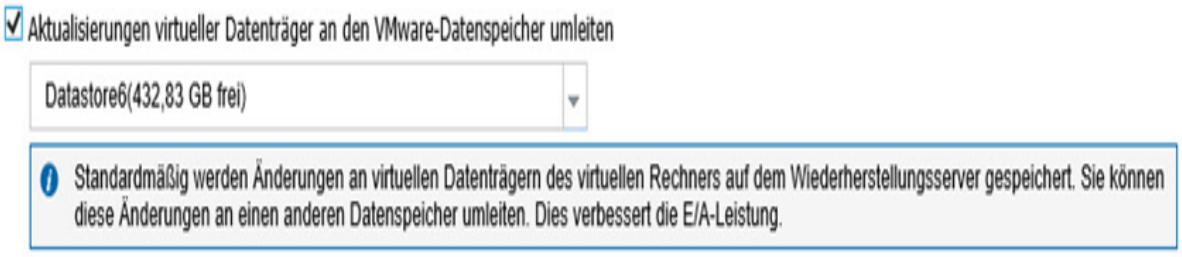
7. Aktivieren Sie das Kontrollkästchen **Geben Sie den Datenträger-Controller-Typ für den virtuellen Rechner an**, und wählen Sie aus der Drop-down-Liste den Typ des Datenträger-Controllers für den virtuellen Rechner aus.



Hinweis: Das Kontrollkästchen **Geben Sie den Datenträger-Controller-Typ für den virtuellen Rechner an** ist verfügbar, wenn Sie **VMware vSphere** als Speicherort für die VM ausgewählt haben.

Die Instant VM wird erstellt, wobei der angegebene Datenträger-Controller in VMware angewendet wird.

8. Um die Aktualisierungen virtueller Datenträger an den VMware-Datenspeicher umzuleiten, gehen Sie folgendermaßen vor:
   a. Aktivieren Sie das Kontrollkästchen **Aktualisierungen virtueller Datenträger an den VMware-Datenspeicher umleiten**.



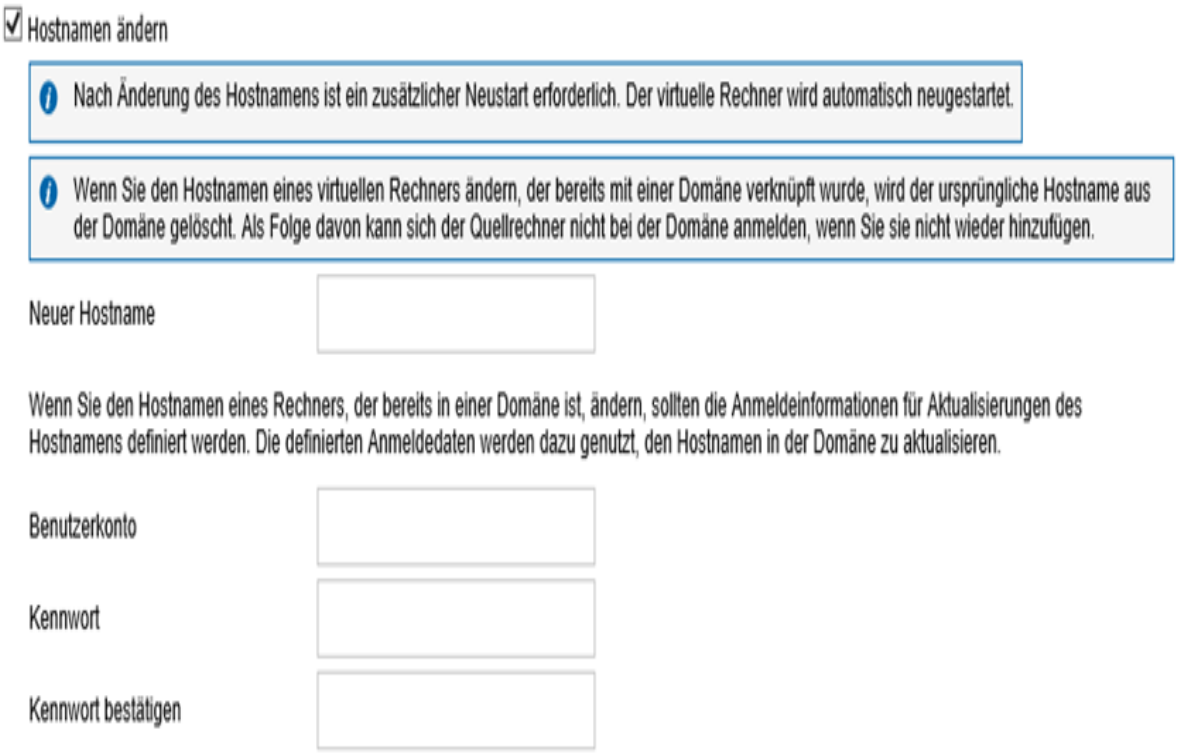
Hinweis: Das Kontrollkästchen **Aktualisierungen virtueller Datenträger an den VMware-Datenspeicher umleiten** ist verfügbar, wenn Sie **VMware vSphere** als Speicherort für die VM ausgewählt haben.

   b. Wählen Sie den erforderlichen VMware-Datenspeicher aus der Drop-down-Liste aus.

Die Aktualisierungen des virtuellen Datenträgers werden an den ausgewählten VMware-Datenspeicher umgeleitet.

9. Um den Instant VM-Hostnamen zu ändern, gehen Sie folgendermaßen vor:

   a. Aktivieren Sie das Kontrollkästchen **Hostnamen ändern**, um den Hostnamen der Instant VM zu aktualisieren.



   b. Geben Sie einen neuen Hostnamen für die Instant VM an. Wenn sich der Quellrechner in einer Domäne befindet, geben Sie das Benutzerkonto und das Kennwort ein.

   Hinweis: Wenn sich der Quellrechner in einer Domäne befindet, muss das Konto über die Berechtigung zum Ändern des Hostnamens in der Domäne verfügen.

10. (Optional) Aktivieren Sie für eine **Linux-Instant VM** die Option **Daten nach dem Start der Instant VM automatisch wiederherstellen**, um die automatische Wiederherstellung von Daten zu aktivieren, wenn das Instant VM-Ziel gestartet wird.

    Nach dem Standardverhalten der **Linux-Instant VM** werden zuerst die notwendigen Daten wiederhergestellt. Anschließend wird die VM gestartet. Wenn die Option nicht aktiviert ist, werden die verbleibenden Daten beim Start der VM nicht wiederhergestellt, auch wenn sie als normale VM verwendet wird. Wenn die Option aktiviert ist, werden die verbleibenden Daten auf dem Back-End wiederhergestellt,

sobald Sie die VM verwenden. Sie können das Instant VM-Ziel auch dauerhaft beibehalten, wenn die Datenwiederherstellung abgeschlossen ist.

Hinweis: Wenn der Status der Linux-Instant VM-Ziels "Ausgeschaltet" lautet, schlägt der Instant VM-Job fehl. Wenn dieser Wiederherstellungspunkt zusammengeführt wird, kann die Linux-Instant VM nicht eingeschaltet werden.

Jetzt können Sie den Job übergeben.

Übergeben des Instant VM-Jobs

Um die Instant VM zu erstellen, übergeben Sie den Instant VM-Job. Wenn der Job abgeschlossen ist, können Sie die Instant VM unter **Ressourcen**, **Infrastruktur**, **Instant VM** sehen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf **Fertig stellen**.

   Das Dialogfeld **VM starten** wird geöffnet.

2. Wählen Sie eine der folgenden Optionen:

   Jetzt starten

   Übermittelt einen Job, um die Instant VM zu erstellen. Nachdem die VM erstellt wurde, wird sie automatisch gestartet.

   Später starten

   Erstellt eine Instant VM. Sie müssen die VM manuell starten. Wenn der Instant VM-Job abgeschlossen ist, können Sie die VM starten.

   Abbrechen

   Schließt das Dialogfeld "VM erstellen" ohne eine VM zu erstellen. Sie werden zur Seite "VM erstellen" zurückgeleitet.

Der Instant VM-Job wurde erfolgreich erstellt.

Verwalten von Instant VMs

Sie können die Instant VM über die Konsole verwalten. Sie können eine Instant VM von der Konsole aus ein- und ausschalten. Außerdem können Sie alle Instant VMs löschen.

Hinweis: Die Konsole zeigt nur die Instant VMs an, die aus den Wiederherstellungspunkten erstellt wurden, die vom ausgewählten Standort verwaltet werden.

- Starten und Anhalten von Instant VMs
- Neustarten von Instant VMs
- Löschen von Instant VMs
- Konvertieren der Linux-Instant VM in eine unabhängige VM
- Migrieren der Linux-Instant VM auf einen physischen Rechner

Starten und Anhalten von Instant VMs

Sie können eine Instant VM nach der Erstellung starten oder anhalten. Je nach Status des virtuellen Rechners wird die Schaltfläche "Starten" oder "Anhalten" angezeigt.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie zu **Infrastrukturen**, und klicken Sie auf **Instant VM**.
3. Wählen Sie im mittleren Fensterbereich den virtuellen Rechner aus, und klicken Sie auf **Aktionen**.
4. Wählen Sie entsprechend dem Status des virtuellen Rechners **Einschalten** oder **Ausschalten** aus.

   Der virtuelle Rechner wird erfolgreich gestartet oder angehalten.

Neustarten von Instant VMs

Sie können eine Instant VM nach der Erstellung neu starten.

Hinweis: Sie können eine Instant VM nur dann neu starten, wenn sie den Status **Fehler/Job abgestürzt** aufweist.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie zu **Infrastruktur**, und klicken Sie auf **Instant VMs**.
3. Wählen Sie im mittleren Fensterbereich den virtuellen Rechner mit dem Status **Fehler/Job abgestürzt** aus, und klicken Sie auf **Aktionen**.
4. Klicken Sie auf **Neu starten**.

   Der virtuelle Rechner wird neu gestartet.

Löschen von Instant VMs

Sie können alle Instant VMs löschen, die Sie nicht mehr benötigen.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie zu **Infrastrukturen**, und klicken Sie auf **Instant VM**.
3. Wählen Sie im mittleren Fensterbereich den virtuellen Rechner aus, und klicken Sie auf **Aktionen**.
4. Klicken Sie auf **Löschen**.

   Ein Bestätigungsdialogfeld wird geöffnet.
5. Klicken Sie auf **OK**.

   Der virtuelle Rechner wurde erfolgreich gelöscht.

Konvertieren der Linux-Instant VM in eine unabhängige VM

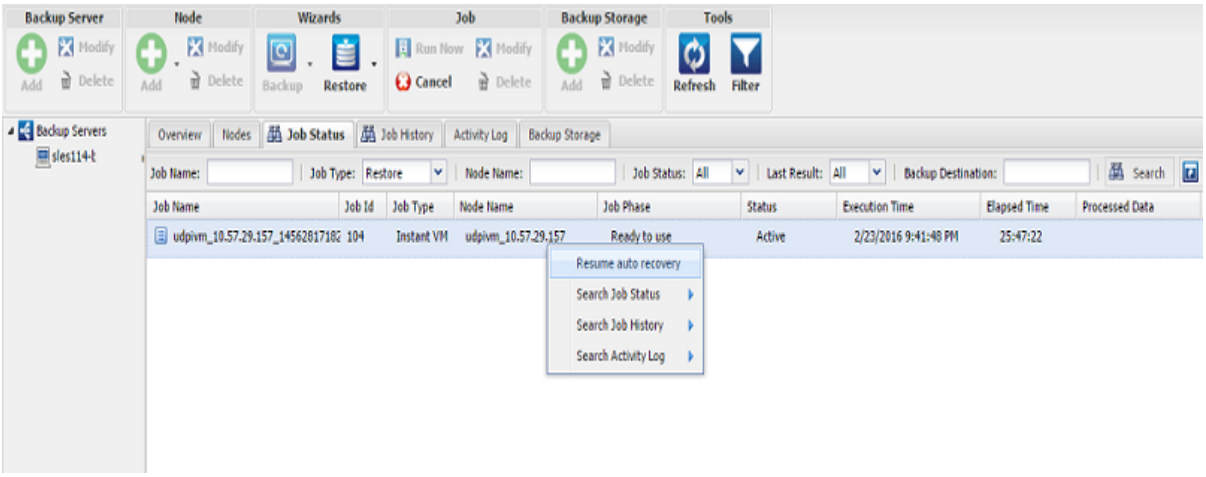
Sie können eine Linux Instant Virtual Machine (IVM) in einen unabhängigen virtuellen Rechner (VM) ändern.

Hinweise:

- Um den Vorgang fortzusetzen, benötigen Sie ein Menüelement, das erst verfügbar ist, wenn die IVM die Jobphase "Bereit zur Verwendung" erreicht hat.
- Die Option ist nicht verfügbar, wenn der Wiederherstellungspunkt eine agentenlose Sicherung und vSphere ESX/VC der Ziel-Hypervisor ist. Um die IVM in eine unabhängige VM zu konvertieren, müssen Sie VMware Storage vMotion verwenden.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Benutzeroberfläche des Linux-Sicherungsservers.



2. Wählen Sie auf der Registerkarte "Jobstatus" den IVM-Job aus, und klicken Sie mit der rechten Maustaste auf den Job, um das Kontextmenü aufzurufen.
3. Wählen Sie "Automatische Wiederherstellung wieder aufnehmen".

   Nach erfolgreichem Abschluss des Vorgangs wird der IVM-Job in die Jobübersicht verschoben.

Migrieren der Linux-Instant VM auf einen physischen Rechner

Informationen zur Migration der Linux-Instant VM auf einen physischen Rechner finden Sie im Abschnitt **Durchführen einer Migrations-BMR für Linux-Rechner** im *Agent for Linux-Benutzerhandbuch*.

Erstellen und Verwalten von Instant VMs auf Amazon EC2

Die Option "Instant Virtual Machine (Instant VM)" unterstützt die sofortige Erstellung virtueller Rechner auf Amazon EC2. Eine Instant VM auf Amazon EC2 hat folgende Vorteile:

- Stellt einen direkten Zugriff auf Daten und Programme in denArcserve UDP Backup-Sessions bereit.
- Sie eliminiert die mit einer herkömmlichen Wiederherstellung oder Konvertierung der Sicherungssitzung auf einen virtuellen Rechner einhergehende Ausfallzeit.
- Sie bietet die Alternative, einen virtuellen Rechner in der Cloud zu erstellen statt lokal.

Sie können eine Instant VM aus den folgenden Sicherungssitzungen erstellen:

- Agentenbasierte Linux-Sicherung
- Hostbasierte Backups ohne Agent

Der nächste Schritt?

- Überprüfen der Voraussetzungen
- Erstellen eines Instant VM-Plans auf Amazon EC2
- Verwalten eines Instant VM-Plans auf Amazon EC2

Sie können eine Instant VM aus den folgenden Backupsitzungen erstellen: nach erfolgreichem Abschluss des Auftrags, wird eine Instant VM auf Amazon EC2 erstellt.

Überprüfen der Voraussetzungen für eine Instant VM auf Amazon EC2

Stellen Sie die folgenden Voraussetzungen her, bevor Sie eine Instant VM erstellen:

- Überprüfen Sie in der Kompatibilitätsmatrix, ob die VM von Amazon EC2 und UDP unterstützt wird.
- Stellen Sie sicher, dass Sie mindestens einen Recovery Point Server auf dem lokalen Rechner haben, als Sicherungsziel.
- Stellen Sie sicher, dass Sie mindestens einen Recovery Point Server auf Amazon EC2 haben, als Replikationsziel.
- Stellen Sie sicher, dass Sie mindestens einen lokalen Linux-Sicherungsserver haben, für den Sicherungsjob.
- Stellen Sie sicher, dass Sie mindestens einen Linux-Sicherungsserver auf Amazon EC2 haben, für den Instant VM-Job.
- Stellen Sie sicher, dass das Amazon EC2-Konto ein Kontingent zur Instanzenausführung hat, das für die Instant VM ausreicht.

Einschränkung

Die agentenbasierte Sicherung von Windows-VMs und die hostbasierte agentenlose Sicherung von Windows-VMs werden NICHT unterstützt.

Erstellen einer Instant VM auf Amazon EC2

Die Erstellung einer Instant VM umfasst grob die folgenden fünf Schritte:

1. Öffnen des Instant VM-Assistenten
2. Den Wiederherstellungspunkt auswählen
3. Wählen Sie den Speicherort der VM
4. Wählen Sie den Wiederherstellungsserver
5. Festlegen der Instant VM-Details
6. Übermitteln des Instant VM-Jobs

Öffnen des Instant Virtual Machine-Assistenten

Über den Instant VM-Assistenten können Sie eine Instant VM konfigurieren und erstellen. Es gibt drei Möglichkeiten, den Instant VM-Assistenten zu öffnen:

- Mit der Knotenverwaltung
- Mit der Zielverwaltung: Recovery Point Server
- Mit der Zielverwaltung: Freigegebener Ordner

Öffnen Sie den Assistenten über die Knotenverwaltungsansicht.

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.
3. Alle Knoten werden im mittleren Fensterbereich angezeigt.
4. Klicken Sie mit der rechten Maustaste auf einen Knoten und wählen Sie **Instant VM erstellen**.

   Der Instant VM-Assistent wird geöffnet.

   Hinweis: Wenn ein Knoten nicht mit einem Plan verknüpft ist, enthält ein solcher Knoten nicht über die Option **Instant VM erstellen**.

Öffnen Sie den Assistenten über die Zielverwaltungsansicht.

Mit "Ziele": Recovery Point Server

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Wenn Sie keine Datenspeicher hinzugefügt haben, werden diese Datenspeicher im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf den Datenspeicher.

   Wenn Sie bereits Daten auf dem RPS gesichert haben, werden alle Quellknoten im Fensterbereich aufgelistet.
4. Klicken Sie mit der rechten Maustaste auf einen Knoten und wählen Sie **Instant VM erstellen**.

   Der Instant VM-Assistent wird geöffnet.

Mit "Ziele": Freigegebener Ordner

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Freigegebene Ordner**.
3. Wenn Sie freigegebene Ordner hinzugefügt haben, werden diese im mittleren Fensterbereich angezeigt.
4. Klicken Sie auf einen freigegebenen Ordner, und wählen Sie **Wiederherstellungspunkt-Browser**.

   Wenn Sie bereits Daten im freigegebenen Ordner gesichert haben, werden alle Quellknoten im Fensterbereich aufgelistet.
5. Klicken Sie mit der rechten Maustaste auf einen Knoten, und wählen Sie **Instant VM erstellen**.

   Der Instant VM-Assistent wird geöffnet.

Auswählen eines Wiederherstellungspunkts

Die Seite "Wiederherstellungspunkt auswählen" zeigt den Speicherort des Wiederherstellungspunkts an und ermöglicht es Ihnen, einen Wiederherstellungspunkt auszuwählen. Der Wiederherstellungspunkt kann sich an einem freigegebenen Speicherort oder in einem Datenspeicher auf dem RPS befinden.

Die Konsole erkennt den Speicherort des Wiederherstellungspunkts und wählt die Felder **Lokationstyp**, **Recovery Point Server** und **Datenspeicher** oder **Netzwerkfreigabeordner** automatisch vorab aus.

Hinweis: Wählen Sie als Replikationsziel "Recovery Point Server (Shared folder) session" (Sitzung des Typs "Recovery Point Server" [Freigegebener Ordner]) aus, um Netzwerkbandbreite und Zeit zu sparen.

Erweitern Sie die Datumsliste, wählen Sie den erforderlichen Wiederherstellungspunkt aus der Liste aus, und klicken Sie auf **Weiter**.

Die Seite **VM-Ort** wird geöffnet.

Hinweis: Wenn Sie eine Instant VM in der Knotenverwaltungsansicht erstellen, werden nur die Recovery Point Server aufgeführt, die sich am gleichen Standort wie der Quellknoten befinden. Wenn Sie eine Instant VM über den Recovery Point Server erstellen möchten, die an einem anderen Standort verwaltet wird, navigieren Sie zu diesem Standort, und öffnen Sie den Assistenten in der Zielverwaltungsansicht.

Auswählen eines VM-Orts

Geben Sie den Speicherort des virtuellen Rechners an, auf dem Sie die Instant VM erstellen möchten. Sie können Amazon EC2 oder Amazon EC2 (China) angeben, je nach dem Typ Ihres Kontos.

Gehen Sie wie folgt vor:

1. Wählen Sie Amazon EC2 oder Amazon EC2 (China).
2. Wählen Sie einen Kontonamen aus.

   Hinweis: Wählen Sie das zugehörige Konto aus. Falls es noch nicht hinzugefügt ist, finden Sie Anweisungen unter Hinzufügen eines Cloud-Kontos.
3. Klicken Sie auf **Weiter**.

   Die Seite **Wiederherstellungsserver** wird geöffnet.

Auswählen eines Wiederherstellungsservers

Das Core-Modul der Instant VM wird auf dem Wiederherstellungsserver gehostet. Der Standardwiederherstellungsserver ist der Recovery Point Server. Sie können auch einen Knoten als Wiederherstellungsserver zuweisen.

Bei Linux-Sicherungssitzungen ist der Wiederherstellungsserver ein Linux-Sicherungsserver.

Gehen Sie wie folgt vor:

1. Wählen Sie einen Linux-Sicherungsserver aus der Knotenliste aus.

   Hinweise: Wählen Sie als Replikationsziel "Recovery Point Server (Shared folder) session" (Sitzung des Typs "Recovery Point Server" [Freigegebener Ordner]) aus, um Netzwerkbandbreite und Zeit zu sparen.

2. Klicken Sie auf **Weiter**.

   Die Seite "Instant VM-Details" wird geöffnet.

Angeben der Details zur Instant VM

Geben Sie die Details zur Instant VM an.

Gehen Sie wie folgt vor:

1. Geben Sie den Namen und eine Beschreibung der Instant VM an.

VM-Name

Gibt den Namen der Instant VM an. Der Name des Quellknotens ergänzt um das Präfix "UDPIVM_" wird der Standardname der Instant VM. Sie können den Namen ändern. Einige Sonderzeichen wie "@", "\" usw. dürfen in dem Namen nicht verwendet werden.

Beschreibung

(Optional) Gibt die Beschreibung für die Instant VM an.

Region

Gibt die Region Ihres Amazon EC2-Kontos an.

Instanzentyp

Gibt den unterstützten Instanzentyp an.

Volume-Typ

Gibt den Volume-Typ an.

Netzwerk

Gibt das Netzwerk im Amazon EC2-Konto an.

Subnetz

Gibt das Subnetz im Amazon EC2-Konto an.

Öffentliche IP-Adresse automatisch zuweisen

Gibt die öffentliche IP-Adresse an, die der VM zugewiesen ist. .

Primäre IP

Gibt die primäre IP-Adresse der VM an. Die Option wird automatisch gesetzt, wenn Sie sie nicht festlegen.

Sicherheitsgruppe auswählen

Gibt die Sicherheitsgruppe an. Sie können mehrere Gruppen auswählen. Wenn Sie keine Auswahl treffen, wird automatisch eine neue Sicherheitsgruppe erstellt.

Erweitern: Hostnamen ändern

Gibt den Hostnamen der neuen VM an.

Erweitern: Daten nach Start der Instant VM automatisch wiederherstellen

Legt fest, ob die Datenwiederherstellung automatisch nach Erstellung der Instant VM durchgeführt werden soll.

2. Klicken Sie auf **Fertig stellen**.

Jetzt können Sie den Job übergeben.

Übergeben des Instant VM-Jobs

Um die Instant VM zu erstellen, übergeben Sie den Instant VM-Job. Wenn der Job abgeschlossen ist, können Sie die Instant VM unter **Ressourcen Infrastruktur Instant VM** sehen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf **VM erstellen**.

   Das Dialogfeld **VM erstellen** wird geöffnet.

2. Wählen Sie eine der folgenden Optionen:

   Jetzt starten

   Übermittelt einen Job, um die Instant VM zu erstellen. Nachdem die VM erstellt wurde, wird sie automatisch gestartet.

   Später starten

   Erstellt eine Instant VM. Sie müssen die VM manuell starten. Wenn der Instant VM-Job abgeschlossen ist, können Sie die VM starten.

   Abbrechen

   Schließt das Dialogfeld "VM erstellen" ohne eine VM zu erstellen. Sie werden zur Seite "VM erstellen" zurückgeleitet.

   Der Instant VM-Job wurde erfolgreich erstellt.

Verwalten von Instant VMs

Sie können die Instant VM über die Konsole verwalten. Sie können eine Instant VM von der Konsole aus ein- und ausschalten. Außerdem können Sie alle Instant VMs löschen.

Hinweis: Die Konsole zeigt nur die Instant VMs an, die von den Wiederherstellungspunkten erstellt werden, die von der ausgewählten Seite verwaltet werden.

- Starten und Anhalten von Instant VMs
- Neustarten von Instant VMs
- Löschen von Instant VMs
- Konvertieren der Linux-Instant VM in eine unabhängige VM
- Migrieren der Linux-Instant VM auf einen physischen Rechner

Starten und Anhalten von Instant VMs

Sie können eine Instant VM nach der Erstellung starten oder anhalten. Je nach Status des virtuellen Rechners wird die Schaltfläche "Starten" oder "Anhalten" angezeigt.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie zu **Infrastrukturen**, und klicken Sie auf **Instant VM**.
3. Wählen Sie im mittleren Fensterbereich den virtuellen Rechner aus, und klicken Sie auf **Aktionen**.
4. Wählen Sie entsprechend dem Status des virtuellen Rechners **Einschalten** oder **Ausschalten** aus.

   Der virtuelle Rechner wird erfolgreich gestartet oder angehalten.

Neustarten von Instant VMs

Sie können eine Instant VM nach der Erstellung neu starten.

Hinweis: Sie können eine Instant VM nur dann neu starten, wenn sie den Status **Fehler/Job abgestürzt** aufweist.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie zu **Infrastruktur**, und klicken Sie auf **Instant VMs**.
3. Wählen Sie im mittleren Fensterbereich den virtuellen Rechner mit dem Status **Fehler/Job abgestürzt** aus, und klicken Sie auf **Aktionen**.
4. Klicken Sie auf **Neu starten**.

   Der virtuelle Rechner wird neu gestartet.

Löschen von Instant VMs

Sie können alle Instant VMs löschen, die Sie nicht mehr benötigen.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie zu **Infrastrukturen**, und klicken Sie auf **Instant VM**.
3. Wählen Sie im mittleren Fensterbereich den virtuellen Rechner aus, und klicken Sie auf **Aktionen**.
4. Klicken Sie auf **Löschen**.

   Ein Bestätigungsdialogfeld wird geöffnet.
5. Klicken Sie auf **OK**.

   Der virtuelle Rechner wurde erfolgreich gelöscht.

Konvertieren der Linux-Instant VM in eine unabhängige VM

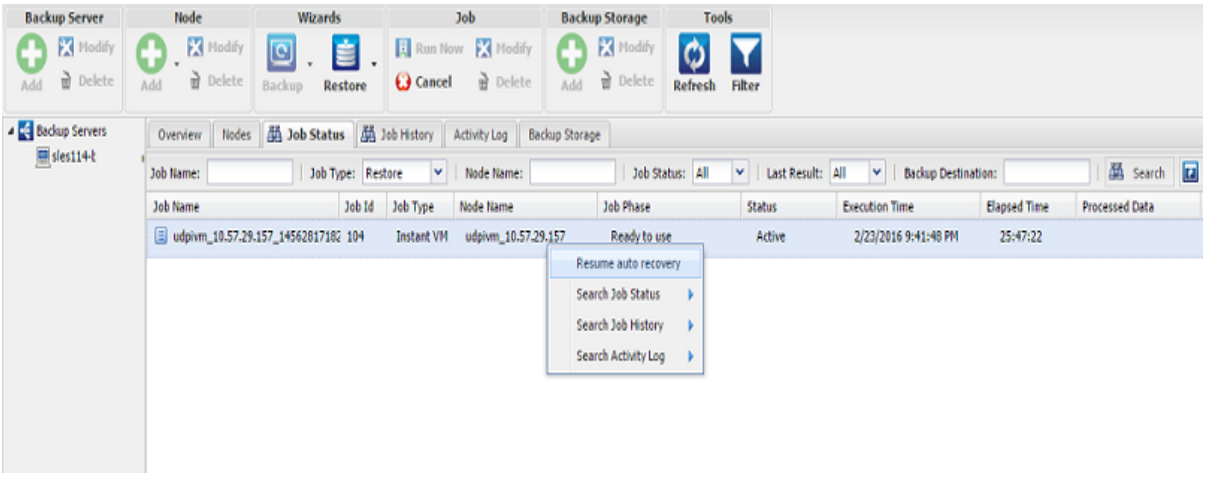
Sie können eine Linux Instant Virtual Machine (IVM) in einen unabhängigen virtuellen Rechner (VM) ändern.

Hinweise:

- Um den Vorgang fortzusetzen, benötigen Sie ein Menüelement, das erst verfügbar ist, wenn die IVM die Jobphase "Bereit zur Verwendung" erreicht hat.
- Die Option ist nicht verfügbar, wenn der Wiederherstellungspunkt eine agentenlose Sicherung und vSphere ESX/VC der Ziel-Hypervisor ist. Um die IVM in eine unabhängige VM zu konvertieren, müssen Sie VMware Storage vMotion verwenden.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Benutzeroberfläche des Linux-Sicherungsservers.



2. Wählen Sie auf der Registerkarte "Jobstatus" den IVM-Job aus, und klicken Sie mit der rechten Maustaste auf den Job, um das Kontextmenü aufzurufen.
3. Wählen Sie "Automatische Wiederherstellung wieder aufnehmen".

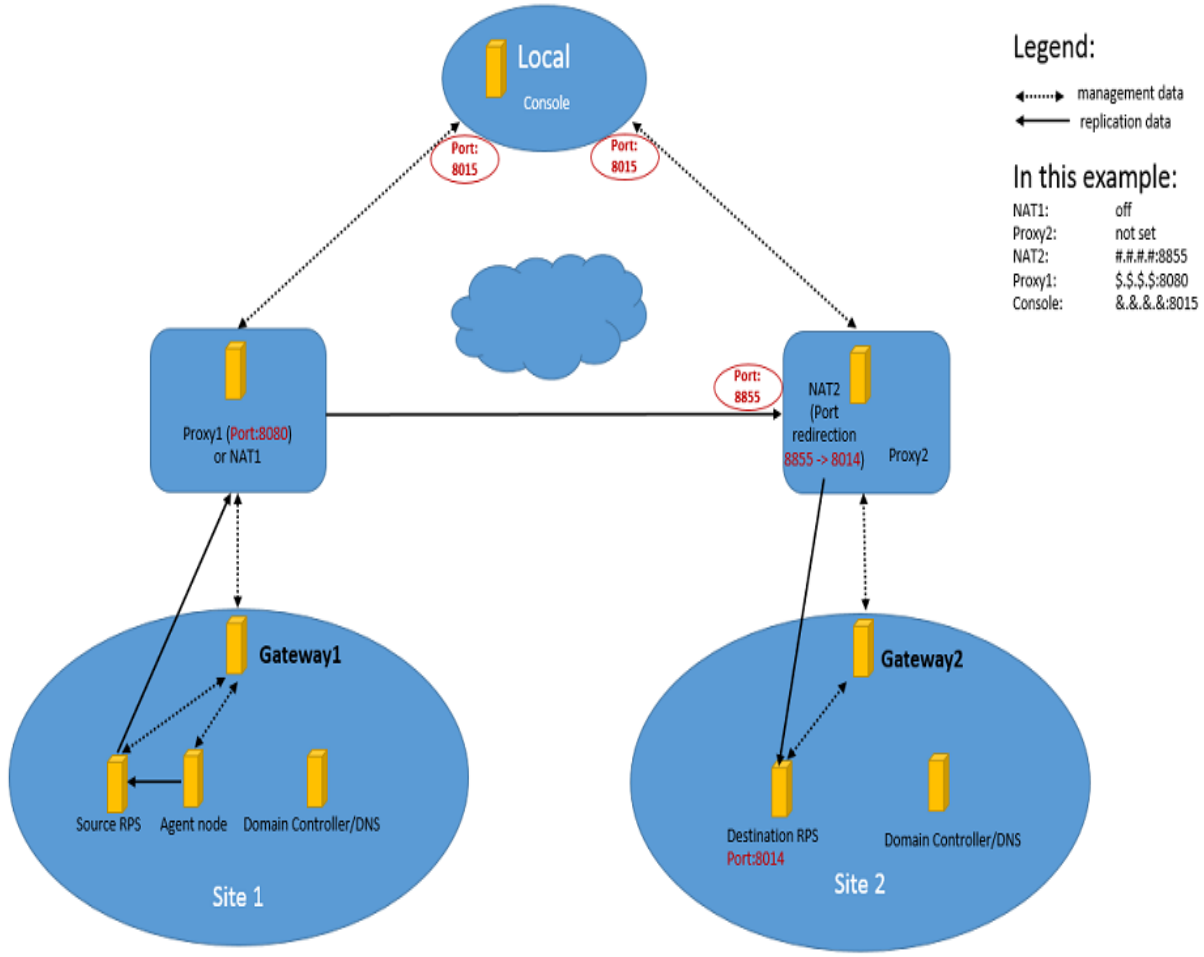
   Nach erfolgreichem Abschluss des Vorgangs wird der IVM-Job in die Jobübersicht verschoben.

Migrieren der Linux-Instant VM von Amazon EC2 auf einen physischen Rechner

Informationen zur Migration der Linux-Instant VM auf einen physischen Rechner finden Sie im Abschnitt **Durchführen einer Migrations-BMR für Linux-Rechner von Amazon EC2 zu lokal** im *Agent for Linux-Benutzerhandbuch*.

So erstellen Sie einen Plan für die Replikation zwischen Standorten

Bei der standortübergreifenden Replikation können Sie Daten zwischen verschiedenen Standorten mit derselben Konsole replizieren. Das folgende Diagramm veranschaulicht die Verbindung zwischen Konsole, Standort 1 und Standort 2:



Die Konsole (z. B. in einem öffentlichen Netzwerk), Standort 1 (z. B. in einem privaten Netzwerk) und Standort 2 (z. B. in einem anderen privaten Netzwerk) können sich in unterschiedlichen Netzwerksegmenten befinden. Standort 1 und Standort 2 werden über das Gateway in der Konsole verwaltet.

Die Abbildung zeigt ein Beispiel zur Erläuterung dieser Funktion von UDP, die nur zu Referenzzwecken dient, da die von Ihnen verwendete Umgebung wahrscheinlich anders ist als die hier beschriebene. In diesem Beispiel sollen Daten vom Quell-RPS am Standort 1 auf den Ziel-RPS am Standort 2 repliziert werden. Das Gateway an Standort 1 und Standort 2 kann mithilfe des Proxys oder von NAT eine Verbindung

zur Konsole herstellen. Der Proxy und NAT müssen ordnungsgemäß konfiguriert sein.

Beschreibung des Diagramms:

- Proxy1 oder NAT1 haben sowohl eine öffentliche als auch eine private Schnittstelle. Beispiel: IP-1 als öffentliche IP befindet sich in demselben Segment wie die Konsole, und IP-2 als private IP befindet sich in demselben Segment wie Standort1. In der Netzwerkeinstellung für den Gateway1-Rechner wird als IP des Standard-Gateways die private IP von Proxy1 oder NAT1 festgelegt.
- Proxy2 und NAT2 haben ebenfalls dieselbe Einstellung wie Proxy1/NAT1, nur dass für NAT2 zusätzlich eine Portumleitungsregel konfiguriert werden muss, damit durch diese Zuordnung vom öffentlichen Netzwerk aus auf den privaten Dienst zugegriffen werden kann. In diesem Beispiel ist dies der Quell-RPS, über den die NAT2-Portumleitung mit dem Ziel-RPS eine Verbindung herstellen kann.
- In Windows Server 2012 R2 können Sie die Portumleitung für NAT sowohl in der grafischen Benutzeroberfläche als auch über einen Befehl festlegen. Nachfolgend ist ein Beispielbefehl aufgeführt, der Folgendes bedeutet: Wenn die Adresse https oder http://<NAT2-IP-1>:<Portnummer=8855> über den Quell-RPS-Web-Explorer eingegeben wird, wird auf die Adresse https oder http://<Ziel-RPS-IP=192.168.30.102>:8014 auf dem Ziel-RPS umgeleitet, sodass die Replikation dann von Standort zu Standort erfolgen kann.

netsh interface portproxy add v4tov4 listenport=8855 connectaddress="192.168.30.102" connectport=8014 protocol=tcp

Erstellen eines Plans für die Replikation zwischen Standorten

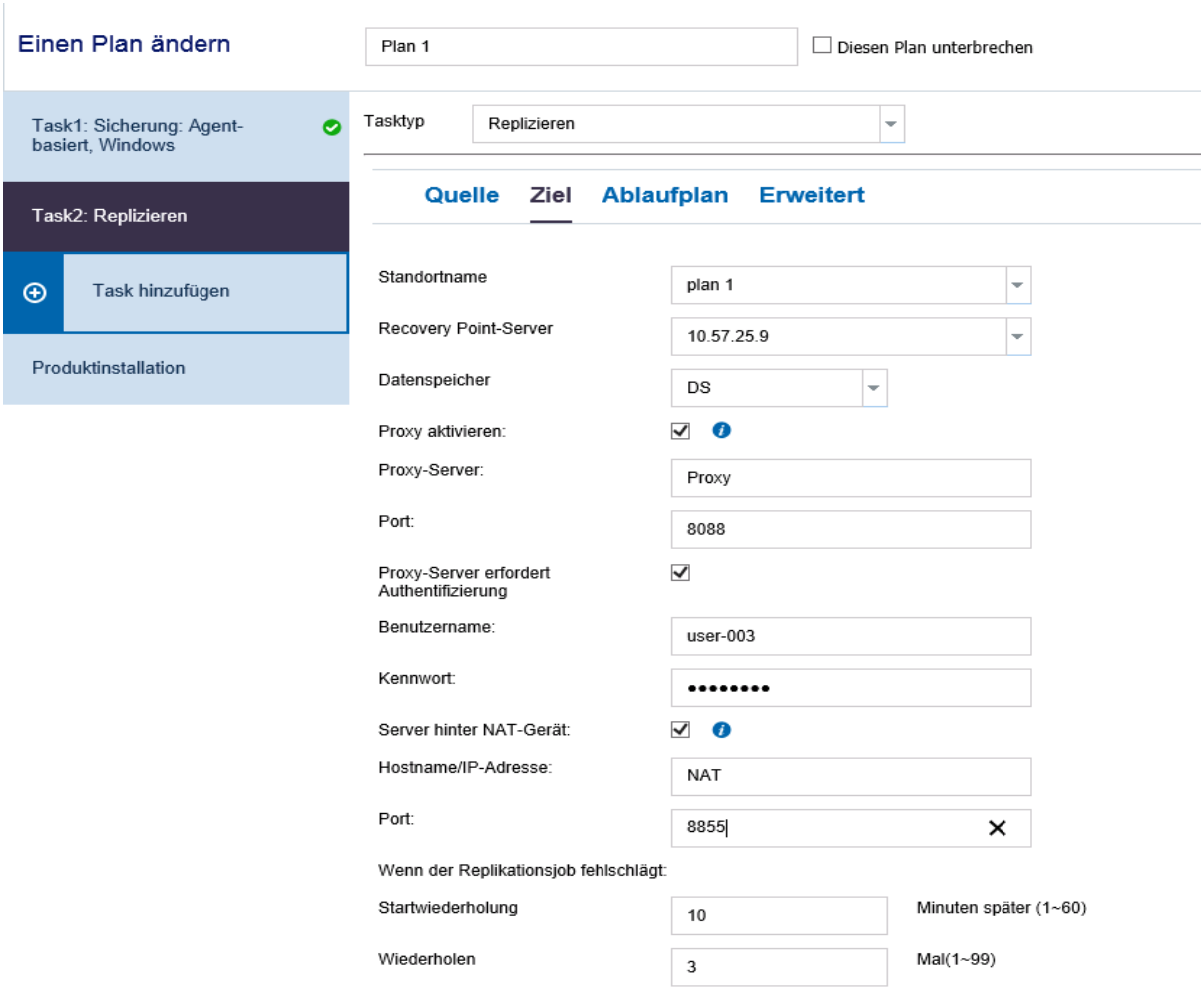
Sie können einen Plan für die Replikation zwischen Standorten erstellen.

Gehen Sie wie folgt vor:

1. Erstellen Sie an Standort 1, dem Quell-RPS, einen Sicherungstask als Task1.
2. Fügen Sie einen Task **Replikation** zum selben Plan hinzu.
3. Wählen Sie auf der Registerkarte **Ziel** den anderen Standort aus (im Beispiel Standort 2), an dem sich der Ziel-RPS oder -Datenspeicher befindet.
4. Optional: Aktivieren Sie die Proxy-Details (Server, Port und Authentifizierung).

   Hinweis: Bevor Sie die Proxy-Details aktivieren, müssen Sie den Proxy-Server zwischen Standort 1 und der Konsole konfigurieren.
5. Aktivieren Sie die NAT-Details (optional).

   Hinweis: Bevor Sie die NAT-Details aktivieren, müssen Sie den NAT-Server und die Portumleitung zwischen der Konsole und Standort 2 konfigurieren.



6. Konfigurieren Sie die anderen Registerkarten wie **Ablaufplan** und **Erweitert**, und speichern Sie den Plan.
7. Wenn der Job ausgeführt wird, überprüfen Sie den Überwachungs- und Protokollstatus für Sicherung, Replikation (ausgehend) und Replikation (eingehend).

Schützen von Microsoft Office 365-Daten

In diesem Abschnitt werden die folgenden Themen behandelt:

Moderne Authentifizierung

Dieser Abschnitt enthält Informationen zum Konfigurieren der Voraussetzungen für die Office 365-Sicherungen mithilfe der modernen Authentifizierung. Gehen Sie zum Konfigurieren der wie folgt vor:

1. Vorbereiten des Proxy-Rechners
2. Konfigurieren einer Anwendung im Azure-Portal
3. Zuweisen der globalen Administratorberechtigungen zur Azure-Anwendung
4. Herunterladen des Zertifikats von UDP und Hochladen in Azure
5. Zuweisen der Rolle für den Identitätswechsel der Anwendung zu dem für die Sicherung angegebenen Benutzerkonto

Vorbereiten des Proxy-Rechners

Dieser Abschnitt enthält Informationen zur Vorbereitung des Proxy-Rechners.

Gehen Sie wie folgt vor:

1. Installieren Sie die PowerShell Version 5.1 oder höher (Teil des Windows Management Framework (WMF)).

   Hinweis: Führen Sie den folgenden Befehl aus, um die PowerShell-Version zu überprüfen:

   Get-Host | Select-Object Version

2. Gehen Sie wie folgt vor, um die erforderlichen Systemkomponenten zu installieren:

   - Gehen Sie folgendermaßen vor, um die erforderlichen Systemkomponenten automatisch zu installieren:

     a. Laden Sie das PowerShell-Skript herunter. Zum Download von klicken Sie auf *Script2InstallPrerequisites.ps1_*.

     b. Benennen Sie *Script2InstallPrerequisites.ps1_* in *Script2InstallPrerequisites.ps1* um.

c. Öffnen Sie das PowerShell-Fenster mithilfe der Option *Als Administrator ausführen*, und führen Sie dann *Script-t2InstallPrerequisites.ps1* aus.

- Führen Sie die folgenden PowerShell-Befehle aus, um die erforderlichen Systemkomponenten manuell zu installieren:
  - *Installationsmodul -Name AzureAD -Force*
  - *Installationsmodul -Name ExchangeOnlineManagement -Force*
  - *Installationsmodul -Name PackageManagement -Force*
  - *Installationsmodul -Name PowerShellGet -Force*

  Hinweis: Wenn Sie PowerShell-Module mithilfe der oben genannten Befehle installieren, wird basierend auf der GA-Version der im Microsoft-Repository verfügbaren Komponente möglicherweise eine neuere Version der Module installiert.

Konfigurieren einer Anwendung im Azure-Portal

Dieser Abschnitt enthält Informationen zum Konfigurieren einer Anwendung im Azure-Portal.

Befolgen Sie diese Schritte:

1. Melden Sie sich beim Azure-Portal an.
2. Führen Sie einen der folgenden Schritte aus, um zur Seite der App-Registrierungen zu navigieren:
   - Wählen Sie im linken Bereich **Azure Active Directory** aus, und klicken Sie dann auf **App-Registrierungen**.
   - Suchen Sie in der Suchleiste nach App-Registrierungen und wählen Sie dann **App-Registrierungen**.
3. Klicken Sie auf der Arcserve-App-Registrierungsseite auf **Neue Registrierung**.
4. Führen Sie auf der Seite Registrieren einer Anwendung die folgenden Schritte aus, und klicken Sie dann auf **Registrieren**:
   - Name: Geben Sie einen Namen für die Anwendung ein. z. B. *UDP365*.
   - Unterstützte Kontotypen: Wählen Sie die Option **Konten nur in diesem Organisationsverzeichnis (nur "Ihre Domäne" – Einzelmandant)**.
5. Kopieren und speichern Sie **Application (Client) ID** für zukünftige Verwendung.

Zuweisen der globalen Administratorberechtigungen zur Azure-Anwendung

Dieser Abschnitt enthält Informationen zum Zuweisen der globalen Administratorberechtigungen zur Azure-Anwendung.

Gehen Sie folgendermaßen vor, um der AzureAD-App die globale Administratorrolle zuzuweisen:

- Gehen Sie folgendermaßen vor, um die Rolle automatisch zuzuweisen:
  1. Laden Sie das PowerShell-Skript herunter. Zum Herunterladen klicken Sie auf *AssignGlobalAdminRoleToADApplication.ps1*.
  2. Öffnen Sie das PowerShell-Fenster mithilfe der Option *Als Administrator ausführen*, navigieren Sie zum Pfad des heruntergeladenen Skripts, und führen Sie dann Folgendes aus:

     .\AssignGlobalAdminRoleToADApplication.ps1 <Vom Azure-Portal generierte Anwendungs-ID (Client)>

     Beispiel:

     .\AssignGlobalAdminRoleToADApplication.ps1 60f92079-d1bf-40f7-9ab5-59caab8e7534
- Um die Rolle mithilfe der PowerShell-Cmdlets manuell zuzuweisen, gehen Sie folgendermaßen vor:
  1. Führen Sie den folgenden Befehl im PowerShell-Fenster unter Verwendung der Option "Als Administrator ausführen" aus, um das MSOnline-Modul zu installieren:

     Install-Module MSOnline
  2. Führen Sie den folgenden Befehl aus, um eine Verbindung zu Azure Active Directory (AzureAD) zu initiieren:

     Connect-MSolService
  3. Rufen Sie die App-ID mithilfe des folgenden Befehls ab:

     $sp = Get-MsolServicePrincipal -AppPrincipalID <APP-ID-GUID>

     Hinweis: APP-ID-GUID ist die Anwendungs-ID der UDP-Anwendung.
  4. Rufen Sie die Rolle "Globaler Administrator/Unternehmensadministrator" mithilfe des folgenden Befehls ab:

     $role = Get-MsolRole -RoleName "Unternehmensadministrator"

5. Verwenden Sie den folgenden Befehl, um der AzureAD-App die Rolle "Globaler Administrator/Unternehmensadministrator" hinzuzufügen:

   Add-MsolRoleMember -RoleObjectId $role.ObjectId -RoleMemberType ServicePrincipal -RoleMemberObjectId $Sp.ObjectId

Herunterladen des Zertifikats von UDP und Hochladen in Azure

Dieser Abschnitt enthält Informationen zum Herunterladen des Zertifikats von UDP und Hochladen des Zertifikats in das Azure-Portal.

Führen Sie auf der UDP-Konsole beim Erstellen eines neuen oder vorhandenen Office 365-Plans für Exchange Online, SharePoint oder OneDrive eine der folgenden Aktionen aus:

Methode 1: Gehen Sie folgendermaßen vor, um ein neues selbstsigniertes Zertifikat für die Authentifizierung zu generieren und herunterzuladen:

1. Um ein neues selbstsigniertes Zertifikat zu generieren, wählen Sie in Schritt **Neues selbstsigniertes Zertifikat generieren und herunterladen** aus.
2. Geben Sie das Zertifikatskennwort ein, und bestätigen Sie es nach Bedarf.
3. Um das Zertifikat herunterzuladen, klicken Sie auf eine der folgenden Optionen:
   - **Öffentliches Zertifikat**: Laden Sie das Zertifikat herunter, um es im Azure-Portal hochzuladen.
   - **Privates Zertifikat:** Laden Sie das Zertifikat herunter, um es für die zukünftige Verwendung auf Ihrem Computer zu speichern.

     Hinweis: Nachdem Sie das öffentliche Zertifikat heruntergeladen haben, wird die Download-Option für das private Zertifikat aktiviert.
4. Melden Sie sich beim Azure-Portal an.
5. Suchen Sie in der Suchleiste nach App-Registrierungen und wählen Sie dann **App-Registrierungen**.
6. Klicken Sie in der Liste der registrierten Apps auf die Anwendung, die zuvor im Abschnitt *Konfigurieren einer Anwendung im Azure-Portal* erstellt wurde.
7. Navigieren Sie zu „Zertifikate & Geheimnisse“, klicken Sie auf **Zertifikat hochladen**, suchen Sie Ihr vorhandenes Zertifikat [.cer-Datei], und klicken Sie dann auf **Hinzufügen**.
8. Wählen Sie im linken Fensterbereich API-Berechtigungen aus, und klicken Sie dann auf **<Admin-Zustimmung> für <Mandantenname>**.

Eine Bestätigungsmeldung wird angezeigt.

9. Klicken Sie auf **Ja**.
10. Klicken Sie in der UDP-Konsole auf **Weiter**, um mit der Knotenregistrierung fortzufahren.

Methode 2: Um sich mit einem vorhandenen Zertifikat zu authentifizieren, gehen Sie folgendermaßen vor:

Hinweise:

- Wenn die Option *Vorhandenes Zertifikat verwenden* aktiviert ist, werden die Zertifikatsdateien (.cer-Datei) und Zertifikate des privaten Schlüssels (.PFX-Datei mit Kennwort) des Benutzers erwartet. Diese Zertifikate können selbst-signiert oder von einer Zertifizierungsstelle signiert sein.
- Wenn dasselbe Zertifikat für mehrere Planerstellungen verwendet wird, reicht es aus, das Zertifikat nur einmal ins Azure-Portal hochzuladen.
- Falls Sie Internet Explorer (IE 11) verwenden, wird der weitere Vorgang bei Auswahl der Option *Vorhandenes Zertifikat verwenden* blockiert. Informationen zur Behebung dieses Problems finden Sie unter Konfigurieren der Sicherheitseinstellungen von Internet Explorer (IE 11).

1. Melden Sie sich beim Azure-Portal an.
2. Suchen Sie in der Suchleiste nach App-Registrierungen und wählen Sie dann **App-Registrierungen**.
3. Klicken Sie in der Liste der registrierten Apps auf die Anwendung, die zuvor im Abschnitt *Konfigurieren einer Anwendung im Azure-Portal* erstellt wurde.
4. Navigieren Sie zu "Zertifikate & Geheimnisse", klicken Sie auf **Zertifikat hochladen**, suchen Sie Ihr vorhandenes Zertifikat [.cer-Datei], und klicken Sie dann auf **Hinzufügen**.
5. Wählen Sie im linken Fensterbereich API-Berechtigungen aus, und klicken Sie dann auf **<Admin-Zustimmung> für <Mandantenname>**.

   Eine Bestätigungsmeldung wird angezeigt.
6. Klicken Sie auf **Ja**.
7. Führen Sie diese Schritte über die UDP-Konsole aus:
   a. Suchen Sie das Zertifikat für den privaten Schlüssel [PFX-Datei], und geben Sie das Kennwort ein.
   b. Klicken Sie auf **Weiter**, um mit der Knotenregistrierung fortzufahren.

Zuweisen der Rolle für den Identitätswechsel der Anwendung zu dem für die Sicherung angegebenen Benutzerkonto

Dieser Abschnitt enthält Informationen zum Hinzufügen des Sicherungskontos zur Rollengruppe "Discoveryverwaltung" und zum Zuweisen der Berechtigung "Anwendungsidentitätswechsel".

Gehen Sie folgendermaßen vor, um die erforderliche Rolle und Gruppe hinzuzufügen:

Methode 1: Verwenden des Office 365-Portals

Befolgen Sie diese Schritte:

1. Melden Sie sich als Administrator oder mit einem Konto, das über globale Administratorberechtigungen verfügt, beim Office 365-Portal an.

   Die Seite "Exchange Online Admin Center" wird angezeigt.

2. Gehen Sie zu **Berechtigungen**, und doppelklicken Sie in der Drop-down-Liste **Hinzufügen** auf **Discoveryverwaltung**.

   Das Dialogfeld "Discoveryverwaltung" wird angezeigt.

   Hinweis: Mitglieder der Rollengruppe "Discoveryverwaltung" können Postfächer in der Exchange-Organisation nach Daten durchsuchen, die bestimmte Kriterien erfüllen.

3. Klicken Sie unter **Rollen** auf **+**, um die Rolle *ApplicationImpersonation* hinzuzufügen.

   Das Dialogfeld "Rolle auswählen" wird angezeigt.

4. Wählen Sie in der Drop-down-Liste **Anzeigename** den Eintrag **ApplicationImpersonation** aus.

   Hinweis: Die Rolle *ApplicationImpersonation* erlaubt es Anwendungen, die Identität eines Benutzers in einer Organisation anzunehmen, um Aufgaben im Namen des Benutzers auszuführen.

5. Klicken Sie auf **Hinzufügen**, um die Rolle "ApplicationImpersonation" hinzuzufügen, und klicken Sie dann auf **OK**.

6. Klicken Sie im Dialogfeld "Discoveryverwaltung" unter **Mitglieder** auf **+**, um das Sicherungskonto als Mitglied hinzuzufügen.

   Das Dialogfeld "Mitglieder auswählen" wird angezeigt.

7. Wählen Sie in der Drop-down-Liste "Name" das Sicherungskonto aus, klicken Sie auf **Hinzufügen**, um das Mitglied hinzuzufügen, und klicken Sie dann auf **OK**.

   Das ausgewählte Sicherungskonto wird unter **Mitglieder** im Dialogfeld **Discoveryverwaltung** angezeigt.

8. Klicken Sie auf **Speichern**.

Methode 2: Verwenden von Remote-PowerShell

Befolgen Sie diese Schritte:

1. Stellen Sie über Remote-PowerShell eine Verbindung zum Exchange Online-Mandanten her. Weitere Informationen finden Sie unter Verbinden mit Exchange Online PowerShell.
2. Sobald die Verbindung aufgebaut ist, können Sie folgendes Cmdlet verwenden, um das Sicherungskonto als Mitglied zur Rollengruppe "Discoveryverwaltung" hinzuzufügen:

   ```
   Cmdlet "Add-RoleGroupMember"
   ```

   Beispiel: *Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.*

3. Verwenden Sie Folgendes, um dem Sicherungskonto die Rolle "ApplicationImpersonation" hinzuzufügen:

   ```
   Cmdlet "New-ManagementRoleAssignment"
   ```

   Beispiel: *New-ManagementRoleAssignment Name: impersonationAssignmentName -Role:ApplicationImpersonation - User: "username@domain.onmicrosoft.com"*

Die Rolle *ApplicationImpersonation* und die Gruppe "Mitglieder" werden zum Exchange Online-Sicherungskonto hinzugefügt.

Erstellen eines Exchange Online-Sicherungsplans

Exchange Online ist eine E-Mail-Anwendung, die in der Microsoft-Cloud gehostet wird. Um Ihre Exchange Online-E-Mail-Elemente (E-Mails, Kalenderelemente, Kontakte usw.) aus der Microsoft-Cloud zu sichern, müssen Sie einen Plan erstellen. Der Plan für Exchange Online besteht aus einem Sicherungstask. In diesem Sicherungstask können Sie die Exchange Online-Knoten, die Sie schützen möchten, das Sicherungsziel und den Ablaufplan für die Sicherung angeben.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen eines Plans für Exchange Online-Sicherungen
3. (Optional) Ausführen einer manuellen Sicherung
4. Konfigurieren der Multi-Faktor-Authentifizierung

Überprüfen der Voraussetzungen und Hinweise

Überprüfen Sie die folgenden Voraussetzungen und Hinweise, bevor Sie einen Exchange Online-Sicherungsplan erstellen.

Erstellen eines Plans für Exchange Online-Sicherungen:

Voraussetzungen:

Für das Sicherungskonto:

- Verwenden Sie ein Sicherungsdienstkonto mit den Rechten für einen globalen Administrator.
- Fügen Sie die Berechtigung zum Identitätswechsel für den Sicherungsbenutzer zum Exchange Online-Sicherungskonto hinzu, um die Online Exchange-Organisation zu verbinden und Sicherungen und Wiederherstellungen durchzuführen.

  Hinweis: Wenn Sie das Sicherungskonto nicht zur Rollengruppe "Discoveryverwaltung" hinzufügen und nicht die Berechtigung "ApplicationImpersonation" zuweisen, schlägt die Sicherung fehl.

- Ordnen Sie dem Backup-Benutzerkonto ein Exchange Online-Postfach zu.

Für Sicherungs-Proxy:

- Melden Sie sich bei der Konsole an.
- Installieren Sie Arcserve UDP Agent auf dem Proxy-Rechner, auf dem die Sicherung/Wiederherstellung ausgeführt werden soll.

Besondere Aspekte:

- Beim Sichern einer großen Gruppe von Benutzern können Sie für eine bessere Sicherung und Optimierung Exchange-Gruppen verwenden.
- Die Standardeinstellung für die Online-Sicherung von Exchange verwendet 4 gleichzeitige Sicherungs-Threads (einen Thread pro Benutzer). Sie können auch die Threads in der Konfigurationsdatei *Engine\BIN\Office365\Arcserve.Office365.Exchange.config* wie folgt ändern:

```
<!--#region for multi thread--> <!--MultiThreadEnable default
value:0. if enable, set 1.--> <add
key="MultiThreadEnable" value ="1"/> <!--set how many thread
will be used to backup mailbox. Standardwert ist 4--> <add
key="MaxDegreeOfParallelismForMailbox" value="4"/> <!--#end-
```

```
region-->
```

Wir empfehlen, den Wert auf 1 bis 5 festzulegen. Der maximal mögliche Wert ist 10. Es wird nicht empfohlen, den Wert von 6 bis 10 festzulegen.

Hinweis: UDP 8.0 unterstützt Folgendes:

- Benutzerpostfach
- Freigegebenes Postfach
- E-Mail-aktivierte öffentliche Ordner
- Raumpostfächer
- Gerätepostfächer
- Gruppenpostfächer

Hinweis: Weitere Informationen zu den Best Practices für Exchange Online finden Sie unter Exchange Online.

Erstellen eines Exchange Online-Sicherungsplans mit Basisauthentifizierung (BA):

Überprüfen Sie die folgenden Voraussetzungen:

- Installieren Sie die PowerShell Version 5.1 oder höher (Teil des Windows Management Framework (WMF)) auf dem Proxy-Server (64-Bit-Computer).
- Installieren Sie mithilfe der Befehlszeile die folgenden PowerShell-Module auf dem Proxy-Server unter Verwendung des PowerShell-Fensters:
  - Führen Sie den folgenden Befehl aus, um das Azure-Modul zu installieren:

    Installationsmodul -Name AzureAD -Force
  - Führen Sie den folgenden Befehl aus, um das ExchangeOnlineManagement-Modul zu installieren:

    Installationsmodul -Name ExchangeOnlineManagement -Force

Hinweis: Wenn Sie PowerShell-Module mithilfe der oben genannten Befehle installieren, wird basierend auf der GA-Version der im Microsoft-Repository verfügbaren Komponente möglicherweise eine neuere Version der Module installiert.

Erstellen eines Exchange Online-Sicherungsplans mithilfe der modernen Authentifizierung (MA):

Überprüfen Sie die Voraussetzungen, bevor Sie einen Plan unter Verwendung der modernen Authentifizierung erstellen.

Zuweisen der Rolle für den Identitätswechsel der Anwendung zu dem für die Sicherung angegebenen Benutzerkonto

Dieser Abschnitt enthält Informationen zum Hinzufügen des Sicherungskontos zur Rollengruppe "Discoveryverwaltung" und zum Zuweisen der Berechtigung "Anwendungsidentitätswechsel".

Gehen Sie folgendermaßen vor, um die erforderliche Rolle und Gruppe hinzuzufügen:

Methode 1: Verwenden des Office 365-Portals

Befolgen Sie diese Schritte:

1. Melden Sie sich als Administrator oder mit einem Konto, das über globale Administratorberechtigungen verfügt, beim Office 365-Portal an.

   Die Seite "Exchange Online Admin Center" wird angezeigt.

2. Gehen Sie zu **Berechtigungen**, und doppelklicken Sie in der Drop-down-Liste **Hinzufügen** auf **Discoveryverwaltung**.

   Das Dialogfeld "Discoveryverwaltung" wird angezeigt.

   Hinweis: Mitglieder der Rollengruppe "Discoveryverwaltung" können Postfächer in der Exchange-Organisation nach Daten durchsuchen, die bestimmte Kriterien erfüllen.

3. Klicken Sie unter **Rollen** auf **+**, um die Rolle *ApplicationImpersonation* hinzuzufügen.

   Das Dialogfeld "Rolle auswählen" wird angezeigt.

4. Wählen Sie in der Drop-down-Liste **Anzeigename** den Eintrag **ApplicationImpersonation** aus.

   Hinweis: Die Rolle *ApplicationImpersonation* erlaubt es Anwendungen, die Identität eines Benutzers in einer Organisation anzunehmen, um Aufgaben im Namen des Benutzers auszuführen.

5. Klicken Sie auf **Hinzufügen**, um die Rolle "ApplicationImpersonation" hinzuzufügen, und klicken Sie dann auf **OK**.

6. Klicken Sie im Dialogfeld "Discoveryverwaltung" unter **Mitglieder** auf **+**, um das Sicherungskonto als Mitglied hinzuzufügen.

   Das Dialogfeld "Mitglieder auswählen" wird angezeigt.

7. Wählen Sie in der Drop-down-Liste "Name" das Sicherungskonto aus, klicken Sie auf **Hinzufügen**, um das Mitglied hinzuzufügen, und klicken Sie dann auf **OK**.

   Das ausgewählte Sicherungskonto wird unter **Mitglieder** im Dialogfeld **Discoveryverwaltung** angezeigt.

8. Klicken Sie auf **Speichern**.

Methode 2: Verwenden von Remote-PowerShell

Befolgen Sie diese Schritte:

1. Stellen Sie über Remote-PowerShell eine Verbindung zum Exchange Online-Mandanten her. Weitere Informationen finden Sie unter Verbinden mit Exchange Online PowerShell.
2. Sobald die Verbindung aufgebaut ist, können Sie folgendes Cmdlet verwenden, um das Sicherungskonto als Mitglied zur Rollengruppe "Discoveryverwaltung" hinzuzufügen:

   ```
   Cmdlet "Add-RoleGroupMember"
   ```

   Beispiel: *Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.*

3. Verwenden Sie Folgendes, um dem Sicherungskonto die Rolle "ApplicationImpersonation" hinzuzufügen:

   ```
   Cmdlet "New-ManagementRoleAssignment"
   ```

   Beispiel: *New-ManagementRoleAssignment Name: impersonationAssignmentName -Role:ApplicationImpersonation - User: "username@domain.onmicrosoft.com"*

Die Rolle *ApplicationImpersonation* und die Gruppe "Mitglieder" werden zum Exchange Online-Sicherungskonto hinzugefügt.

Erstellen eines Plans für Exchange Online-Sicherungen

Ein Sicherungsplan enthält einen Sicherungstask, der Exchange Online-E-Mail-Datenelemente (E-Mails, Kalenderelemente, Kontakte usw.) sichert und die Daten auf einem Datenspeicher ohne oder mit Deduplizierung speichert. Darüber hinaus ermöglicht dieser Sicherungsplan es UDP, Exchange Online-Gruppen zu erkennen und anzugeben, für die ein Sicherungstask ausgeführt wird. Jeder Task besteht aus Parametern, die Quelle, Ziel, Ablaufplan und weitere Sicherungsdetails definieren.

Gehen Sie wie folgt vor:

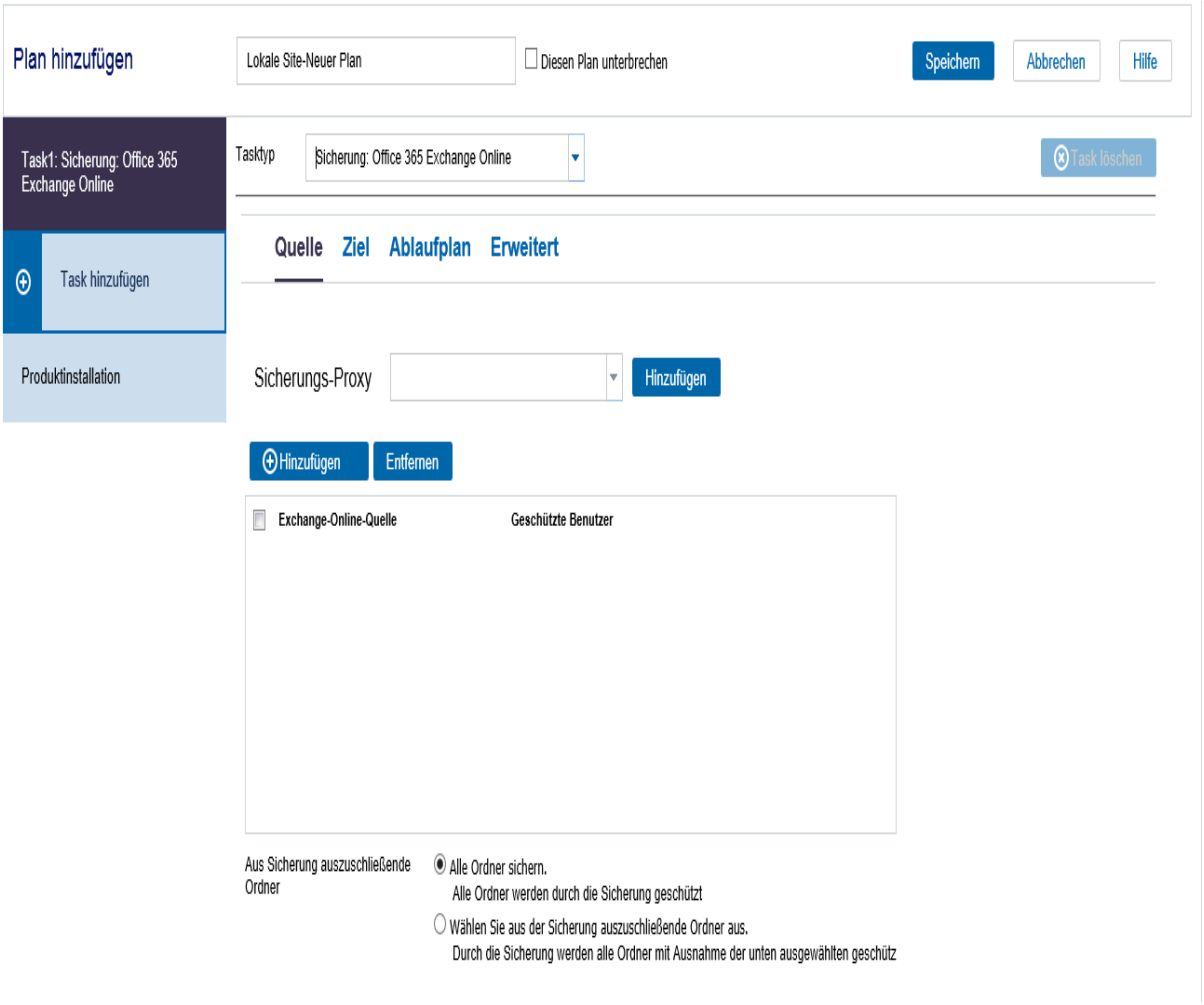
1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Das Dialogfenster **Plan hinzufügen** wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Drop-down-Liste Tasktyp die Option **Sicherung: Office 365 Exchange Online** aus.



Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Angeben der Quelle

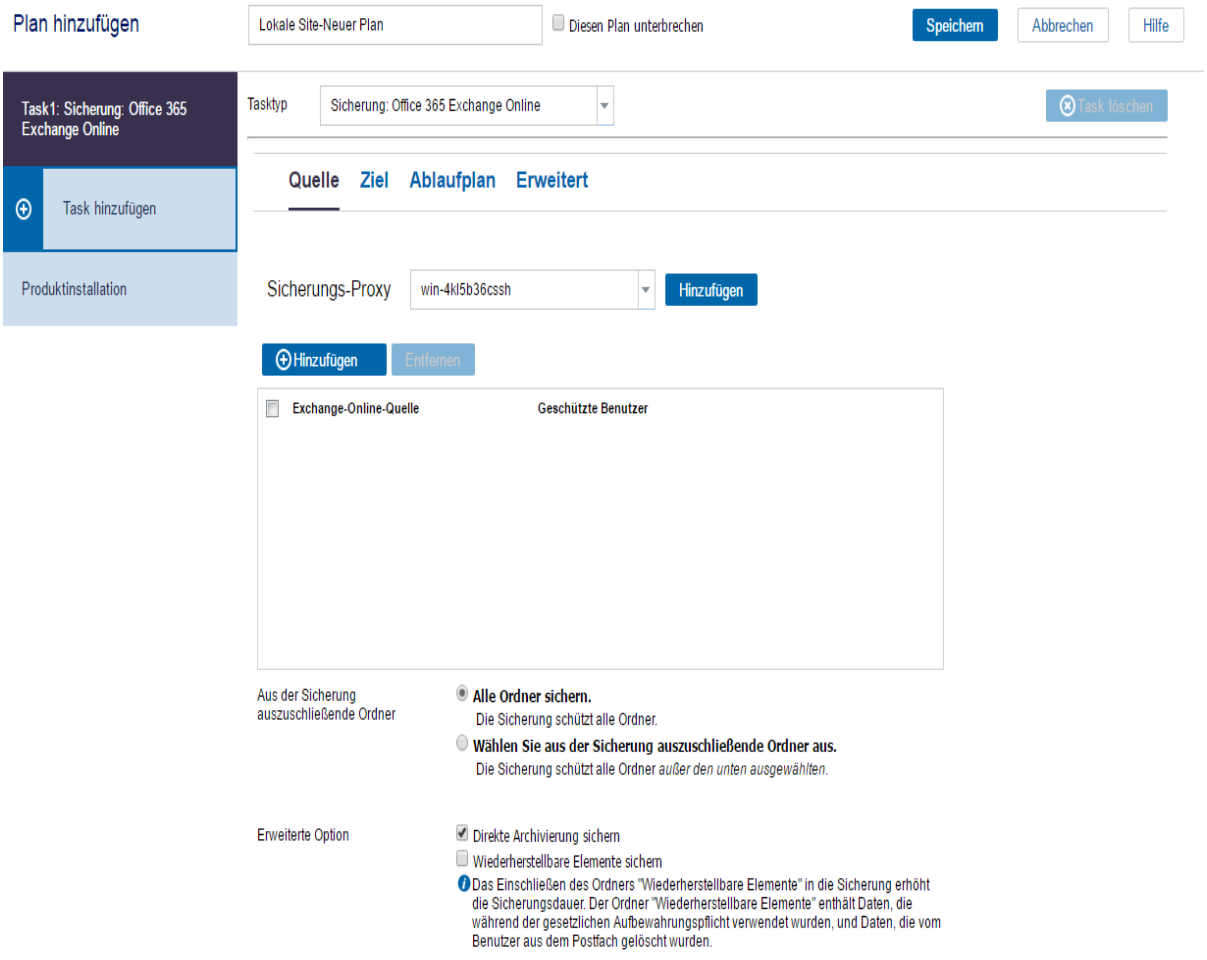
Auf der Seite "Quelle" können Sie die Exchange Online-Quellknoten angeben, die Sie schützen möchten. Sie können für einen Plan mehrere Exchange Online-Quellknoten auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Exchange Online-Quellknoten von der Quellseite hinzufügen.

Hinweis: Sie können einen Plan speichern, ohne Quellknoten hinzuzufügen. Der Plan wird jedoch nur bereitgestellt, wenn Sie Knoten hinzufügen.

Sie können auch Exchange Online Knoten verwalten, indem Sie die Postfachunterstützung für öffentliche Ordner für Exchange Online-Schutz verwenden.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Quelle**.



2. Für "Sicherungs-Proxy" haben Sie folgende Möglichkeiten:

- Wählen Sie in der Drop-down-Liste einen vorhandenen Sicherungs-Proxy aus.
- Um einen neuen Sicherungs-Proxy hinzuzufügen, klicken Sie neben der Drop-down-Liste auf **Hinzufügen**.

3. Fügen Sie mithilfe einer der folgenden Optionen einen Exchange Online-Knoten hinzu:

   Methode 1

   a. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Wählen Sie zu sichernde Quellen in Arcserve UDP aus**.

      Das Dialogfeld "Knoten zu Plan hinzufügen" wird angezeigt.

   b. Wählen Sie einen Knoten aus, und klicken Sie dann auf **Verbinden**.

      Hinweis: Sie können auch in der **Suche** nach den Exchange Online-Knoten suchen, die Sie schützen möchten.

   c. Aktivieren Sie das Kontrollkästchen **Alle Office 365 Exchange-Quellen schützen**, um alle Exchange Online-Konten auf allen Seiten zu schützen.

      Hinweis: Klicken Sie auf den Rechtspfeil (>), um alle Exchange Online-Konten zur Liste der geschützten Knoten hinzuzufügen.

      Die Exchange Online-Konten, die Sie ausgewählt haben, werden hinzugefügt.

   Methode 2

   - Klicken Sie auf **Hinzufügen** und dann auf **Exchange Online-Quelle hinzufügen**.

     Das Dialogfeld "Knoten zu Plan hinzufügen" wird geöffnet.

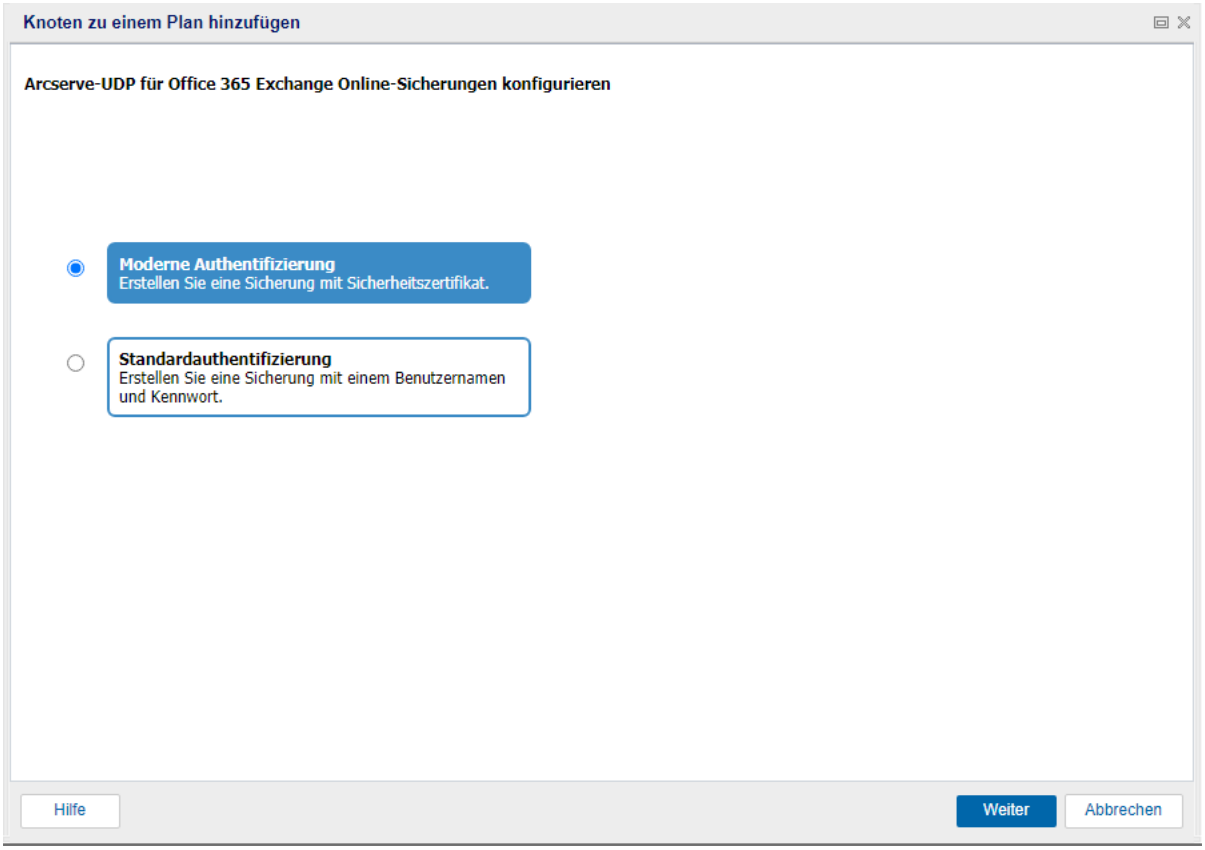
     Hinweis: Anders als andere Knoten können Sie Exchange Online-Knoten nicht über die Seite **Alle Knoten** hinzufügen. Sie können einen Exchange Online-Knoten nur in einem Plan hinzufügen, oder wenn Sie einen Plan ändern.

     Mehrere Exchange Online-Knoten können dasselbe Benutzerkonto (Dienstkonto) von Exchange online verwenden.

4. Gehen Sie folgendermaßen vor, um die Authentifizierung anzuwenden:

   Moderne Authentifizierung

   Bei der modernen Authentifizierung können Sie eine Sicherung mithilfe eines Sicherheitszertifikats ausführen.



Sicherheitszertifikat verwenden

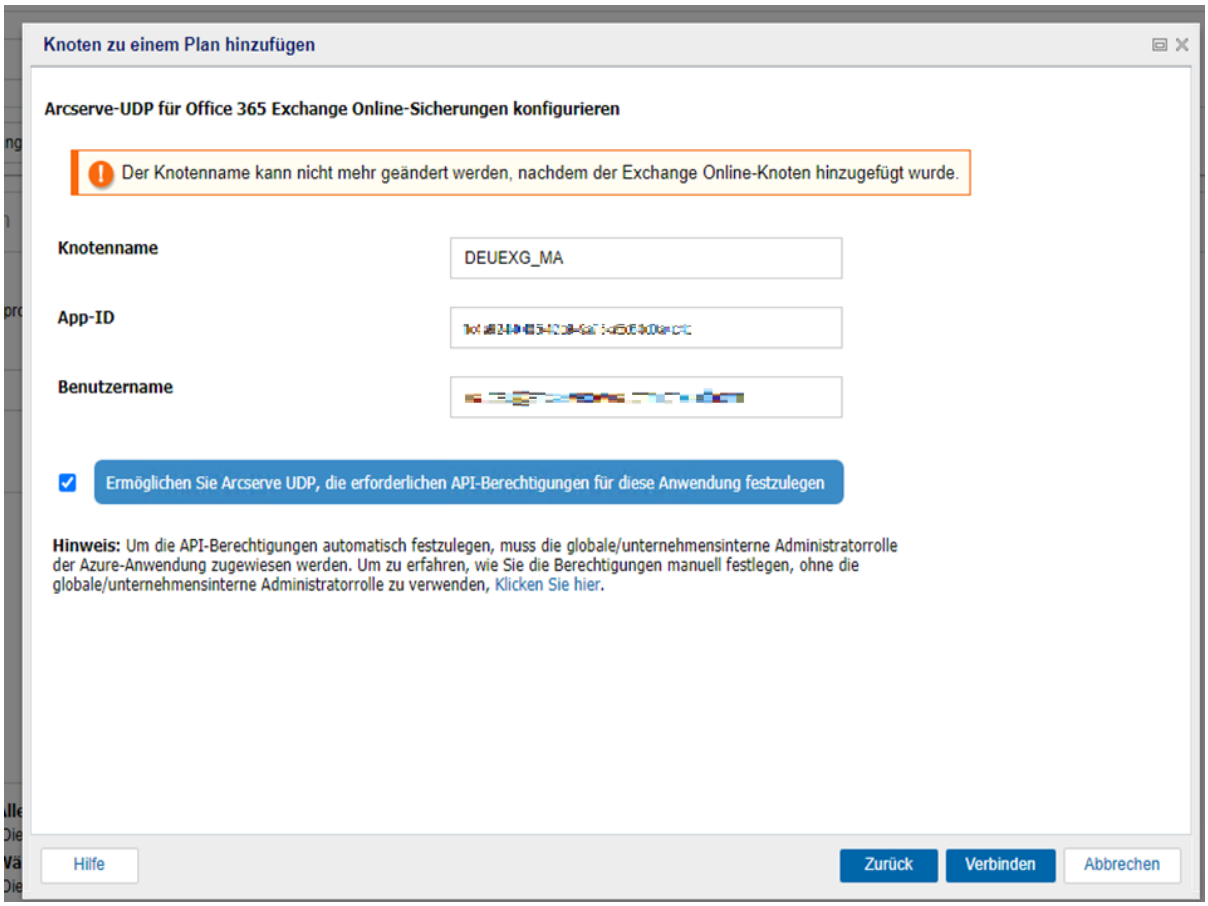
Hinweis: Standardmäßig wählt der Sicherungsplan die Option **Sicherheitszertifikat verwenden** für die moderne Authentifizierung aus.

Gehen Sie wie folgt vor:

a. Informationen zum Authentifizieren der UDP-Anwendung mit Sicherheitszertifikaten finden Sie unter Herunterladen des Zertifikats von UDP und Hochladen in Azure.

b. Geben Sie die folgenden Details ein:

- Knotenname
- App-ID
- Benutzername



c. Um die API-Berechtigungen automatisch anzuwenden, aktivieren Sie das Kontrollkästchen **Arcserve UDP erlauben, die erforderlichen API-Berechtigungen für diese Anwendung festzulegen**.

   Hinweis: Informationen zum manuellen Anwenden der Berechtigungen ohne Verwendung der Administratorrolle "Global/Company" finden Sie unter Manuelles Konfigurieren der API-Berechtigungen ohne Verwendung der Administratorrolle "Global/Company".

d. Klicken Sie auf **Connect**.

Hinweise:

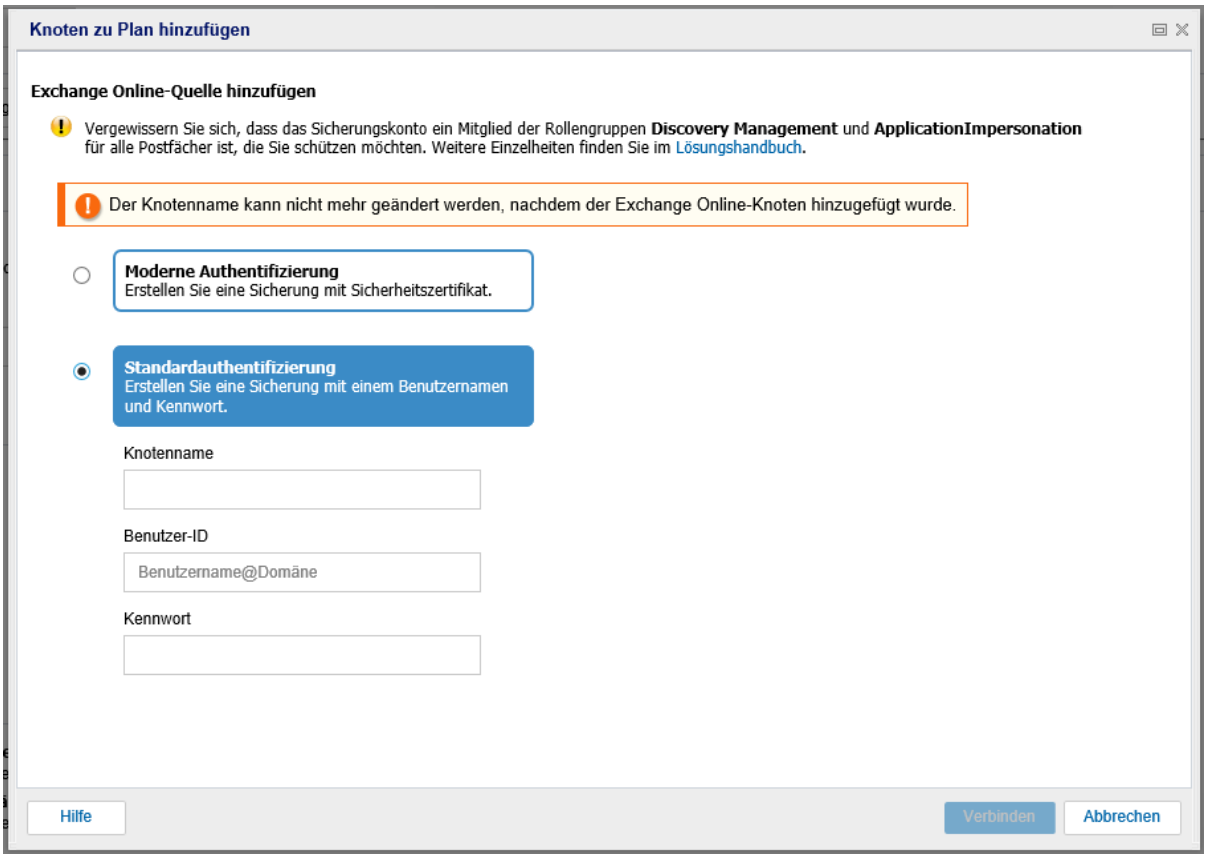
- Der Name des Exchange Online-Knotens kann nicht mehr geändert werden, nachdem der Knoten hinzugefügt wurde.
- Geben Sie in **Admin-Benutzername** den Benutzernamen des Exchange Online-Sicherungskontos ein, der die Voraussetzungen erfüllt.
- Die moderne Authentifizierung gilt nicht für Folgendes:

- Für Kunden, die Microsoft 365 (Office 365) für ihre Arcserve Cloud Hybrid-Instanzen oder Arcserve Cloud Backup für Office 365 mit einem Erstellungsdatum von vor dem 18. Oktober 2020 verwenden, ist die moderne Authentifizierung nicht möglich.
- Kunden, die weiterhin die Standardauthentifizierung verwenden

Standardauthentifizierung

Um bei Verwendung der Standardauthentifizierung mit der Sicherung fortzufahren, geben Sie die folgenden Informationen an, und klicken Sie dann auf **Verbinden**:

- Knotenname
- Benutzer-ID
- Kennwort



Hinweis: Das Aktualisieren oder Ändern des Benutzerkontos kann die Anzahl geschützter Postfächer ändern. Sie müssen sicherstellen, dass die neuen oder aktualisierten Dienstkonten Identitätswechselrechte für zu schützende Postfächer besitzen.

5. Zum Schützen von Exchange Online-Postfächern haben Sie folgende Möglichkeiten:

   - Um alle Exchange Online-Postfächer und -Gruppen zu schützen, aktivieren Sie das Kontrollkästchen **Die gesamte Office 365 Exchange-Quelle schützen**.

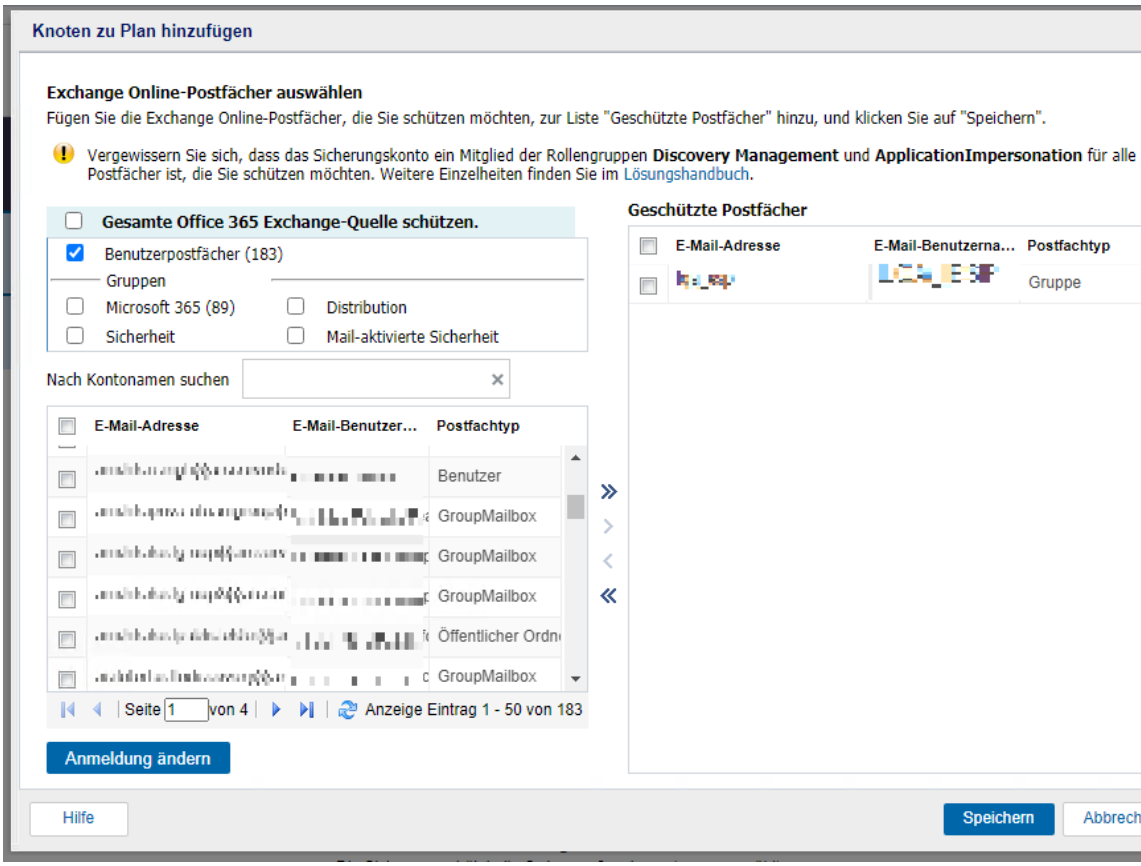
     Hinweis: Bei Anzeige des Bildschirms "Exchange Online-Postfächer auswählen" ist diese Option standardmäßig automatisch ausgewählt.

   - Gehen Sie für Benutzerpostfächer folgendermaßen vor:

     a. Aktivieren Sie das Kontrollkästchen **Benutzerpostfächer**.

        Eine Liste von Benutzerpostfächern wird angezeigt.

     b. (Optional) Um in der Liste nach einem Konto zu suchen, geben Sie den Kontonamen im Feld "Nach Kontonamen suchen" ein.



     c. Wählen Sie die zu schützenden Postfächer in der Liste der Benutzerpostfächer aus.

     d. Klicken Sie auf den Nach-rechts-Pfeil (>), um die ausgewählten Postfächer in die Liste "Geschützte Postfächer" zu verschieben.

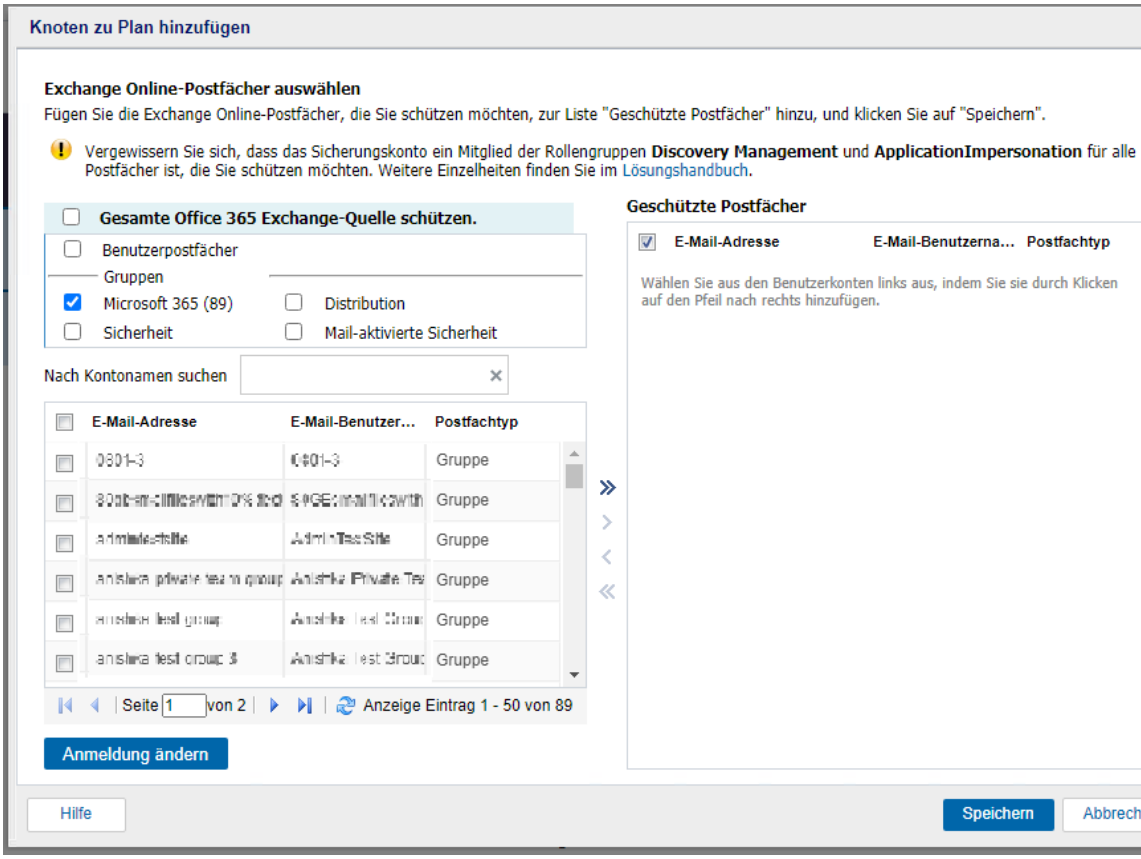
- Gehen Sie für Gruppen folgendermaßen vor:

  a. Aktivieren Sie das Kontrollkästchen **Microsoft 365**.

     Eine Liste von Gruppen wird angezeigt.

     Hinweis: Wenn Sie Gruppen zusammen mit Untergruppen wie **Distribution**, **Sicherheit** oder **Mail-aktivierte Sicherheit** auswählen möchten, aktivieren Sie das Kontrollkästchen **Microsoft 365** und anschließend nach Bedarf das Kontrollkästchen für eine Untergruppe.

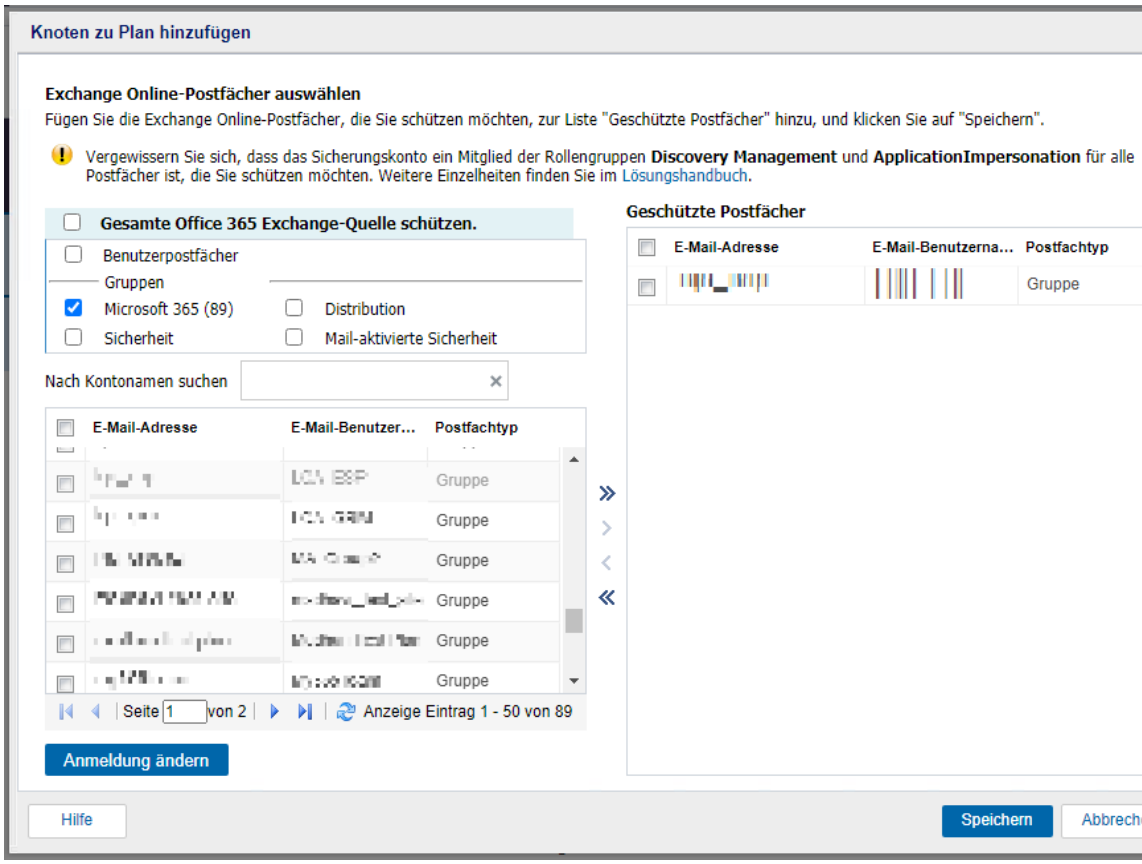
  b. (Optional) Um in der Liste nach einem Konto zu suchen, geben Sie den Kontonamen im Feld "Nach Kontonamen suchen" ein.



  c. Wählen Sie die zu schützenden Gruppen in der Liste der Gruppen aus.

  d. Klicken Sie auf den Nach-rechts-Pfeil (>), um die ausgewählten

Gruppen in die Liste "Geschützte Postfächer" zu verschieben.



6. Klicken Sie auf **Speichern**.
7. Gehen Sie auf der Registerkarte "Quellen" zu **Aus der Sicherung auszuschließende Ordner**, und aktivieren Sie dann das gewünschte Kontrollkästchen.
8. Wählen Sie unter erweiterte Option das gewünschte Kontrollkästchen aus.
   - Damit der Exchange Online-Schutz die Postfacharchivierung erlaubt, aktivieren Sie das Kontrollkästchen **Direkte Archivierung sichern**.

     Hinweis: Weitere Informationen über die Postfacharchivierung finden Sie unter diesem Link.
   - Wählen Sie das Kontrollkästchen **Wiederherstellbare Elemente sichern** aus, um das Postfach zu schützen, das die In-Place-Hold oder Litigation-Hold-Funktion ermöglicht.

     Hinweis: Informationen zur Archivierung von In-Place-Hold und Litigation-Hold für Exchange Online finden Sie unter diesem Link.

   Hinweis: Um beide Funktionen im Postfach gleichzeitig zu aktivieren, um wiederherstellbare Elemente in der Postfacharchivierung zu sichern, wählen Sie

die Optionen **In-Place-Archivierung sichern** und **Wiederherstellbare Elemente sichern** aus.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ziel**.
2. Wählen Sie die Option **Arcserve UDP Recovery Point Server** aus. **Arcserve UDP Recovery Point Server** gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.
3. Geben Sie folgende Details an:
    a. Wählen Sie einen Recovery Point Server aus.
    b. Wählen Sie einen für Deduplizierung bzw. nicht für Deduplizierung aktivierten Datenspeicher. Die Liste zeigt alle auf dem angegebenen Recovery Point-Server erstellten Datenspeicher an.
    c. Geben Sie ein Sitzungskennwort ein. Das Sitzungskennwort ist optional, wenn das Sicherungsziel ein unverschlüsselter RPS-Datenspeicher ist.
    d. Bestätigen Sie das Sitzungskennwort.

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

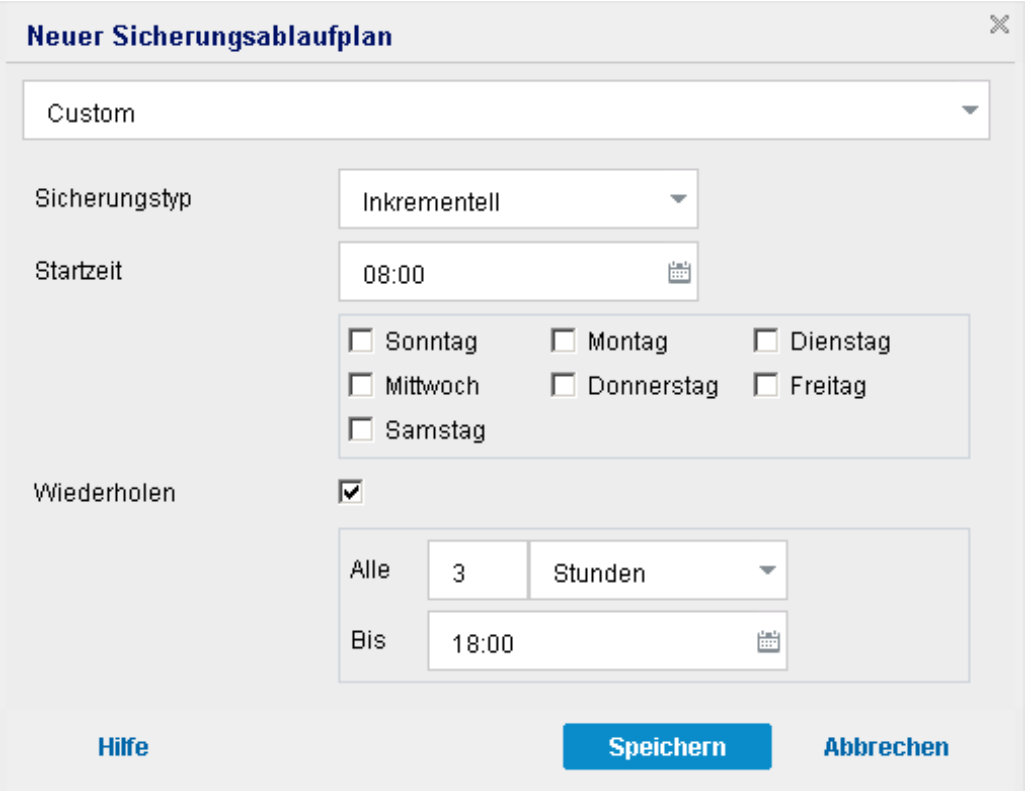
Gehen Sie wie folgt vor:

1. Fügen Sie Ablaufpläne für Sicherungen, Zusammenführungen und Drosselungsvorgänge hinzu.

   Hinzufügen eines Sicherungsablaufplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke

des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

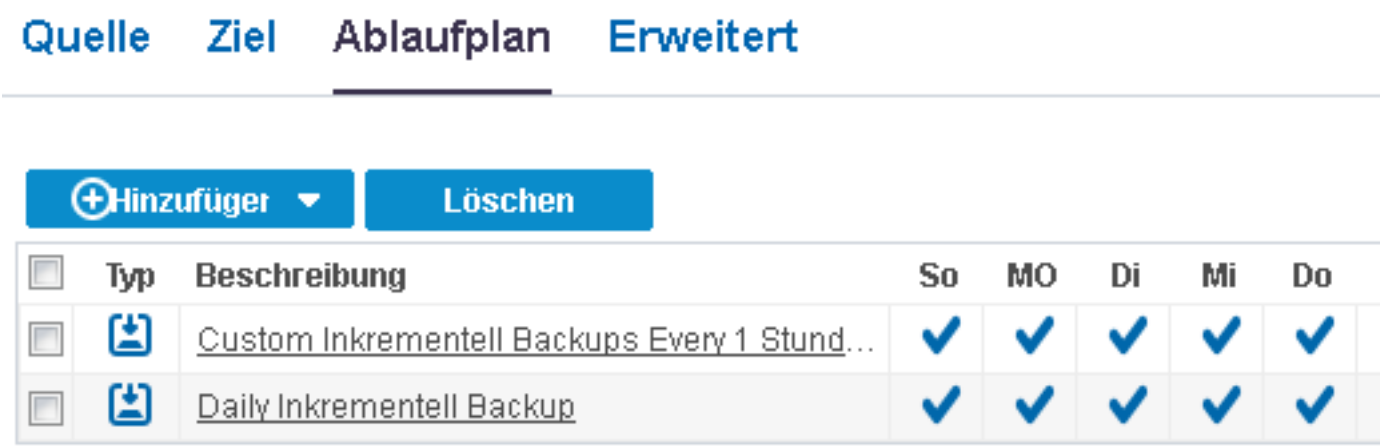
Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die nach der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.



Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zusammenführungsplan hinzufügen** aus.

Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

b. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

d. Klicken Sie auf **Speichern**.

Der Zusammenführungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Drosselungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

   Das Dialogfeld **Drosselungsplan hinzufügen** wird geöffnet.

b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

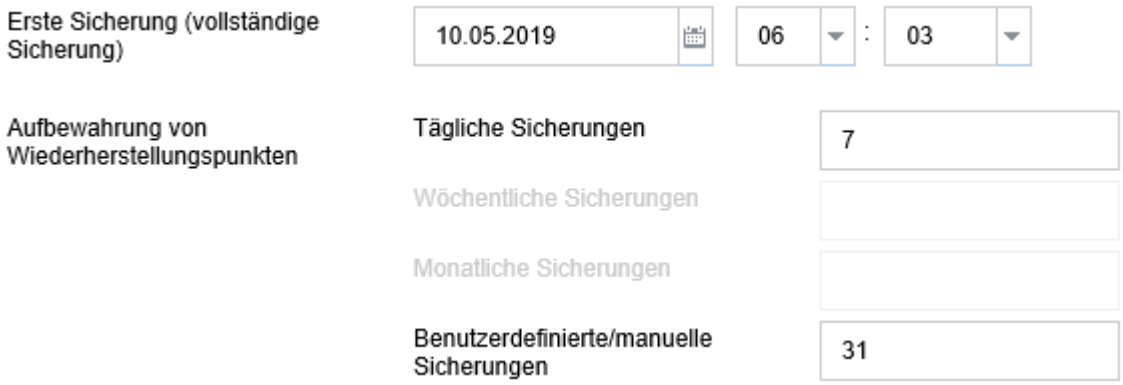
c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Drosselungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

2. Geben Sie die Startzeit für die geplante Sicherung an.



3. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld **Sicherungsablaufplan** übernommen.

   Der Ablaufplan ist nun angegeben.

Funktionsweise der erweiterten Planung und Aufbewahrung

Mit der Ablaufplanoption können Sie einen benutzerdefinierten Ablaufplan, einen Ablaufplan für tägliche/wöchentliche/monatliche Sicherungen oder beides festlegen. Im benutzerdefinierten Ablaufplan können Sie den Sicherungsablaufplan für jeden Tag der Woche konfigurieren und bis zu vier Sicherungsablaufpläne für jeden Tag hinzufügen. Sie können einen bestimmten Wochentag auswählen und ein Zeitfenster erstellen, um anzugeben, wann und wie oft die Sicherung durchgeführt werden soll.

Ablaufplan	Unterstützter Job	Kommentare
Sichern	Sicherungsjob	Gibt Zeitfenster für die Ausführung von Sicherungsjobs an.
Sicherungsdrosselung	Sicherungsjob	Gibt die Zeitfenster an, um die Sicherungsgeschwindigkeit zu steuern.
Zusammenführen	Zusammenführungsjob	Gibt an, wann Zusammenführungsjobs ausgeführt werden sollen.
Täglicher Ablaufplan	Sicherungsjob	Gibt an, wann tägliche Sicherungsjobs ausgeführt werden sollen.
Wöchentlicher Ablaufplan	Sicherungsjob	Gibt an, wann wöchentliche Sicherungsjobs ausgeführt werden sollen.
Monatlicher Ablaufplan	Sicherungsjob	Gibt an, wann monatliche Sicherungsjobs ausgeführt werden sollen.

Sie können auch die Aufbewahrungseinstellungen für die Wiederherstellungspunkte angeben.

Hinweis: Legen Sie innerhalb der einzelnen Pläne Einstellungen für die Aufbewahrungszeit fest, um zu steuern, wie die Daten für die Knoten des entsprechenden Plans im Zieldatenspeicher aufbewahrt werden.

Ablaufpläne für tägliche/wöchentliche/monatliche Sicherungen sind vom benutzerdefinierten Ablaufplan und voneinander unabhängig. Sie können die Ausführung einer täglichen, wöchentlichen oder monatlichen Sicherung konfigurieren, ohne einen benutzerdefinierten Ablaufplan zu konfigurieren.

Jobplan der Sicherung

Sie können vier Zeitfenster pro Tag in Ihrem Sicherungsablaufplan hinzufügen. Ein gültiges Zeitfenster liegt im Bereich 12:00 Uhr bis 23:59 Uhr. Sie können kein Zeitfenster wie z. B. 18:00 Uhr bis 06:00 Uhr angeben. In solchen Fällen müssen Sie manuell zwei verschiedene Zeitfenster angeben.

Für jedes Zeitfenster wird die Startzeit einbezogen, und die Endzeit wird nicht einbezogen. Zum Beispiel haben Sie das Ausführen einer Zuwachssicherung konfiguriert, die stündlich zwischen 06:00 Uhr und 09:00 Uhr stattfinden soll, und die Sicherung wird um 06:00 Uhr gestartet. Das bedeutet, dass die Sicherung um 06:00 Uhr, 07:00 Uhr und 08:00 Uhr ausgeführt wird, NICHT aber um 09:00 Uhr.

Hinweis: Wenn Sie die Sicherung bis zum Ende des Tages wiederholt ausführen möchten, legen Sie den Ablaufplan bis 12:00 Uhr fest. Um den Sicherungsjob beispielsweise alle 15 Minuten während des gesamten Tages auszuführen, legen Sie den Ablaufplan von 00:00 Uhr bis 00:00 Uhr alle 15 Minuten fest.

Drosselungsplan der Sicherung

Mit dem Drosselungsplan der Sicherung können Sie die Geschwindigkeit des Sicherungsdurchsatzes steuern, die wiederum die Ressourcenverwendung (Datenträger-E/A, CPU, Netzwerkbandbreite) des Servers, der gesichert wird, steuert. Dies ist hilfreich, wenn die Serverleistung während der Geschäftszeiten nicht beeinträchtigt werden soll. Sie können vier Zeitfenster pro Tag in Ihrem Drosselungsplan der Sicherung hinzufügen. Für jedes Zeitfenster können Sie einen Wert in MB pro Minute angeben. Dieser Wert wird verwendet, um den Sicherungsdurchsatz zu steuern. Gültige Werte liegen im Bereich zwischen 1 MB/Minute bis 99.999 MB/Minute.

Wenn ein Sicherungsjob die angegebene Zeit überschreitet, dann wird das Drosselungslimit entsprechend dem angegebenen Zeitfenster angepasst. Zum Beispiel haben Sie als Drosselungslimit der Sicherung den Wert 500 MB/Minute von 08:00 Uhr bis 20:00 Uhr und 2500 MB/Minute von 20:00 Uhr bis 22:00 Uhr angegeben. Wenn ein Sicherungsjob um 19:00 Uhr startet und drei Stunden ausgeführt wird, dann hat das Drosselungslimit von 19:00 Uhr bis 20:00 Uhr den Wert 500 MB/Minute. Von 20:00 Uhr bis 22:00 Uhr hat das Drosselungslimit den Wert 2.500 MB/Minute.

Wenn Sie keinen Sicherungsablaufplan und keinen Ablaufplan für den Sicherungsdurchsatz angeben, dann wird die Sicherung so schnell wie möglich ausgeführt.

Ablaufplan für Zusammenführung

Ermöglicht es Ihnen, Wiederherstellungspunkte basierend auf dem angegebenen Ablaufplan zusammenzuführen.

Beachten Sie folgende Punkte für den Zusammenführungsjob:

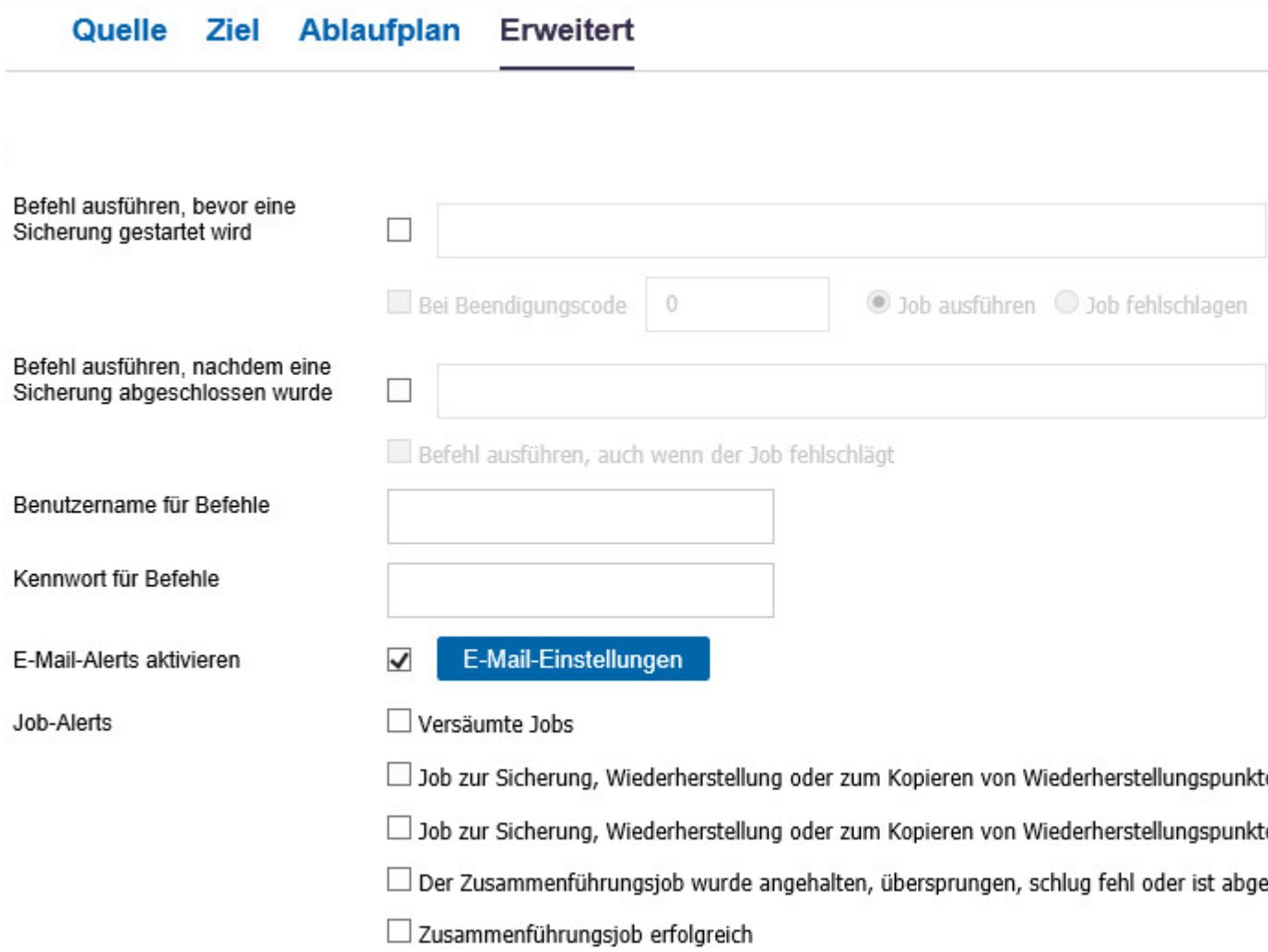
- Es kann immer nur ein Zusammenführungsjob für einen Knoten ausgeführt werden.

- Wenn ein Zusammenführungsjob gestartet wird, muss er abgeschlossen werden, bevor der nächste Zusammenführungsjob gestartet werden kann. Das bedeutet: Wenn ein oder mehrere Sätze an Wiederherstellungspunkten zusammengeführt werden, dann kann der neue Wiederherstellungspunkt nicht zu diesem Zusammenführungsprozess hinzugefügt werden, bis der Zusammenführungsprozess für den aktuellen Satz an Wiederherstellungspunkten abgeschlossen ist.
- Wenn ein Zusammenführungsjob mehr als einen Satz an Wiederherstellungspunkten bearbeitet (zum Beispiel Satz [1~4], Satz [5~11] und Satz [12~14], also drei Sätze), dann werden diese Sätze nacheinander vom Recovery Point Server bearbeitet.
- Wenn ein Zusammenführungsjob nach einer Pause fortgesetzt wird, erkennt der Job an welchem Punkt er unterbrochen wurde, und die Zusammenführung wird ab der Abbruchstelle fortgesetzt.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte **Erweitert**:



Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

   Befehl ausführen, bevor eine Sicherung gestartet wird

   Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, unter dem das Skript auf dem Proxy-Knoten gespeichert ist. Klicken Sie auf **Bei Beendigungscode**, und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den

Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist.

Befehl ausführen, auch wenn der Job fehlschlägt

Wenn dieses Kontrollkästchen aktiviert ist, wird das unter **Befehl ausführen, nachdem eine Sicherung abgeschlossen ist** angegebene Skript ausgeführt, selbst wenn der Sicherungsjob fehlschlägt. Andernfalls wird das Skript nur dann ausgeführt, wenn der Sicherungsjob erfolgreich abgeschlossen wurde.

Benutzername für Befehle

Ermöglicht die Angabe des Benutzernamens zum Ausführen der Befehle.

Kennwort für Befehle

Ermöglicht die Angabe des Kennworts zum Ausführen der Befehle.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Typen der Warnmeldungen angeben, die Sie in einer E-Mail erhalten möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers. Weitere Informationen zum Konfigurieren von E-Mail-Einstellungen finden Sie unter E-Mail- und Alert-Konfiguration.

Job-Alerts

Ermöglicht es Ihnen, die Arten von Job-Alerts auszuwählen, die Sie per E-Mail empfangen möchten.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, überprüft Arcserve UDP, ob der Agent auf dem Proxy-Knoten installiert ist und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agenten oder kein Agent installiert ist. Um den Agenten auf diesen Knoten zu

installieren bzw. um ein Upgrade der Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus und klicken auf **Speichern**.

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie einen anderen Task hinzufügen müssen, müssen Sie den Plan auf der Registerkarte **Ressourcen** auswählen und anschließend ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern. Sie können die Tasks **Kopieren von Wiederherstellungspunkten**, **Auf Band kopieren**, **Replizieren** und **Von einem Remote-RPS replizieren** als Folgetasks hinzufügen.

Der Plan wird automatisch auf dem Proxy-Serverknoten bereitgestellt.

Der Exchange Online-Sicherungsplan für den Proxy-Server wird erstellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

(Optional) Ausführen einer manuellen Sicherung

In der Regel werden die Sicherungen basierend auf den von Ihnen angewendeten Ablaufplaneinstellungen automatisch ausgeführt. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern. Wenn Sie z. B. einen Wiederholungsplan für vollständige Sicherungen und Zuwachssicherungen festgelegt haben und größere Veränderungen an Ihrem Rechner vornehmen möchten, können Sie sofort eine manuelle Sicherung durchführen, ohne auf die nächste geplante Sicherung zu warten.

Führen Sie die folgenden Schritte aus, um Exchange Online-Knoten manuell zu sichern:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Die Exchange Online-Knoten werden im mittleren Fensterbereich angezeigt.
3. Wählen Sie den Exchange Online-Knoten aus, den Sie sichern möchten (z. B. Mailbox@<organizationname.com>), und vergewissern Sie sich, dass ihm ein Plan zugewiesen ist. Der Knotenname ist das Konto, das verwendet wurde, als der Exchange Online-Knoten hinzugefügt und verbunden wurde.
4. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
5. Wählen Sie den gewünschten Sicherungstyp aus, und klicken Sie dann auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.
6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.
7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Gehen Sie wie folgt vor, um eine manuelle Sicherung des Exchange Online-Plans durchzuführen:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie dann auf **Alle Pläne**.

Die Exchange Online-Sicherungspläne werden im mittleren Fensterbereich angezeigt.

3. Wählen Sie den Plan aus, den Sie sichern möchten, und vergewissern Sie sich, dass ihm ein Plan zugewiesen ist.
4. Klicken Sie mit der rechten Maustaste auf den Plan, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
5. Wählen Sie den gewünschten Sicherungstyp aus, und klicken Sie dann auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.
6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.
7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Überprüfen der Sicherung

Zur Überprüfung Ihres Sicherungsjobs bestätigen Sie, dass Sie den Sicherungsplan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Sie können den Status von Sicherungsjobs auf der Registerkarte **Jobs** überprüfen.

Gehen Sie wie folgt vor, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Wenden Sie zur Überprüfung von Sicherungsjobs eine der folgenden Methoden an:

Methode 1

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs vollständig**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Methode 2

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Jobs erfolgreich abgeschlossen**.

   Die Liste der abgeschlossenen Sicherungsjobs wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf den Job, den Sie überprüfen möchten.

   Der rechte Fensterbereich wird aktualisiert.
4. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
5. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Konfigurieren der Multi-Faktor-Authentifizierung

Wenn in einer Organisation die Multi-Faktor-Authentifizierung (MFA) für die Benutzer aktiviert ist, verwenden Sie die moderne Authentifizierung, um Knoten hinzuzufügen.

Hinweis: Auch wenn die Standardauthentifizierung für den Mandanten aktiviert ist, können Sie die moderne Authentifizierung zum Hinzufügen von Knoten verwenden. Weitere Informationen zum Hinzufügen von Knoten zu einem Plan mithilfe der modernen Authentifizierung finden Sie unter Moderne Authentifizierung.

So erstellen Sie einen SharePoint Online-Sicherungsplan

Der SharePoint-Schutz wird verwendet, um Microsoft SharePoint Online-Websites und -Listenelemente zu sichern und wiederherzustellen. SharePoint Online ist eines der wichtigsten Produkte in Microsoft Office 365. Um Ihre SharePoint-Inhalte zu schützen, müssen Sie einen Plan erstellen.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen eines SharePoint Online-Sicherungsplans
3. Überprüfen des Sicherungsplans
4. Konfigurieren der Multi-Faktor-Authentifizierung

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie einen SharePoint Online-Sicherungsplan erstellen.

Erstellen eines SharePoint Online-Sicherungsplans:

Voraussetzungen:

Das Sicherungskonto ist ein Mitglied der Gruppen „Administratoren der Websitesammlung“ oder mit der Rolle *SharePoint-Administrator* zugewiesen.

Um ein Konto zur Gruppe "Administratoren der Websitesammlung" hinzuzufügen, verwenden Sie diesen Link.

Erstellen eines SharePoint Online-Sicherungsplans mit Basisauthentifizierung (BA):

Überprüfen Sie die folgenden Voraussetzungen:

- Installieren Sie die PowerShell Version 5.1 oder höher (Teil des Windows Management Framework (WMF)) auf dem Proxy-Server (64-Bit-Computer).
- Installieren Sie mithilfe der Befehlszeile die folgenden PowerShell-Module auf dem Proxy-Server unter Verwendung des PowerShell-Fensters:
  - Führen Sie den folgenden Befehl aus, um das Azure-Modul zu installieren:

    Installationsmodul -Name AzureAD -Force
  - Führen Sie den folgenden Befehl aus, um das ExchangeOnlineManagement-Modul zu installieren:

    Installationsmodul -Name ExchangeOnlineManagement -Force

  Hinweis: Wenn Sie PowerShell-Module mithilfe der oben genannten Befehle installieren, wird basierend auf der GA-Version der im Microsoft-Repository verfügbaren Komponente möglicherweise eine neuere Version der Module installiert.

Erstellen eines SharePoint Online-Sicherungsplans mithilfe der modernen Authentifizierung (MA):

Überprüfen Sie die Voraussetzungen, bevor Sie einen Plan unter Verwendung der modernen Authentifizierung erstellen.

Erstellen einer persönlichen Site in SharePoint

Dieser Abschnitt enthält Informationen zum Erstellen einer persönlichen Site in SharePoint.

Gehen Sie wie folgt vor:

1. Gehen Sie zur Microsoft-Anmeldeseite, und melden Sie sich dann beim Microsoft Office 365-Administratorkonto an.
2. Navigieren Sie zur Seite **SharePoint Admin Center**, und klicken Sie dann im linken Fensterbereich auf **Weitere Funktionen**.
3. Klicken Sie unter "Seite 'Klassische Websitesammlungen'" auf **Öffnen**.

   Die Seite "Websitesammlungen" wird angezeigt.
4. Klicken Sie auf der Seite "Websitesammlungen" auf **Neu** > **Private Websitesammlung**.

   Das Dialogfeld "Neue Websitesammlung" wird angezeigt.
5. Geben Sie im Dialogfeld "Neue Websitesammlung" die folgenden Details an, und klicken Sie auf **OK**.
   - **Titel**: Geben Sie einen Namen für die Website ein.
   - **Websiteadresse**: Wählen Sie in den Drop-down-Listen einen Domänennamen und einen URL-Pfad nach Bedarf aus, und geben Sie dann einen URL-Namen für die Website ein.
   - **Vorlagenauswahl**: Gehen Sie im Abschnitt "Vorlagenauswahl" wie folgt vor:
     - Wählen Sie in der Drop-down-Liste **Sprache auswählen** eine Sprache für die Website aus.
     - Wählen Sie unter **Vorlage auswählen** eine Vorlage für die Website aus.
   - **Zeitzone**: Wählen Sie die Zeitzone basierend auf dem Standort der Website aus.
   - **Administrator**: Geben Sie den Namen der Person ein, die als Website-Administrator fungieren soll. Sie können auch die Schaltfläche "Namen überprüfen" oder "Durchsuchen" verwenden, um nach Benutzern zu suchen und diese als Website-Administrator festzulegen.
   - **Speicherkontingent**: Geben Sie die Größe (MB) der Website ein, die Sie zuweisen möchten.
   - **Serverressourcenkontingent**: Übernehmen Sie das Standard-Ressourcenkontingent.

   Die persönliche Site in SharePoint wird erstellt.

Erstellen eines SharePoint Online-Sicherungsplans

Ein Sicherungsplan enthält einen Task **Sicherung: Office 365 SharePoint Online**, der eine Sicherung von SharePoint Online-Elementen (Listen, Bibliotheken, Dokumente usw.) durchführt und Daten in einem Datenspeicher mit oder ohne Deduplizierung speichert. Außerdem ermöglicht dieser Sicherungsplan es UDP, SharePoint Online-Elemente zu erkennen und anzugeben, für die ein Sicherungstask ausgeführt wird. Jeder Task besteht aus Parametern, die Quelle, Ziel, Ablaufplan und weitere Sicherungsdetails definieren.

Gehen Sie wie folgt vor:

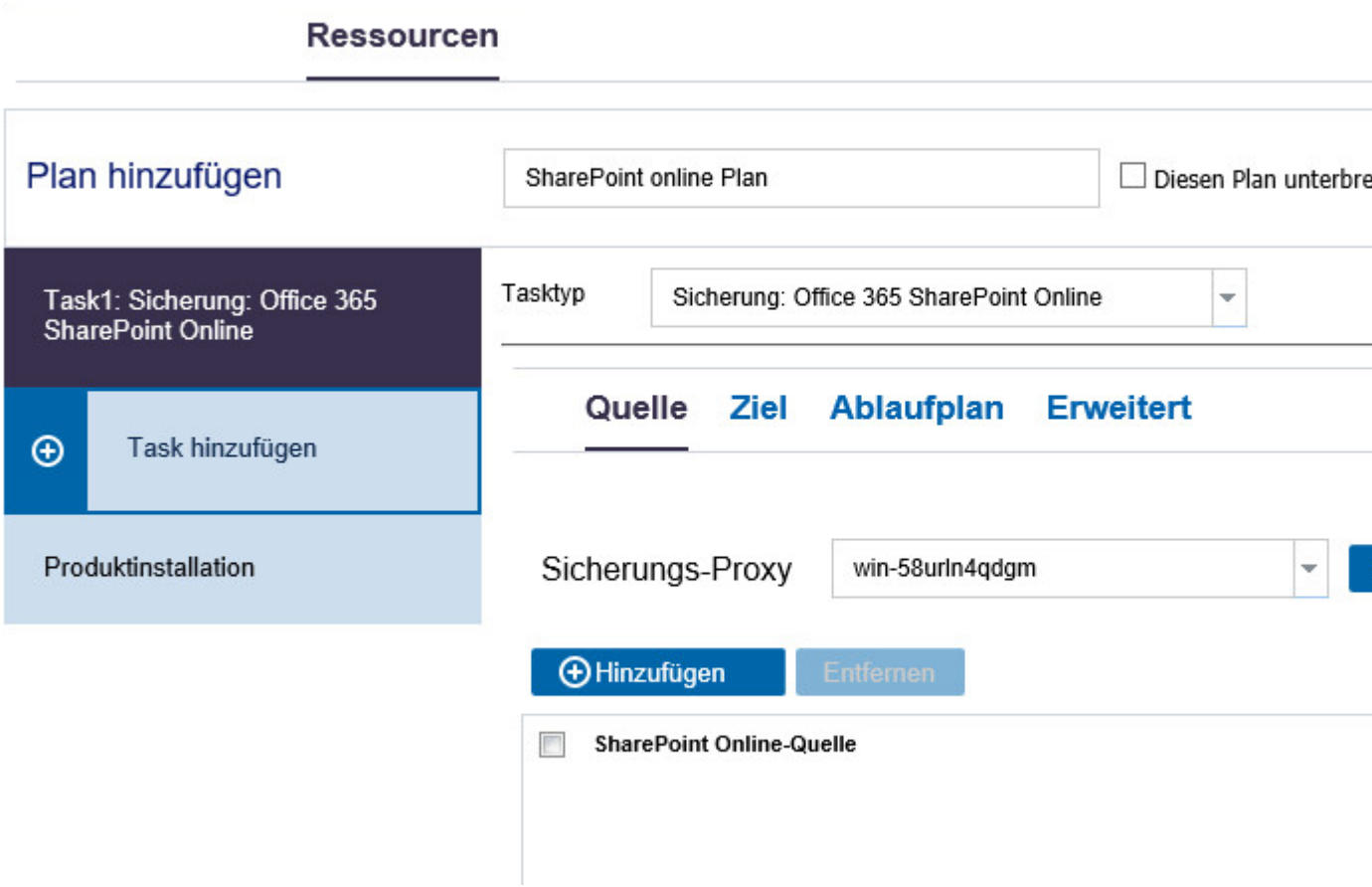
1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Das Dialogfenster **Plan hinzufügen** wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Drop-down-Liste Tasktyp die Option **Sicherung: Office 365 SharePoint Online** aus.



Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die SharePoint Online-Quellknoten angeben, die Sie schützen möchten. Sie können für einen Plan mehrere SharePoint Online-Quellknoten auswählen.

Hinweis: Sie können einen Plan speichern, ohne Quellknoten hinzuzufügen. Der Plan wird jedoch nur bereitgestellt, wenn Sie einen Knoten hinzufügen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Quelle**.
2. Wählen Sie in der Drop-down-Liste **Sicherungs-Proxy** den Server aus.
3. Fügen Sie mithilfe einer der folgenden Methoden einen SharePoint Online-Knoten hinzu:

   Methode 1:

   a. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Wählen Sie zu sichernde Quellen in Arcserve UDP aus**.

      Das Dialogfeld Knoten zu Plan hinzufügen wird angezeigt.

      Hinweis: Verwenden Sie diese Option nur, wenn Sie bereits zuvor einen SharePoint-Knoten hinzugefügt haben.

   b. Wählen Sie einen Knoten aus, und klicken Sie dann auf **Verbinden**.

      Hinweis: Um die SharePoint Online-Knoten zu suchen, die Sie schützen möchten, verwenden Sie **Suchen**.

   Methode 2:

   - Klicken Sie auf **Hinzufügen** und dann auf **SharePoint Online-Quelle hinzufügen**.

     Das Dialogfeld "Knoten zu Plan hinzufügen" wird geöffnet.

     Hinweis:

     - Verwenden Sie diese Option, um Online-Elemente für die SharePoint Online-Quelle zu erkennen und anzugeben.
     - Anders als andere Knoten können Sie den SharePoint Online-Knoten nicht über die Seite "Alle Knoten" hinzufügen. Sie können einen SharePoint Online-Knoten nur beim Erstellen oder Ändern eines Plans in einem Plan hinzufügen.

4. Gehen Sie folgendermaßen vor, um die Authentifizierung anzuwenden:

Moderne Authentifizierung

Bei der modernen Authentifizierung können Sie eine Sicherung mithilfe eines Sicherheitszertifikats ausführen.

Sicherheitszertifikat verwenden

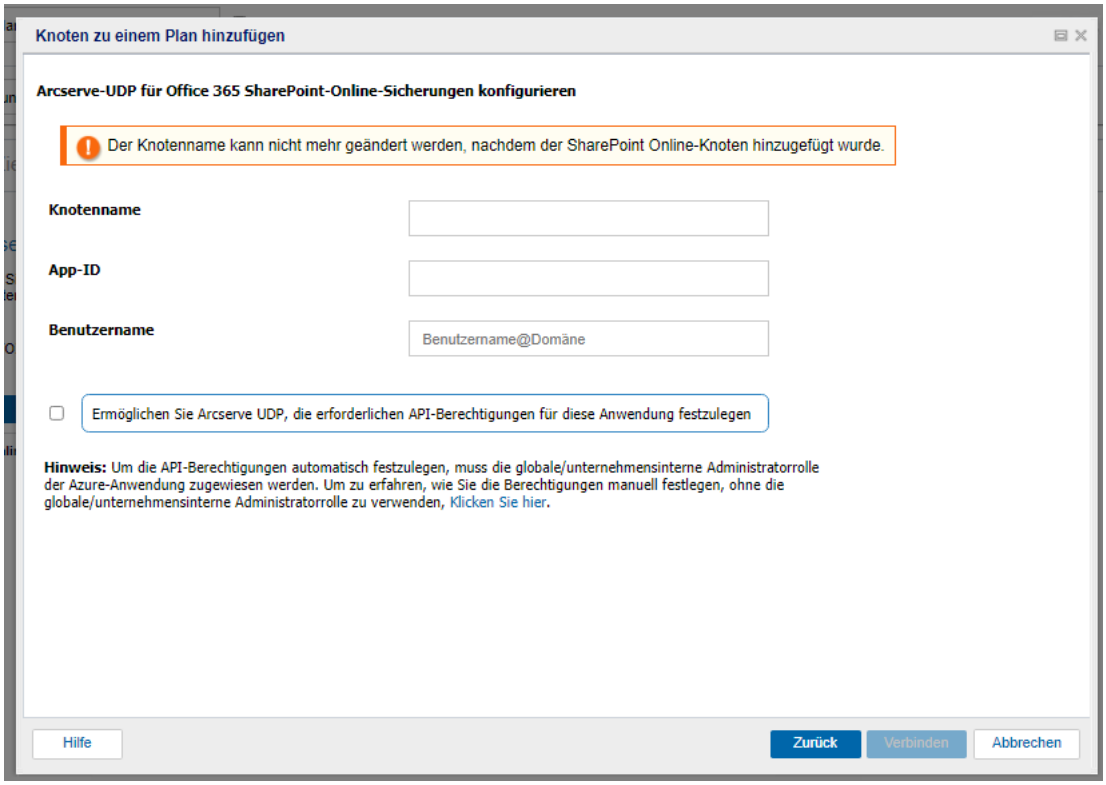
Hinweis: Standardmäßig wählt der Sicherungsplan die Option **Sicherheitszertifikat verwenden** für die moderne Authentifizierung aus.

Gehen Sie wie folgt vor:

a. Informationen zum Authentifizieren der UDP-Anwendung mit Sicherheitszertifikaten finden Sie unter Herunterladen des Zertifikats von UDP und Hochladen in Azure.

b. Geben Sie die folgenden Details ein:

- Knotenname
- App-ID
- Benutzername



c. Um die API-Berechtigungen automatisch anzuwenden, aktivieren Sie das Kontrollkästchen **Arcserve UDP erlauben, die erforderlichen API-Berechtigungen für diese Anwendung festzulegen**.

Hinweis: Informationen zum manuellen Anwenden der Berechtigungen ohne Verwendung der Administratorrolle "Global/Company" finden Sie unter Manuelles Konfigurieren der API-Berechtigungen ohne Verwendung der Administratorrolle "Global/Company".

d. Klicken Sie auf **Connect**.

Hinweise:

- Namen von SharePoint Online-Quellknoten können nach dem Erstellen des Knotens nicht mehr geändert werden.
- Sie können ein einzelnes Konto verwenden, um mehrere SharePoint Online-Knoten zu schützen.

Standardauthentifizierung

Um bei Verwendung der Standardauthentifizierung mit der Sicherung fortzufahren, geben Sie die folgenden Informationen an, und klicken Sie dann auf **Verbinden**:

- Knotenname
- Benutzer-ID
- Kennwort

5. Um SharePoint Online-Elemente zu schützen, führen Sie die folgenden Schritte aus, und klicken Sie dann auf **Speichern**.
   - Wählen Sie in der Drop-down-Liste "Site-Typen" den Site-Typ aus, den Sie schützen möchten, z. B. "SharePoint-Websites" oder "Persönliche Sites".
   - Führen Sie unter "Alle Websites/Unterwebsites schützen" die folgenden Schritte aus:

     Hinweise:

     - Bei Anzeige des Bildschirms "SharePoint Online-Inhalte auswählen" ist diese Option standardmäßig automatisch ausgewählt.
       - Um alle Elemente im ausgewählten Site-Typ zu schützen, aktivieren Sie das Kontrollkästchen **Alle Websites/Unterwebsites schützen**.
       - Um bestimmte Elemente im ausgewählten Site-Typ zu schützen, deaktivieren Sie das Kontrollkästchen **Alle Web-**

sites/Unterwebsites schützen, und wählen Sie dann die spezifischen Elemente aus, die Sie schützen möchten.

- Wenn Sie beim Konfigurieren des vorhandenen SharePoint Online-Plans Sites manuell zum Schutz ausgewählt haben und nun das Kontrollkästchen **Alle Sites/untergeordneten Sites schützen** möchten, gehen Sie folgendermaßen vor:
  a. Ändern Sie den vorhandenen SharePoint Online-Plan.
  b. Löschen Sie die SharePoint-Websites, die manuell zum Schutz ausgewählt wurden.
  c. Aktivieren Sie das Kontrollkästchen **Alle Standorte/untergeordneten Standorte schützen**, und speichern Sie den Plan.

- Um bestimmte Elemente nicht zu schützen, aktivieren Sie das Kontrollkästchen **Ausgewählte Websites ausschließen**, und wählen Sie dann spezifische Elemente im ausgewählten Site-Typ aus.

Die SharePoint Online-Quellen, die Sie schützen möchten, werden zum Plan hinzugefügt.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ziel**.

   Wählen Sie die Option **Arcserve UDP Recovery Point Server** aus. **Arcserve UDP Recovery Point Server** gibt an, dass das Sicherungsziel ein Recovery Point Server ist.

   Sie können Daten nicht als Wiederherstellungssätze speichern.

2. Führen Sie die folgenden Schritte aus:

   a. Wählen Sie einen Recovery Point Server aus.

   b. Wählen Sie einen für Deduplizierung bzw. nicht für Deduplizierung aktivierten Datenspeicher.

      Die Liste zeigt alle auf dem angegebenen Recovery Point-Server erstellten Datenspeicher an.

   c. Geben Sie ein Sitzungskennwort ein.

      Das Sitzungskennwort ist optional, wenn das Sicherungsziel ein unverschlüsselter RPS-Datenspeicher ist.

   d. Bestätigen Sie das Sitzungskennwort.

   Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

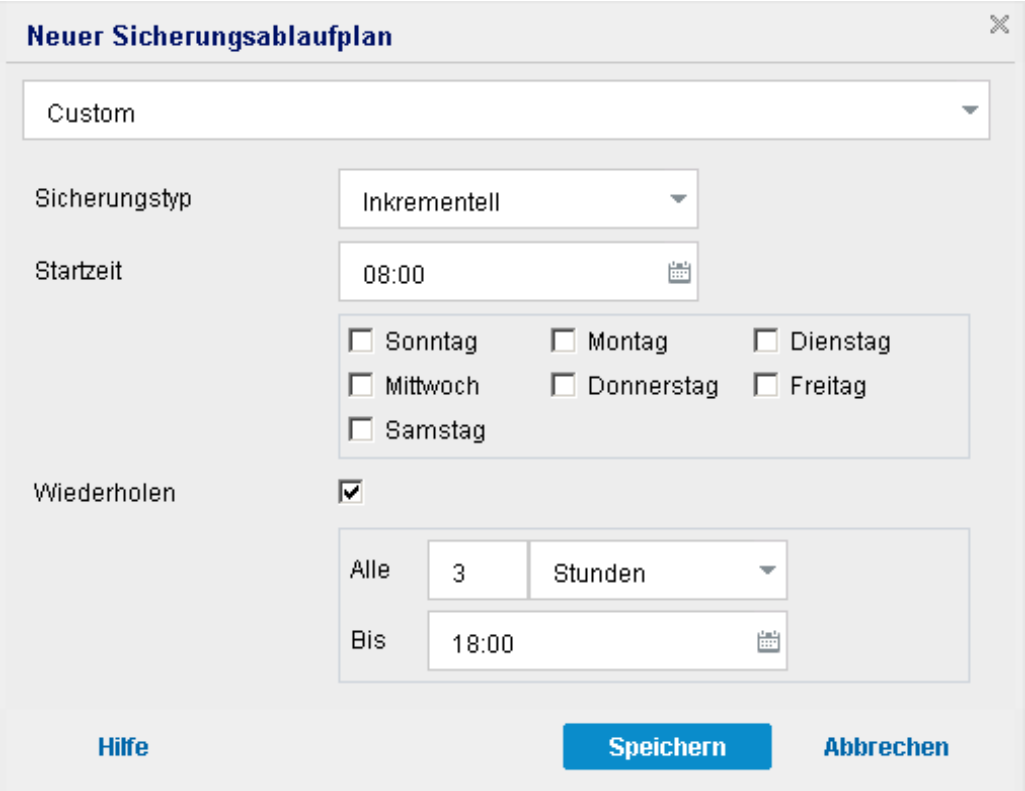
Gehen Sie wie folgt vor:

1. Fügen Sie Ablaufpläne für Sicherungen, Zusammenführungen und Drosselungsvorgänge hinzu.

   Hinzufügen eines Sicherungsablaufplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke

des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

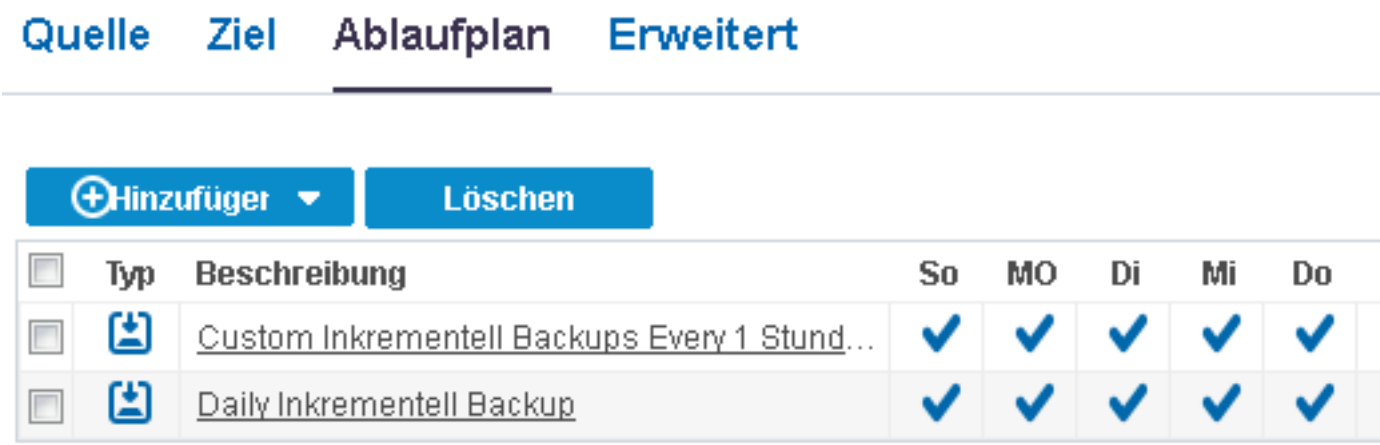
Arcserve UDP erstellt wie geplant nur inkrementelle Sicherungen der Blöcke, die nach der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.



Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zusammenführungsplan hinzufügen** aus.

Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

b. Geben Sie die Startzeit für den Zusammenführungsjob an.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende des Zusammenführungsjobs bereitzustellen.

d. Klicken Sie auf **Speichern**.

Der Zusammenführungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Drosselungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

   Das Dialogfeld **Drosselungsplan hinzufügen wird geöffnet.**

b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

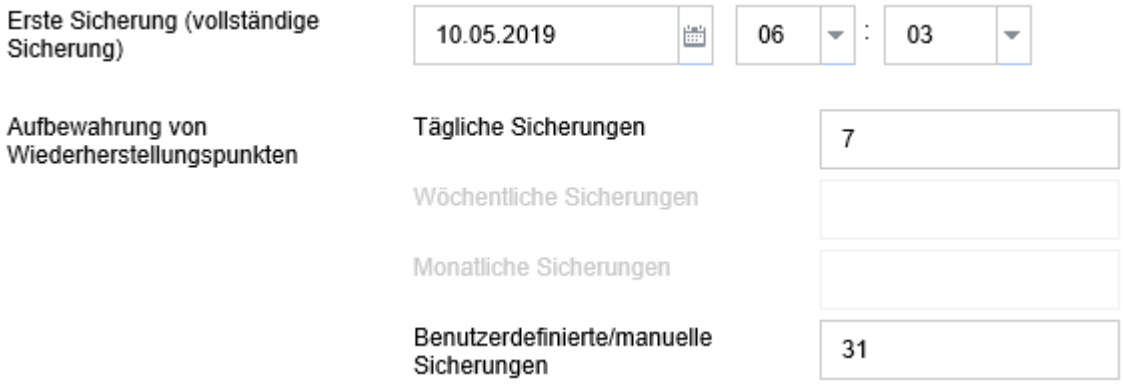
c. Geben Sie die Startzeit für den Sicherungsdurchsatzjob an.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende des Durchsatzjobs bereitzustellen.

e. Klicken Sie auf **Speichern**.

Der Drosselungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

2. Geben Sie die Startzeit für die geplante Sicherung an.



3. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

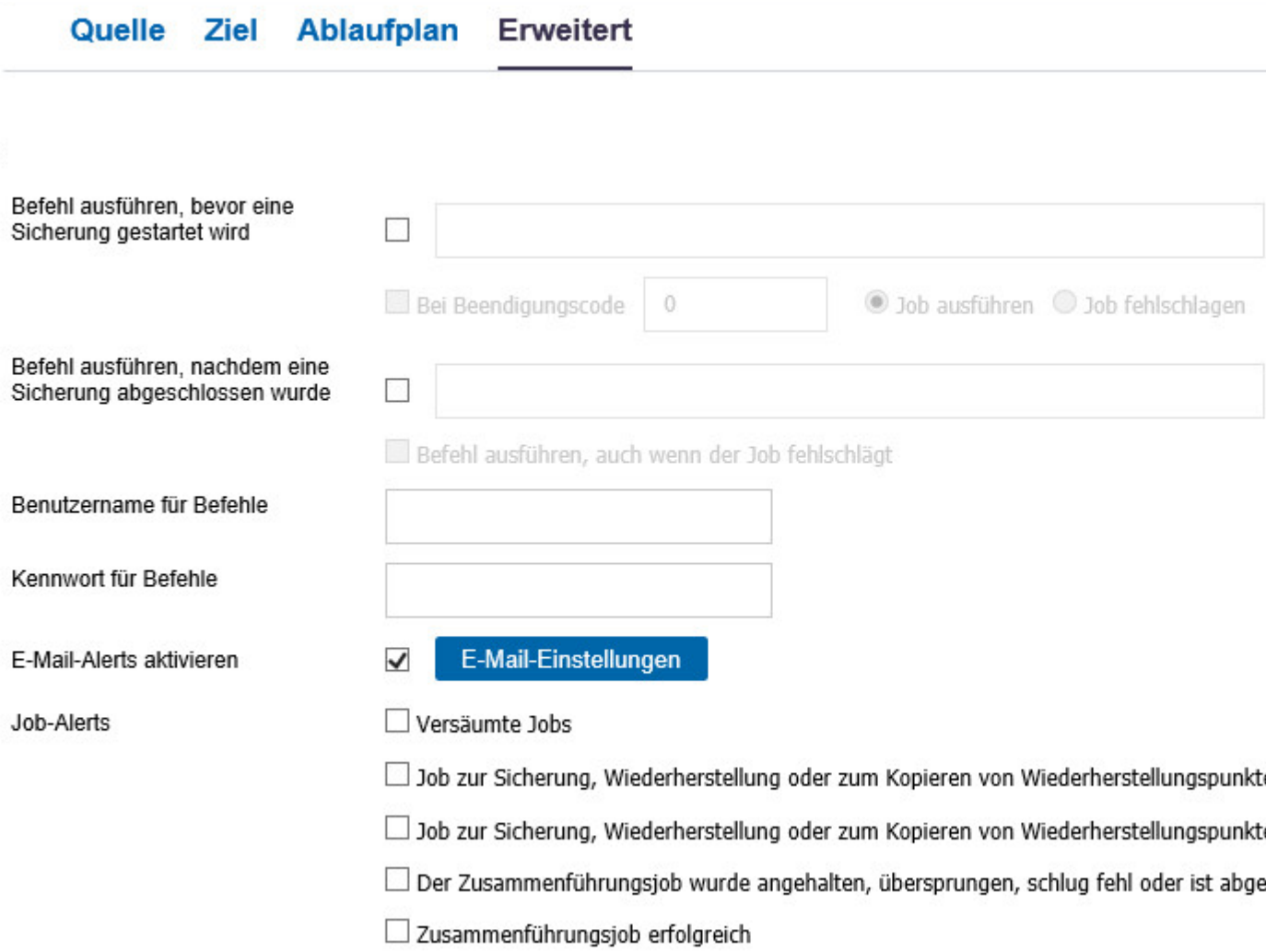
   Die Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld **Sicherungsablaufplan** übernommen.

   Der Ablaufplan ist nun angegeben.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte **Erweitert**:



Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

   Befehl ausführen, bevor eine Sicherung gestartet wird

   Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, unter dem das Skript auf dem Proxy-Knoten gespeichert ist. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den

Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist.

Befehl ausführen, auch wenn der Job fehlschlägt

Wenn dieses Kontrollkästchen aktiviert ist, wird das unter **Befehl ausführen, nachdem eine Sicherung abgeschlossen ist** angegebene Skript ausgeführt, selbst wenn der Sicherungsjob fehlschlägt. Andernfalls wird das Skript nur dann ausgeführt, wenn der Sicherungsjob erfolgreich abgeschlossen wurde.

Benutzername für Befehle

Ermöglicht die Angabe des Benutzernamens zum Ausführen der Befehle.

Kennwort für Befehle

Ermöglicht die Angabe des Kennworts zum Ausführen der Befehle.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Typen der Warnmeldungen angeben, die Sie in einer E-Mail erhalten möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers. Weitere Informationen zum Konfigurieren von E-Mail-Einstellungen finden Sie unter E-Mail- und Alert-Konfiguration.

Job-Alerts

Ermöglicht es Ihnen, die Arten von Job-Alerts auszuwählen, die Sie per E-Mail empfangen möchten.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Proxy-Knoten installiert und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agent oder kein Agent installiert ist. Um den Agent auf diesen

Knoten zu installieren bzw. um ein Upgrade der Agents auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus und klicken auf **Speichern**.

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie einen andere Task hinzufügen müssen, müssen Sie den Plan auf der Registerkarte **Ressourcen** auswählen und anschließend ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern. Sie können die Tasks **Kopieren von Wiederherstellungspunkten**, **Auf Band kopieren**, **Replizieren** und **Von einem Remote-RPS replizieren** als Folgetasks hinzufügen.

Der Plan wird automatisch auf dem Proxy-Serverknoten bereitgestellt.

Der SharePoint Online-Sicherungsplan für den Proxy-Server wird erstellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

(Optional) Ausführen einer manuellen Sicherung

In der Regel werden die Sicherungen basierend auf den von Ihnen angewendeten Ablaufplaneinstellungen automatisch ausgeführt. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern. Wenn Sie z. B. einen Wiederholungsplan für vollständige Sicherungen und Zuwachssicherungen festgelegt haben und größere Veränderungen an Ihrem Rechner vornehmen möchten, können Sie sofort eine manuelle Sicherung durchführen, ohne auf die nächste geplante Sicherung zu warten.

Gehen Sie wie folgt vor, um eine manuelle Sicherung von SharePoint Online-Knoten durchzuführen:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Die SharePoint Online-Knoten werden im mittleren Fensterbereich angezeigt.
3. Wählen Sie den SharePoint Online-Knoten aus, den Sie sichern möchten (z. B. Mailbox@<organizationname.com>), und vergewissern Sie sich, dass ihm ein Plan zugewiesen ist. Der Knotenname ist das Konto, das beim Hinzufügen und Verbinden des SharePoint Online-Knotens verwendet wurde.
4. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.

5. Wählen Sie den gewünschten Sicherungstyp aus, und klicken Sie dann auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.

6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.
7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Gehen Sie wie folgt vor, um eine manuelle Sicherung des SharePoint Online-Plans durchzuführen:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie dann auf **Alle Pläne**.

   Die SharePoint Online-Sicherungspläne werden im mittleren Fensterbereich angezeigt.

3. Wählen Sie den Plan aus, den Sie sichern möchten, und vergewissern Sie sich, dass ihm ein Plan zugewiesen ist.
4. Klicken Sie mit der rechten Maustaste auf den Plan, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.

5. Wählen Sie den gewünschten Sicherungstyp aus, und klicken Sie dann auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.

6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.
7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Überprüfen der Sicherung

Zur Überprüfung Ihres Sicherungsjobs bestätigen Sie, dass Sie den Sicherungsplan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Sie können den Status von Sicherungsjobs auf der Registerkarte **Jobs** überprüfen.

Gehen Sie wie folgt vor, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Wenden Sie zur Überprüfung von Sicherungsjobs eine der folgenden Methoden an:

Methode 1

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs vollständig**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Methode 2

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Jobs erfolgreich abgeschlossen**.

   Die Liste der abgeschlossenen Sicherungsjobs wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf den Job, den Sie überprüfen möchten.

   Der rechte Fensterbereich wird aktualisiert.
4. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
5. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Konfigurieren der Multi-Faktor-Authentifizierung

Wenn in einer Organisation die Multi-Faktor-Authentifizierung (MFA) für die Benutzer aktiviert ist, verwenden Sie die moderne Authentifizierung, um Knoten hinzuzufügen.

Hinweis: Auch wenn die Standardauthentifizierung für den Mandanten aktiviert ist, können Sie die moderne Authentifizierung zum Hinzufügen von Knoten verwenden. Weitere Informationen zum Hinzufügen von Knoten zu einem Plan mithilfe der modernen Authentifizierung finden Sie unter Moderne Authentifizierung.

So erstellen Sie einen Sicherungsplan für Microsoft Office 365 OneDrive

OneDrive, Teil des Microsoft Office 365 Cloud-Dienstes, erleichtert die Cloud-Speicherung und die gemeinsame Nutzung von Dateien. Um Ihre Onedrive Elemente (Dateien, Ordner und so weiter) von Microsoft-Cloud zu schützen, müssen Sie einen Plan erstellen. Der Plan für OneDrive besteht aus einem Sicherungsauftrag. Mit dieser Sicherungsaufgabe können Sie die zu schützenden OneDrive Knoten, das Sicherungsziel und den Sicherungsplan festlegen.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Erstellen Sie einen OneDrive Sicherungsplan
3. (Optional) Ausführen einer manuellen Sicherung
4. Konfigurieren der Multi-Faktor-Authentifizierung

Überprüfen der Voraussetzungen und Hinweise

Überprüfen Sie die folgenden Voraussetzungen und Hinweise, bevor Sie einen OneDrive-Sicherungsplan erstellen.

Erstellen eines OneDrive Sicherungsplans:

Voraussetzung:

- Die Ausführung des PowerShell-Skripts ist auf dem Proxy-Server aktiviert. Wenn nicht aktiviert, führen Sie den folgenden Befehl aus: *Set-ExecutionPolicy RemoteSigned*
- Der Proxy-Server muss eine Verbindung zu Microsoft Azure herstellen.

Besondere Aspekte:

Microsoft Cloud Services sind für nationale Clouds von Deutschland, China und der US-Regierung unterschiedlich. Weitere Informationen finden Sie unter Link. Sie müssen die Einstellung ändern, wenn Sie das Produkt in diesen Regionen einsetzen.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Konfig-Datei, deren Pfad der $UDP Installationspfad ist.

   $/Engine/Bin/Office365/Arcserve.Office365.Onedrive.json

2. Suchen Sie die Einstellung **Region**, und setzen Sie den Wert auf Deutschland,

China oder die US-Regierung.

Standardwert: Normal

Erstellen eines OneDrive-Sicherungsplans mit Basisauthentifizierung (BA):

Überprüfen Sie Folgendes:

- Installieren Sie die PowerShell Version 5.1 oder höher (Teil des Windows Management Framework (WMF)) auf dem Proxy-Server (64-Bit-Computer).
- Installieren Sie mithilfe der Befehlszeile die folgenden PowerShell-Module auf dem Proxy-Server unter Verwendung des PowerShell-Fensters:
  - Führen Sie den folgenden Befehl aus, um das Azure-Modul zu installieren:

    Installationsmodul -Name AzureAD -Force
  - Führen Sie den folgenden Befehl aus, um das ExchangeOnlineManagement-Modul zu installieren:

    Installationsmodul -Name ExchangeOnlineManagement -Force

  Hinweis: Wenn Sie PowerShell-Module mithilfe der oben genannten Befehle installieren, wird basierend auf der GA-Version der im Microsoft-Repository verfügbaren Komponente möglicherweise eine neuere Version der Module installiert.

Erstellen eines OneDrive-Sicherungsplans mithilfe der modernen Authentifizierung (MA):

Überprüfen Sie die Voraussetzungen, bevor Sie einen Plan unter Verwendung der modernen Authentifizierung erstellen.

Erstellen Sie einen OneDrive Sicherungsplan

Ein Sicherungsplan beinhaltet einen Sicherungstask, der eine Sicherung von OneDrive-Datenelementen (Dateien, Ordner usw.) durchführt und Daten entweder in einem Nicht-Deduplizierungsdatenspeicher oder einem Deduplizierungsdatenspeicher speichert. Darüber hinaus ermöglicht dieser Sicherungsplan es UDP, OneDrive-Gruppen zu erkennen und anzugeben, für die ein Sicherungstask ausgeführt wird. Jeder Task besteht aus Parametern, die Quelle, Ziel, Ablaufplan und weitere Sicherungsdetails definieren.

Gehen Sie wie folgt vor:

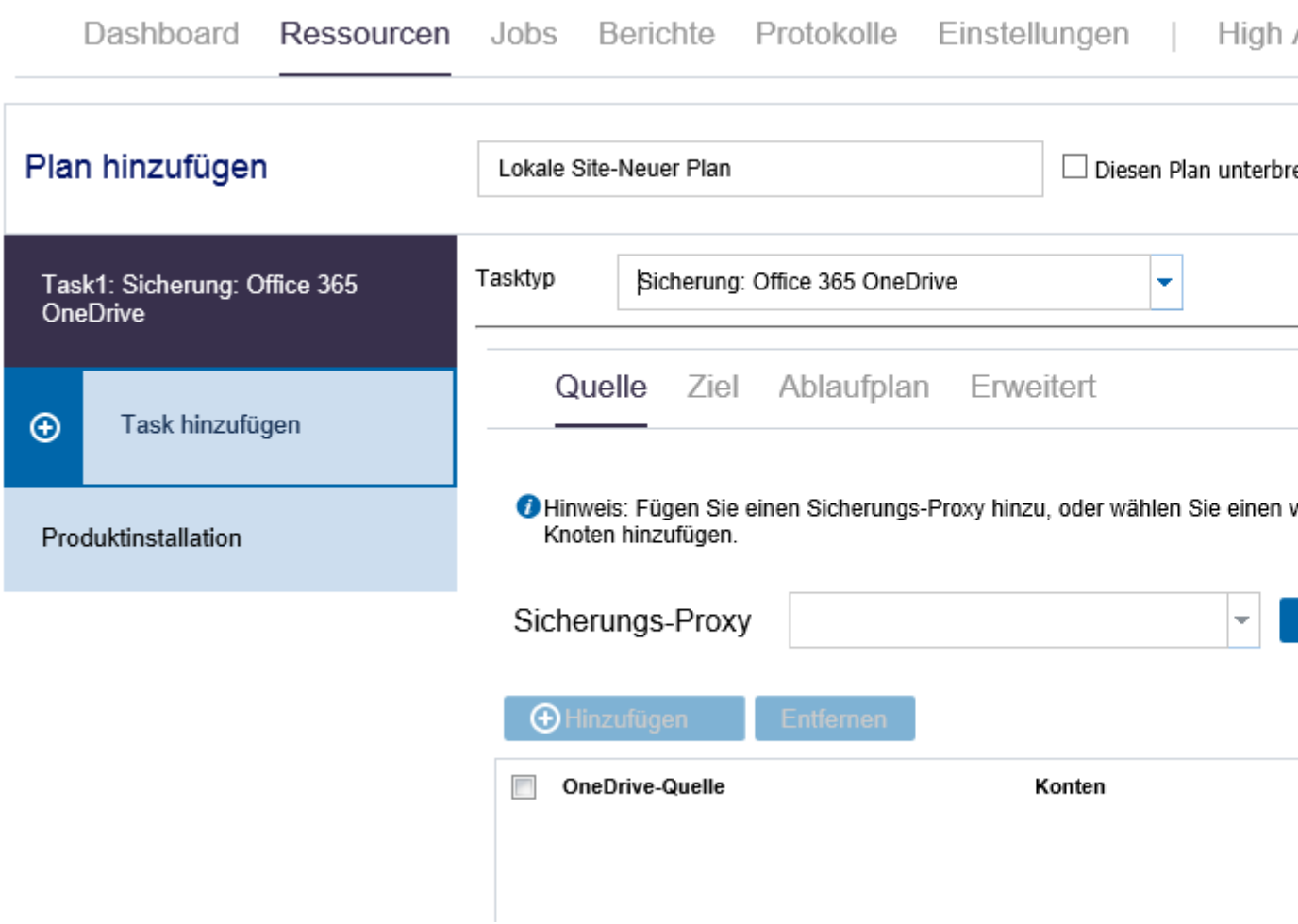
1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Das Dialogfenster **Plan hinzufügen** wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Dropdown-Liste "Tasktyp" die Option **Sicherung: Office 365 OneDrive** aus.



Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Angeben der Quelle

Auf der Seite Source (Quelle) können Sie die OneDrive-Quellknoten angeben, die Sie schützen möchten. Sie können mehr als einen OneDrive-Quellknoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, können Sie OneDrive-Quellknoten von der Seite Source hinzufügen.

Hinweis: Sie können einen Plan speichern, ohne Quellknoten hinzuzufügen. Der Plan wird jedoch nur bereitgestellt, wenn Sie Knoten hinzufügen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Quelle**.
2. Wählen Sie in der Drop-down-Liste **Sicherungs-Proxy** den Server aus.
3. Fügen Sie den OneDrive-Knoten mit einer der folgenden Methoden hinzu:

   Methode 1

a. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Wählen Sie zu sichernde Quellen in Arcserve UDP aus**.

   Das Dialogfeld "Knoten zu Plan hinzufügen" wird angezeigt.

b. Wählen Sie einen Knoten aus, und klicken Sie dann auf **Verbinden**.

   Hinweis: Sie können nach den OneDrive-Knoten, die Sie schützen möchten, auch in Suche suchen.

c. Wählen Sie das **Alle OneDrive Konten schützen** Kontrollkästchen aus, um alle OneDrive-Konten auf allen Seiten zu schützen. Um nur einige wenige Konten auszuwählen, klicken Sie auf den Pfeil auf der rechten Seite des Kontrollkästchens und geben Sie die Konten an.

   Die von Ihnen ausgewählten OneDrive-Konten werden hinzugefügt.

Methode 2

a. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **OneDrive-Quelle hinzufügen**.

   Hinweise:

   - Verwenden Sie diese Option, um Verteilergruppen für OneDrive zu erkennen und anzugeben.
   - Im Gegensatz zu anderen Knoten können Sie den OneDrive-Knoten nicht auf der Seite "Alle Knoten" hinzufügen. Sie können einen OneDrive-Knoten nur in einem Plan hinzufügen oder wenn Sie einen Plan ändern.

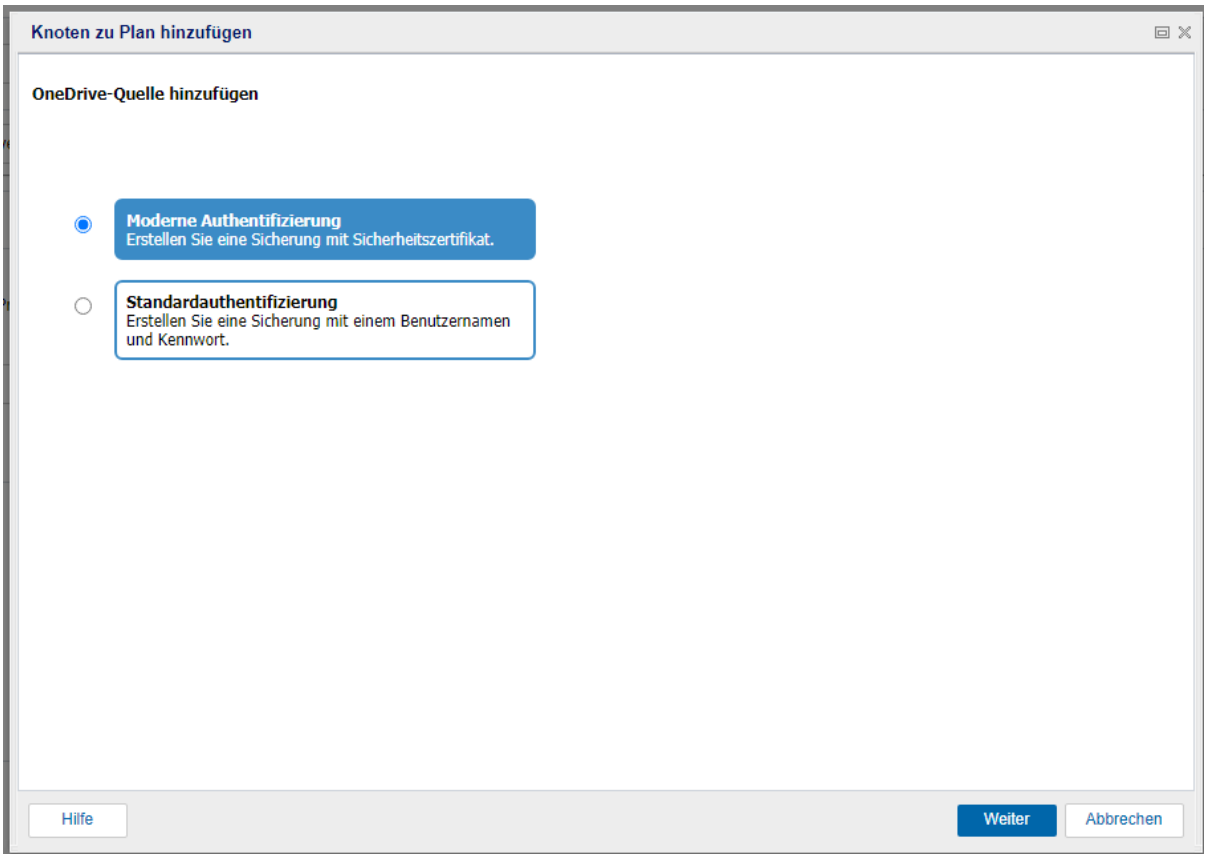
b. Um den OneDrive-Knoten nach Plan hinzuzufügen, müssen Sie den Knotennamen, die Benutzer-ID und das Kennwort angeben. Sie können den Knotennamen nicht ändern, nachdem Sie den OneDrive-Knoten erstellt haben. Mehrere OneDrive-Knoten können das gleiche Benutzerkonto (Servicekonto) von OneDrive verwenden.

   Hinweis: Es wird empfohlen, Benutzerkonten von Azure Active Directory-Administratoren auszuwählen.

4. Gehen Sie folgendermaßen vor, um die Authentifizierung anzuwenden:

   Moderne Authentifizierung

   Bei der modernen Authentifizierung können Sie eine Sicherung mithilfe eines Sicherheitszertifikats ausführen.



Sicherheitszertifikat verwenden

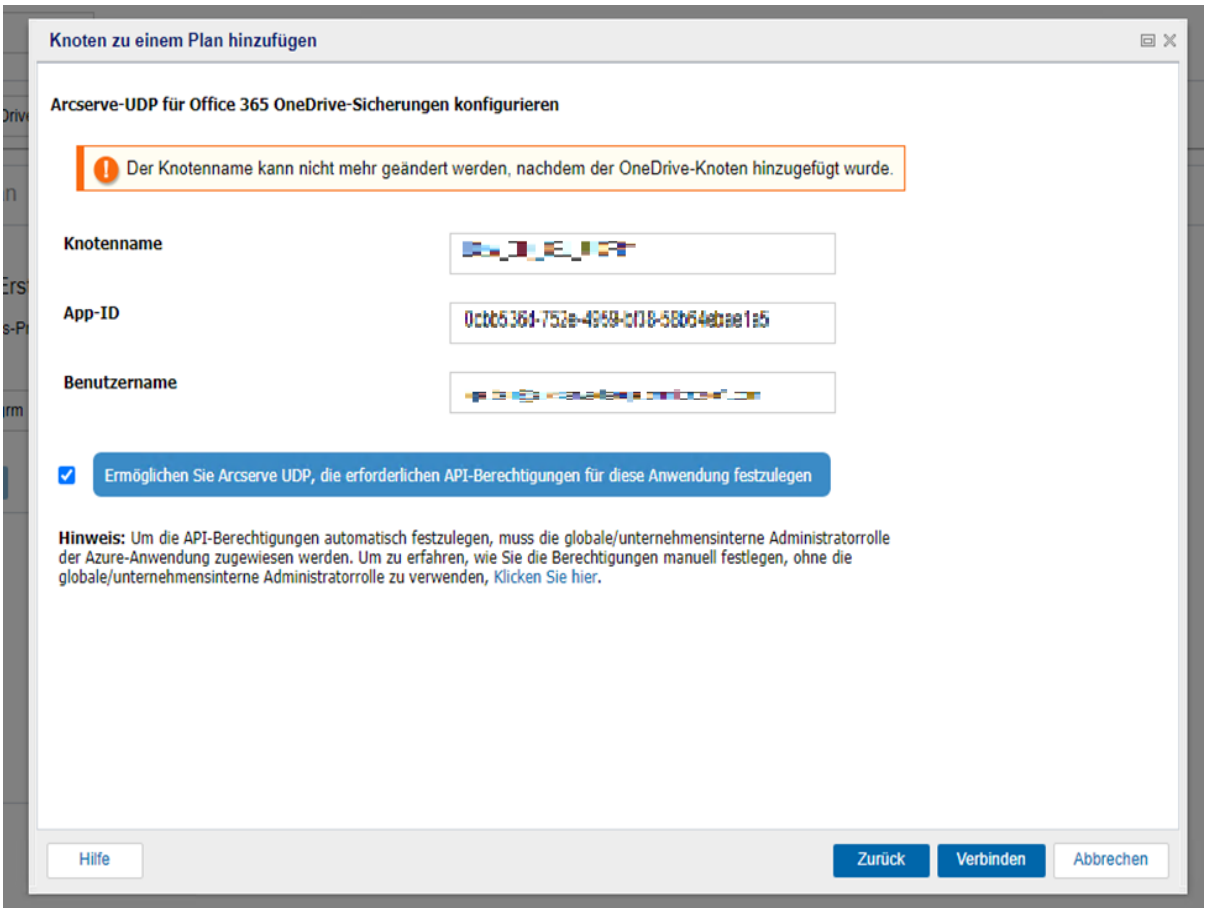
Hinweis: Standardmäßig wählt der Sicherungsplan die Option **Sicherheitszertifikat verwenden** für die moderne Authentifizierung aus.

Gehen Sie wie folgt vor:

a. Informationen zum Authentifizieren der UDP-Anwendung mit Sicherheitszertifikaten finden Sie unter Herunterladen des Zertifikats von UDP und Hochladen in Azure.

b. Geben Sie die folgenden Details ein:

- Knotenname
- App-ID
- Benutzername



Hinweis: Die OneDrive-Knotennamen können nach dem Erstellen eines Knotens nicht mehr geändert werden.

c. Um die API-Berechtigungen automatisch anzuwenden, aktivieren Sie das Kontrollkästchen **Arcserve UDP erlauben, die erforderlichen API-Berechtigungen für diese Anwendung festzulegen**.

   Hinweis: Informationen zum manuellen Anwenden der Berechtigungen ohne Verwendung der Administratorrolle "Global/Company" finden Sie unter Manuelles Konfigurieren der API-Berechtigungen ohne Verwendung der Administratorrolle "Global/Company".

d. Klicken Sie auf **Connect**.

Standardauthentifizierung

Um bei Verwendung der Standardauthentifizierung mit der Sicherung fortzufahren, gehen Sie wie folgt vor:

a. Wählen Sie "Standardauthentifizierung" aus, geben Sie Knotennamen, Benutzernamen und Kennwort ein, und klicken Sie dann auf **Verbinden**.

Die Arcserve UDP-URL wird in einem Browser geöffnet und fordert die Lese- und Schreibberechtigung für alle Arcserve UDP-Daten vom OneDrive-Portal an.

b. Verwenden Sie im Browser die Anmeldeinformationen des Microsoft Azure-Administrators, um sich anzumelden.

Das Azure-Portal wird geöffnet.

c. Führen Sie vom Microsoft Azure-Portal aus die folgenden Schritte aus, um die UDP-App zu konfigurieren:

i. Klicken Sie auf **API-Berechtigungen**.

ii. Klicken Sie im rechten Fensterbereich auf die Schaltfläche **Berechtigungen erteilen für**.

iii. Klicken Sie auf **Ja** um "Berechtigungen erteilen" zuzustimmen.

iv. Nachdem Sie die Berechtigung erteilt haben, navigieren Sie in Arcserve UDP zu **Plan hinzufügen > Knoten zu einem Plan hinzufügen**, und klicken Sie dann auf **Weiter**.

Hinweis: Wenn Sie die Berechtigungs-URL schließen und sie erneut öffnen möchten, klicken Sie im UDP-Fenster "Knoten zum Plan hinzufügen" auf die Schaltfläche **Hier**.

Arcserve UDP listet alle Konten unter dem aktuellen Nutzer auf.

5. Um OneDrive-Konten zu schützen, führen Sie einen der folgenden Schritte aus:

- Um alle OneDrive-Konten und -Gruppen zu schützen, aktivieren Sie das Kontrollkästchen **Alle OneDrive-Konten schützen**.

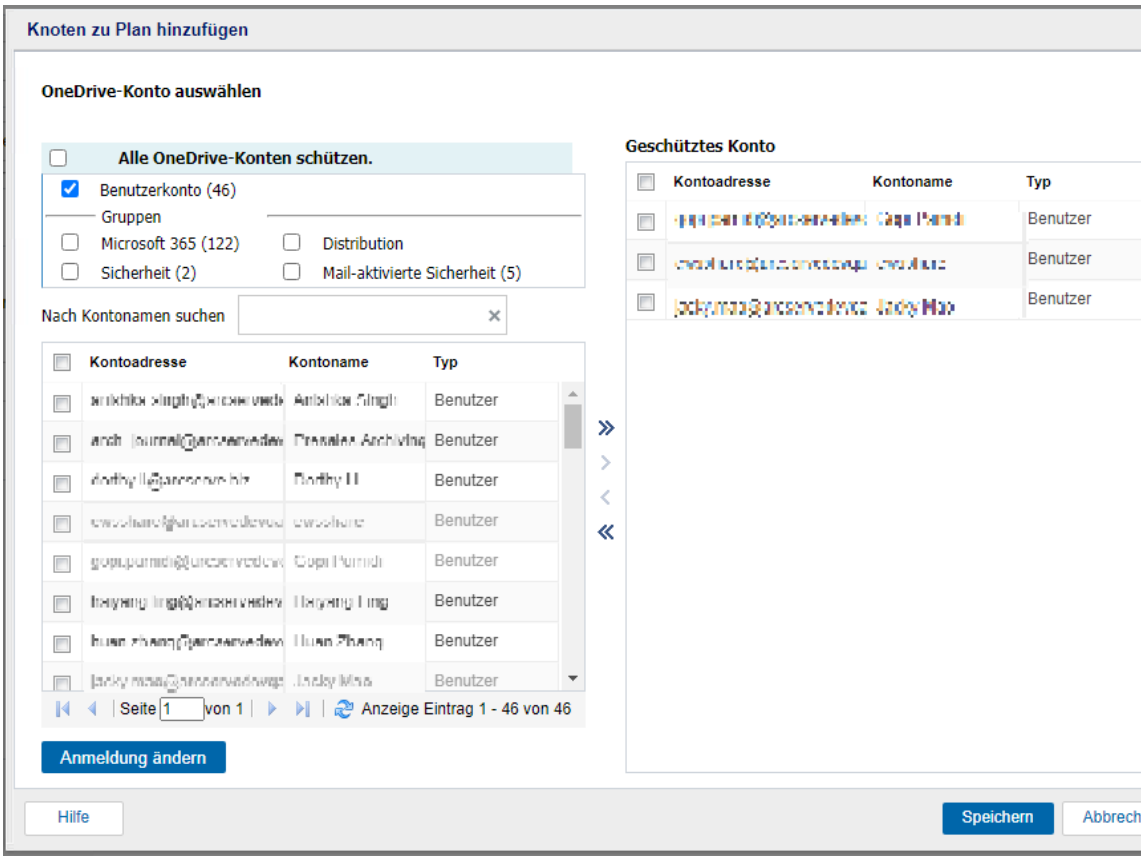
  Hinweis: Bei Anzeige des Bildschirms "OneDrive-Konto auswählen" ist diese Option standardmäßig automatisch ausgewählt.

- Gehen Sie für "Benutzerkonto" wie folgt vor:

  a. Aktivieren Sie das Kontrollkästchen **Benutzerkonto**.

  Eine Liste von Benutzerkonten wird angezeigt.

  b. (Optional) Um in der Liste nach einem Konto zu suchen, geben Sie den Kontonamen im Feld "Nach Kontonamen suchen" ein.



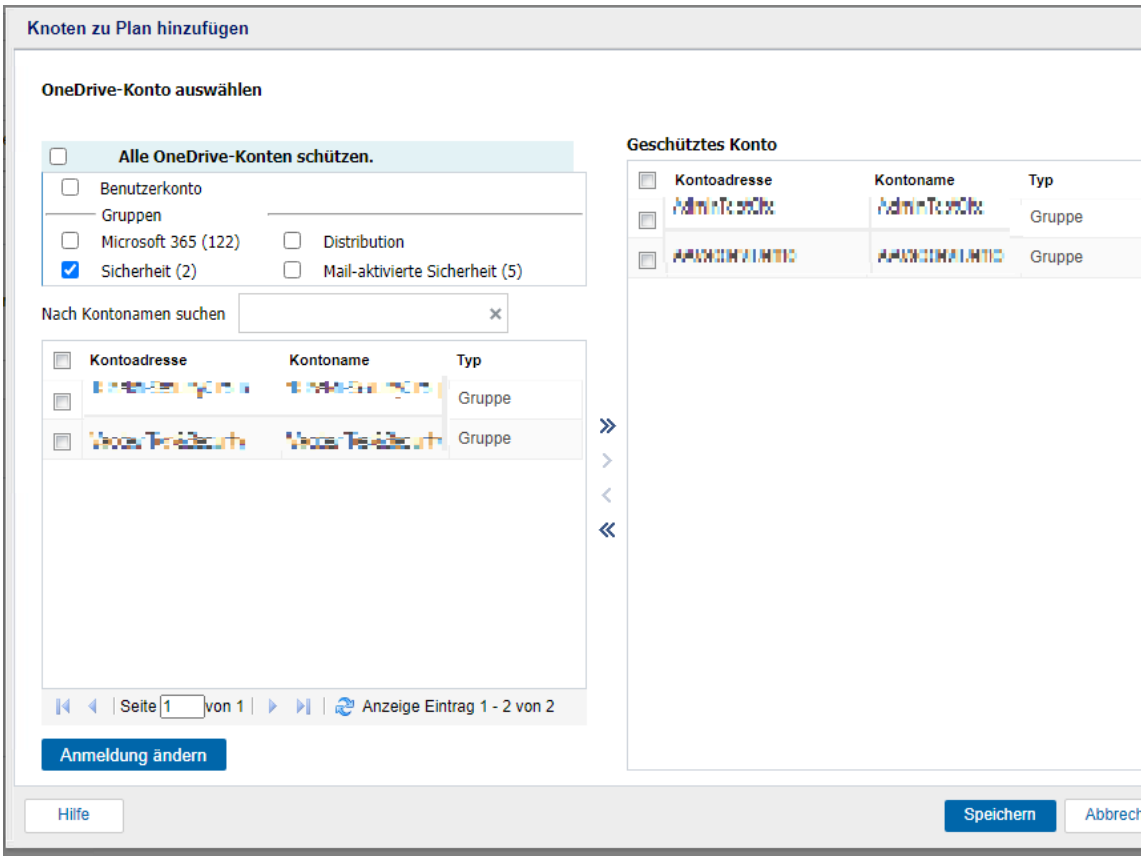
c. Wählen Sie die zu schützenden Konten in der Liste der Benutzerkonten aus.

d. Klicken Sie auf den Nach-rechts-Pfeil (>), um die ausgewählten Konten in die Liste "Geschütztes Konto" zu verschieben.

- Gehen Sie für Gruppen folgendermaßen vor:

  a. Aktivieren Sie das Kontrollkästchen **Microsoft 365** oder **Sicherheit**.

     Basierend auf der Auswahl wird eine Liste von Gruppen angezeigt.



b. (Optional) Um in der Liste nach einem Konto zu suchen, geben Sie den Kontonamen im Feld "Nach Kontonamen suchen" ein.

c. Wählen Sie die zu schützenden Gruppen in der Liste der Gruppen aus.

d. Klicken Sie auf den Nach-rechts-Pfeil (>), um die ausgewählten Gruppen in die Liste "Geschütztes Konto" zu verschieben.

6. Klicken Sie auf **Speichern**.

   Die ausgewählten OneDrive-Konten werden hinzugefügt.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ziel**.

   Die Option **Arcserve UDP Wiederherstellungspunkt-Server**wird automatisch ausgewählt. **Arcserve UDP Recovery Point Server** gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als

Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.

2. Geben Sie folgende Details an:
   a. Wählen Sie einen Recovery Point Server aus.
   b. Wählen Sie einen für Deduplizierung bzw. nicht für Deduplizierung aktivierten Datenspeicher. Die Liste zeigt alle auf dem angegebenen Recovery Point-Server erstellten Datenspeicher an.
   c. Geben Sie ein Sitzungskennwort ein. Das Sitzungskennwort ist optional, wenn das Sicherungsziel ein unverschlüsselter RPS-Datenspeicher ist.
   d. Bestätigen Sie das Sitzungskennwort.

Das Ziel ist nun angegeben. Geben Sie nun die Details zu Zeitplan und Erweitert an.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

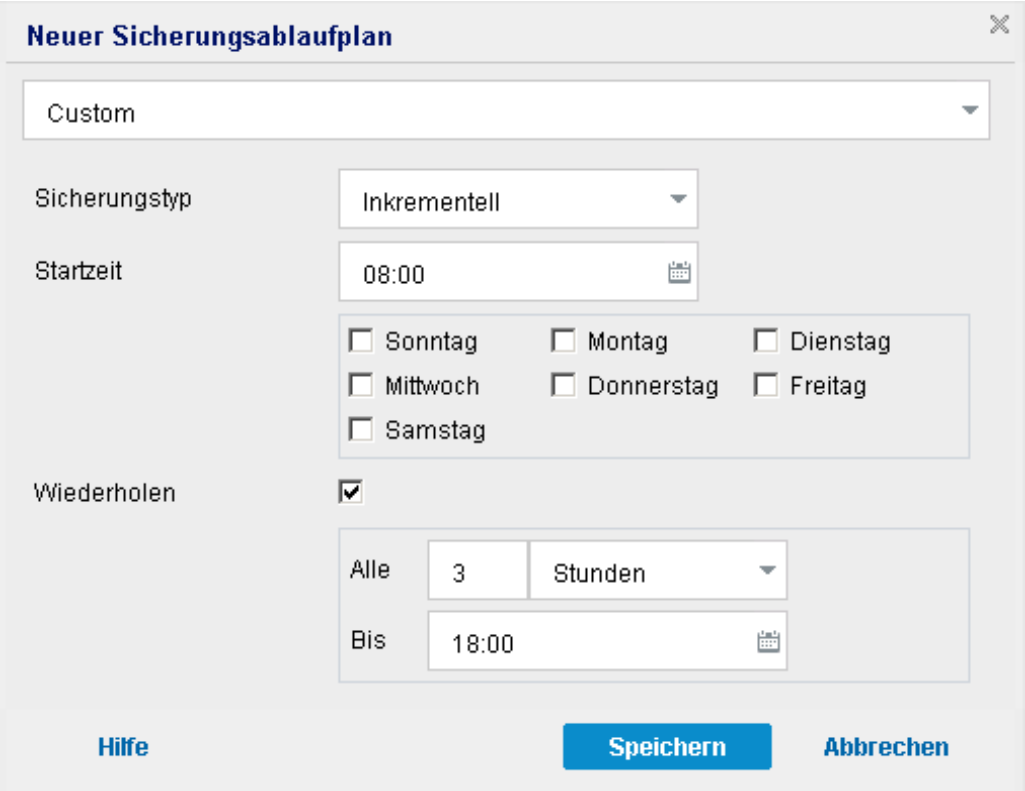
Gehen Sie wie folgt vor:

1. Fügen Sie Ablaufpläne für Sicherungen, Zusammenführungen und Drosselungsvorgänge hinzu.

   Hinzufügen eines Sicherungsablaufplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke

des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

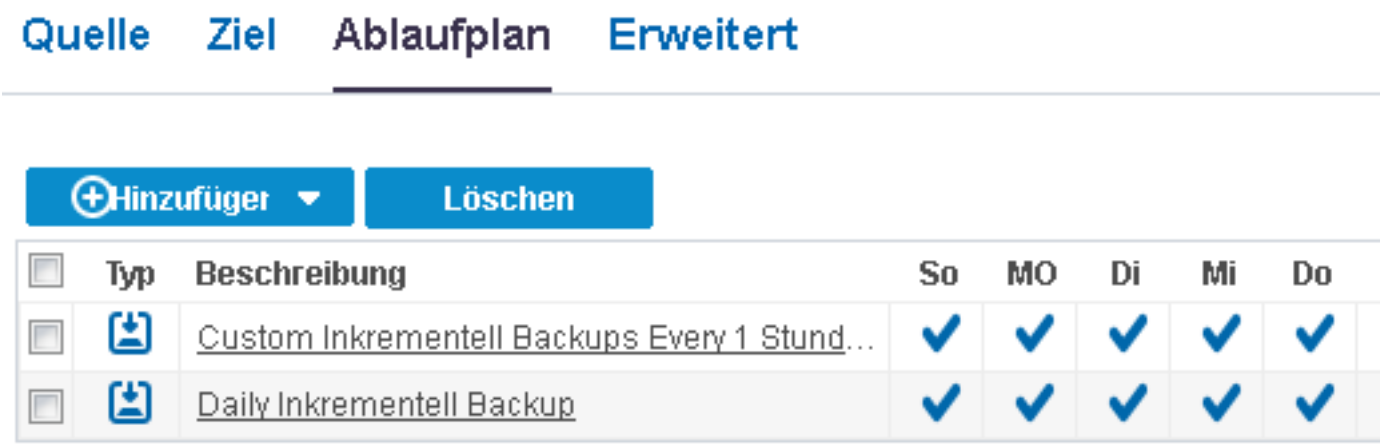
Arcserve UDP erstellt wie geplant nur inkrementelle Sicherungen der Blöcke, die nach der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Diese Option ist der optimale Weg, um eine Sicherung durchzuführen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.



Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zusammenführungsplan hinzufügen** aus.

Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

b. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

d. Klicken Sie auf **Speichern**.

Der Zusammenführungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Drosselungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

   Das Dialogfeld **Drosselungsplan hinzufügen wird geöffnet.**

b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

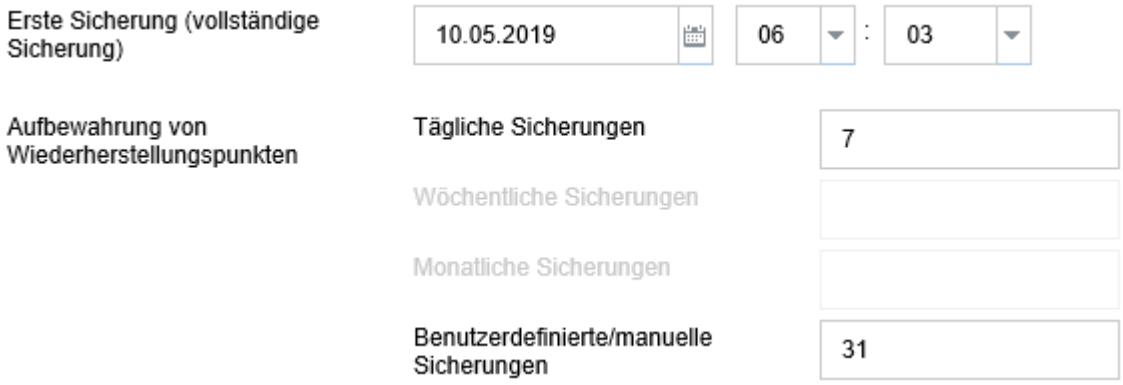
c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Drosselungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

2. Geben Sie die Startzeit für die geplante Sicherung an.



3. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

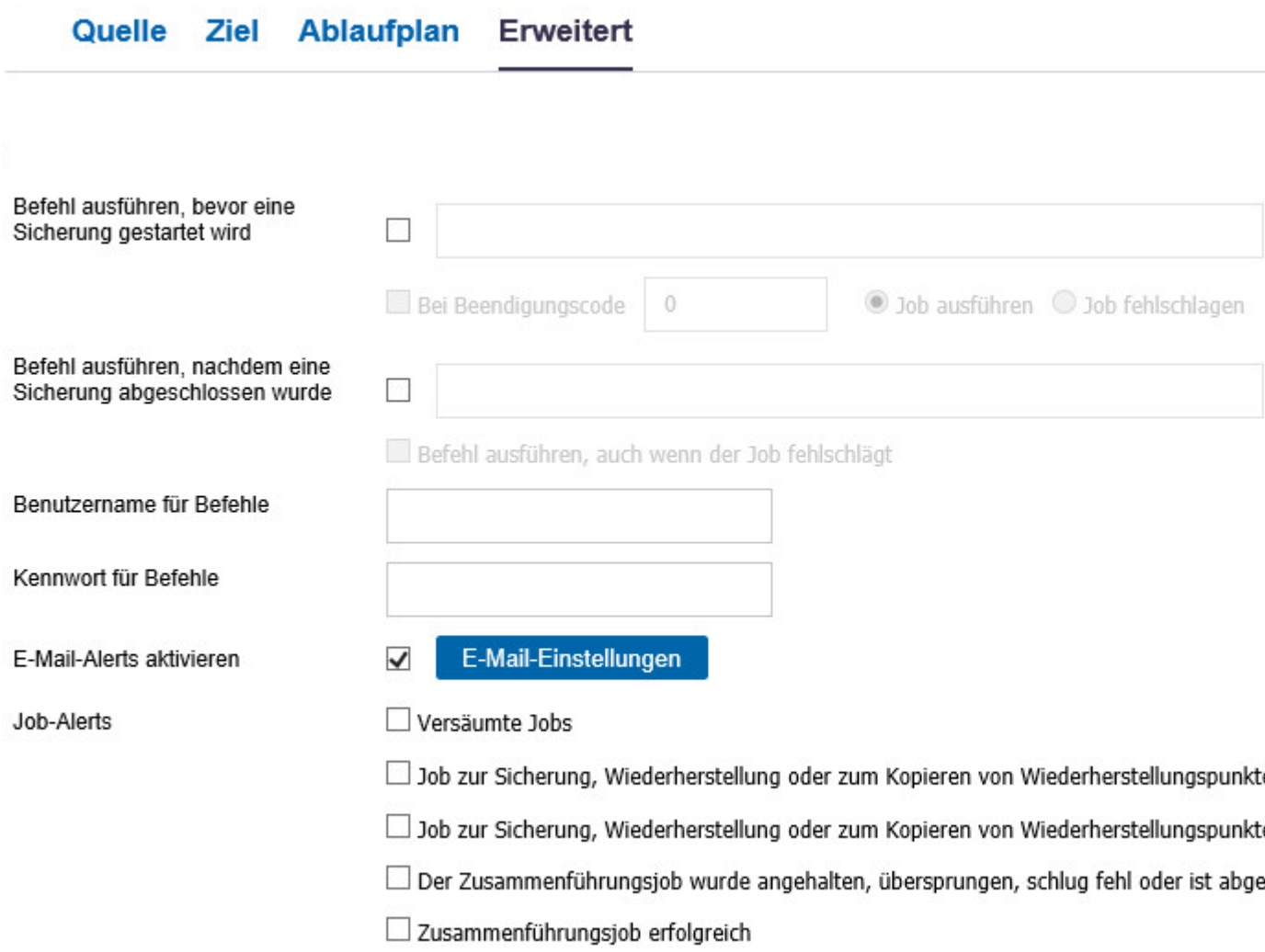
   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld **Sicherungsablaufplan** übernommen.

   Der Ablaufplan ist nun angegeben. Geben Sie nun die Details für Erweitert an.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte **Erweitert**:



Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

Befehl ausführen, bevor eine Sicherung gestartet wird

Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, unter dem das Skript auf dem Proxy-Knoten gespeichert ist. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist.

Befehl ausführen, auch wenn der Job fehlschlägt

Wenn dieses Kontrollkästchen aktiviert ist, wird das unter **Befehl ausführen, nachdem eine Sicherung abgeschlossen ist** angegebene Skript ausgeführt, selbst wenn der Sicherungsjob fehlschlägt. Andernfalls wird das Skript nur dann ausgeführt, wenn der Sicherungsjob erfolgreich abgeschlossen wurde.

Benutzername für Befehle

Ermöglicht die Angabe des Benutzernamens zum Ausführen der Befehle.

Kennwort für Befehle

Ermöglicht die Angabe des Kennworts zum Ausführen der Befehle.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Typen der Warnmeldungen angeben, die Sie in einer E-Mail erhalten möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers. Weitere Informationen zum Konfigurieren von E-Mail-Einstellungen finden Sie unter E-Mail- und Alert-Konfiguration.

Job-Alerts

Ermöglicht es Ihnen, die Arten von Job-Alerts auszuwählen, die Sie per E-Mail empfangen möchten.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Proxy-Knoten installiert und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agent oder kein Agent installiert ist. Um den Agent auf diesen Knoten zu installieren bzw. um ein Upgrade der Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus und klicken auf **Speichern**.

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie einen andere Task hinzufügen müssen, müssen Sie den Plan auf der Registerkarte **Ressourcen** auswählen und anschließend ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern. Sie können die Tasks **Kopieren von Wie-**

derherstellungspunkten, **Auf Band kopieren**, **Replizieren** und **Von einem Remote-RPS replizieren** als Folgetasks hinzufügen.

Der Plan wird automatisch auf dem Proxy-Serverknoten bereitgestellt.

Der Exchange Online-Sicherungsplan für den Proxy-Server wird erstellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

(Optional) Ausführen einer manuellen Sicherung

In der Regel werden die Sicherungen basierend auf den von Ihnen angewendeten Ablaufplaneinstellungen automatisch ausgeführt. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern. Wenn Sie z. B. einen Wiederholungsplan für vollständige Sicherungen und Zuwachssicherungen festgelegt haben und größere Veränderungen an Ihrem Rechner vornehmen möchten, können Sie sofort eine manuelle Sicherung durchführen, ohne auf die nächste geplante Sicherung zu warten. Sie können den Sicherungsjob sowohl von der Konsole als auch von der Proxy-Benutzeroberfläche aus übermitteln. Mit dem Job-Monitor können Sie den Jobstatus einsehen und den laufenden Job abbrechen.

Um eine manuelle Sicherung von OneDrive-Knoten durchzuführen, Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Die OneDrive-Knoten werden im mittleren Bereich angezeigt.
3. Wählen Sie die OneDrive-Knoten aus, die Sie sichern möchten und denen ein Plan zugeordnet ist.
4. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Jetzt sichern**.

   Das Dialogfeld **Sicherung jetzt ausführen** wird geöffnet.
5. Wählen Sie einen Sicherungstyp aus, und geben Sie optional einen Namen für den Sicherungsjob an.
6. Klicken Sie auf **OK**.

   Der Sicherungsjob wird ausgeführt.

Gehen Sie wie folgt vor: um eine manuelle Sicherung eines OneDrive-Plans durchzuführen.

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

Die Sicherungspläne von OneDrive werden im mittleren Bereich angezeigt.

3. Wählen Sie den Plan aus, den Sie sichern möchten, und vergewissern Sie sich, dass ihm ein Plan zugewiesen ist.
4. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Jetzt sichern**.

   Das Dialogfeld **Sicherung jetzt ausführen** wird geöffnet.
5. Wählen Sie einen Sicherungstyp aus, und geben Sie optional einen Namen für den Sicherungsjob an.
6. Klicken Sie auf **OK**.

   Der Sicherungsjob wird ausgeführt.

   Die manuelle Sicherung wird erfolgreich ausgeführt. Sie können jetzt die Sicherung überprüfen.

Überprüfen der Sicherung

Zur Überprüfung Ihres Sicherungsjobs bestätigen Sie, dass Sie den Sicherungsplan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Sie können den Status von Sicherungsjobs auf der Registerkarte **Jobs** überprüfen.

Gehen Sie wie folgt vor, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

   Wenden Sie zur Überprüfung von Sicherungsjobs eine der folgenden Methoden an:

   Methode 1

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs vollständig**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

   Methode 2

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Jobs erfolgreich abgeschlossen**.

   Die Liste der abgeschlossenen Sicherungsjobs wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf den Job, den Sie überprüfen möchten.

   Der rechte Fensterbereich wird aktualisiert.
4. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
5. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Konfigurieren der Multi-Faktor-Authentifizierung

Wenn in einer Organisation die Multi-Faktor-Authentifizierung (MFA) für die Benutzer aktiviert ist, verwenden Sie die moderne Authentifizierung, um Knoten hinzuzufügen.

Hinweis: Auch wenn die Standardauthentifizierung für den Mandanten aktiviert ist, können Sie die moderne Authentifizierung zum Hinzufügen von Knoten verwenden. Weitere Informationen zum Hinzufügen von Knoten zu einem Plan mithilfe der modernen Authentifizierung finden Sie unter Moderne Authentifizierung.

Verwalten der Sicherung und Wiederherstellung von Microsoft Teams-Daten

Dieser Abschnitt enthält Informationen zum Sichern und Wiederherstellen von Microsoft Teams-Daten mithilfe von Exchange Online und SharePoint Online. Arcserve UDP ermöglicht das Sichern von Nachrichten (Chats) und Dateien, die über private und öffentliche Kanäle sowie Gruppenkanäle freigegeben wurden.

Jedes Mal, wenn Sie einen privaten oder öffentlichen Kanal oder einen Gruppenkanal in Microsoft Teams erstellen, wird automatisch eine SharePoint Online-Website für den Kanal erstellt. Diese SharePoint Online-Website verfügt über einen Standardordner für Dokumentbibliotheken, in dem alle in Unterhaltungen freigegebenen Dateien automatisch gespeichert werden. Sie können auch die Berechtigungen und Sicherheitsoptionen für vertrauliche Informationen anpassen.

In diesem Abschnitt werden die folgenden Themen behandelt:

Sichern und Wiederherstellen von Microsoft Teams-Nachrichten (Chats) mit Exchange Online

Sie können einzelne Chats mithilfe des Benutzerpostfachs in der UDP-Sicherung des Exchange Online-Knotens sichern. Alle Nachrichten werden auf dem Exchange Online-Server im Ordner "TeamsMessagesData" gespeichert, der sich unter einem Stammordner befindet. Dieser Abschnitt enthält Informationen zum Sichern und Wiederherstellen von Microsoft Teams-Nachrichten (Chats) mit Exchange Online.

In diesem Abschnitt werden die folgenden Themen behandelt:

Sichern von Microsoft Teams-Nachrichten (Chats) mit Exchange Online

Dieser Abschnitt enthält Informationen zum Sichern von Microsoft Teams-Nachrichten (Chats) mit Exchange Online.

In diesem Abschnitt werden die folgenden Themen behandelt:

Erstellen eines Exchange Online-Sicherungsplans

Exchange Online ist eine E-Mail-Anwendung, die in der Microsoft-Cloud gehostet wird. Um Ihre Exchange Online-E-Mail-Elemente (E-Mails, Kalenderelemente, Kontakte usw.) aus der Microsoft-Cloud zu sichern, müssen Sie einen Plan erstellen. Der Plan für Exchange Online besteht aus einem Sicherungstask. In diesem Sicherungstask können Sie die Exchange Online-Knoten, die Sie schützen möchten, das Sicherungsziel und den Ablaufplan für die Sicherung angeben.

In diesem Abschnitt werden die folgenden Themen behandelt:

Überprüfen der Voraussetzungen und Hinweise

Überprüfen Sie die folgenden Voraussetzungen und Hinweise, bevor Sie einen Exchange Online-Sicherungsplan erstellen.

Erstellen eines Plans für Exchange Online-Sicherungen:

Voraussetzungen:

Für das Sicherungskonto:

- Verwenden Sie ein Sicherungsdienstkonto mit den Rechten für einen globalen Administrator.
- Fügen Sie die Berechtigung zum Identitätswechsel für den Sicherungsbenutzer zum Exchange Online-Sicherungskonto hinzu, um die Online Exchange-Organisation zu verbinden und Sicherungen und Wiederherstellungen durchzuführen.

  Hinweis: Wenn Sie das Sicherungskonto nicht zur Rollengruppe "Discoveryverwaltung" hinzufügen und nicht die Berechtigung "ApplicationImpersonation" zuweisen, schlägt die Sicherung fehl.

- Ordnen Sie dem Backup-Benutzerkonto ein Exchange Online-Postfach zu.

Für Sicherungs-Proxy:

- Melden Sie sich bei der Konsole an.
- Installieren Sie Arcserve UDP Agent auf dem Proxy-Rechner, auf dem die Sicherung/Wiederherstellung ausgeführt werden soll.

Besondere Aspekte:

- Beim Sichern einer großen Gruppe von Benutzern können Sie für eine bessere Sicherung und Optimierung Exchange-Gruppen verwenden.
- Die Standardeinstellung für die Online-Sicherung von Exchange verwendet 4 gleichzeitige Sicherungs-Threads (einen Thread pro Benutzer). Sie können auch die Threads in der Konfigurationsdatei *Engine\BIN\Office365\Arcserve.Office365.Exchange.config* wie folgt ändern:

```
<!--#region for multi thread--> <!--MultiThreadEnable default
value:0. if enable, set 1.--> <add
key="MultiThreadEnable" value ="1"/> <!--set how many thread
will be used to backup mailbox. Standardwert ist 4--> <add
key="MaxDegreeOfParallelismForMailbox" value="4"/> <!--#end-
```

```
region-->
```

Wir empfehlen, den Wert auf 1 bis 5 festzulegen. Der maximal mögliche Wert ist 10. Es wird nicht empfohlen, den Wert von 6 bis 10 festzulegen.

Hinweis: UDP 8.0 unterstützt Folgendes:

- Benutzerpostfach
- Freigegebenes Postfach
- E-Mail-aktivierte öffentliche Ordner
- Raumpostfächer
- Gerätepostfächer
- Gruppenpostfächer

Hinweis: Weitere Informationen zu den Best Practices für Exchange Online finden Sie unter Exchange Online.

Erstellen eines Exchange Online-Sicherungsplans mit Basisauthentifizierung (BA):

Überprüfen Sie die folgenden Voraussetzungen:

- Installieren Sie die PowerShell Version 5.1 oder höher (Teil des Windows Management Framework (WMF)) auf dem Proxy-Server (64-Bit-Computer).
- Installieren Sie mithilfe der Befehlszeile die folgenden PowerShell-Module auf dem Proxy-Server unter Verwendung des PowerShell-Fensters:
  - Führen Sie den folgenden Befehl aus, um das Azure-Modul zu installieren:

    Installationsmodul -Name AzureAD -Force
  - Führen Sie den folgenden Befehl aus, um das ExchangeOnlineManagement-Modul zu installieren:

    Installationsmodul -Name ExchangeOnlineManagement -Force

Hinweis: Wenn Sie PowerShell-Module mithilfe der oben genannten Befehle installieren, wird basierend auf der GA-Version der im Microsoft-Repository verfügbaren Komponente möglicherweise eine neuere Version der Module installiert.

Erstellen eines Exchange Online-Sicherungsplans mithilfe der modernen Authentifizierung (MA):

Überprüfen Sie die Voraussetzungen, bevor Sie einen Plan unter Verwendung der modernen Authentifizierung erstellen.

Hinzufügen der erforderlichen Rolle und Gruppe zum Exchange Online-Sicherungskonto zur Durchführung von Sicherungen und Wiederherstellungen

Fügen Sie das Sicherungskonto zur Rollengruppe "Discoveryverwaltung" hinzu, und weisen Sie ihm die Berechtigung "ApplicationImpersonation" zu.

Gehen Sie wie folgt vor:

1. Fügen Sie die erforderliche Rolle und Gruppe mit einer der folgenden Methoden zu:

   Über das Office 365-Portal

a. Melden Sie sich als Administrator oder mit einem Konto, das über globale Administratorberechtigungen verfügt, beim Office 365-Portal an.

   Die Seite "Exchange Online Admin Center" wird angezeigt.

b. Gehen Sie zu **Berechtigungen**, und doppelklicken Sie in der Drop-down-Liste "Hinzufügen" auf **Discoveryverwaltung**.

   Das Dialogfeld "Discoveryverwaltung" wird angezeigt.

   Hinweis: Mitglieder der Rollengruppe "Discoveryverwaltung" können Postfächer in der Exchange-Organisation nach Daten durchsuchen, die bestimmte Kriterien erfüllen.

c. Klicken Sie unter **Rollen** auf **+**, um die Rolle "ApplicationImpersonation" hinzuzufügen.

   Das Dialogfeld "Rolle auswählen" wird angezeigt.

d. Wählen Sie in der Drop-down-Liste **Anzeigename** den Eintrag **ApplicationImpersonation** aus.

   Hinweis: Die Rolle "ApplicationImpersonation" erlaubt es Anwendungen, die Identität eines Benutzers in einer Organisation anzunehmen, um Aufgaben im Namen des Benutzers auszuführen.

e. Klicken Sie auf **Hinzufügen**, um die Rolle "ApplicationImpersonation" hinzuzufügen, und klicken Sie dann auf **OK**.

f. Klicken Sie im Dialogfeld "Discoveryverwaltung" unter **Mitglieder** auf **+**, um das Sicherungskonto als Mitglied hinzuzufügen.

Das Dialogfeld "Mitglieder auswählen" wird angezeigt.

g. Wählen Sie in der Drop-down-Liste "Name" das Sicherungskonto aus, klicken Sie auf **Hinzufügen**, um das Mitglied hinzuzufügen, und klicken Sie dann auf **OK**.

   Das ausgewählte Sicherungskonto wird unter **Mitglieder** im Dialogfeld **Discoveryverwaltung** angezeigt.

h. Klicken Sie auf **Speichern**.

Über die Remote-PowerShell

a. Um eine Verbindung zum Exchange Online-Tenant über die Remote-PowerShell herzustellen, siehe Link.

b. Sobald die Verbindung aufgebaut ist, können Sie folgendes Cmdlet verwenden, um das Sicherungskonto als Mitglied zur Rollengruppe "Discoveryverwaltung" hinzuzufügen:

   `Cmdlet "Add-RoleGroupMember"`

   Beispiel: Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.

c. Verwenden Sie das folgende Cmdlet, um dem Sicherungskonto die Rolle "ApplicationImpersonation" hinzuzufügen:

   `Cmdlet "New-ManagementRoleAssignment"`

   Beispiel:

   New-ManagementRoleAssignment -Name: impersonationAssignmentName -Role:ApplicationImpersonation - User: "username@domain.onmicrosoft.com"

Die Rolle "ApplicationImpersonation" und die Gruppe "Mitglieder" werden zum Exchange Online-Sicherungskonto hinzugefügt.

Erstellen eines Plans für Exchange Online-Sicherungen

Ein Sicherungsplan enthält einen Sicherungstask, der Exchange Online-E-Mail-Datenelemente (E-Mails, Kalenderelemente, Kontakte usw.) sichert und die Daten auf einem Datenspeicher ohne oder mit Deduplizierung speichert. Darüber hinaus ermöglicht dieser Sicherungsplan es UDP, Exchange Online-Gruppen zu erkennen und anzugeben, für die ein Sicherungstask ausgeführt wird. Jeder Task besteht aus Parametern, die Quelle, Ziel, Ablaufplan und weitere Sicherungsdetails definieren.

Gehen Sie wie folgt vor:

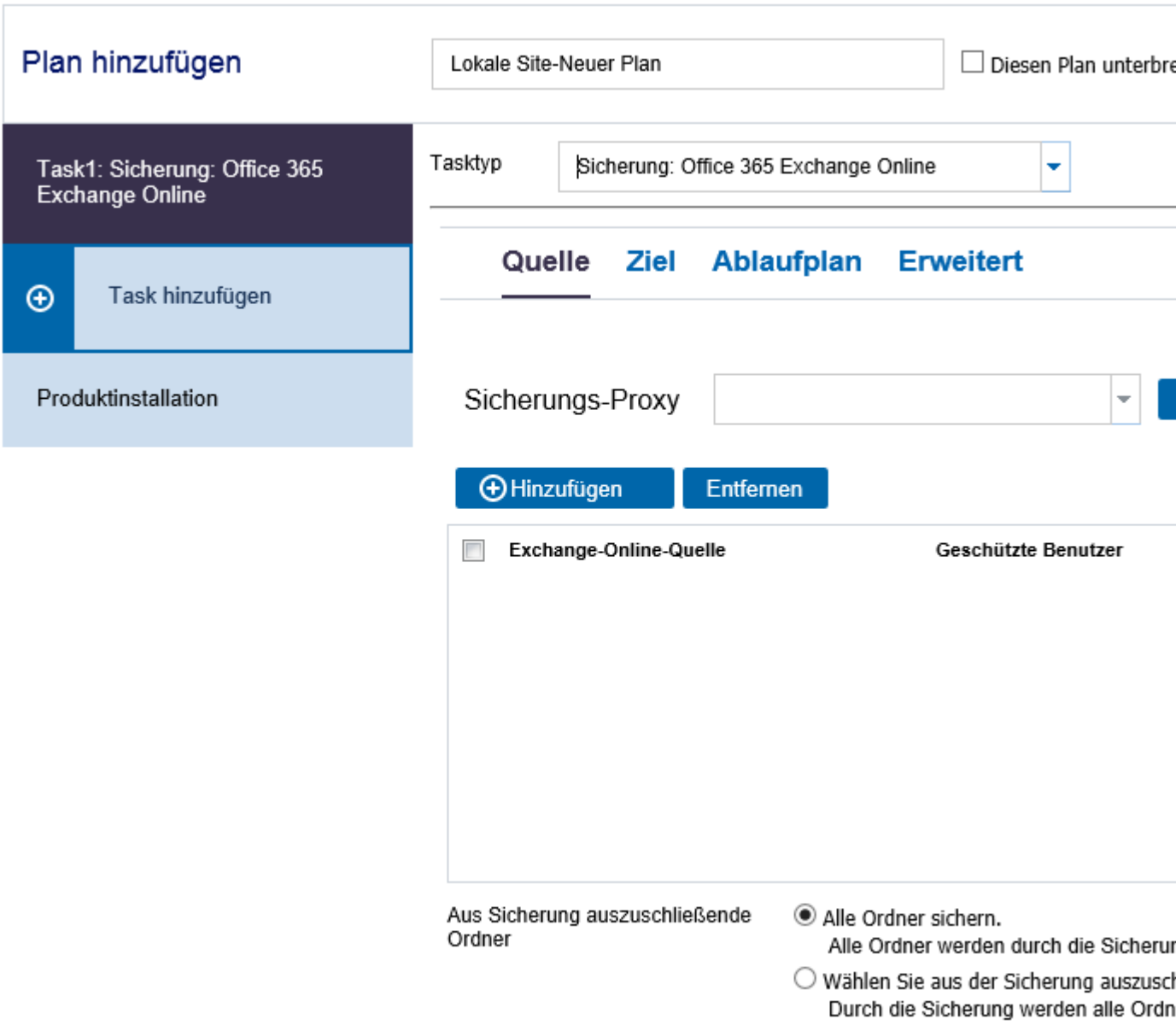
1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Das Dialogfenster **Plan hinzufügen** wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Drop-down-Liste Tasktyp die Option **Sicherung: Office 365 Exchange Online** aus.



Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Angeben der Quelle

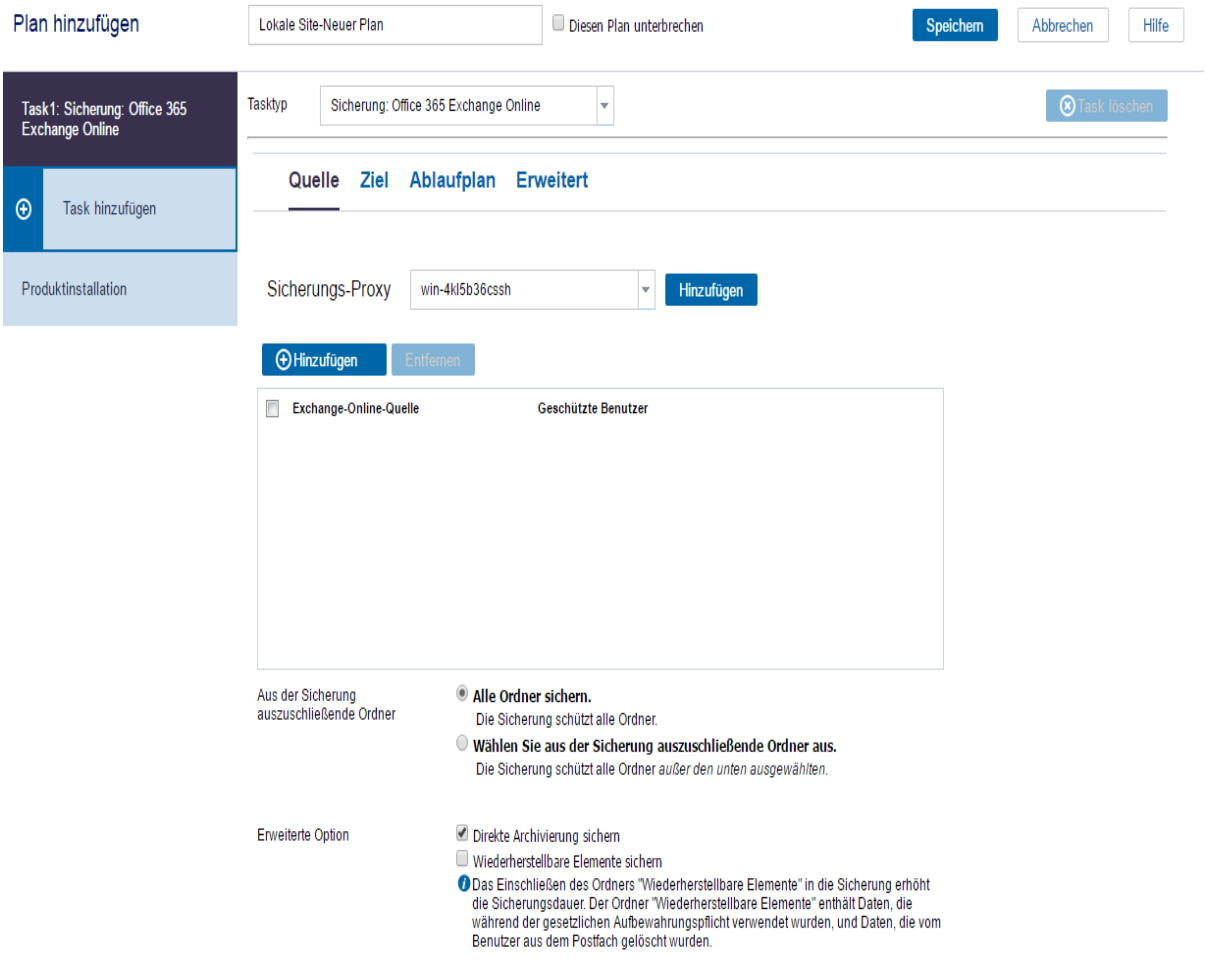
Auf der Seite "Quelle" können Sie die Exchange Online-Quellknoten angeben, die Sie schützen möchten. Sie können für einen Plan mehrere Exchange Online-Quellknoten auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Exchange Online-Quellknoten von der Quellseite hinzufügen.

Hinweis: Sie können einen Plan speichern, ohne Quellknoten hinzuzufügen. Der Plan wird jedoch nur bereitgestellt, wenn Sie Knoten hinzufügen.

Sie können auch Exchange Online Knoten verwalten, indem Sie die Postfachunterstützung für öffentliche Ordner für Exchange Online-Schutz verwenden.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Quelle**.



2. Für "Sicherungs-Proxy" haben Sie folgende Möglichkeiten:

- Wählen Sie in der Drop-down-Liste einen vorhandenen Sicherungs-Proxy aus.
- Um einen neuen Sicherungs-Proxy hinzuzufügen, klicken Sie neben der Drop-down-Liste auf **Hinzufügen**.

3. Fügen Sie mithilfe einer der folgenden Optionen einen Exchange Online-Knoten hinzu:

   Methode 1

   a. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Wählen Sie zu sichernde Quellen in Arcserve UDP aus**.

      Das Dialogfeld "Knoten zu Plan hinzufügen" wird angezeigt.

   b. Wählen Sie einen Knoten aus, und klicken Sie dann auf **Verbinden**.

      Hinweis: Sie können auch in der **Suche** nach den Exchange Online-Knoten suchen, die Sie schützen möchten.

   c. Aktivieren Sie das Kontrollkästchen **Alle Office 365 Exchange-Quellen schützen**, um alle Exchange Online-Konten auf allen Seiten zu schützen.

      Hinweis: Klicken Sie auf den Rechtspfeil (>), um alle Exchange Online-Konten zur Liste der geschützten Knoten hinzuzufügen.

      Die Exchange Online-Konten, die Sie ausgewählt haben, werden hinzugefügt.

   Methode 2

   - Klicken Sie auf **Hinzufügen** und dann auf **Exchange Online-Quelle hinzufügen**.

     Das Dialogfeld "Knoten zu Plan hinzufügen" wird geöffnet.

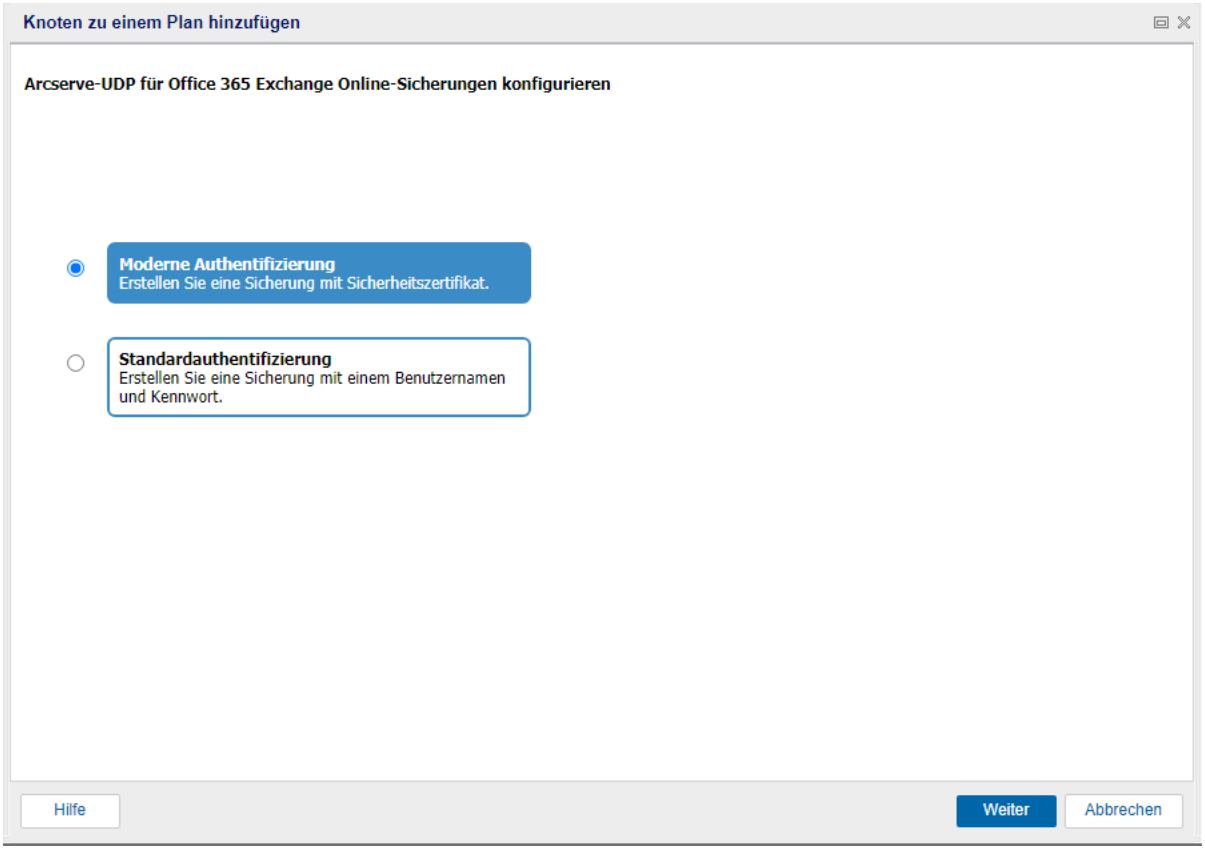
     Hinweis: Anders als andere Knoten können Sie Exchange Online-Knoten nicht über die Seite **Alle Knoten** hinzufügen. Sie können einen Exchange Online-Knoten nur in einem Plan hinzufügen, oder wenn Sie einen Plan ändern.

     Mehrere Exchange Online-Knoten können dasselbe Benutzerkonto (Dienstkonto) von Exchange online verwenden.

4. Gehen Sie folgendermaßen vor, um die Authentifizierung anzuwenden:

   Moderne Authentifizierung

   Bei der modernen Authentifizierung können Sie eine Sicherung mithilfe eines Sicherheitszertifikats ausführen.



Sicherheitszertifikat verwenden

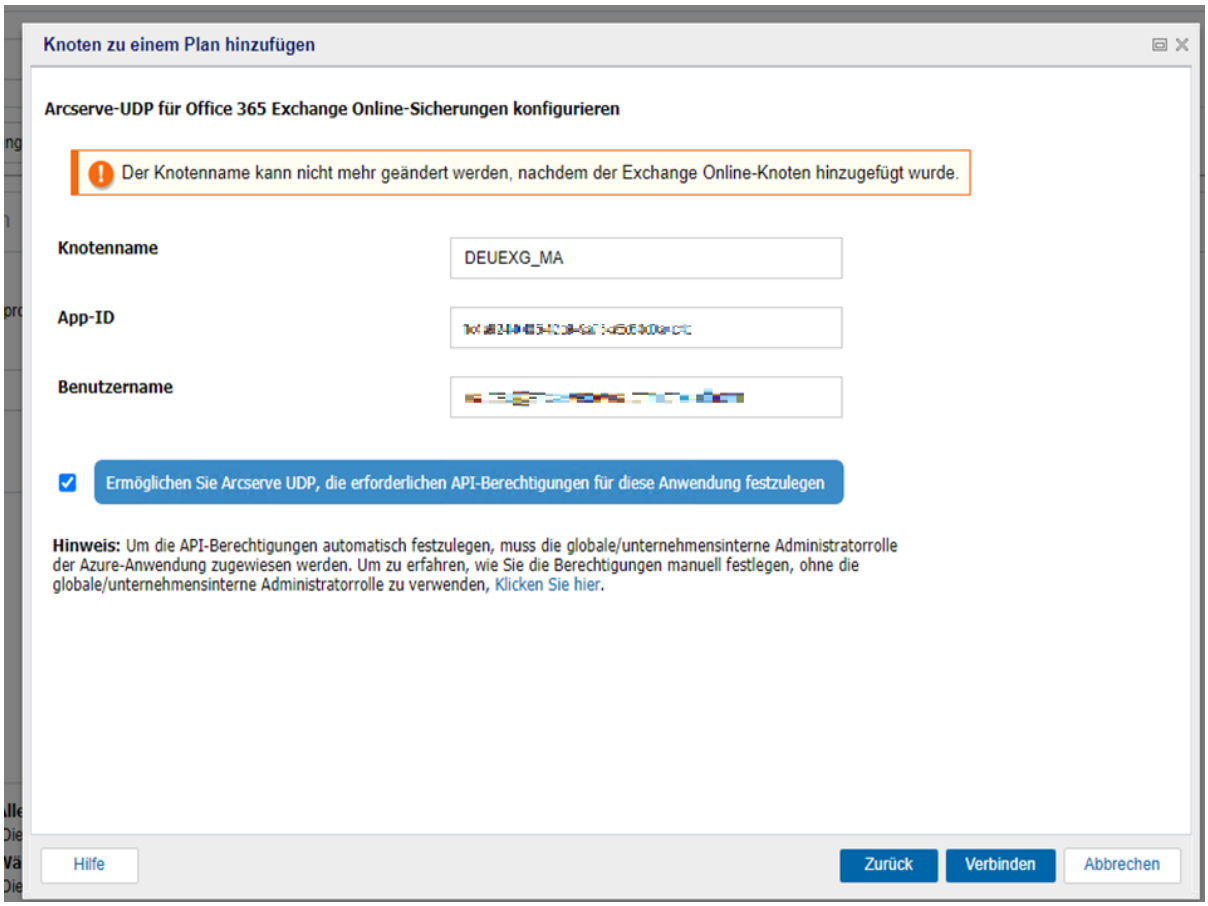
Hinweis: Standardmäßig wählt der Sicherungsplan die Option **Sicherheitszertifikat verwenden** für die moderne Authentifizierung aus.

Gehen Sie wie folgt vor:

a. Informationen zum Authentifizieren der UDP-Anwendung mit Sicherheitszertifikaten finden Sie unter Herunterladen des Zertifikats von UDP und Hochladen in Azure.

b. Geben Sie die folgenden Details ein:

- Knotenname
- App-ID
- Benutzername



c. Um die API-Berechtigungen automatisch anzuwenden, aktivieren Sie das Kontrollkästchen **Arcserve UDP erlauben, die erforderlichen API-Berechtigungen für diese Anwendung festzulegen**.

   Hinweis: Informationen zum manuellen Anwenden der Berechtigungen ohne Verwendung der Administratorrolle "Global/Company" finden Sie unter Manuelles Konfigurieren der API-Berechtigungen ohne Verwendung der Administratorrolle "Global/Company".

d. Klicken Sie auf **Connect**.

Hinweise:

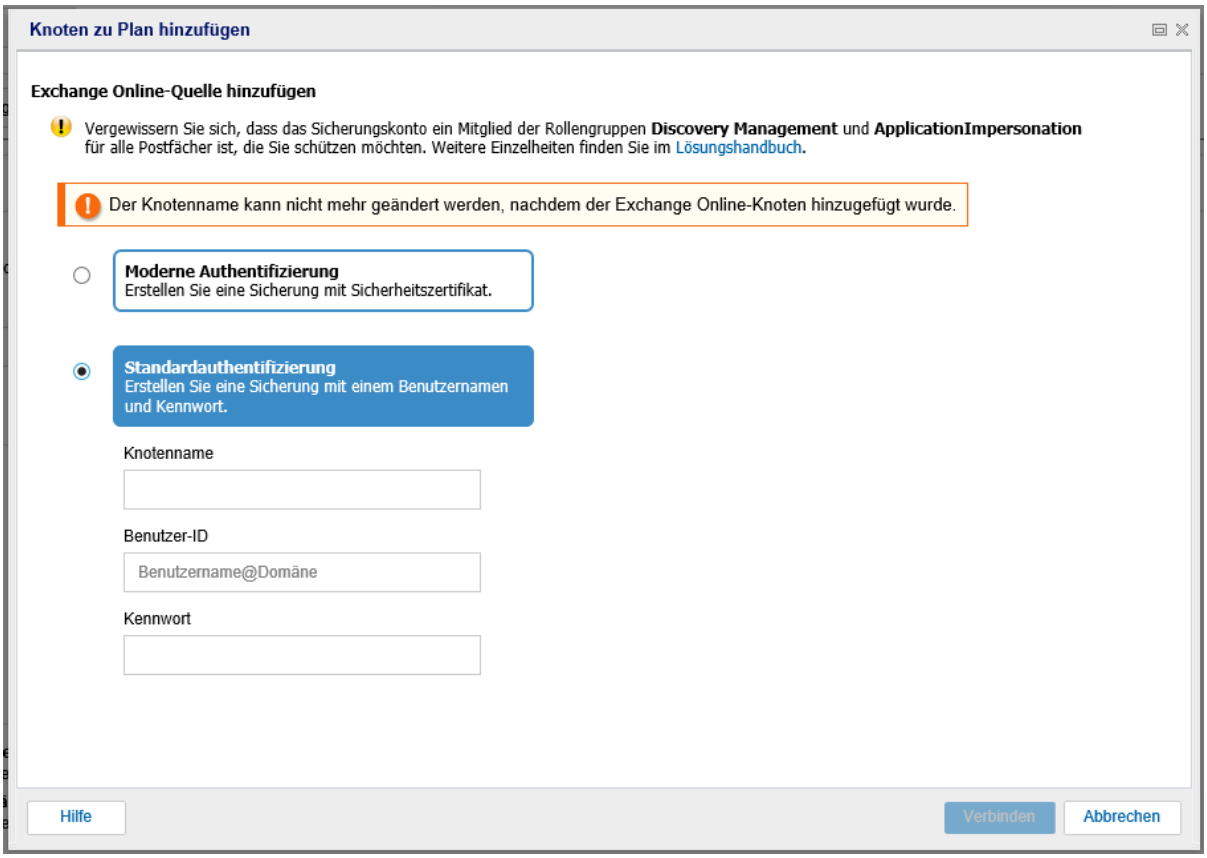
- Der Name des Exchange Online-Knotens kann nicht mehr geändert werden, nachdem der Knoten hinzugefügt wurde.
- Geben Sie in **Admin-Benutzername** den Benutzernamen des Exchange Online-Sicherungskontos ein, der die Voraussetzungen erfüllt.
- Die moderne Authentifizierung gilt nicht für Folgendes:

- Für Kunden, die Microsoft 365 (Office 365) für ihre Arcserve Cloud Hybrid-Instanzen oder Arcserve Cloud Backup für Office 365 mit einem Erstellungsdatum von vor dem 18. Oktober 2020 verwenden, ist die moderne Authentifizierung nicht möglich.
- Kunden, die weiterhin die Standardauthentifizierung verwenden.

Standardauthentifizierung

Um bei Verwendung der Standardauthentifizierung mit der Sicherung fortzufahren, geben Sie die folgenden Informationen an, und klicken Sie dann auf **Verbinden**:

- Knotenname
- Benutzer-ID
- Kennwort



Hinweis: Das Aktualisieren oder Ändern des Benutzerkontos kann die Anzahl geschützter Postfächer ändern. Sie müssen sicherstellen, dass die neuen oder aktualisierten Dienstkonten Identitätswechselrechte für zu schützende Postfächer besitzen.

5. Zum Schützen von Exchange Online-Postfächern haben Sie folgende Möglichkeiten:

   - Um alle Exchange Online-Postfächer und -Gruppen zu schützen, aktivieren Sie das Kontrollkästchen **Die gesamte Office 365 Exchange-Quelle schützen**.

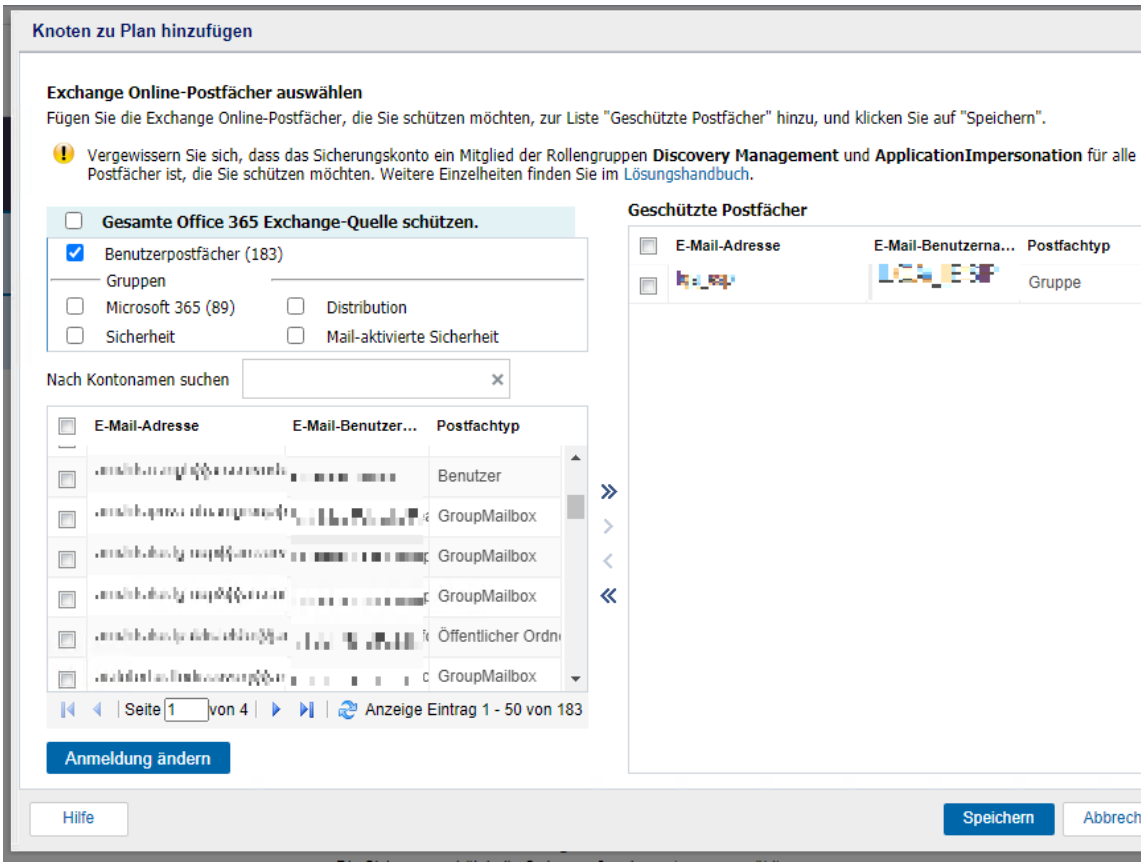
     Hinweis: Bei Anzeige des Bildschirms "Exchange Online-Postfächer auswählen" ist diese Option standardmäßig automatisch ausgewählt.

   - Gehen Sie für Benutzerpostfächer folgendermaßen vor:

     a. Aktivieren Sie das Kontrollkästchen **Benutzerpostfächer**.

        Eine Liste von Benutzerpostfächern wird angezeigt.

     b. (Optional) Um in der Liste nach einem Konto zu suchen, geben Sie den Kontonamen im Feld "Nach Kontonamen suchen" ein.



     c. Wählen Sie die zu schützenden Postfächer in der Liste der Benutzerpostfächer aus.

     d. Klicken Sie auf den Nach-rechts-Pfeil (>), um die ausgewählten Postfächer in die Liste "Geschützte Postfächer" zu verschieben.

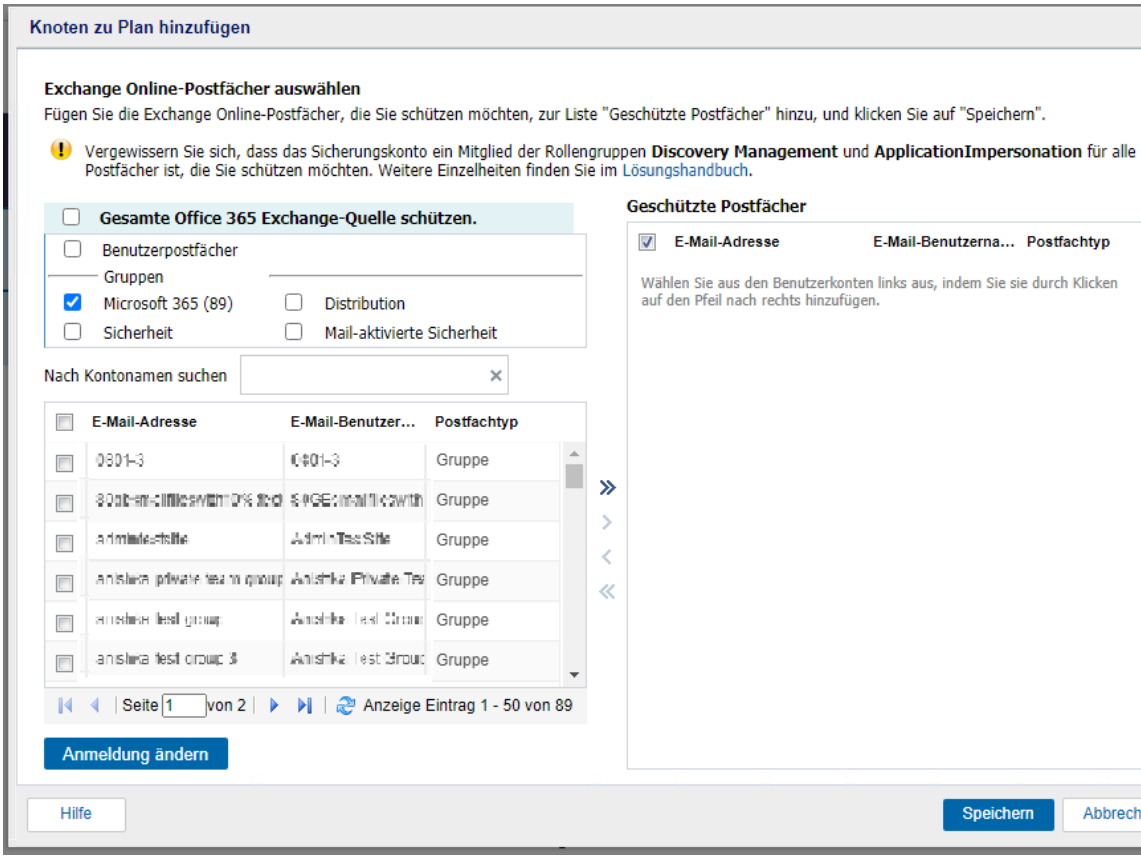
- Gehen Sie für Gruppen folgendermaßen vor:

  a. Aktivieren Sie das Kontrollkästchen **Microsoft 365**.

     Eine Liste von Gruppen wird angezeigt.

     Hinweis: Wenn Sie Gruppen zusammen mit Untergruppen wie **Distribution**, **Sicherheit** oder **Mail-aktivierte Sicherheit** auswählen möchten, aktivieren Sie das Kontrollkästchen **Microsoft 365** und anschließend nach Bedarf das Kontrollkästchen für eine Untergruppe.

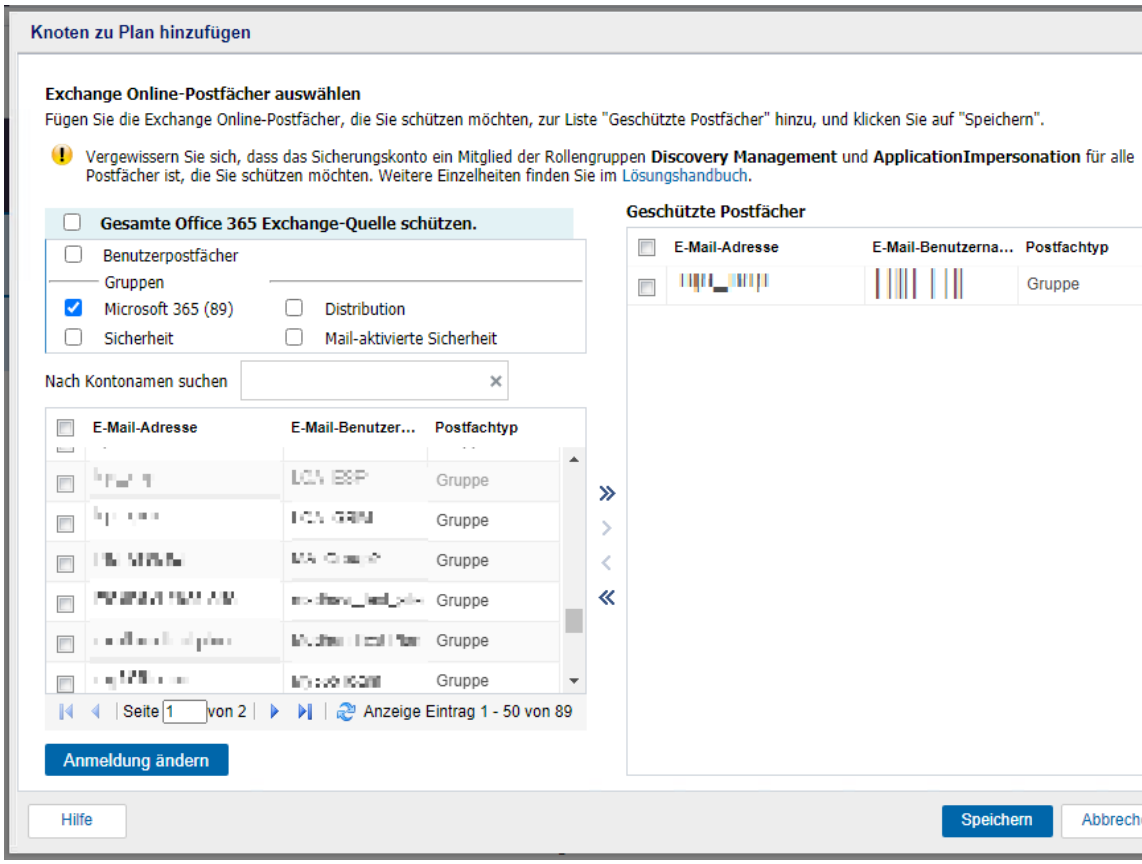
  b. (Optional) Um in der Liste nach einem Konto zu suchen, geben Sie den Kontonamen im Feld "Nach Kontonamen suchen" ein.



  c. Wählen Sie die zu schützenden Gruppen in der Liste der Gruppen aus.

  d. Klicken Sie auf den Nach-rechts-Pfeil (>), um die ausgewählten

Gruppen in die Liste "Geschützte Postfächer" zu verschieben.



6. Klicken Sie auf **Speichern**.
7. Gehen Sie auf der Registerkarte "Quellen" zu **Aus der Sicherung auszuschließende Ordner**, und aktivieren Sie dann das gewünschte Kontrollkästchen.
8. Wählen Sie unter erweiterte Option das gewünschte Kontrollkästchen aus.
    - Damit der Exchange Online-Schutz die Postfacharchivierung erlaubt, aktivieren Sie das Kontrollkästchen **Direkte Archivierung sichern**.

      Hinweis: Weitere Informationen über die Postfacharchivierung finden Sie unter diesem Link.
    - Wählen Sie das Kontrollkästchen **Wiederherstellbare Elemente sichern** aus, um das Postfach zu schützen, das die In-Place-Hold oder Litigation-Hold-Funktion ermöglicht.

      Hinweis: Informationen zur Archivierung von In-Place-Hold und Litigation-Hold für Exchange Online finden Sie unter diesem Link.

    Hinweis: Um beide Funktionen im Postfach gleichzeitig zu aktivieren, um wiederherstellbare Elemente in der Postfacharchivierung zu sichern, wählen Sie

die Optionen **In-Place-Archivierung sichern** und **Wiederherstellbare Elemente sichern** aus.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ziel**.
2. Wählen Sie die Option **Arcserve UDP Recovery Point Server** aus. **Arcserve UDP Recovery Point Server** gibt an, dass das Sicherungsziel ein Recovery Point Server ist. Wenn Sie diese Option auswählen, werden Daten als Wiederherstellungspunkte gespeichert. Sie können Daten nicht als Wiederherstellungssätze speichern.
3. Geben Sie folgende Details an:
    a. Wählen Sie einen Recovery Point Server aus.
    b. Wählen Sie einen für Deduplizierung bzw. nicht für Deduplizierung aktivierten Datenspeicher. Die Liste zeigt alle auf dem angegebenen Recovery Point-Server erstellten Datenspeicher an.
    c. Geben Sie ein Sitzungskennwort ein. Das Sitzungskennwort ist optional, wenn das Sicherungsziel ein unverschlüsselter RPS-Datenspeicher ist.
    d. Bestätigen Sie das Sitzungskennwort.

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

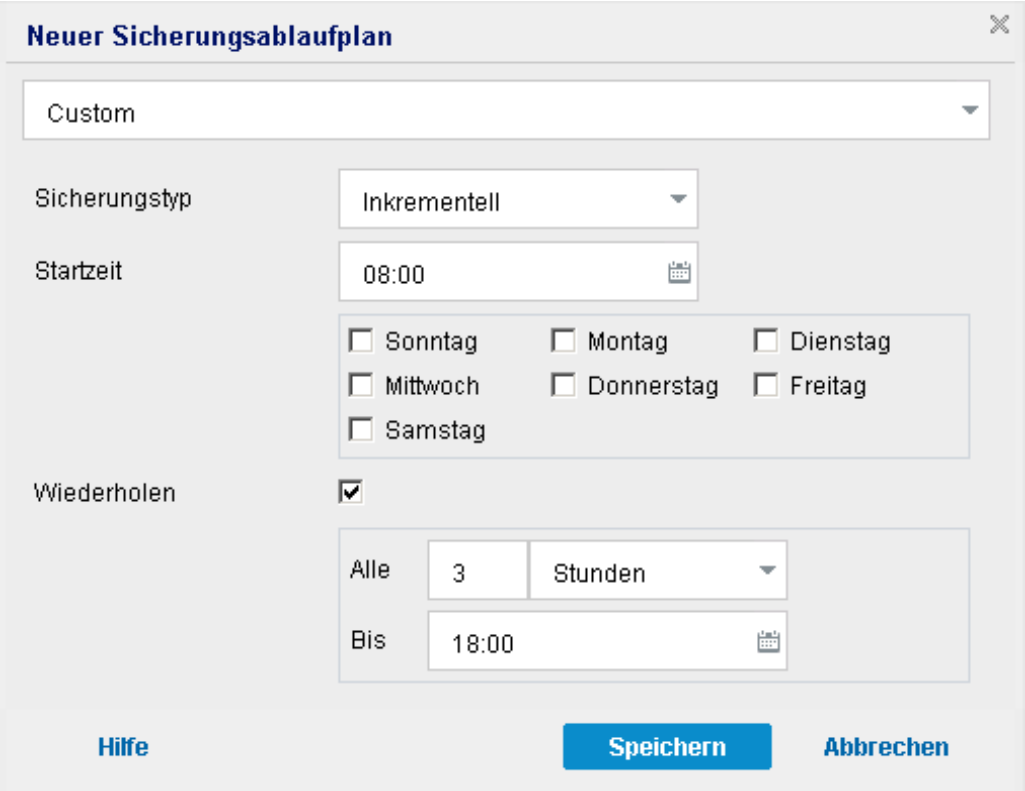
Gehen Sie wie folgt vor:

1. Fügen Sie Ablaufpläne für Sicherungen, Zusammenführungen und Drosselungsvorgänge hinzu.

   Hinzufügen eines Sicherungsablaufplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke

des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

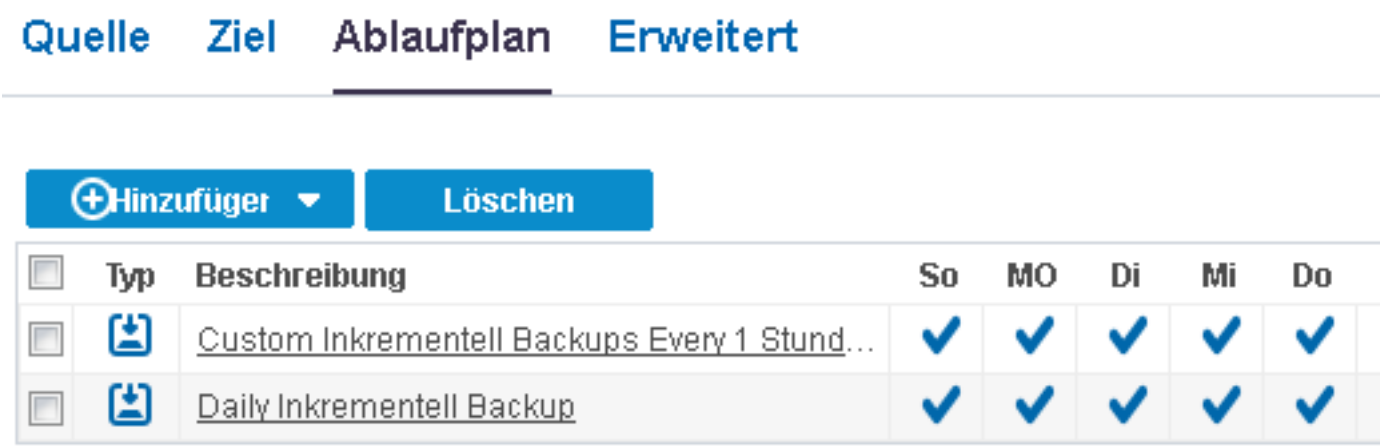
Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Blöcken, die nach der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass die Sicherung schnell durchgeführt und ein kleines Sicherungs-Image erstellt wird. Diese ist der optimale Weg, um eine Sicherung durchzuführen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.



Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zusammenführungsplan hinzufügen** aus.

Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

b. Geben Sie die Startzeit an, zu der die Zusammenführung starten soll.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Zusammenführung anzugeben.

d. Klicken Sie auf **Speichern**.

Der Zusammenführungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Drosselungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

   Das Dialogfeld **Drosselungsplan hinzufügen wird geöffnet.**

b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

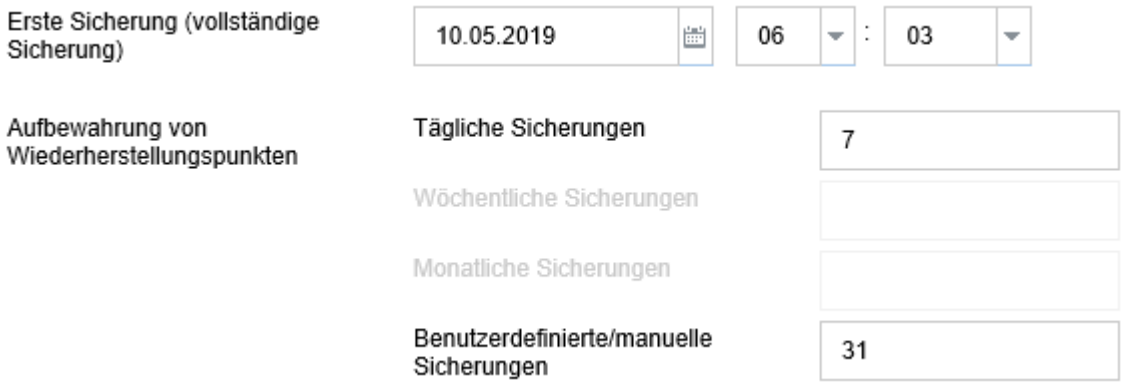
c. Geben Sie die Startzeit an, zu der die Drosselung starten soll.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende der Drosselung anzugeben.

e. Klicken Sie auf **Speichern**.

Der Drosselungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

2. Geben Sie die Startzeit für die geplante Sicherung an.



3. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld **Sicherungsablaufplan** übernommen.

   Der Ablaufplan ist nun angegeben.

Funktionsweise der erweiterten Planung und Aufbewahrung

Mit der Ablaufplanoption können Sie einen benutzerdefinierten Ablaufplan, einen Ablaufplan für tägliche/wöchentliche/monatliche Sicherungen oder beides festlegen. Im benutzerdefinierten Ablaufplan können Sie den Sicherungsablaufplan für jeden Tag der Woche konfigurieren und bis zu vier Sicherungsablaufpläne für jeden Tag hinzufügen. Sie können einen bestimmten Wochentag auswählen und ein Zeitfenster erstellen, um anzugeben, wann und wie oft die Sicherung durchgeführt werden soll.

Ablaufplan	Unterstützter Job	Kommentare
Sichern	Sicherungsjob	Gibt Zeitfenster für die Ausführung von Sicherungsjobs an.
Sicherungsdrosselung	Sicherungsjob	Gibt die Zeitfenster an, um die Sicherungsgeschwindigkeit zu steuern.
Zusammenführen	Zusammenführungsjob	Gibt an, wann Zusammenführungsjobs ausgeführt werden sollen.
Täglicher Ablaufplan	Sicherungsjob	Gibt an, wann tägliche Sicherungsjobs ausgeführt werden sollen.
Wöchentlicher Ablaufplan	Sicherungsjob	Gibt an, wann wöchentliche Sicherungsjobs ausgeführt werden sollen.
Monatlicher Ablaufplan	Sicherungsjob	Gibt an, wann monatliche Sicherungsjobs ausgeführt werden sollen.

Sie können auch die Aufbewahrungseinstellungen für die Wiederherstellungspunkte angeben.

Hinweis: Legen Sie innerhalb der einzelnen Pläne Einstellungen für die Aufbewahrungszeit fest, um zu steuern, wie die Daten für die Knoten des entsprechenden Plans im Zieldatenspeicher aufbewahrt werden.

Ablaufpläne für tägliche/wöchentliche/monatliche Sicherungen sind vom benutzerdefinierten Ablaufplan und voneinander unabhängig. Sie können die Ausführung einer täglichen, wöchentlichen oder monatlichen Sicherung konfigurieren, ohne einen benutzerdefinierten Ablaufplan zu konfigurieren.

Jobplan der Sicherung

Sie können vier Zeitfenster pro Tag in Ihrem Sicherungsablaufplan hinzufügen. Ein gültiges Zeitfenster liegt im Bereich 12:00 Uhr bis 23:59 Uhr. Sie können kein Zeitfenster wie z. B. 18:00 Uhr bis 06:00 Uhr angeben. In solchen Fällen müssen Sie manuell zwei verschiedene Zeitfenster angeben.

Für jedes Zeitfenster wird die Startzeit einbezogen, und die Endzeit wird nicht einbezogen. Zum Beispiel haben Sie das Ausführen einer Zuwachssicherung konfiguriert, die stündlich zwischen 06:00 Uhr und 09:00 Uhr stattfinden soll, und die Sicherung wird um 06:00 Uhr gestartet. Das bedeutet, dass die Sicherung um 06:00 Uhr, 07:00 Uhr und 08:00 Uhr ausgeführt wird, NICHT aber um 09:00 Uhr.

Hinweis: Wenn Sie die Sicherung bis zum Ende des Tages wiederholt ausführen möchten, legen Sie den Ablaufplan bis 12:00 Uhr fest. Um den Sicherungsjob beispielsweise alle 15 Minuten während des gesamten Tages auszuführen, legen Sie den Ablaufplan von 00:00 Uhr bis 00:00 Uhr alle 15 Minuten fest.

Drosselungsplan der Sicherung

Mit dem Drosselungsplan der Sicherung können Sie die Geschwindigkeit des Sicherungsdurchsatzes steuern, die wiederum die Ressourcenverwendung (Datenträger-E/A, CPU, Netzwerkbandbreite) des Servers, der gesichert wird, steuert. Dies ist hilfreich, wenn die Serverleistung während der Geschäftszeiten nicht beeinträchtigt werden soll. Sie können vier Zeitfenster pro Tag in Ihrem Drosselungsplan der Sicherung hinzufügen. Für jedes Zeitfenster können Sie einen Wert in MB pro Minute angeben. Dieser Wert wird verwendet, um den Sicherungsdurchsatz zu steuern. Gültige Werte liegen im Bereich zwischen 1 MB/Minute bis 99.999 MB/Minute.

Wenn ein Sicherungsjob die angegebene Zeit überschreitet, dann wird das Drosselungslimit entsprechend dem angegebenen Zeitfenster angepasst. Zum Beispiel haben Sie als Drosselungslimit der Sicherung den Wert 500 MB/Minute von 08:00 Uhr bis 20:00 Uhr und 2500 MB/Minute von 20:00 Uhr bis 22:00 Uhr angegeben. Wenn ein Sicherungsjob um 19:00 Uhr startet und drei Stunden ausgeführt wird, dann hat das Drosselungslimit von 19:00 Uhr bis 20:00 Uhr den Wert 500 MB/Minute. Von 20:00 Uhr bis 22:00 Uhr hat das Drosselungslimit den Wert 2.500 MB/Minute.

Wenn Sie keinen Sicherungsablaufplan und keinen Ablaufplan für den Sicherungsdurchsatz angeben, dann wird die Sicherung so schnell wie möglich ausgeführt.

Ablaufplan für Zusammenführung

Ermöglicht es Ihnen, Wiederherstellungspunkte basierend auf dem angegebenen Ablaufplan zusammenzuführen.

Beachten Sie folgende Punkte für den Zusammenführungsjob:

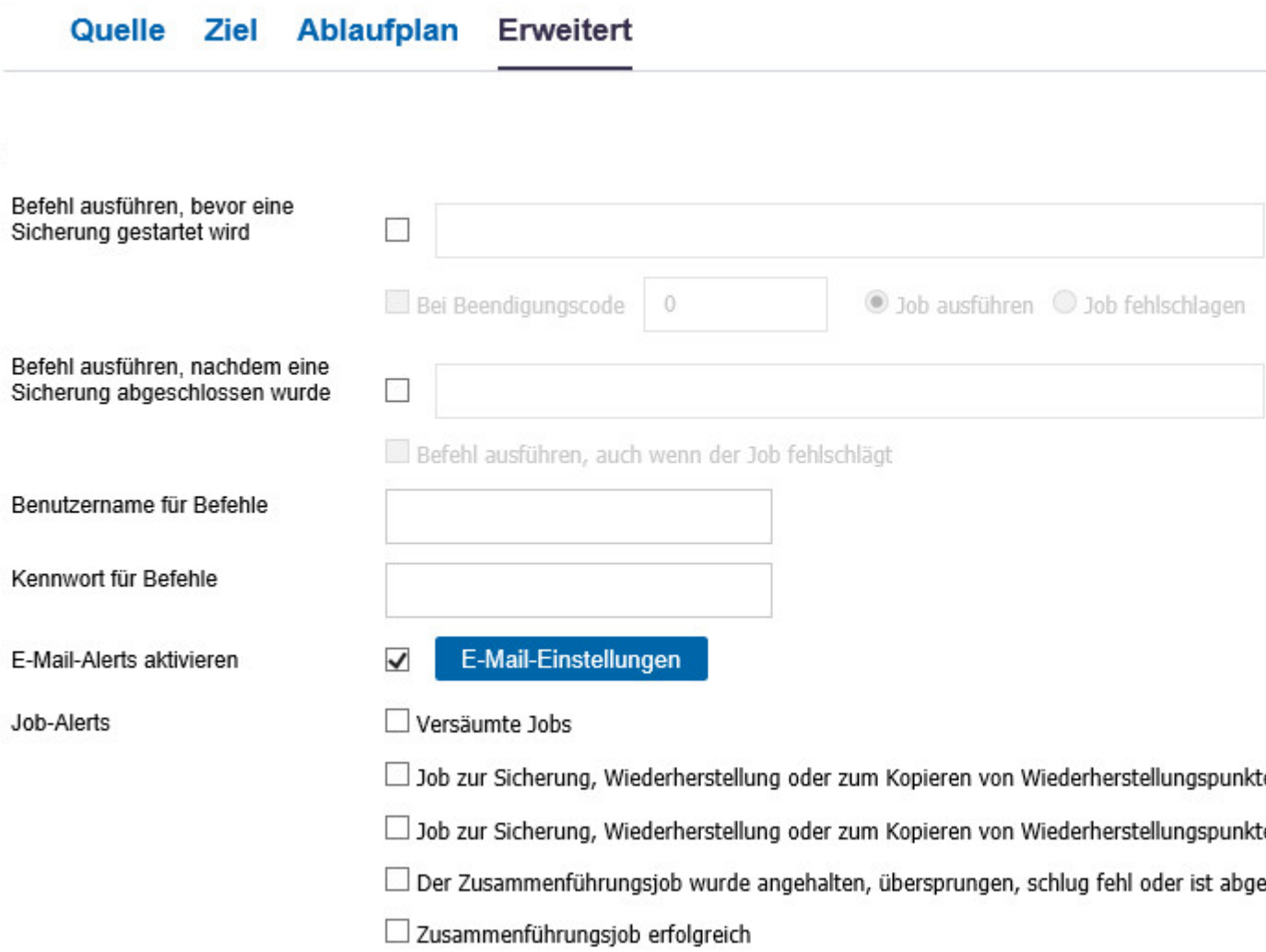
- Es kann immer nur ein Zusammenführungsjob für einen Knoten ausgeführt werden.

- Wenn ein Zusammenführungsjob gestartet wird, muss er abgeschlossen werden, bevor der nächste Zusammenführungsjob gestartet werden kann. Das bedeutet: Wenn ein oder mehrere Sätze an Wiederherstellungspunkten zusammengeführt werden, dann kann der neue Wiederherstellungspunkt nicht zu diesem Zusammenführungsprozess hinzugefügt werden, bis der Zusammenführungsprozess für den aktuellen Satz an Wiederherstellungspunkten abgeschlossen ist.
- Wenn ein Zusammenführungsjob mehr als einen Satz an Wiederherstellungspunkten bearbeitet (zum Beispiel Satz [1~4], Satz [5~11] und Satz [12~14], also drei Sätze), dann werden diese Sätze nacheinander vom Recovery Point Server bearbeitet.
- Wenn ein Zusammenführungsjob nach einer Pause fortgesetzt wird, erkennt der Job an welchem Punkt er unterbrochen wurde, und die Zusammenführung wird ab der Abbruchstelle fortgesetzt.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte **Erweitert**:



Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

   Befehl ausführen, bevor eine Sicherung gestartet wird

   Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, unter dem das Skript auf dem Proxy-Knoten gespeichert ist. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den

Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist.

Befehl ausführen, auch wenn der Job fehlschlägt

Wenn dieses Kontrollkästchen aktiviert ist, wird das unter **Befehl ausführen, nachdem eine Sicherung abgeschlossen ist** angegebene Skript ausgeführt, selbst wenn der Sicherungsjob fehlschlägt. Andernfalls wird das Skript nur dann ausgeführt, wenn der Sicherungsjob erfolgreich abgeschlossen wurde.

Benutzername für Befehle

Ermöglicht die Angabe des Benutzernamens zum Ausführen der Befehle.

Kennwort für Befehle

Ermöglicht die Angabe des Kennworts zum Ausführen der Befehle.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Typen der Warnmeldungen angeben, die Sie in einer E-Mail erhalten möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers. Weitere Informationen zur Konfiguration von E-Mail-Einstellungen finden Sie unter Konfigurieren von E-Mails und Alerts.

Job-Alerts

Ermöglicht es Ihnen, die Arten von Job-Alerts auszuwählen, die Sie per E-Mail empfangen möchten.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Proxy-Knoten installiert und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agent oder kein Agent installiert ist. Um den Agent auf diesen

Knoten zu installieren bzw. um ein Upgrade der Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus und klicken auf **Speichern**.

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie einen andere Task hinzufügen müssen, müssen Sie den Plan auf der Registerkarte **Ressourcen** auswählen und anschließend ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern. Sie können die Tasks **Kopieren von Wiederherstellungspunkten**, **Auf Band kopieren**, **Replizieren** und **Von einem Remote-RPS replizieren** als Folgetasks hinzufügen.

Der Plan wird automatisch auf dem Proxy-Serverknoten bereitgestellt.

Der Exchange Online-Sicherungsplan für den Proxy-Server wird erstellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

(Optional) Ausführen einer manuellen Sicherung

Normalerweise werden Ihre Sicherungen automatisch durchgeführt und von den Ablaufplan-Einstellungen gesteuert. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern. Wenn Sie z. B. einen Wiederholungsplan für vollständige Sicherungen und Zuwachssicherungen festgelegt haben und größere Veränderungen an Ihrem Rechner vornehmen möchten, sollten Sie sofort eine manuelle Sicherung durchführen, ohne auf die nächste geplante Sicherung zu warten.

Führen Sie die folgenden Schritte aus, um Exchange Online-Knoten manuell zu sichern:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Die Exchange Online-Knoten werden im mittleren Fensterbereich angezeigt.
3. Wählen Sie die Exchange Online-Knoten aus, die Sie sichern möchten und denen ein Plan zugewiesen ist (z. B. Mailbox@<organisationsname.com>). Der Knotenname ist das Konto, das verwendet wurde, als der Exchange Online-Knoten hinzugefügt und verbunden wurde.
4. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
5. Wählen Sie den gewünschten Sicherungstyp aus, und klicken Sie dann auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.
6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.
7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Gehen Sie wie folgt vor, um eine manuelle Sicherung des Exchange Online-Plans durchzuführen:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

   Die Exchange Online-Sicherungspläne werden im mittleren Fensterbereich angezeigt.

3. Wählen Sie den Plan aus, den Sie sichern möchten und dem ein Plan zugewiesen ist.
4. Klicken Sie mit der rechten Maustaste auf den Plan, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
5. Wählen Sie den gewünschten Sicherungstyp aus, und klicken Sie dann auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.
6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.
7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Überprüfen der Sicherung

Um Ihre Sicherung zu überprüfen, bestätigen Sie, dass Sie den Sicherungsplan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Sie können den Status von Sicherungsjobs auf der Registerkarte **Jobs** überprüfen.

Gehen Sie wie folgt vor, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Wenden Sie zur Überprüfung von Sicherungsjobs eine der folgenden Methoden an:

Methode 1

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Methode 2

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Jobs erfolgreich abgeschlossen**.

   Die Liste der abgeschlossenen Sicherungsjobs wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf den Job, den Sie überprüfen möchten.

   Der rechte Fensterbereich wird aktualisiert.
4. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
5. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Wiederherstellen von Microsoft Teams-Nachrichten (Chats) mit Exchange Online

Sie können Microsoft Teams-Nachrichten (Chats) mithilfe von Exchange Online aus der Microsoft Cloud auf einem beliebigen Computer wiederherstellen. Sie können Daten von einem Wiederherstellungspunkt am ursprünglichen Speicherort oder an einem alternativen Speicherort wiederherstellen.

Führen Sie die folgenden Aufgaben aus, um Exchange Online-Postfachdaten wiederherzustellen:

1. Auswählen der wiederherzustellenden Exchange Online-Postfachelemente
2. Definieren der Wiederherstellungsoptionen
3. Wiederherstellbare Elemente wiederherstellen
4. Wiederherstellen des Inhalts des Wiederherstellungspunkts
5. Überprüfen, ob der Inhalt wiederhergestellt wurde

Auswählen der wiederherzustellenden Exchange Online-E-Mail-Elemente

Sie können Exchange Online-E-Mail-Daten von einem Wiederherstellungspunkt aus wiederherstellen. Wenn Sie ein Wiederherstellungsdatum auswählen und dann die Uhrzeit angeben, werden alle zugeordneten Wiederherstellungspunkte für diesen Zeitraum angezeigt. Sie können die Inhalte (einschließlich Anwendungen) für die Wiederherstellung suchen und auswählen.

Gehen Sie wie folgt vor:

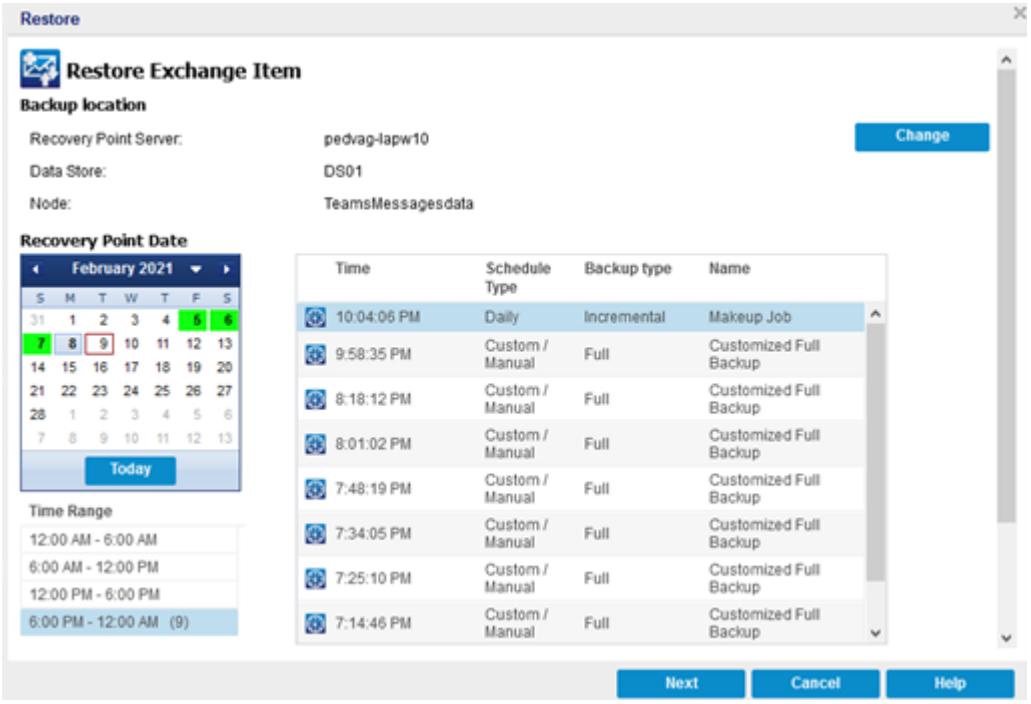
1. Melden Sie sich bei Arcserve UDP an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

   Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.
4. Wählen Sie im mittleren Fensterbereich den Exchange Online-Knoten aus, und klicken Sie dann auf **Aktionen**.
5. Klicken Sie in der Drop-down-Liste **Aktionen** auf Wiederherstellen.

   Das Dialogfeld Exchange-Element wiederherstellen wird geöffnet.

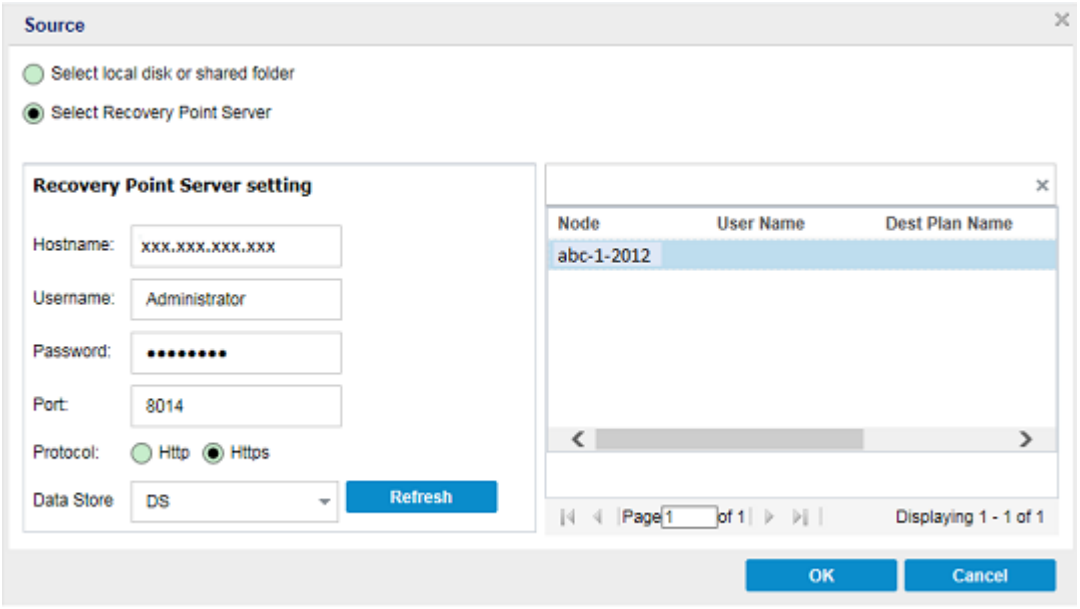
   Hinweis: Sie werden automatisch in den Agent-Knoten eingeloggt und das Dialogfeld **Exchange-Element wiederherstellen** wird geöffnet.

   Die Details zum Recovery Point Server werden im Sicherungsspeicherort angezeigt.



6. (Optional) Klicken Sie auf **Ändern**, um den Speicherort für die Sicherung zu ändern.

   Das Dialogfeld Quelle wird geöffnet. Sie können den Sicherungsspeicherort in diesem Dialogfeld auswählen.



Hinweis: Wenn Sie dem Plan einen Task "Kopie auf Band" hinzufügen und nun den Wiederherstellungspunkt "Kopie auf Band" wiederherstellen möchten, wählen Sie den Wiederherstellungspunkt aus der Sicherung auf Kopie auf Band aus. Weitere Informationen finden Sie unter Durchsuchen der Kopie auf Band nach Wiederherstellungspunkten.

7. Um die Quelle anzugeben, wählen Sie eine der folgenden Optionen aus, und klicken Sie dann auf **OK**.

   Lokalen Datenträger oder freigegebenen Ordner auswählen

   Hinweis: In Arcserve UDP wird die Auswahl der Option **Lokalen Datenträger oder freigegebenen Ordner auswählen** nicht empfohlen.

   Recovery Point Server auswählen

   a. Geben Sie die Details für die Einstellungen des Recovery Point Servers an, und klicken Sie dann auf **Aktualisieren**.

      Alle Agenten werden in der Spalte "Data Protection Agent" im Dialogfeld Quelle aufgelistet.

   b. Wählen Sie den Agenten in der angezeigten Liste aus, und klicken Sie auf **OK**.

      Die Wiederherstellungspunkte werden im Dialogfeld Exchange-Element wiederherstellen aufgelistet.

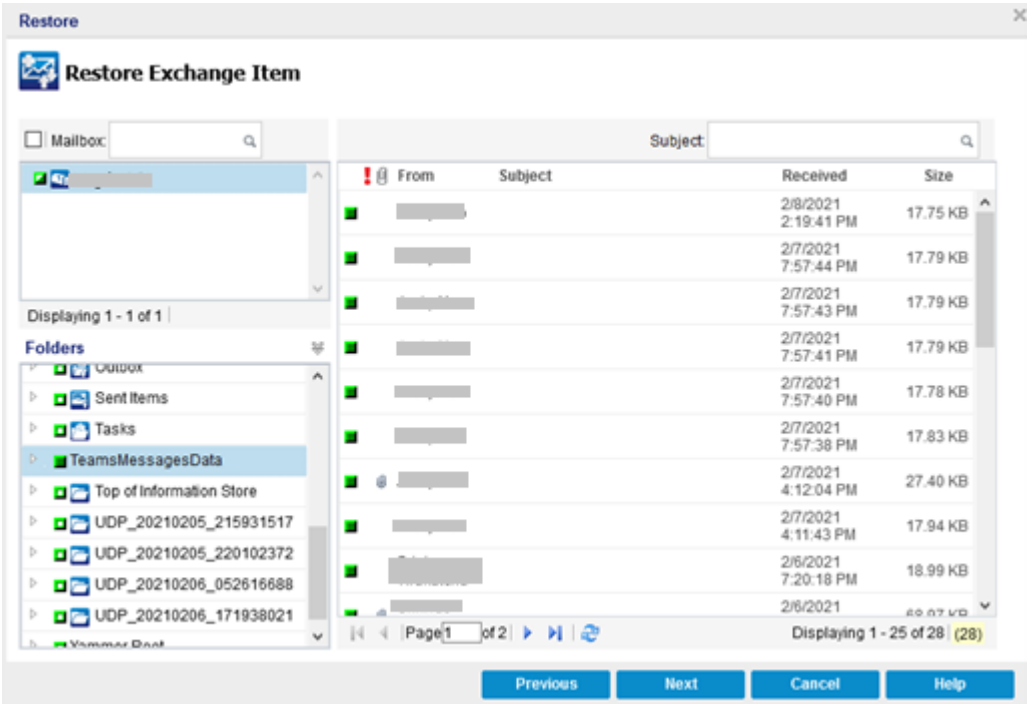
      Hinweis: Vom Wiederherstellungspunkt **Ordner** aus sehen Sie möglicherweise viele Ordner mit demselben Namen zusammen mit den Exchange Online-Knoten. Dies geschieht, weil die Knoten-GUID geändert wird und ein neuer Wiederherstellungspunkt-Ordner erstellt wird, wenn Sie einen Knoten löschen und wieder zum Prüfplan hinzufügen.

8. Wählen Sie das Kalenderdatum des wiederherzustellenden Sicherungs-Images aus, und klicken Sie dann auf **Weiter**.

   Alle Daten, die Wiederherstellungspunkte für die angegebene Sicherungsquelle enthalten, werden grün hervorgehoben.

   Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp (vollständige Sicherung, Zuwachssicherung oder Überprüfungssicherung) und der Name der Sicherung angezeigt.

9. Wählen Sie im Fenster **Postfach** das Postfach aus, das Sie wiederherstellen möchten.



Alle E-Mail-Elemente in Verbindung mit dem Postfach werden im Fensterbereich Ordner angezeigt.

10. Wählen Sie den Ordner **TeamsMessagesData** aus, und klicken Sie dann auf **Weiter**.

    Hinweise:

    - Sie können den gesamten Inhalt oder Teile des Inhalts des wiederherzustellenden Exchange-Objekts auswählen. Um Teile des Inhalts auszuwählen, erweitern Sie das Objekt, und klicken Sie auf das Kontrollkästchen des Inhalts.
    - Sie können mehrere wiederherzustellende Exchange-Objekte auswählen.

    Das Dialogfeld Wiederherstellungsoptionen wird geöffnet.

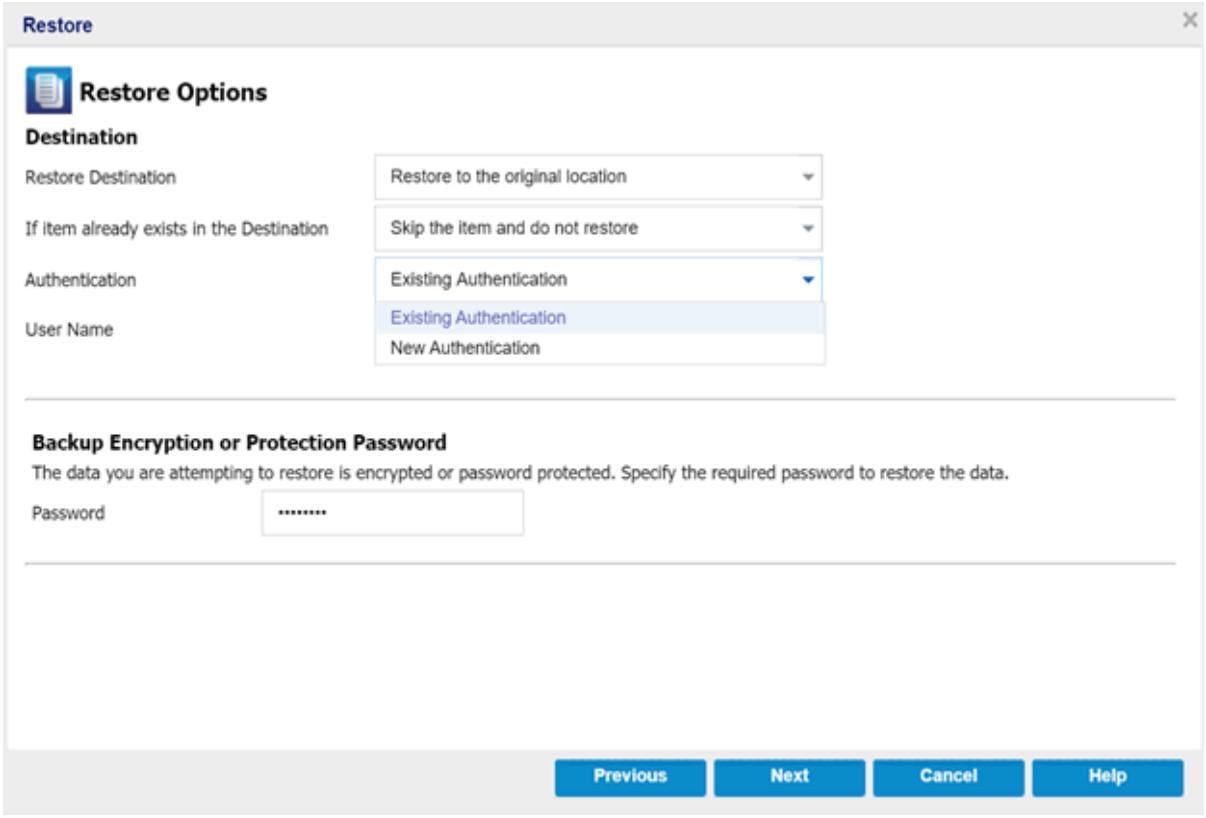
    Die Exchange Online-E-Mail-Elemente, die wiederhergestellt werden sollen, sind ausgewählt. Nun können Sie die Wiederherstellungsoptionen definieren.

Definieren der Wiederherstellungsoptionen

Nachdem Sie die wiederherzustellenden Exchange Online-Informationen angegeben haben, legen Sie die Wiederherstellungsoptionen für die ausgewählten Inhalte fest.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld Wiederherstellungsoptionen das Wiederherstellungsziel aus.



Es sind folgende Zieloptionen verfügbar:

Am ursprünglichen Speicherort wiederherstellen

Stellt die E-Mail-Daten am selben Speicherort wieder her, an dem Sie eine Sicherung ausgeführt haben.

Hinweise:

- Wenn Sie am ursprünglichen Speicherort wiederherstellen, werden die Daten nicht in die Teams-Nachrichten übernommen. Dies ist keine vollständige Wiederherstellung am ursprünglichen Speicherort, da den Stammordner nicht wiederherstellen können.

- Wenn Sie ein E-Mail-Element am ursprünglichen Speicherort unter Verwendung der Überschreibungsoption zweimal wiederherstellen, wird nach der zweiten Wiederherstellung das erste wiederhergestellte E-Mail-Element nicht überschrieben. Dadurch werden die zwei ähnliche E-Mail-Objekte am ursprünglichen Speicherort angezeigt.
- Wenn Sie E-Mail-Nachrichten am ursprünglichen Speicherort mit der Option "Überspringen" wiederherstellen, und im ursprünglichen Ordner bereits ein Element vorhanden ist, das dem wiederhergestellten ähnelt, zeigt der Sicherungsjob das Ergebnis "Unvollständig" an.

An einem anderen Speicherort wiederherstellen

Stellt die E-Mail-Daten in einem anderen Postfach oder einem anderen Ordner im ursprüngliche Postfach wieder her. Wenn Sie diese Option auswählen, können Sie das Ziel auswählen.

2. Geben Sie eine der folgenden Optionen aus der Drop-down-Liste **Wenn das Element auf dem Ziel bereits vorhanden ist** an:

Objekt überspringen und nicht wiederherstellen

Elemente werden übersprungen und nicht wiederhergestellt.

Standard: Elemente werden übersprungen und nicht wiederhergestellt.

Das Element im Ziel überschreiben

Das Element im Ziel wird überschrieben.

Hinweis: Die Drop-down-Liste Wenn das Element auf dem Ziel bereits vorhanden ist verfügbar, wenn Sie die Option **Am ursprünglichen Speicherort wiederherstellen** in der Drop-down-Liste Wiederherstellungsziel auswählen.

Authentifizierung

Validiert und identifiziert das Benutzerkonto. Wählen Sie eine der folgenden Optionen:

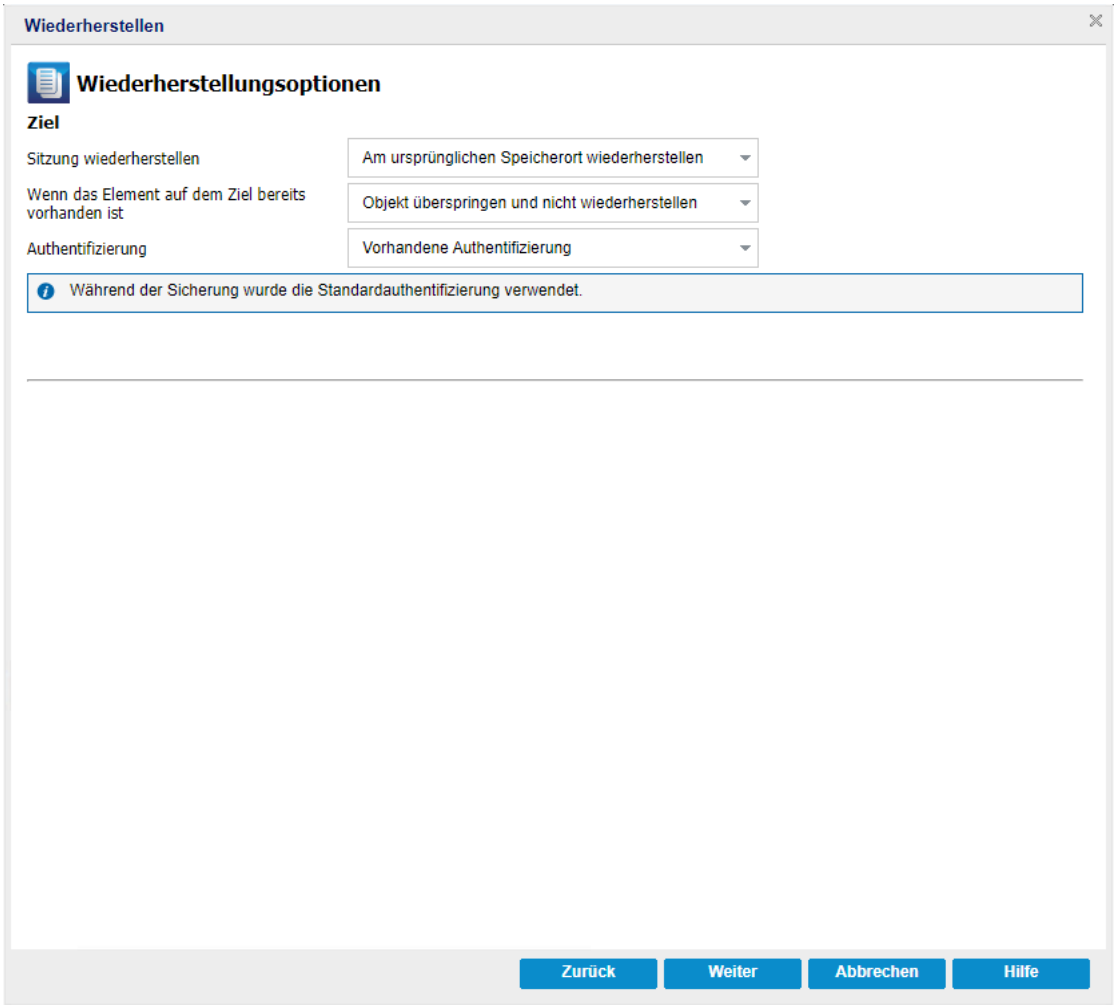
- **Vorhandene Authentifizierung**

  Wenn Sie "Vorhandene Authentifizierung" auswählen, wird der Authentifizierungstyp verwendet, der während der Knotenerstellung ausgewählt wurde.

  - Wenn es sich bei der Knotenauthentifizierung um die Standardauthentifizierung handelt, werden Parameter wie Benutzername, Kennwort und Sicherungsverschlüsselung oder

Schutzkennwort [falls verschlüsselt] automatisch geladen, um mit der Wiederherstellung fortzufahren.

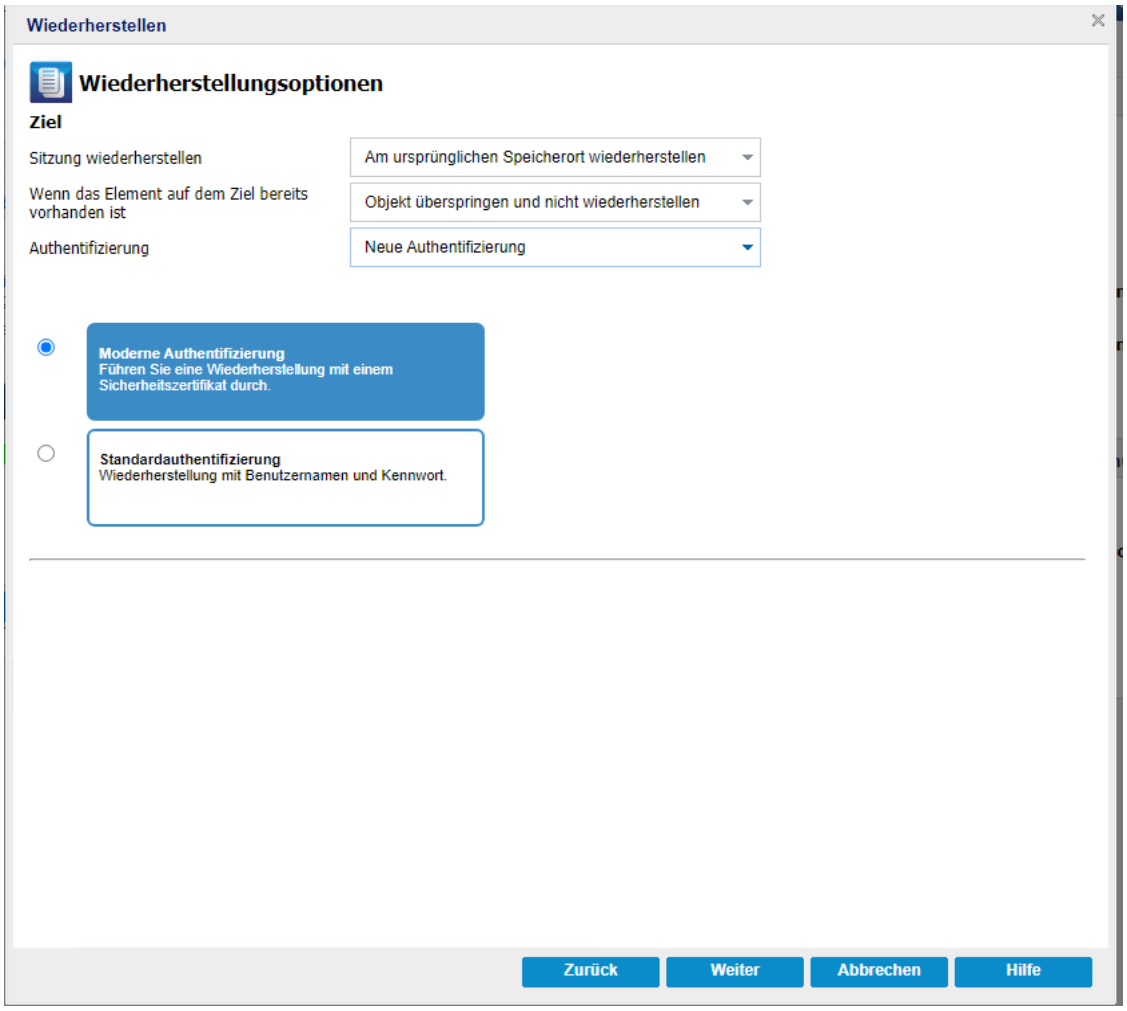
- Wenn es sich bei der Knotenauthentifizierung um die moderne Authentifizierung handelt, werden Parameter wie Benutzername und Sicherungsverschlüsselung oder Schutzkennwort [falls verschlüsselt] automatisch geladen, um mit der Wiederherstellung fortzufahren.



- **Neue Authentifizierung**

  Während der Wiederherstellung können Sie eine der folgenden Optionen auswählen, um den Authentifizierungstyp zu ändern:

  - Moderne Authentifizierung
  - Standardauthentifizierung



3. Gehen Sie folgendermaßen vor, um die Authentifizierung anzuwenden:

   Moderne Authentifizierung

   Bei der modernen Authentifizierung können Sie eine Wiederherstellung mithilfe eines Sicherheitszertifikats ausführen.

   Sicherheitszertifikat verwenden

   Hinweis: Standardmäßig wählt der Sicherungsplan die Option **Sicherheitszertifikat verwenden** für die moderne Authentifizierung aus.

   Gehen Sie wie folgt vor:

   a. Informationen zur Authentifizierung mithilfe eines selbstsignierten Zertifikats finden Sie unter Herunterladen des Zertifikats von UDP und Hochladen in Azure

   b. Geben Sie die Anwendungs-ID und den Benutzernamen ein.

c. Um die erforderlichen Rollen und Berechtigungen anzuwenden, aktivieren Sie das Kontrollkästchen **Ermöglichen Sie Arcserve UDP, die erforderlichen Azure-Rollen und -Berechtigungen für diese Anwendung festzulegen**, und klicken Sie dann auf **Weiter**.

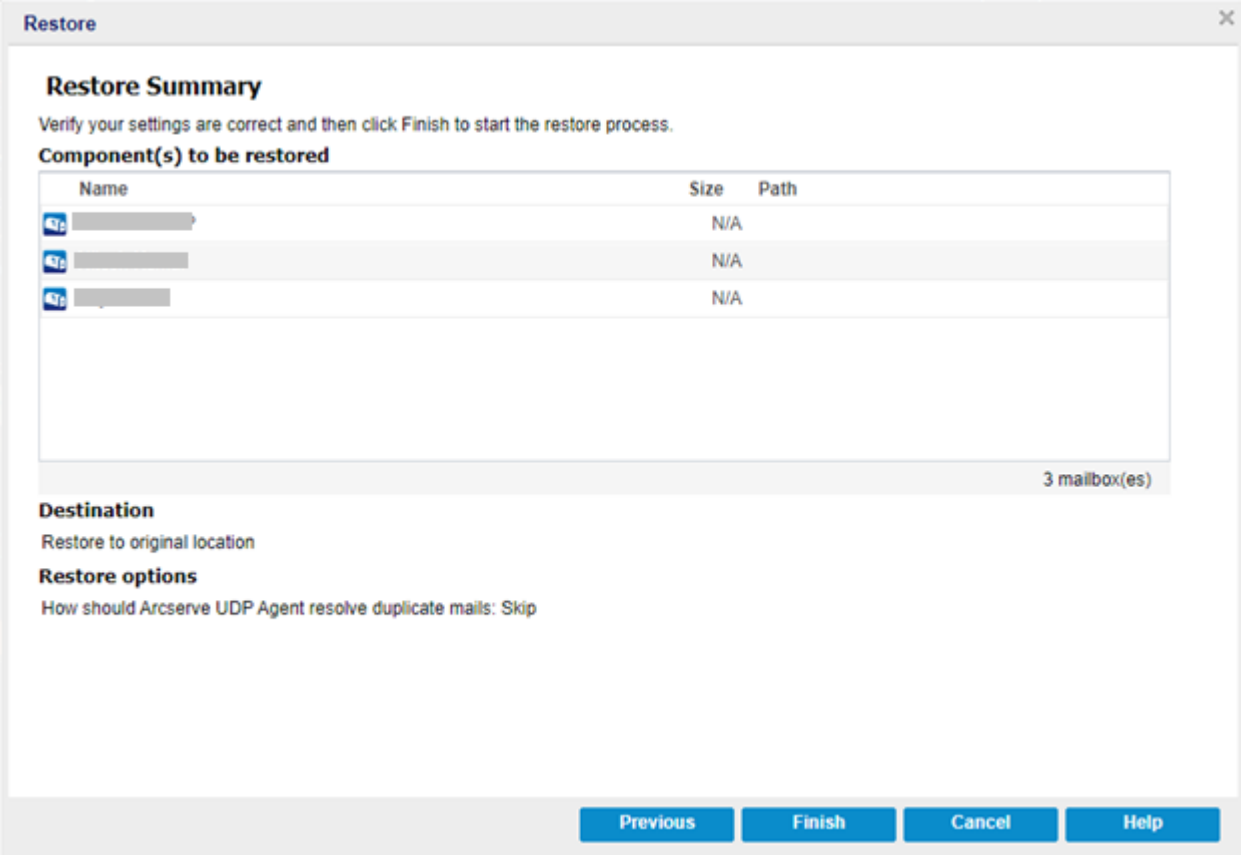
Standardauthentifizierung

Um bei Verwendung der Standardauthentifizierung mit der Wiederherstellung fortzufahren, geben Sie Benutzername und Kennwort ein.

Hinweis: Diese Option schlägt fehl, wenn Sie die moderne Authentifizierung für den Mandanten oder das Konto aktiviert haben.

4. Klicken Sie auf **Weiter**.

   Das Dialogfeld Wiederherstellungsübersicht wird geöffnet.



5. Überprüfen Sie die Einstellungen im Fenster "Wiederherstellungs-Übersicht", und klicken Sie dann auf **Fertig stellen**.

Die Wiederherstellungsoptionen für die Wiederherstellung von Exchange Online-Informationen sind festgelegt.

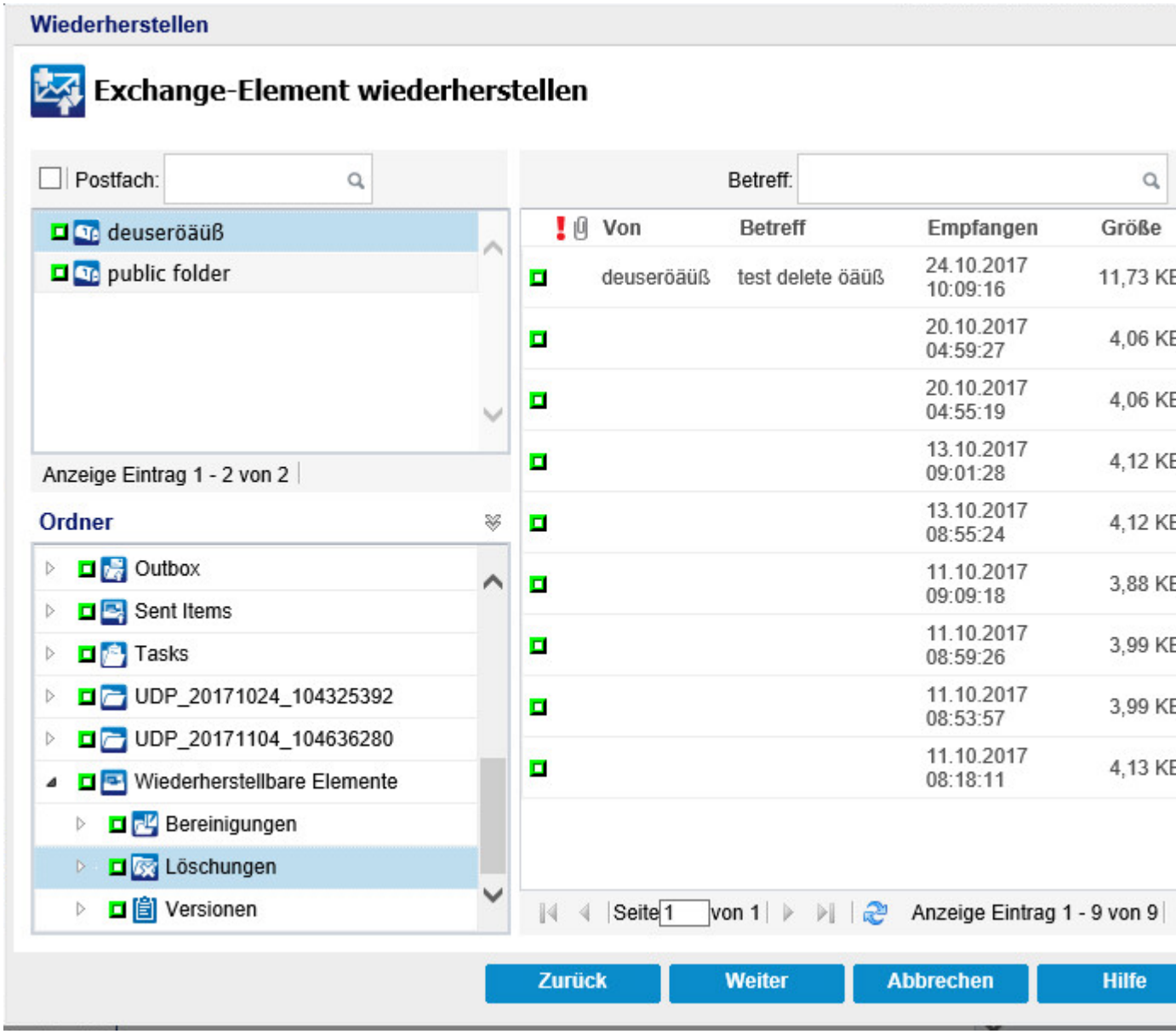
Wiederherstellbare Elemente wiederherstellen

Sie können wiederherstellbare Elemente aus dem Postfach wiederherstellen, das die In-Place-Hold- und Litigation-Hold-Funktion ermöglicht – vom Exchange Online-Knoten-UI bis zum Durchsuchen einer Backup-Sitzung. Informationen zur Aktivierung dieser Funktion finden Sie unter Angeben der Quelle.

Nachdem Sie die Funktion aktiviert haben, können Sie mit dem Wiederherstellungsassistenten wiederherstellbare Elemente wiederherstellen.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld Exchange-Element wiederherstellen die erforderlichen Ordner unter **Wiederherstellbare Elemente** aus, und klicken Sie anschließend auf **Weiter**.



Der Bildschirm "Wiederherstellungsoption" wird angezeigt.

2. Führen Sie im Bildschirm "Wiederherstellungsoption" die folgenden Schritte aus, und klicken Sie dann auf **Weiter**:

   - Wählen Sie ein Ziel für die Wiederherstellung aus.
   - Überspringen oder überschrieben Sie, wenn das Element bereits im Ziel vorhanden ist.

     Sie können eine originale oder alternative Wiederherstellung durchführen.

     Originale Wiederherstellung

     Die Elemente unter „Wiederherstellbare Elemente“ werden im Ordner *UDP_RecoverableItems_yyyyMMdd_HHmmssfff* wiederhergestellt, der

im Zielpostfach erstellt wird. Die Wiederherstellungsoptionen „Überspringen“ und „Überschreiben“ sind nicht für diese Elemente anwendbar.

Alternative Wiederherstellung

Bei einem Benutzerpostfach werden ausgewählte Elemente in einem Zielverzeichnis mit einem Ordner mit einzigartigem Zeitstempel wiederhergestellt, beispielsweise mit dem Namen */restore_yyyyMMdd-mmssff*.

- Geben Sie die Benutzer-ID und das Passwort des Ziels an, in dem Sie die Wiederherstellung durchführen möchten.

Die ausgewählten wiederherstellbaren Elemente werden wiederhergestellt.

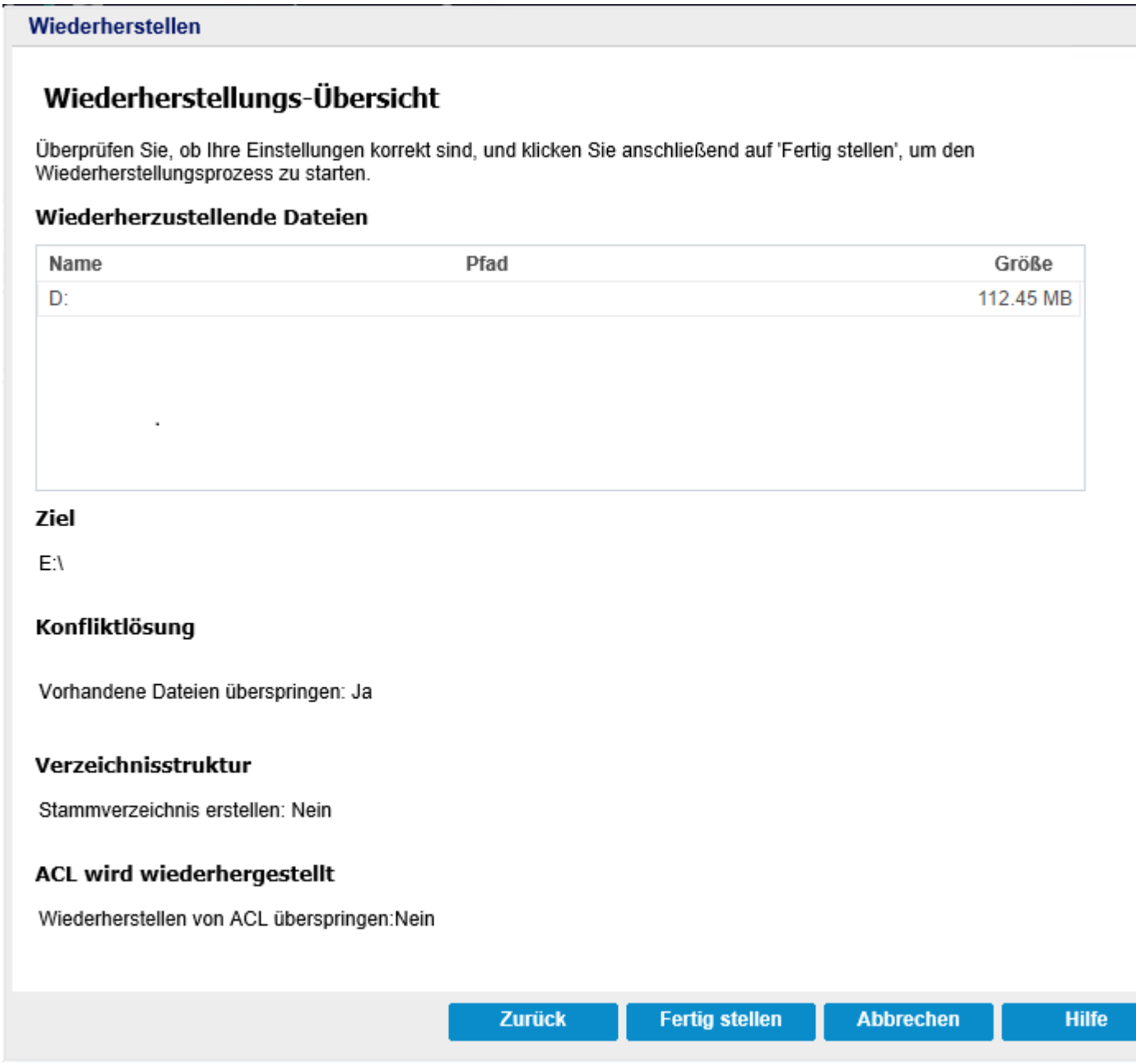
Der Wiederherstellungspunktinhalt wird wiederhergestellt.

Wiederherstellen des Inhalts des Wiederherstellungspunkts

Nachdem Sie die Wiederherstellungsoptionen definiert haben, überprüfen Sie, dass Ihre Einstellungen korrekt sind, und bestätigen Sie den Wiederherstellungsprozess. Die **Wiederherstellungsübersicht** ist hilfreich, um sämtliche Wiederherstellungsoptionen, die Sie festgelegt haben, zu überprüfen und bei Bedarf zu ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Informationen im Dialogfeld Wiederherstellungsübersicht, um die Richtigkeit aller Wiederherstellungsoptionen und Einstellungen sicherzustellen.



- Wenn die Übersichtsinformationen Fehler enthalten, klicken Sie auf **Zurück**, und ändern Sie die inkorrekten Einstellungen im entsprechenden Dialogfeld.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsjob zu starten.

Der Wiederherstellungspunktinhalt wird wiederhergestellt.

Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen Sie nach dem Abschluss der Wiederherstellung, dass der Inhalt auf dem angegebenen Ziel wiederhergestellt wurde.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Zielpostfach an.
2. Überprüfen Sie das Postfachelement, das Sie wiederhergestellt haben.
3. Überprüfen die wiederhergestellten Inhalte.

   Der wiederhergestellte Inhalt wurde erfolgreich überprüft.

Sichern und Wiederherstellen von Microsoft Teams-Dateien mit SharePoint Online

Jedes Mal, wenn Sie einen privaten oder öffentlichen Kanal oder einen Gruppenkanal in Microsoft Teams erstellen, wird automatisch eine SharePoint Online-Website für den Kanal erstellt. Diese SharePoint Online-Website verfügt über einen Standardordner für Dokumentbibliotheken, in dem alle in Unterhaltungen freigegebenen Dateien automatisch gespeichert werden. Sie können auch die Berechtigungen und Sicherheitsoptionen für vertrauliche Informationen anpassen.

Wenn Sie eine Gruppe in Microsoft Teams erstellen, wird automatisch eine SharePoint Online-Website mit dem Namen **Team - Name_der_Gruppe** erstellt. Alle in den öffentlichen Kanälen freigegebenen Dateien werden auf dieser Website gespeichert.

Wenn Sie einen privaten Kanal unter der Microsoft Teams-Gruppe erstellen, wird neben der für die Teamgruppe erstellten Website eine weitere SharePoint Online-Website mit dem Namen **Name_der_Teams-Gruppe - Name_des_privaten_Kanals** erstellt.

Dieser Abschnitt enthält Informationen zum Sichern und Wiederherstellen von Microsoft Teams-Dateien mit SharePoint Online.

In diesem Abschnitt werden die folgenden Themen behandelt:

Sichern von Microsoft Teams-Dateien mit SharePoint Online

Dieser Abschnitt enthält Informationen zum Sichern von Microsoft Teams-Dateien mit SharePoint Online.

In diesem Abschnitt werden die folgenden Themen behandelt:

So erstellen Sie einen SharePoint Online-Sicherungsplan

Der SharePoint-Schutz wird verwendet, um Microsoft SharePoint Online-Websites und -Listenelemente zu sichern und wiederherzustellen. SharePoint Online ist eines der wichtigsten Produkte in Microsoft Office 365. Um Ihre SharePoint-Inhalte zu schützen, müssen Sie einen Plan erstellen.

In diesem Abschnitt werden die folgenden Themen behandelt:

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie einen SharePoint Online-Sicherungsplan erstellen.

Erstellen eines SharePoint Online-Sicherungsplans:

Voraussetzungen:

Das Sicherungskonto ist ein Mitglied der Gruppen „Administratoren der Websitesammlung“ oder mit der Rolle *SharePoint-Administrator* zugewiesen.

Um ein Konto zur Gruppe "Administratoren der Websitesammlung" hinzuzufügen, verwenden Sie diesen Link.

Erstellen eines SharePoint Online-Sicherungsplans mit Basisauthentifizierung (BA):

Überprüfen Sie die folgenden Voraussetzungen:

- Installieren Sie die PowerShell Version 5.1 oder höher (Teil des Windows Management Framework (WMF)) auf dem Proxy-Server (64-Bit-Computer).
- Installieren Sie mithilfe der Befehlszeile die folgenden PowerShell-Module auf dem Proxy-Server unter Verwendung des PowerShell-Fensters:
  - Führen Sie den folgenden Befehl aus, um das Azure-Modul zu installieren:

    Installationsmodul -Name AzureAD -Force
  - Führen Sie den folgenden Befehl aus, um das ExchangeOnlineManagement-Modul zu installieren:

    Installationsmodul -Name ExchangeOnlineManagement -Force

  Hinweis: Wenn Sie PowerShell-Module mithilfe der oben genannten Befehle installieren, wird basierend auf der GA-Version der im Microsoft-Repository verfügbaren Komponente möglicherweise eine neuere Version der Module installiert.

Erstellen eines SharePoint Online-Sicherungsplans mithilfe der modernen Authentifizierung (MA):

Überprüfen Sie die Voraussetzungen, bevor Sie einen Plan unter Verwendung der modernen Authentifizierung erstellen.

Erstellen eines SharePoint Online-Sicherungsplans

Ein Sicherungsplan enthält einen Task **Sicherung: Office 365 SharePoint Online**, der eine Sicherung von SharePoint Online-Elementen (Listen, Bibliotheken, Dokumente usw.) durchführt und Daten in einem Datenspeicher mit oder ohne Deduplizierung speichert. Außerdem ermöglicht dieser Sicherungsplan es UDP, SharePoint Online-Elemente zu erkennen und anzugeben, für die ein Sicherungstask ausgeführt wird. Jeder Task besteht aus Parametern, die Quelle, Ziel, Ablaufplan und weitere Sicherungsdetails definieren.

Gehen Sie wie folgt vor:

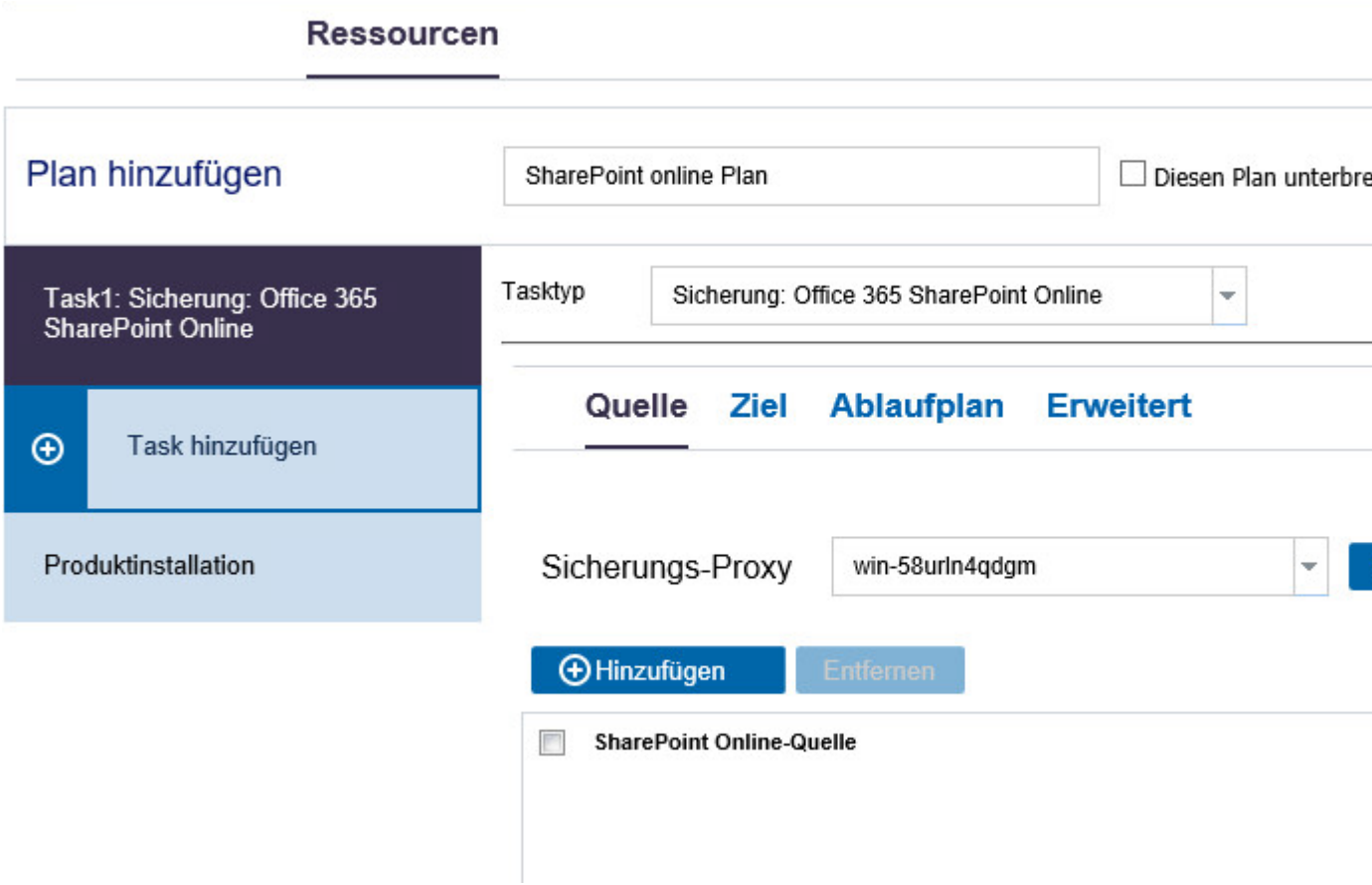
1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie dann auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Das Dialogfenster Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Drop-down-Liste Tasktyp die Option **Sicherung: Office 365 SharePoint Online** aus.



Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die SharePoint Online-Quellknoten angeben, die Sie schützen möchten. Sie können für einen Plan mehrere SharePoint Online-Quellknoten auswählen.

Hinweis: Sie können einen Plan speichern, ohne Quellknoten hinzuzufügen. Der Plan wird jedoch nur bereitgestellt, wenn Sie einen Knoten hinzufügen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Quelle**.
2. Wählen Sie in der Drop-down-Liste **Sicherungs-Proxy** den Server aus.
3. Fügen Sie mithilfe einer der folgenden Methoden einen SharePoint Online-Knoten hinzu:

   Methode 1:

   a. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Wählen Sie zu sichernde Quellen in Arcserve UDP aus**.

      Das Dialogfeld Knoten zu Plan hinzufügen wird angezeigt.

      Hinweis: Verwenden Sie diese Option nur, wenn Sie bereits zuvor einen SharePoint-Knoten hinzugefügt haben.

   b. Wählen Sie einen Knoten aus, und klicken Sie dann auf **Verbinden**.

      Hinweis: Um die SharePoint Online-Knoten zu suchen, die Sie schützen möchten, verwenden Sie **Suchen**.

   Methode 2:

   - Klicken Sie auf **Hinzufügen** und dann auf **SharePoint Online-Quelle hinzufügen**.

     Das Dialogfeld "Knoten zu Plan hinzufügen" wird geöffnet.

     Hinweis:

     - Verwenden Sie diese Option, um Online-Elemente für die SharePoint Online-Quelle zu erkennen und anzugeben.
     - Anders als andere Knoten können Sie den SharePoint Online-Knoten nicht über die Seite "Alle Knoten" hinzufügen. Sie können einen SharePoint Online-Knoten nur beim Erstellen oder Ändern eines Plans in einem Plan hinzufügen.
4. Gehen Sie folgendermaßen vor, um die Authentifizierung anzuwenden:

Moderne Authentifizierung

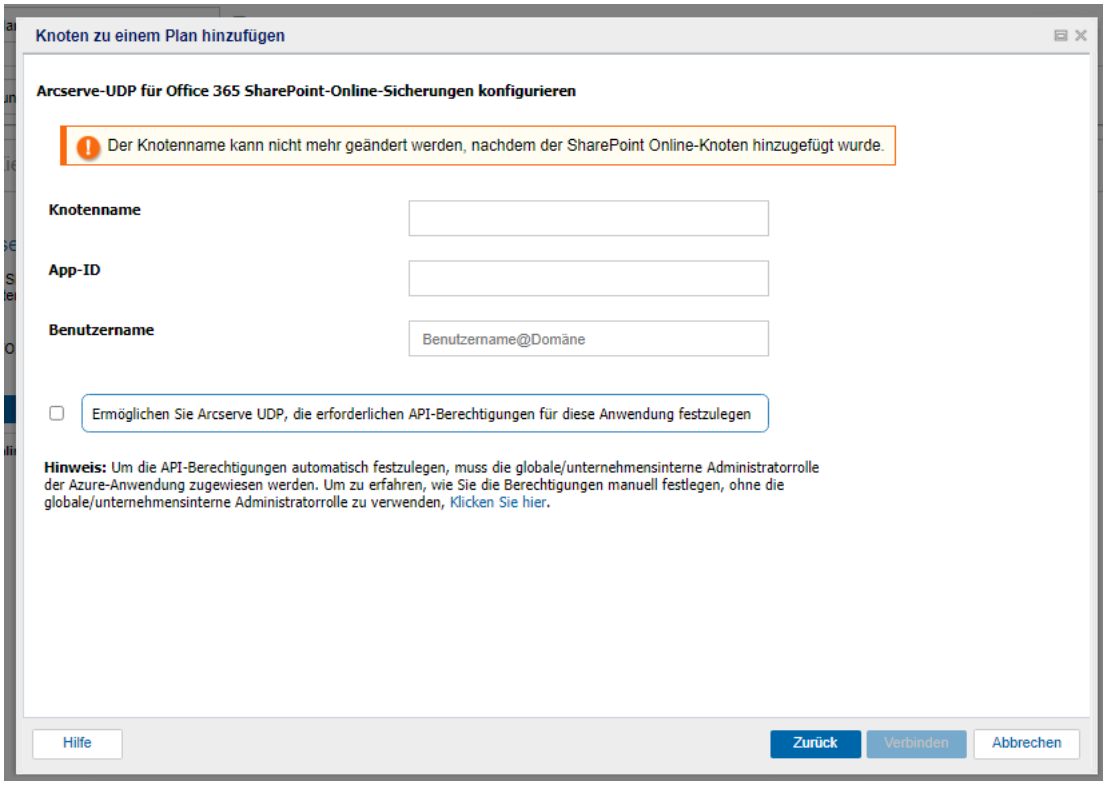
Bei der modernen Authentifizierung können Sie eine Sicherung mithilfe eines Sicherheitszertifikats ausführen.

Sicherheitszertifikat verwenden

Hinweis: Standardmäßig wählt der Sicherungsplan die Option **Sicherheitszertifikat verwenden** für die moderne Authentifizierung aus.

Gehen Sie wie folgt vor:

1. Informationen zum Authentifizieren der UDP-Anwendung mit Sicherheitszertifikaten finden Sie unter Herunterladen des Zertifikats von UDP und Hochladen in Azure.
2. Geben Sie die folgenden Details ein:
   - Knotenname
   - App-ID
   - Benutzername



c. Um die API-Berechtigungen automatisch anzuwenden, aktivieren Sie das Kontrollkästchen **Arcserve UDP erlauben, die erforderlichen API-Berechtigungen für diese Anwendung festzulegen**.

Hinweis: Informationen zum manuellen Anwenden der Berechtigungen ohne Verwendung der Administratorrolle "Global/Company" finden Sie unter Manuelles Konfigurieren der API-Berechtigungen ohne Verwendung der Administratorrolle "Global/Company".

d. Klicken Sie auf **Connect**.

Hinweise:

- Namen von SharePoint Online-Quellknoten können nach dem Erstellen des Knotens nicht mehr geändert werden.
- Sie können ein einzelnes Konto verwenden, um mehrere SharePoint Online-Knoten zu schützen.
- Füllen Sie das App-Kennwort aus, wenn die Multifaktor-Authentifizierung aktiviert ist und der Mandant so eingestellt ist, dass er die Standardauthentifizierung verwendet.

Standardauthentifizierung

Um bei Verwendung der Standardauthentifizierung mit der Sicherung fortzufahren, geben Sie die folgenden Informationen an, und klicken Sie dann auf **Verbinden**:

- Knotenname
- Websitesammlungs-URL
- Benutzer-ID
- Kennwort

5. Gehen Sie zum Schützen von SharePoint Online-Elementen wie folgt vor:
   - Wählen Sie in der Drop-down-Liste "Site-Typen" den Site-Typ aus, den Sie schützen möchten, z. B. "SharePoint-Websites" oder "Persönliche Sites".
   - Führen Sie unter "Alle Websites/Unterwebsites schützen" die folgenden Schritte aus:

     Hinweise:

     - Bei Anzeige des Bildschirms "SharePoint Online-Inhalte auswählen" ist diese Option standardmäßig automatisch ausgewählt.
       - Um alle Elemente im ausgewählten Site-Typ zu schützen, aktivieren Sie das Kontrollkästchen **Alle**

Websites/Unterwebsites schützen.

- Um bestimmte Elemente im ausgewählten Site-Typ zu schützen, deaktivieren Sie das Kontrollkästchen **Alle Websites/Unterwebsites schützen**, und wählen Sie dann die spezifischen Elemente aus, die Sie schützen möchten.

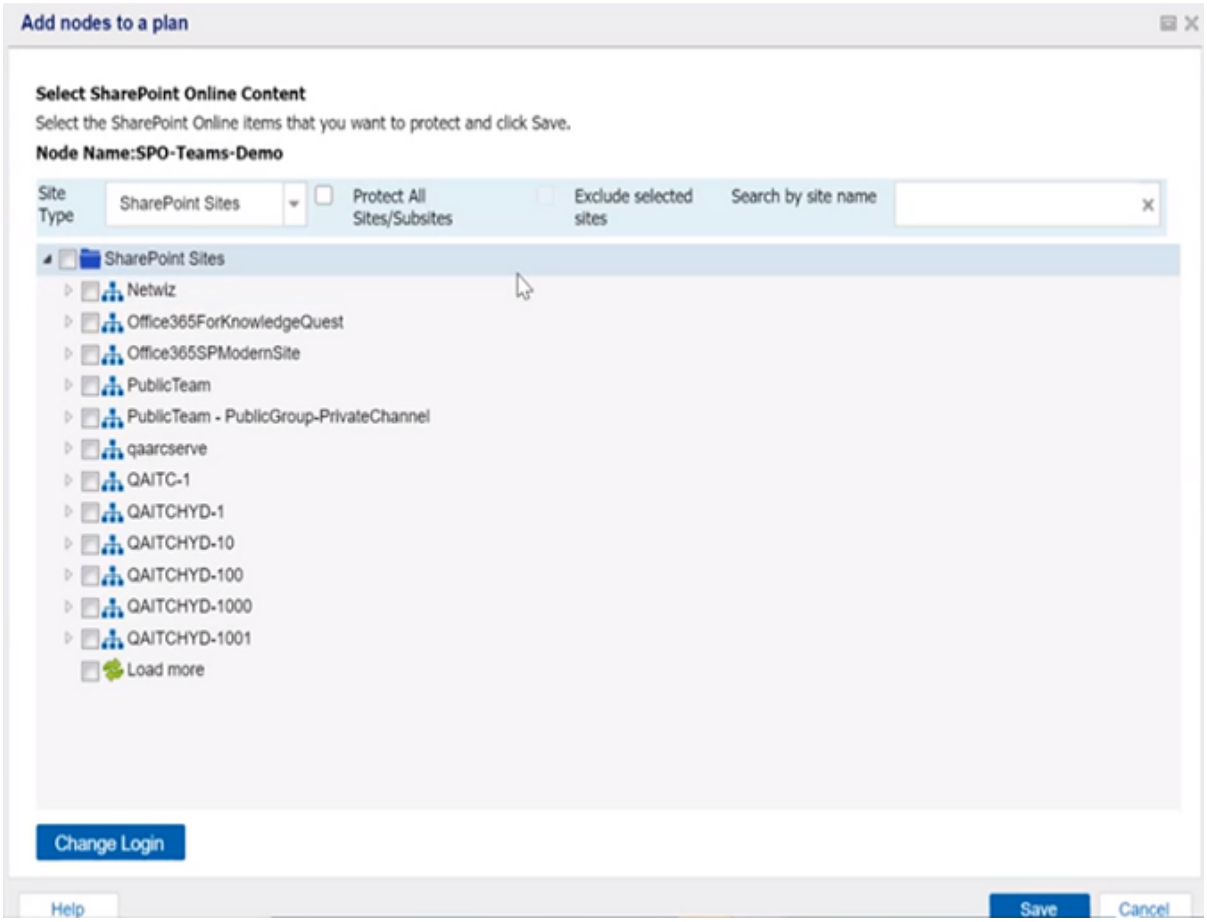
- Wenn Sie beim Konfigurieren des vorhandenen SharePoint Online-Plans Sites manuell zum Schutz ausgewählt haben und nun das Kontrollkästchen **Alle Sites/untergeordneten Sites schützen** möchten, gehen Sie folgendermaßen vor:

  a. Ändern Sie den vorhandenen SharePoint Online-Plan.

  b. Löschen Sie die SharePoint-Websites, die manuell zum Schutz ausgewählt wurden.

  c. Aktivieren Sie das Kontrollkästchen **Alle Standorte/untergeordneten Standorte schützen**, und speichern Sie den Plan.

- Um bestimmte Elemente nicht zu schützen, aktivieren Sie das Kontrollkästchen **Ausgewählte Websites ausschließen**, und wählen Sie dann spezifische Elemente im ausgewählten Site-Typ aus.



6. Klicken Sie auf **Speichern**.

   Die SharePoint Online-Quellen, die Sie schützen möchten, werden zum Plan hinzugefügt.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ziel**.

   Die Option "Arcserve UDP-Recovery Point Server" gibt an, dass das Sicherungsziel ein Recovery Point Server ist.

   Sie können Daten nicht als Wiederherstellungssätze speichern.

2. Führen Sie die folgenden Schritte aus:

   a. Wählen Sie einen Recovery Point Server aus.

   b. Wählen Sie einen für Deduplizierung bzw. nicht für Deduplizierung aktivierten Datenspeicher.

      Die Liste zeigt alle auf dem angegebenen Recovery Point-Server erstellten Datenspeicher an.

   c. Geben Sie ein Sitzungskennwort ein.

      Das Sitzungskennwort ist optional, wenn das Sicherungsziel ein unverschlüsselter RPS-Datenspeicher ist.

   d. Bestätigen Sie das Sitzungskennwort.

   Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Hinweis: Weitere Informationen zu Einstellungen für Ablaufpläne und Aufbewahrungszeiten finden Sie unter Funktionsweise der erweiterten Planung und Aufbewahrung.

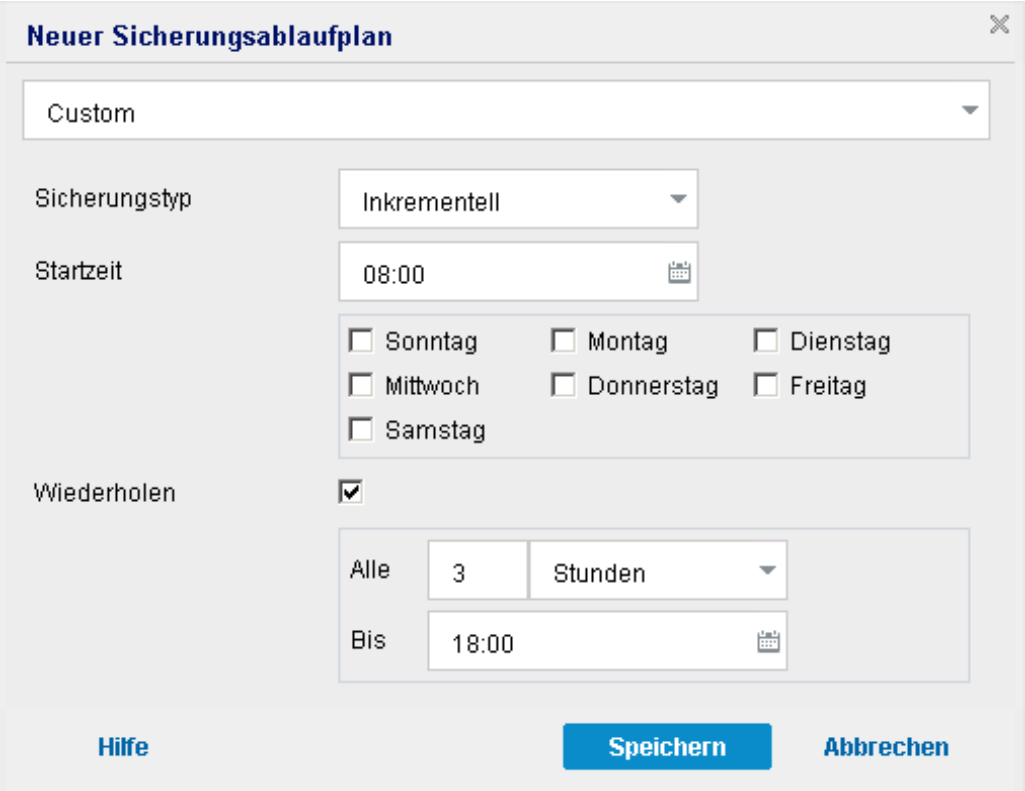
Gehen Sie wie folgt vor:

1. Fügen Sie Ablaufpläne für Sicherungen, Zusammenführungen und Drosselungsvorgänge hinzu.

   Hinzufügen eines Sicherungsablaufplans

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Sicherungsablaufplan hinzufügen** aus.

      Das Dialogfeld **Neuer Sicherungsablaufplan** wird geöffnet.



b. Wählen Sie eine der folgenden Optionen:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

c. Wählen Sie den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke

des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

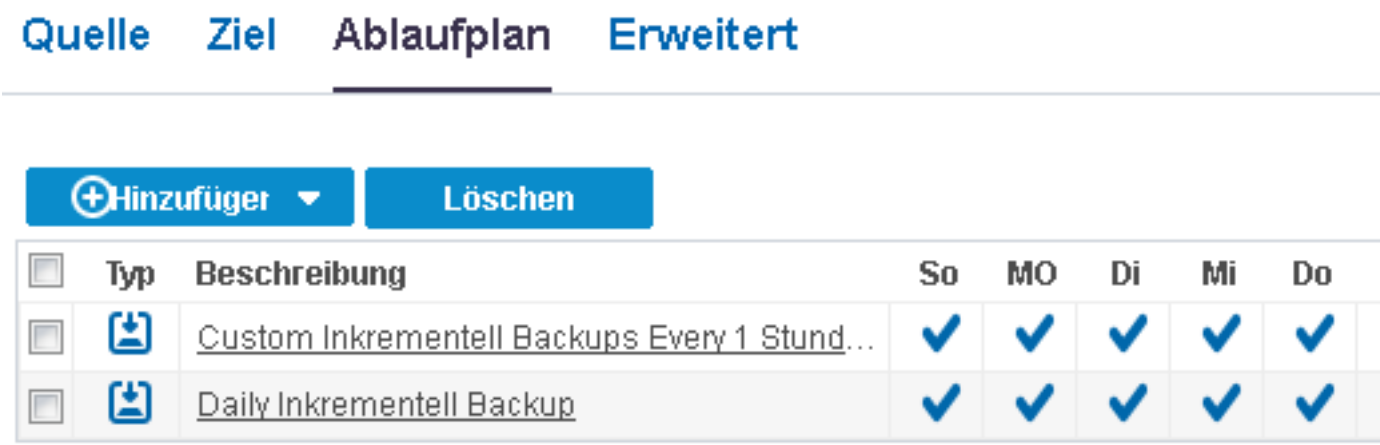
Arcserve UDP erstellt wie geplant nur inkrementelle Sicherungen der Blöcke, die nach der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass die Sicherung schnell durchgeführt und ein kleines Sicherungs-Image erstellt wird. Diese ist der optimale Weg, um eine Sicherung durchzuführen.

d. Geben Sie die Startzeit für die Sicherung an.

e. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.



Hinzufügen eines Zusammenführungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zusammenführungsplan hinzufügen** aus.

Das Dialogfeld **Zusammenführungsplan hinzufügen** wird geöffnet.

b. Geben Sie die Startzeit für den Zusammenführungsjob an.

c. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende des Zusammenführungsjobs bereitzustellen.

d. Klicken Sie auf **Speichern**.

Der Zusammenführungsplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

Hinzufügen eines Drosselungsplans

a. Klicken Sie auf **Hinzufügen**, und wählen Sie **Drosselungsplan hinzufügen** aus.

   Das Dialogfeld **Drosselungsplan hinzufügen wird geöffnet.**

b. Geben Sie die Begrenzung für den Durchsatz in MB pro Minute an.

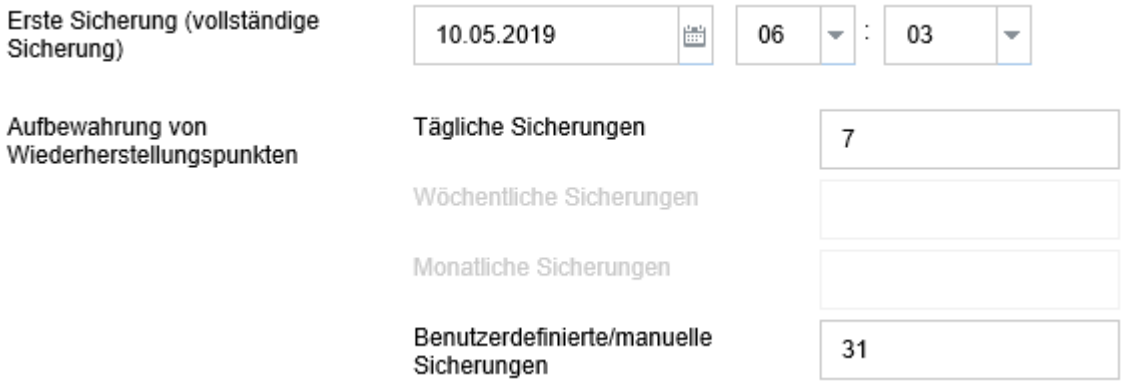
c. Geben Sie die Startzeit für den Sicherungsdurchsatzjob an.

d. Nehmen Sie eine Eingabe unter **Bis** vor, um einen Zeitpunkt für das Ende des Durchsatzjobs bereitzustellen.

e. Klicken Sie auf **Speichern**.

Der Drosselungsablaufplan ist nun festgelegt und wird auf der Seite **Ablaufplanung** angezeigt.

2. Geben Sie die Startzeit für die geplante Sicherung an.



3. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

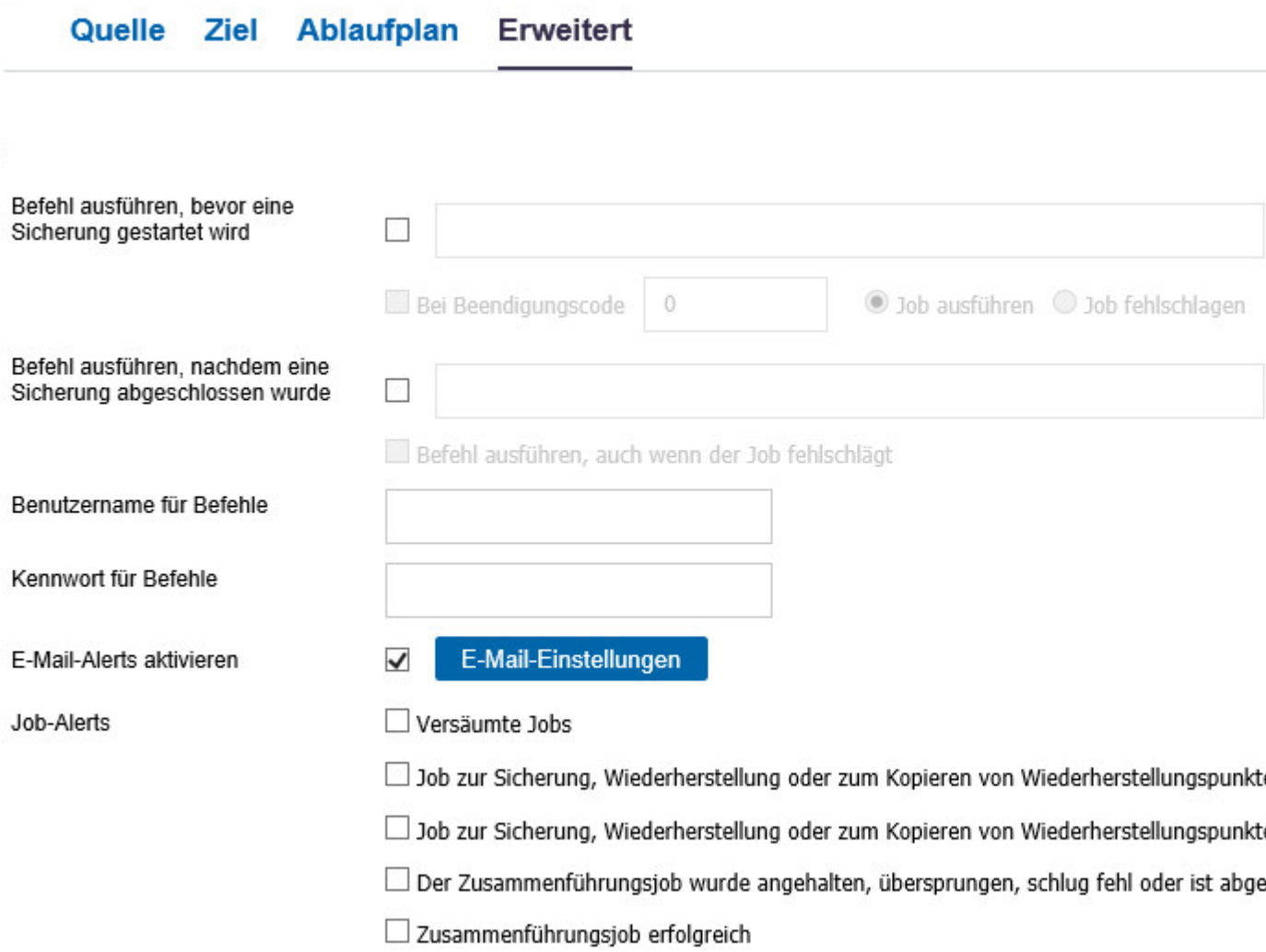
   Die Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld **Sicherungsablaufplan** übernommen.

   Der Ablaufplan ist nun angegeben.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte **Erweitert** können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben. Die erweiterten Einstellungen umfassen das Angeben des Speicherorts von Skripten und E-Mail-Einstellungen.

Die folgende Abbildung zeigt die Registerkarte **Erweitert**:



Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an.

   Befehl ausführen, bevor eine Sicherung gestartet wird

   Ermöglicht es Ihnen, ein Skript auszuführen, bevor der Sicherungsjob gestartet wird. Geben Sie den Pfad an, unter dem das Skript auf dem Proxy-Knoten gespeichert ist. Klicken Sie auf **Bei Beendigungscode** und geben Sie den Beendigungscode für **Job ausführen** oder **Job fehlschlagen** an. **Job ausführen** gibt an, dass der Sicherungsjob fortgesetzt wird, wenn das Skript den

Beendigungscode zurückgibt. **Job fehlschlagen** gibt an, dass der Sicherungsjob angehalten wird, wenn das Skript den Beendigungscode zurückgibt.

Befehl ausführen, nachdem eine Sicherung abgeschlossen ist

Ermöglicht es Ihnen, ein Skript auszuführen, nachdem der Sicherungsjob abgeschlossen wurde. Geben Sie den vollständigen Pfad an, unter dem das Skript gespeichert ist.

Befehl ausführen, auch wenn der Job fehlschlägt

Wenn dieses Kontrollkästchen aktiviert ist, wird das unter **Befehl ausführen, nachdem eine Sicherung abgeschlossen ist** angegebene Skript ausgeführt, selbst wenn der Sicherungsjob fehlschlägt. Andernfalls wird das Skript nur dann ausgeführt, wenn der Sicherungsjob erfolgreich abgeschlossen wurde.

Benutzername für Befehle

Ermöglicht die Angabe des Benutzernamens zum Ausführen der Befehle.

Kennwort für Befehle

Ermöglicht die Angabe des Kennworts zum Ausführen der Befehle.

E-Mail-Alerts aktivieren

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Typen der Warnmeldungen angeben, die Sie in einer E-Mail erhalten möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

E-Mail-Einstellungen

Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren. Klicken Sie auf **E-Mail-Einstellungen**, und konfigurieren Sie die Details des E-Mail-Servers und des Proxy-Servers. Weitere Informationen zur Konfiguration von E-Mail-Einstellungen finden Sie unter Konfigurieren von E-Mails und Alerts.

Job-Alerts

Ermöglicht es Ihnen, die Arten von Job-Alerts auszuwählen, die Sie per E-Mail empfangen möchten.

2. Klicken Sie auf **Speichern**.

Hinweis: Wenn Sie einen Knoten als Sicherungsquelle oder Sicherungs-Proxy auswählen, dann überprüft Arcserve UDP, ob der Agent auf dem Proxy-Knoten installiert und ob die Version aktuell ist. Arcserve UDP zeigt ein Dialogfeld zur Überprüfung an, in dem alle Knoten aufgeführt sind, auf denen entweder eine veraltete Version des Agent oder kein Agent installiert ist. Um den Agent auf diesen

Knoten zu installieren bzw. um ein Upgrade der Agenten auf diesen Knoten durchzuführen, wählen Sie die Installationsmethode aus und klicken auf **Speichern**.

Die Änderungen werden gespeichert, und neben dem Namen des Tasks wird ein grünes Häkchen angezeigt. Die Planungsseite wird geschlossen.

Hinweis: Wenn Sie einen andere Task hinzufügen müssen, müssen Sie den Plan auf der Registerkarte **Ressourcen** auswählen und anschließend ändern. Um den Plan zu ändern, klicken Sie im mittleren Fensterbereich darauf. Der Plan wird geöffnet, und Sie können ihn ändern. Sie können die Tasks **Kopieren von Wiederherstellungspunkten**, **Auf Band kopieren**, **Replizieren** und **Von einem Remote-RPS replizieren** als Folgetasks hinzufügen.

Der Plan wird automatisch auf dem Proxy-Serverknoten bereitgestellt.

Der SharePoint Online-Sicherungsplan für den Proxy-Server wird erstellt. Die Sicherung wird gemäß dem Ablaufplan durchgeführt, den Sie auf der Registerkarte **Ablaufplan** konfiguriert haben. Darüber hinaus können Sie jederzeit manuelle Sicherungen ausführen.

(Optional) Ausführen einer manuellen Sicherung

In der Regel werden die Sicherungen basierend auf den von Ihnen angewendeten Ablaufplaneinstellungen automatisch ausgeführt. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern. Wenn Sie z. B. einen Wiederholungsplan für vollständige Sicherungen und Zuwachssicherungen festgelegt haben und größere Veränderungen an Ihrem Rechner vornehmen möchten, können Sie sofort eine manuelle Sicherung durchführen, ohne auf die nächste geplante Sicherung zu warten.

Gehen Sie wie folgt vor, um eine manuelle Sicherung von SharePoint Online-Knoten durchzuführen:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Die SharePoint Online-Knoten werden im mittleren Fensterbereich angezeigt.
3. Wählen Sie den SharePoint Online-Knoten aus, den Sie sichern möchten (z. B. Mailbox@<organizationname.com>), und vergewissern Sie sich, dass ihm ein Plan zugewiesen ist. Der Knotenname ist das Konto, das beim Hinzufügen und Verbinden des SharePoint Online-Knotens verwendet wurde.
4. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
5. Wählen Sie den gewünschten Sicherungstyp aus, und klicken Sie dann auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.
6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.
7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Gehen Sie wie folgt vor, um eine manuelle Sicherung des SharePoint Online-Plans durchzuführen:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie dann auf **Alle Pläne**.

Die SharePoint Online-Sicherungspläne werden im mittleren Fensterbereich angezeigt.

3. Wählen Sie den Plan aus, den Sie sichern möchten, und vergewissern Sie sich, dass ihm ein Plan zugewiesen ist.
4. Klicken Sie mit der rechten Maustaste auf den Plan, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
5. Wählen Sie den gewünschten Sicherungstyp aus, und klicken Sie dann auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.
6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.
7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Überprüfen der Sicherung

Zur Überprüfung Ihres Sicherungsjobs bestätigen Sie, dass Sie den Sicherungsplan erfolgreich erstellt haben. Nachdem Sie sichergestellt haben, dass der Plan erfolgreich erstellt wurde, überprüfen Sie, ob der Sicherungsjob planmäßig ausgeführt wird. Sie können den Status von Sicherungsjobs auf der Registerkarte **Jobs** überprüfen.

Gehen Sie wie folgt vor, um Pläne zu überprüfen:

1. Klicken Sie auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Im mittleren Fensterbereich wird eine Liste aller Knoten angezeigt.
3. Stellen Sie sicher, dass Pläne zu Knoten zugeordnet sind.

Wenden Sie zur Überprüfung von Sicherungsjobs eine der folgenden Methoden an:

Methode 1

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Alle Jobs vollständig**.

   Der Status des einzelnen Jobs wird im mittleren Fensterbereich aufgelistet.
3. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Methode 2

1. Klicken Sie auf die Registerkarte **Jobs**.
2. Klicken Sie im linken Fensterbereich auf **Jobs erfolgreich abgeschlossen**.

   Die Liste der abgeschlossenen Sicherungsjobs wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf den Job, den Sie überprüfen möchten.

   Der rechte Fensterbereich wird aktualisiert.
4. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
5. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

   Der Sicherungsjob wurde überprüft.

Wiederherstellen von SharePoint Online-Websitesammlungsdaten

Sie können SharePoint Online-Listen/-Bibliotheken oder -Listenelemente auf der Website wiederherstellen. Die Websitesammlung und Website werden noch nicht in Arcserve UDP 8.0 unterstützt. Sie können die Daten auf der ursprünglichen Website mit einem neuen Namen wiederherstellen, die Daten am ursprünglichen Speicherort wiederherstellen und von den Wiederherstellungspunkten auf einen Datenträger exportieren.

Führen Sie die folgenden Tasks aus, um SharePoint Online-Listenelemente wiederherzustellen:

1. Auswählen der SharePoint Online-Website-Listenelemente für die Wiederherstellung
2. Definieren der Wiederherstellungsoptionen
3. Überprüfen, ob der Inhalt wiederhergestellt wurde

Auswählen der SharePoint Online-Website-Listenelemente für die Wiederherstellung

Sie können SharePoint Online-Listenelementdaten von einem Wiederherstellungspunkt wiederherstellen. Wenn Sie ein Wiederherstellungsdatum auswählen und dann die Uhrzeit angeben, werden alle zugeordneten Wiederherstellungspunkte für diesen Zeitraum angezeigt. Sie können die Inhalte (einschließlich Anwendungen) für die Wiederherstellung suchen und auswählen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve UDP an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

   Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   Oder

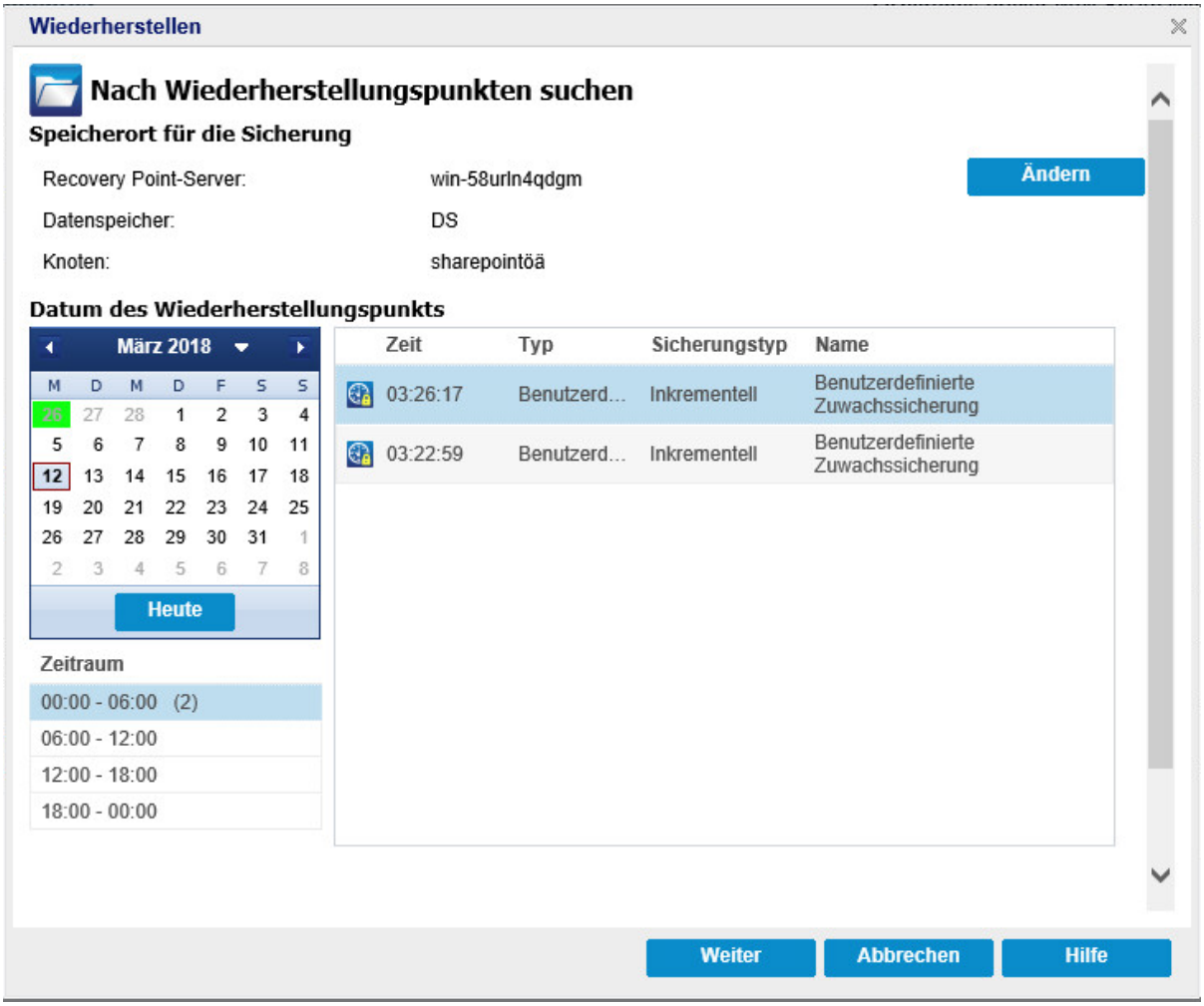
   Wählen Sie die Gruppe **SharePoint Online-Knoten**.

   Alle hinzugefügten SharePoint-Knoten werden im mittleren Fensterbereich angezeigt.
4. Wählen Sie im mittleren Fensterbereich den SharePoint Online-Knoten aus, und klicken Sie dann auf **Aktionen**.
5. Klicken Sie im Drop-down-Menü **Aktionen** auf Wiederherstellen.

   Das Dialogfeld SharePoint-Element wiederherstellen wird geöffnet.

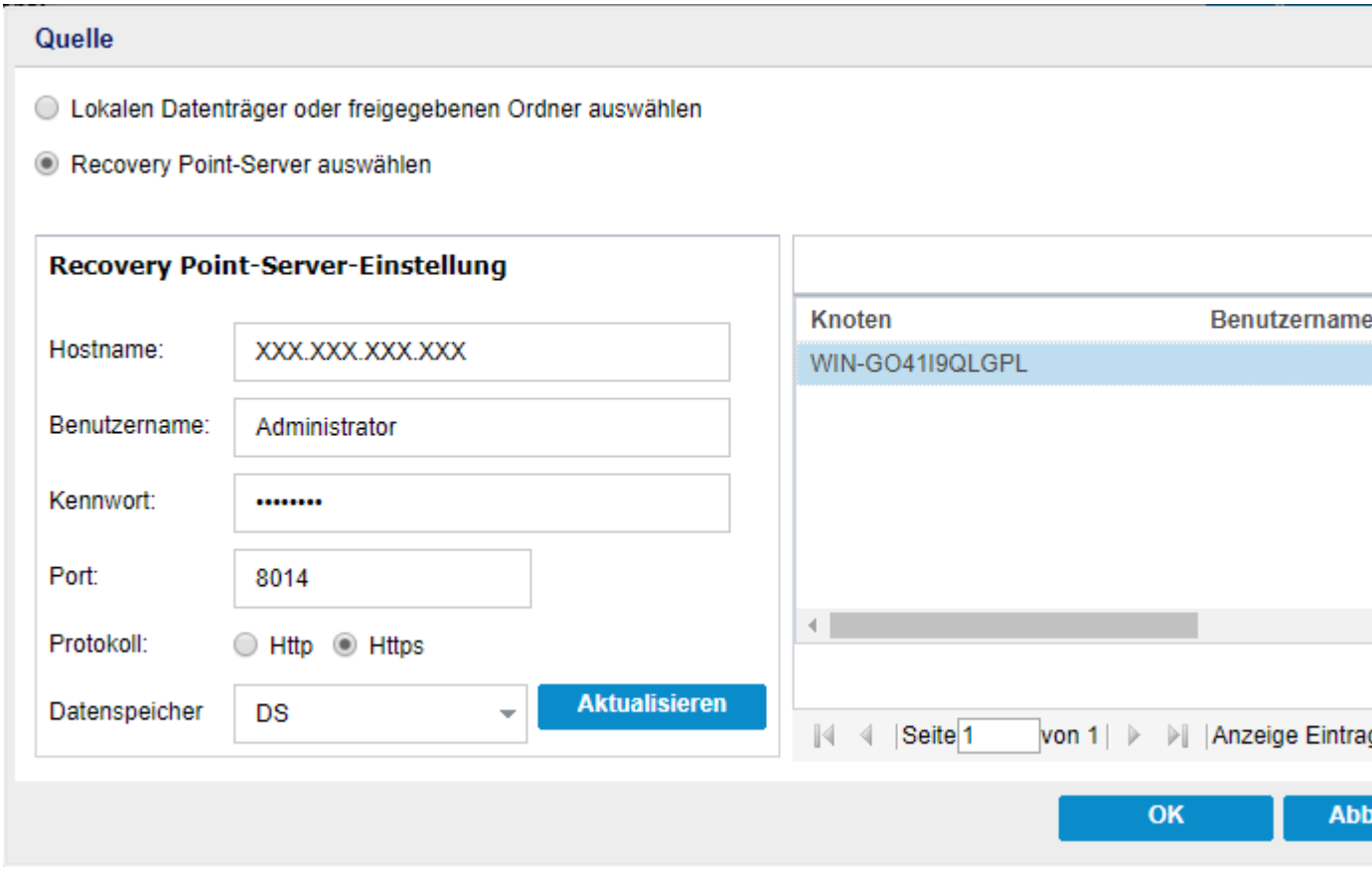
   Hinweis: Sie werden automatisch beim Agent-Knoten angemeldet, und das Dialogfeld SharePoint-Element wiederherstellen wird geöffnet.

   Speicherort für die Sicherung zeigt die Recovery Point Server-Details an.



6. (Optional) Klicken Sie auf **Ändern**, um den Speicherort für die Sicherung zu ändern.

   Das Dialogfeld Quelle wird geöffnet. Sie können den Sicherungsspeicherort in diesem Dialogfeld auswählen.



Hinweis: Wenn Sie dem Plan einen Task "Kopie auf Band" hinzufügen und nun den Wiederherstellungspunkt "Kopie auf Band" wiederherstellen möchten, wählen Sie den Wiederherstellungspunkt aus der Sicherung auf Kopie auf Band aus. Weitere Informationen finden Sie unter Durchsuchen der Kopie auf Band nach Wiederherstellungspunkten.

7. Um die Quelle anzugeben, wählen Sie eine der folgenden Optionen aus, und klicken Sie dann auf **OK**.

   Lokalen Datenträger oder freigegebenen Ordner auswählen

   Hinweis: In Arcserve UDP wird die Auswahl der Option **Lokalen Datenträger oder freigegebenen Ordner auswählen** nicht empfohlen.

   Recovery Point Server auswählen

   a. Geben Sie die Details für die Einstellungen des Recovery Point Servers an, und klicken Sie dann auf **Aktualisieren**.

      Alle Agenten werden in der Spalte "Data Protection Agent" im Dialogfeld Quelle aufgelistet.

b. Wählen Sie den Agenten in der angezeigten Liste/Bibliothek aus, und klicken Sie dann auf **OK**.

   Die Wiederherstellungspunkte werden im Dialogfeld SharePoint-Element wiederherstellen aufgelistet.

8. Wählen Sie das Kalenderdatum des wiederherzustellenden Sicherungs-Images aus, und klicken Sie dann auf **Weiter**.

   Alle Daten, die Wiederherstellungspunkte für die angegebene Sicherungsquelle enthalten, werden grün hervorgehoben.

   Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp (vollständig oder inkrementell) und Name der Sicherung angezeigt.

9. Erweitern Sie im Dialogfeld SharePoint Online-Elemente wiederherstellen die Websitesammlung.

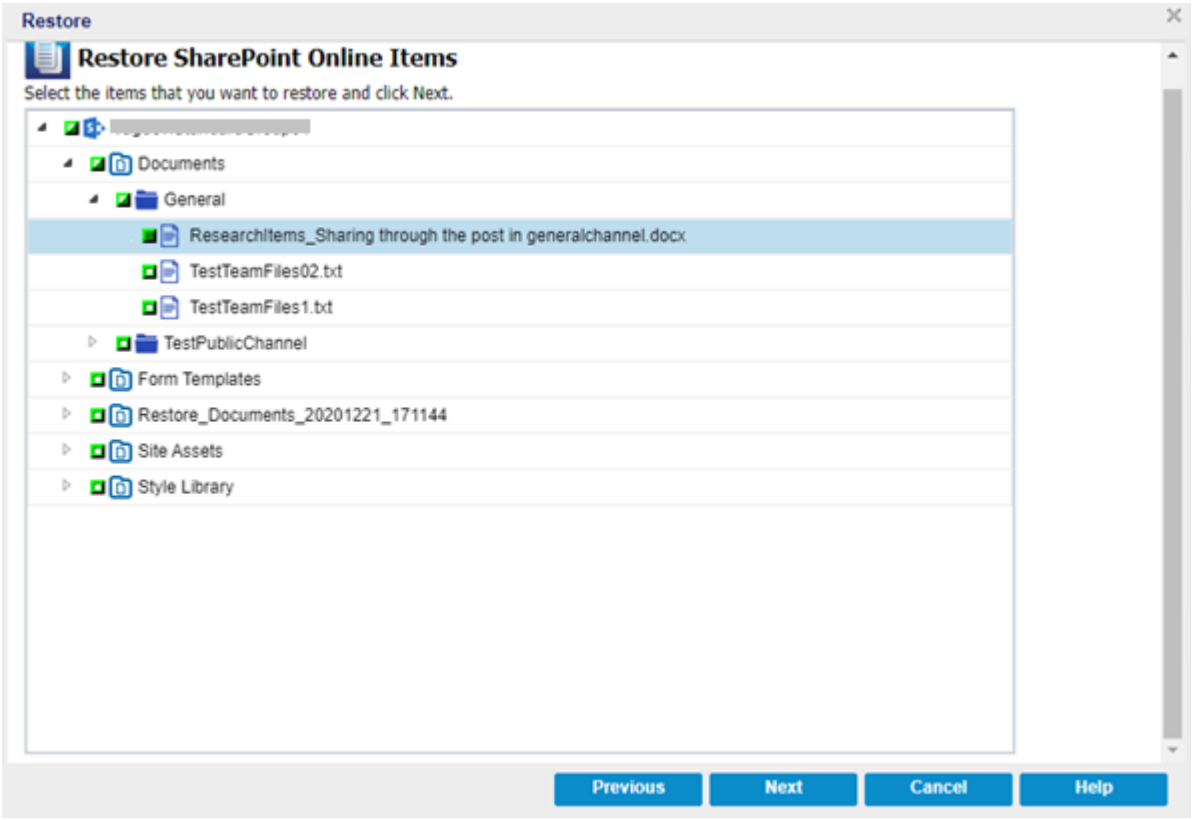
   Alle Listen/Bibliotheken und Elemente werden angezeigt.

10. Wählen Sie die Website oder den bestimmten Kanal in der Websitesammlung, die bzw. den Sie wiederherstellen möchten, in der SharePoint-Websitesammlung aus, und klicken Sie dann auf **Weiter**.

    Hinweise:

    - Sie können den gesamten Inhalt oder Teile des Inhalts des wiederherzustellenden SharePoint-Objekts auswählen. Um Teile des Inhalts auszuwählen, erweitern Sie das Objekt, und klicken Sie dann auf das Kontrollkästchen des Inhalts.
    - Sie können mehrere SharePoint-Listen/-Bibliotheken oder -Listenelemente wiederherstellen.

    Das Dialogfeld Wiederherstellungsoptionen wird geöffnet.



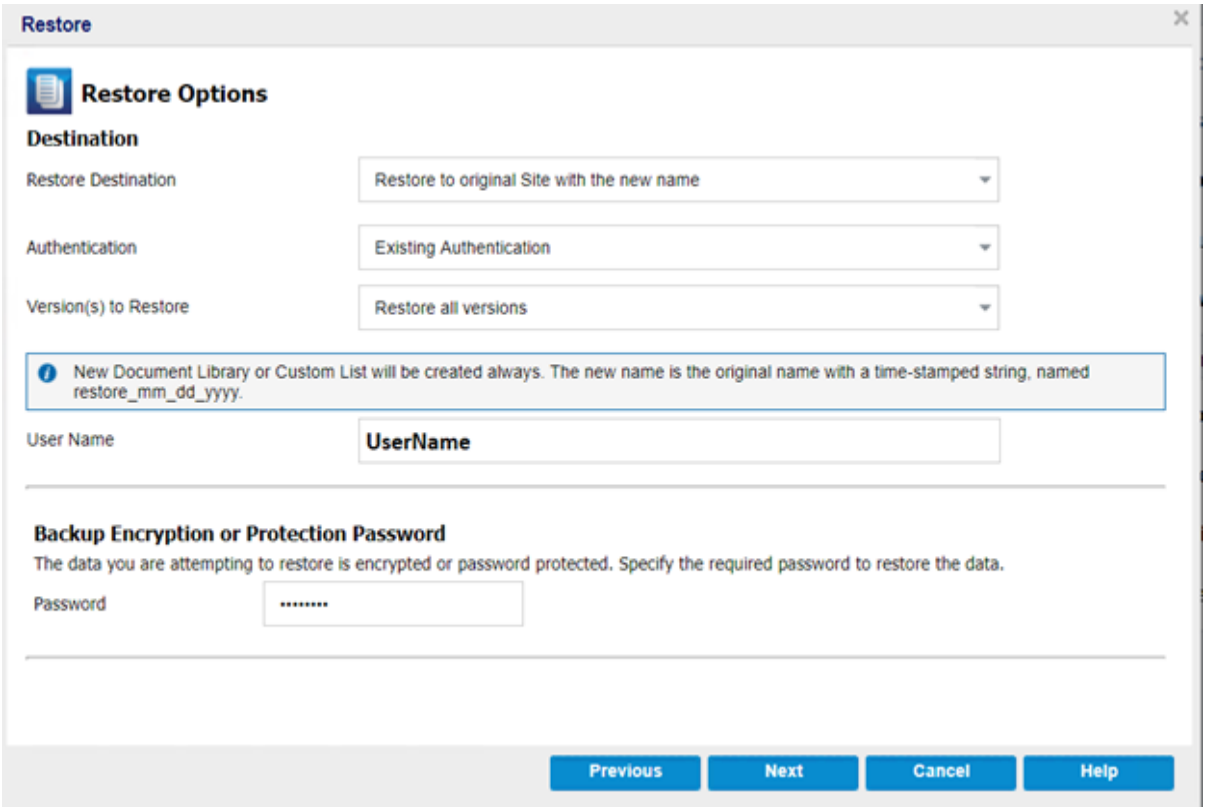
Die SharePoint Online-Listen/Bibliotheken oder -Listenelemente für die Wiederherstellung werden ausgewählt. Nun können Sie die Wiederherstellungsoptionen definieren.

Definieren der Wiederherstellungsoptionen

Nachdem Sie die wiederherzustellenden SharePoint Online-Informationen angegeben haben, legen Sie die Wiederherstellungsoptionen für die ausgewählten Inhalte fest.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld Wiederherstellungsoptionen das Wiederherstellungsziel aus.



Es sind folgende Zieloptionen verfügbar:

Auf ursprüngliche Website mit dem neuen Namen wiederherstellen

Stellt die Daten der Liste/Bibliothek und der Listenelemente auf derselben Website mit einem neuen Listennamen her, von der Sie die Sicherung erstellt haben.

Wiederherstellen am ursprünglichen Speicherort

Stellt die Daten der Liste/Bibliothek und der Listenelemente am selben Speicherort wieder her, an dem Sie die Sicherung erstellt haben.

2. Geben Sie eine der folgenden Optionen aus der Drop-down-Liste "Wenn das Element auf dem Ziel bereits vorhanden ist" an:

Bei aktivierter Versionierung als neue Version anfügen

Diese Option funktioniert, wenn Ihre Versionseinstellung in der Bibliothekseinstellung auf der SharePoint-Website aktiviert ist. Wenn Sie diese Option auswählen, wird die neue Version an die aktuellen Versionen der Listenelemente angehängt, wenn die Listenelemente vorhanden sind.

Objekt überspringen und nicht wiederherstellen

Elemente werden übersprungen und nicht wiederhergestellt.

Das Element im Ziel überschreiben

Das Element im Ziel wird überschrieben.

Auf Datenträger exportieren

Stellt die Listen/Bibliotheken oder Listenelemente in der Websitesammlung im Ordner oder freigegebenen Ordner auf dem Datenträger wieder her.

Hinweis: Wenn Sie für die Listenwiederherstellung die Wiederherstellungsoption "Auf Datenträger exportieren" auswählen, werden nur Anhänge der Liste auf den Datenträger exportiert.

Authentifizierung

Validiert und identifiziert das Benutzerkonto. Wählen Sie eine der folgenden Optionen:

- **Vorhandene Authentifizierung**

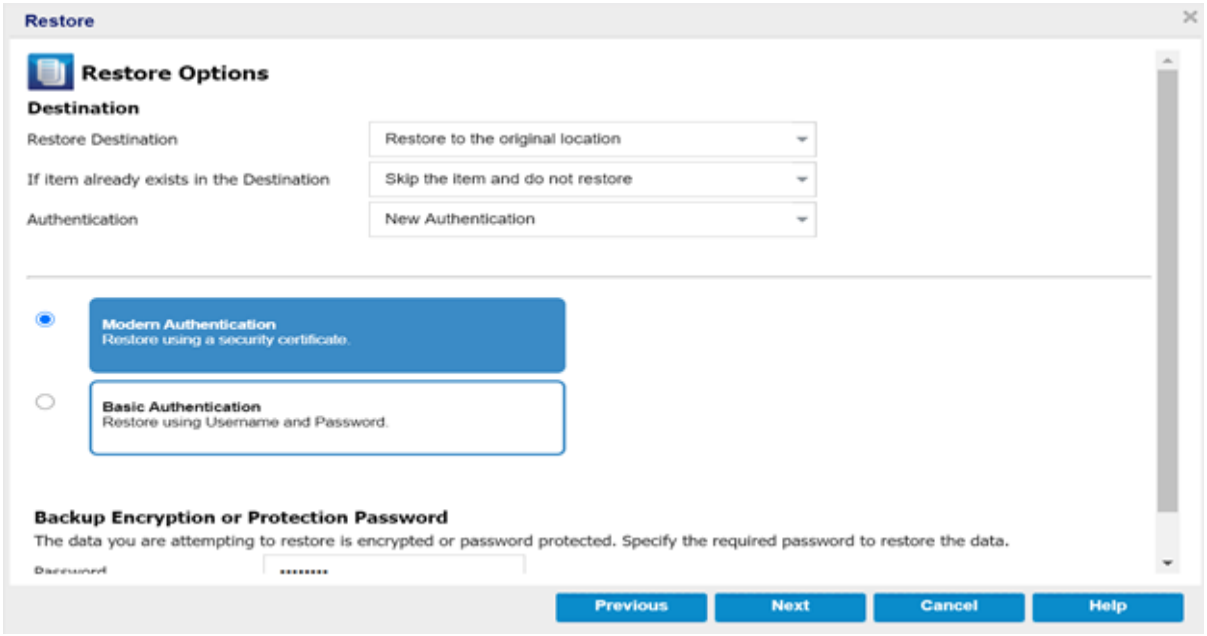
  Wenn Sie "Vorhandene Authentifizierung" auswählen, wird der Authentifizierungstyp verwendet, der während der Knotenerstellung ausgewählt wurde.

  - Wenn es sich bei der Knotenauthentifizierung um die Standardauthentifizierung handelt, werden Parameter wie Benutzername, Kennwort und Sicherungsverschlüsselung oder Schutzkennwort [falls verschlüsselt] automatisch geladen, um mit der Wiederherstellung fortzufahren.
  - Wenn es sich bei der Knotenauthentifizierung um die moderne Authentifizierung handelt, werden Parameter wie Benutzername und Sicherungsverschlüsselung oder Schutzkennwort [falls verschlüsselt] automatisch geladen, um mit der Wiederherstellung fortzufahren.

- **Neue Authentifizierung**

  Während der Wiederherstellung können Sie eine der folgenden Optionen auswählen, um den Authentifizierungstyp zu ändern:

- Moderne Authentifizierung
- Standardauthentifizierung



3. Gehen Sie folgendermaßen vor, um die Authentifizierung anzuwenden:

Moderne Authentifizierung

Bei der modernen Authentifizierung können Sie eine Wiederherstellung mithilfe eines Sicherheitszertifikats ausführen.

Sicherheitszertifikat verwenden

Hinweis: Standardmäßig wählt der Sicherungsplan die Option **Sicherheitszertifikat verwenden** für die moderne Authentifizierung aus.

Gehen Sie wie folgt vor:

a. Informationen zur Authentifizierung mithilfe eines selbstsignierten Zertifikats finden Sie unter Herunterladen des Zertifikats von UDP und Hochladen in Azure

b. Geben Sie die Anwendungs-ID und den Benutzernamen ein.

c. Um die erforderlichen Rollen und Berechtigungen anzuwenden, aktivieren Sie das Kontrollkästchen **Ermöglichen Sie Arcserve UDP, die erforderlichen Azure-Rollen und -Berechtigungen für diese Anwendung festzulegen**, und klicken Sie dann auf **Weiter**.

Standardauthentifizierung

Um bei der Standardauthentifizierung mit der Wiederherstellung fortzufahren, geben Sie Benutzername und Kennwort ein.

Hinweis: Diese Option schlägt fehl, wenn Sie die moderne Authentifizierung für den Mandanten oder das Konto aktiviert haben.

4. Geben Sie die Listenelementversionen an, die Sie wiederherstellen möchten, wenn Ihre Versionseinstellung in der Bibliothekseinstellung auf der SharePoint-Website aktiviert wird.

   Alle Versionen wiederherstellen

   Stellt alle Versionen bei Sicherung wieder her.

   Nur die neueste Version wiederherstellen

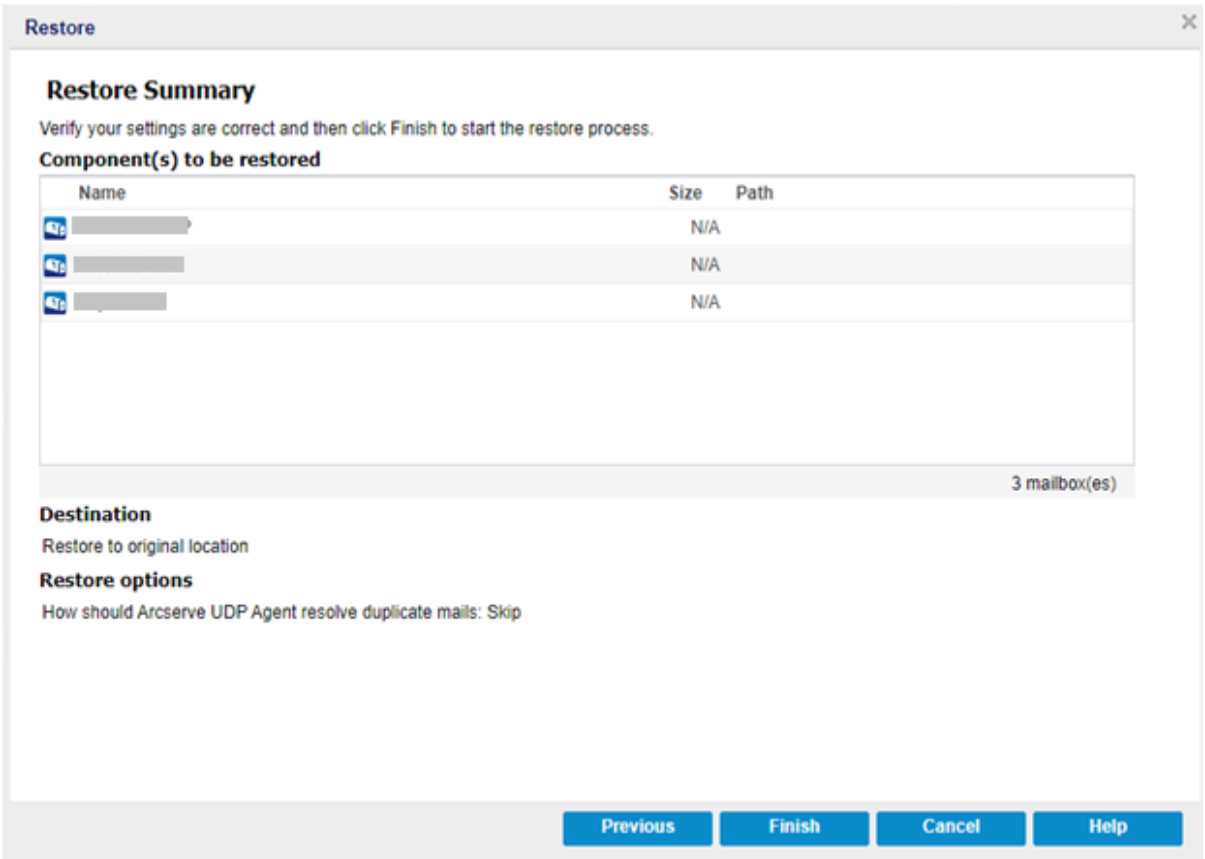
   Stellt nur die neuste Version bei Sicherung wieder her.

   Nur die neueste Hauptversion wiederherstellen

   Stellt nur die neueste Hauptversion bei Sicherung wieder her.

5. Geben Sie das Sitzungskennwort an, falls vorhanden.
6. Klicken Sie auf **Weiter**.

   Das Dialogfeld Wiederherstellungsübersicht wird geöffnet.



Sie können die Wiederherstellungsinformationen aus dem Dialogfeld "Wiederherstellungsübersicht" wiederherstellen.

7. Klicken Sie auf **Fertig stellen**, um den Wiederherstellungsjob zu senden.

   Die Wiederherstellungsoptionen für die Wiederherstellung von SharePoint Online-Informationen sind festgelegt.

Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen Sie nach dem Abschluss der Wiederherstellung, dass der Inhalt auf dem angegebenen Ziel wiederhergestellt wurde.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der SharePoint-Websitesammlung an.
2. Überprüfen Sie die Listen/Bibliotheken und die Listenelemente.
3. Überprüfen die wiederhergestellten Inhalte.

Der wiederhergestellte Inhalt wurde erfolgreich überprüft.

Datenschutzübersicht für Microsoft Teams

Wichtig! Teams-Daten für eine gesamte Organisation werden automatisch geschützt, wenn für Exchange-, SharePoint- und OneDrive-Jobs die Option *Alle schützen* für Konten und Websites verwendet wird.

Die folgende Tabelle beschreibt die Datenschutzübersicht für Microsoft-Teams:

Team-Element	Was in UDP gesichert werden soll	Speicherort der Wiederherstellung
Aufzeichnungen geplanter Besprechungen	OneDrive-Konto des Benutzers, der die Aufzeichnungen erstellt	Agent-Benutzeroberfläche für das OneDrive-Konto des Benutzers
1-1 Private Chats/Posts/Unterhaltungen	Exchange-Postfach des Benutzers	Agent-Benutzeroberfläche für Exchange-Benutzer
Dateien, die über den 1-1-Chat gesendet wurden	Exchange-Postfach/OneDrive-Konto des Benutzers	Agent-Benutzeroberfläche für Exchange-Benutzer und OneDrive-Konto des Benutzers
Elemente im Teams-Standardkanal		
Chats/Posts/Unterhaltungen	Gruppenpostfach des Standardkanals	Agent-Benutzeroberfläche für Gruppenpostfach
Team-Kalender für den Kanal	Gruppenpostfach des Standardkanals	Agent-Benutzeroberfläche für Gruppenpostfach

Dateien, die über Chat-Unterhaltungen gesendet wurden	Wählen Sie den Sharepoint-Standort des Kanals/*Alle Standorte schützen* oder das Gruppenpostfach des Kanals aus	Sharepoint Agent-Benutzeroberfläche > Standort für Standard-Channel > Dokumentbibliothek ODER Exchange Agent-Benutzeroberfläche > Gruppenpostfach
Dateien/Ordner, die über die Registerkarte "Dateien" hochgeladen wurden	Wählen Sie den Sharepoint-Standort des Kanals aus/*Alle Standorte schützen*	Sharepoint Agent-Benutzeroberfläche > Site für Standard-Channel > Dokumentbibliothek
Elemente im privaten Teams-Kanal		
Chats/Posts/Unterhaltungen	Exchange-Postfach des Benutzers	Agent-Benutzeroberfläche für Benutzerpostfach
Dateien, die über Chat-Unterhaltungen gesendet wurden	Wählen Sie den Sharepoint-Standort des Kanals/*Alle Standorte schützen* oder das Benutzerpostfach aus	Sharepoint Agent-Benutzeroberfläche > Standort für Standard-Channel > Dokumentbibliothek ODER Exchange Agent-Benutzeroberfläche > Benutzerpostfach
Dateien/Ordner, die über die Registerkarte "Dateien" hochgeladen wurden	Wählen Sie den Sharepoint-Standort des Kanals aus/*Alle Standorte schützen*	Sharepoint Agent-Benutzeroberfläche > Site für Standard-Channel > Dokumentbibliothek

Erstellen und Konfigurieren von gleichzeitigen Instant Virtual Machine(s) auf mehreren Hypervisoren

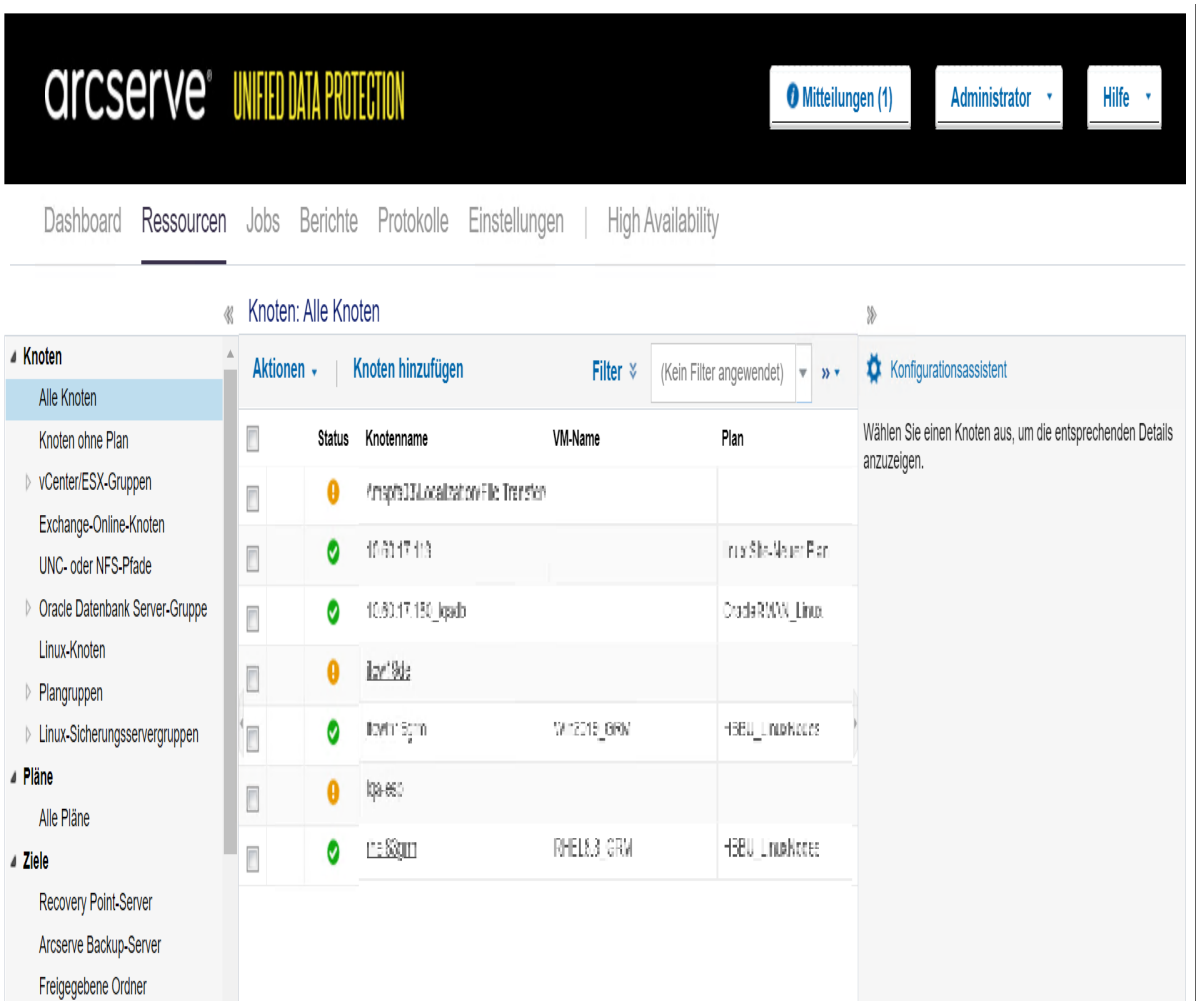
Dieser Abschnitt enthält Informationen zum Erstellen und Konfigurieren von gleichzeitigen Instant VMs auf mehreren Hypervisoren wie Hyper-V, VMware, Nutanix AHV, Amazon EC2 und Microsoft Azure.

Sie können gleichzeitige Instant VMs über die Arcserve UDP-Konsole mithilfe des Assistenten zum Erstellen einer Instant VM erstellen.

Gehen Sie wie folgt vor, um den Assistenten zum Erstellen einer Instant VM zu öffnen:

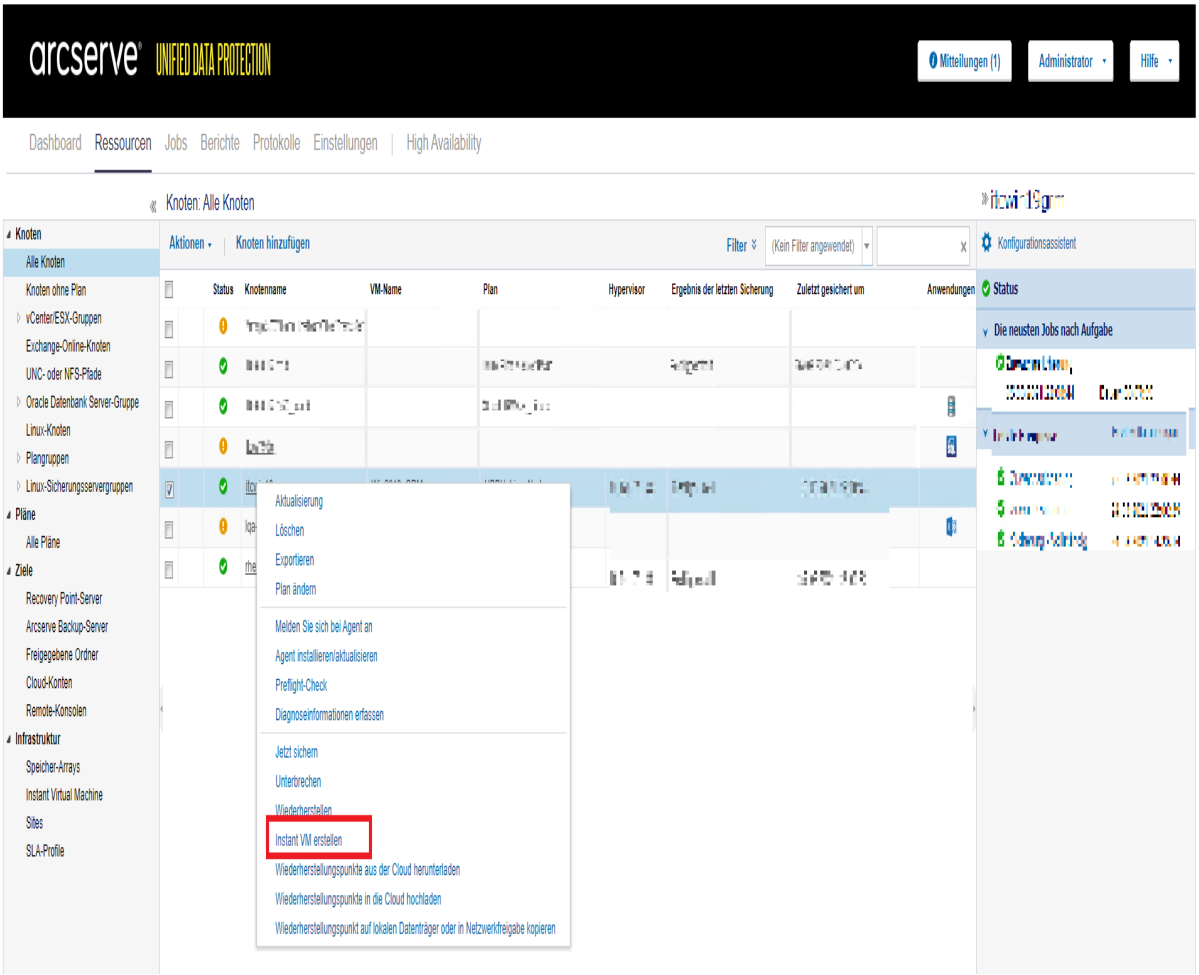
1. Melden Sie sich beim UDP-Konsolenkonto an.
2. Klicken Sie auf der Seite der UDP-Konsole auf die Registerkarte **Ressourcen**.
3. Navigieren Sie im linken Fensterbereich zu **Knoten** > **Alle Knoten**.

   Die Liste der vorhandenen Knoten wird im mittleren Fensterbereich angezeigt.



4. Wählen Sie einen oder mehrere Knoten aus, die bereits einem Plan zugeordnet sind.

   Hinweis: Wenn ein Knoten keinem Plan zugeordnet ist, wird die Option "Instant VM erstellen" nicht angezeigt.



5. Klicken Sie mit der rechten Maustaste auf die ausgewählten Knoten, und wählen Sie dann die Option **Instant VM erstellen** aus.

Der Assistent zum Erstellen einer Instant VM wird angezeigt. Mit dem Assistenten können Sie gleichzeitige Instant VMs konfigurieren.

Führen Sie zum Konfigurieren der gleichzeitigen Instant VMs die folgenden Schritte aus:

1. Auswählen eines oder mehrerer Quell-Recovery Point Server
2. Auswählen des Speicherorts der VM(s)
3. Auswählen eines oder mehrerer Wiederherstellungsserver
4. Konfigurieren der Einstellungen von virtuellen Rechnern
5. Überprüfen der Zusammenfassung

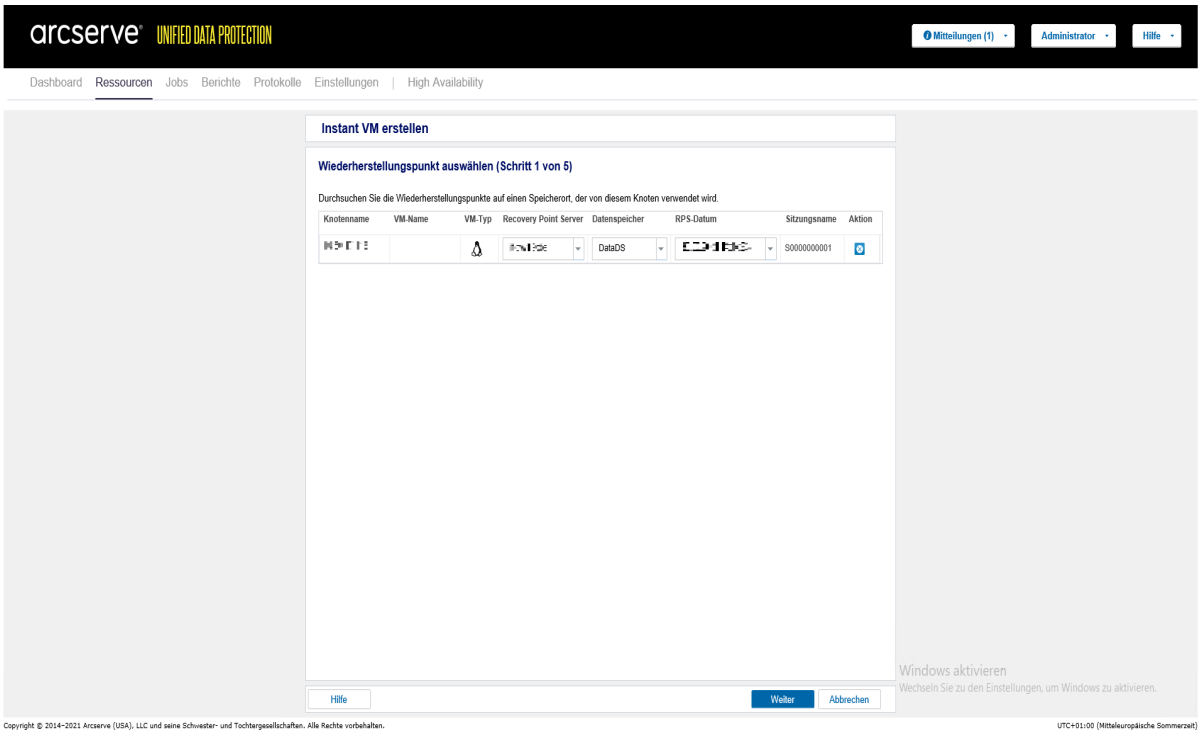
Auswählen eines oder mehrerer Quell-Recovery Point Server

Dieser Abschnitt enthält Informationen zum ersten Schritt der Auswahl eines Quell-Wiederherstellungspunkts.

Im Bildschirm "Wählen Sie einen oder mehrere Quell-Recovery Point Server aus" wird die Liste der ausgewählten Knoten mit Details wie Knotenname, VM-Name, VM-Typ, Recovery Point Server, Datenspeicher, RPS-Datum, Sitzungsname und Aktion angezeigt. Die Details für Recovery Point Server, Datenspeicher und RPS-Datum werden in der Konsole für jeden Knoten in der Liste automatisch ausgewählt. Sie können diese Details auch ändern, wenn auf jedem Knoten mehrere Recovery Point Server verfügbar sind.

Gehen Sie wie folgt vor:

1. Führen Sie im Bildschirm "Wählen Sie einen oder mehrere Quell-Recovery Point Server aus" für jedem Knoten die folgenden Schritte aus:



   - Wählen Sie in der Drop-down-Liste "Recovery Point Server" den gewünschten Recovery Point Server aus.
   - Wählen Sie in der Drop-down-Liste "Datenspeicher" den gewünschten Datenspeicher aus.

- Wählen Sie in der Drop-down-Liste "RPS-Datum" das gewünschte RPS-Datum aus.

2. Klicken Sie auf **Weiter**.
3. (Optional) Wenn die Sicherungssitzung für einen der ausgewählten Knoten verschlüsselt ist, geben Sie das Kennwort ein.

   Der Bildschirm "Speicherort der VM(s)" wird angezeigt.

Führen Sie den nächsten Schritt aus: Auswählen des Speicherorts der VM(s).

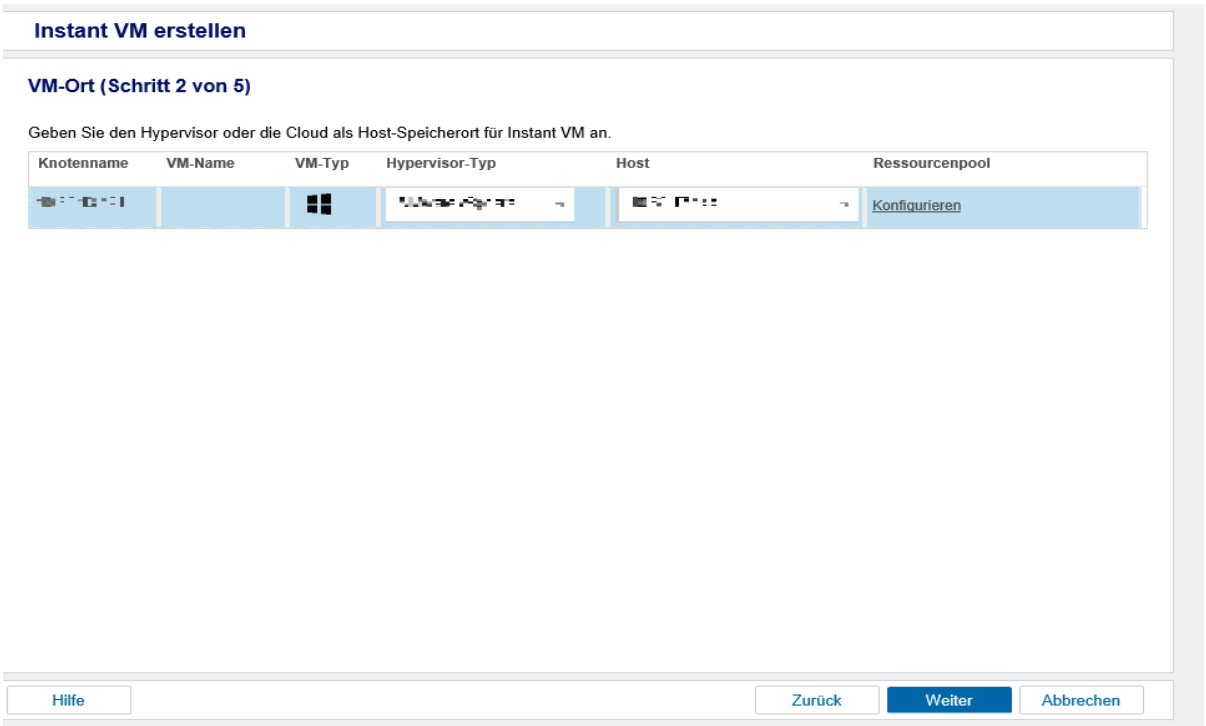
Auswählen des Speicherorts der VM(s)

Dieser Abschnitt enthält Informationen zum zweiten Schritt der Auswahl eines Speicherorts für einen virtuellen Rechner als Host der Instant VM.

Im Bildschirm "Speicherort der VM(s)" wird die Liste der ausgewählten Knoten mit Details wie VM-Name, VM-Typ, Hypervisor-Typ und Host angezeigt. Sie können für jeden Knoten in der Liste den Hypervisor-Typ und den Speicherort des virtuellen Rechners auswählen, der als Host für die Instant VM dienen soll.

Gehen Sie wie folgt vor:

1. Führen Sie im Bildschirm "Speicherort der VM(s)" für jeden Knoten die folgenden Schritte aus:



Windows-Knoten

- Wählen Sie in der Drop-down-Liste "Hypervisor-Typ" den gewünschten Hypervisor-Typ aus.

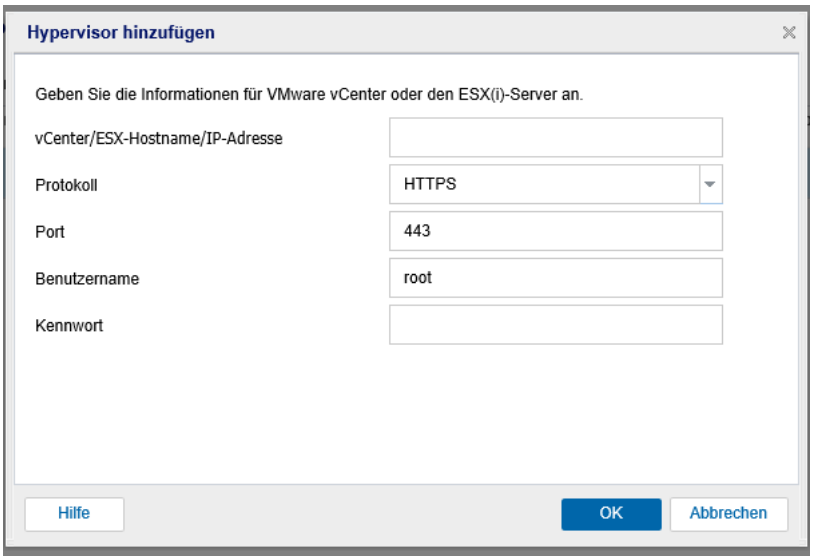
  Hinweis: Arcserve UDP unterstützt VMware und Hyper-V zum Hosten der Instant VM für Windows-Knoten.

- Wählen Sie in der Drop-down-Liste "Host" den vorhandenen Hypervisor aus, oder fügen Sie einen neuen Hypervisor hinzu.

  Gehen Sie wie folgt vor, um einen neuen Hypervisor hinzuzufügen:

  a. Klicken Sie in der Drop-down-Liste "Host" auf **+Neuen Hypervisor hinzufügen**.

  Das Dialogfeld "Hypervisor hinzufügen" wird angezeigt.



  b. Geben Sie im Dialogfeld "Hypervisor hinzufügen" die folgenden Details nach Bedarf an:

  - **vCenter/ESX-Hostname/IP-Adresse:** Geben Sie den Hostnamen oder die vCenter-IP-Adresse ein.
  - **Protokoll:** Wählen Sie das Protokoll aus, z. B. HTTP oder HTTPS.
  - **Port:** Geben Sie die Portnummer ein.
  - **Benutzername:** Geben Sie den Benutzernamen ein.
  - **Kennwort:** Geben Sie das Kennwort ein.

c. Klicken Sie auf **OK**.

Der neue Hypervisor wird hinzugefügt.

- Klicken Sie für "VM-Speicherort" auf **Konfiguriert**, um die Auswahl des VMware-Speicherorts zu konfigurieren.

Linux-Knoten

- Wählen Sie in der Drop-down-Liste "Hypervisor-Typ" den gewünschten Hypervisor-Typ aus.

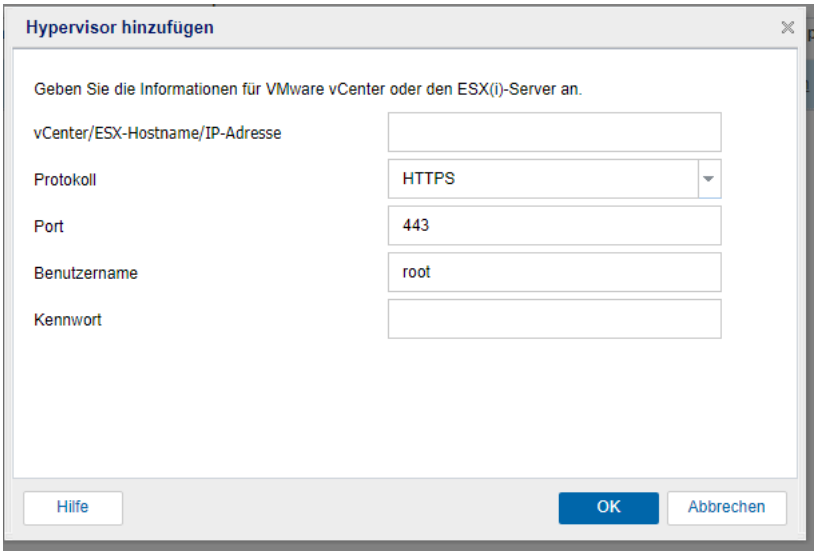
  Hinweis: Arcserve UDP unterstützt VMware, Hyper-V, Nutanix AHV, Amazon EC2 und Microsoft Azure zum Hosten der Instant VM für Linux-Knoten.

- Wählen Sie in der Drop-down-Liste "Host" den vorhandenen Hypervisor aus, oder fügen Sie einen neuen Hypervisor hinzu.

  Gehen Sie wie folgt vor, um einen neuen Hypervisor hinzuzufügen:

  a. Klicken Sie in der Drop-down-Liste "Host" auf **+Neuen Hypervisor hinzufügen**.

  Das Dialogfeld "Hypervisor hinzufügen" wird angezeigt.



  b. Wählen Sie im Dialogfeld "Hypervisor hinzufügen" in der Drop-down-Liste "Virtualisierungstyp" eine der folgenden Optionen aus:

  VMware

  Geben Sie folgende Details nach Bedarf an:

- **ESX-Host/vCenter:** Geben Sie den Hostnamen oder die vCenter-IP-Adresse ein.
- **Benutzername:** Geben Sie den Benutzernamen ein.
- **Kennwort:** Geben Sie das Kennwort ein.
- **Protokoll:** Wählen Sie das Protokoll aus, z. B. HTTP oder HTTPS.
- **Port:** Geben Sie die Portnummer ein.
- **ESX-Knoten:** Wählen Sie einen der verfügbaren Knoten in der Drop-down-Liste aus.

Hyper-V

Geben Sie folgende Details nach Bedarf an:

- **Name des Hyper-V-Host:** Geben Sie den Hostnamen für den Hyper-V-Hypervisor ein.
- **Benutzername:** Geben Sie den Benutzernamen ein.
- **Kennwort:** Geben Sie das Kennwort ein.

Nutanix AHV

Geben Sie folgende Details nach Bedarf an:

- **Virtuelle IP-Adresse des Nutanix AHV-Clusters:** Geben Sie die IP-Adresse ein.
- **Benutzername:** Geben Sie den Benutzernamen ein.
- **Kennwort:** Geben Sie das Kennwort ein.
- **Port:** Geben Sie die Portnummer ein.

EC2

Geben Sie folgende Details nach Bedarf an:

- **Kontoname:** Geben Sie den Namen des Cloud-Kontos ein. Wenn das Cloud-Konto nicht hinzugefügt wird, klicken Sie auf "Hinzufügen". Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.

- **Region:** Wählen Sie die verfügbare Region in der Drop-down-Liste aus.

Azure

Geben Sie folgende Details nach Bedarf an:

- **Kontoname:** Geben Sie den Namen des Cloud-Kontos ein. Wenn das Cloud-Konto nicht hinzugefügt wird, klicken Sie auf "Hinzufügen". Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
- **Ressourcengruppe:** Wählen Sie die verfügbare Ressourcengruppe in der Drop-down-Liste aus.
- **Region:** Wählen Sie die verfügbare Region in der Drop-down-Liste aus.

c. Klicken Sie auf **OK**.

Der neue Hypervisor wird hinzugefügt.

- Klicken Sie für "VM-Speicherort" auf **Konfiguriert**, um die Auswahl des VMware-Speicherorts zu konfigurieren.

2. Klicken Sie auf **Weiter**.

Der Bildschirm "Wiederherstellungsserver" wird angezeigt.

Führen Sie den nächsten Schritt aus: Auswählen eines oder mehrerer Wiederherstellungsserver.

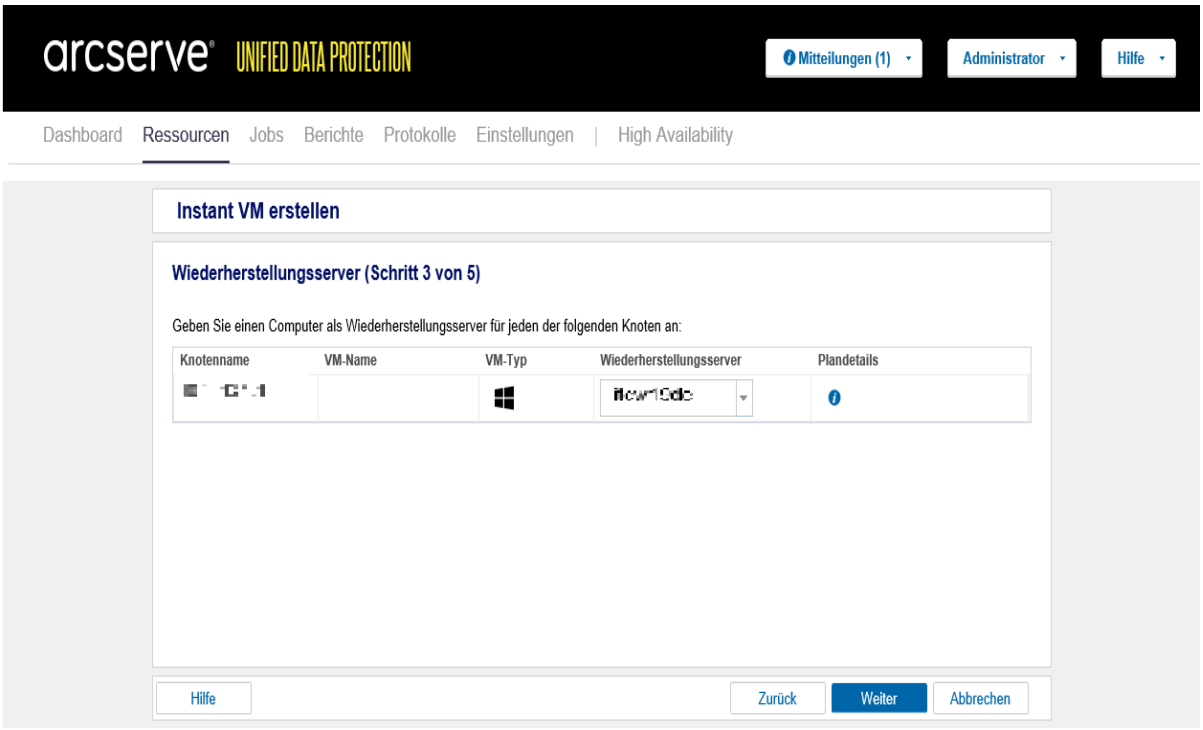
Auswählen eines oder mehrerer Wiederherstellungsserver

Dieser Abschnitt enthält Informationen zum dritten Schritt der Auswahl eines Wiederherstellungsservers zur Ausführung der Instant VM.

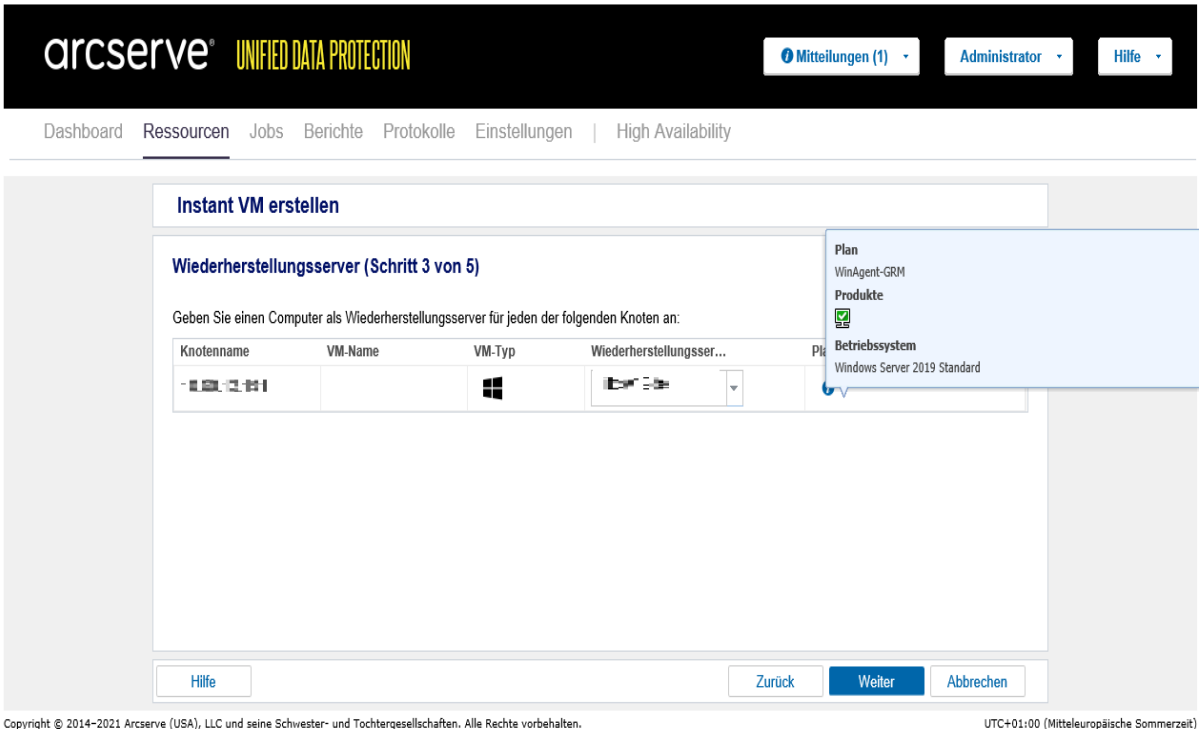
Im Bildschirm "Wiederherstellungsserver" wird die Liste der ausgewählten Knoten mit Details wie VM-Name, VM-Typ, Wiederherstellungsserver und Plandetails angezeigt. Sie können für jeden Knoten in der Liste den Wiederherstellungsserver auswählen, um die Instant VM auszuführen.

Gehen Sie wie folgt vor:

1. Führen Sie im Bildschirm "Wiederherstellungsserver" für jeden Knoten die folgenden Schritte aus:



- Wählen Sie in der Drop-down-Liste "Wiederherstellungsserver" den gewünschten Wiederherstellungsserver aus.
- Zeigen Sie mit der Maus auf das Informationssymbol für "Plandetails", um die Details des Plans zu überprüfen.



Hinweise:

- Bei Linux-Sicherungssitzungen ist der Wiederherstellungsserver ein Linux-Sicherungsserver.
- Wenn als Hypervisor VMware vSphere verwendet wird, muss die Windows NFS-Rolle (Network File System, Netzwerkdateisystem) auf dem Recovery Point Server installiert sein. Sie wird während des Instant VM-Prozesses automatisch installiert. Informationen zur manuellen Installation des Netzwerkdateisystems finden Sie unter So installieren Sie das Netzwerkdateisystem manuell auf einem Windows-Server.

2. Klicken Sie auf **Weiter**.

   Der Bildschirm "Einstellungen der virtuellen Rechner" wird angezeigt.

Führen Sie den nächsten Schritt aus: Konfigurieren der Einstellungen von virtuellen Rechnern.

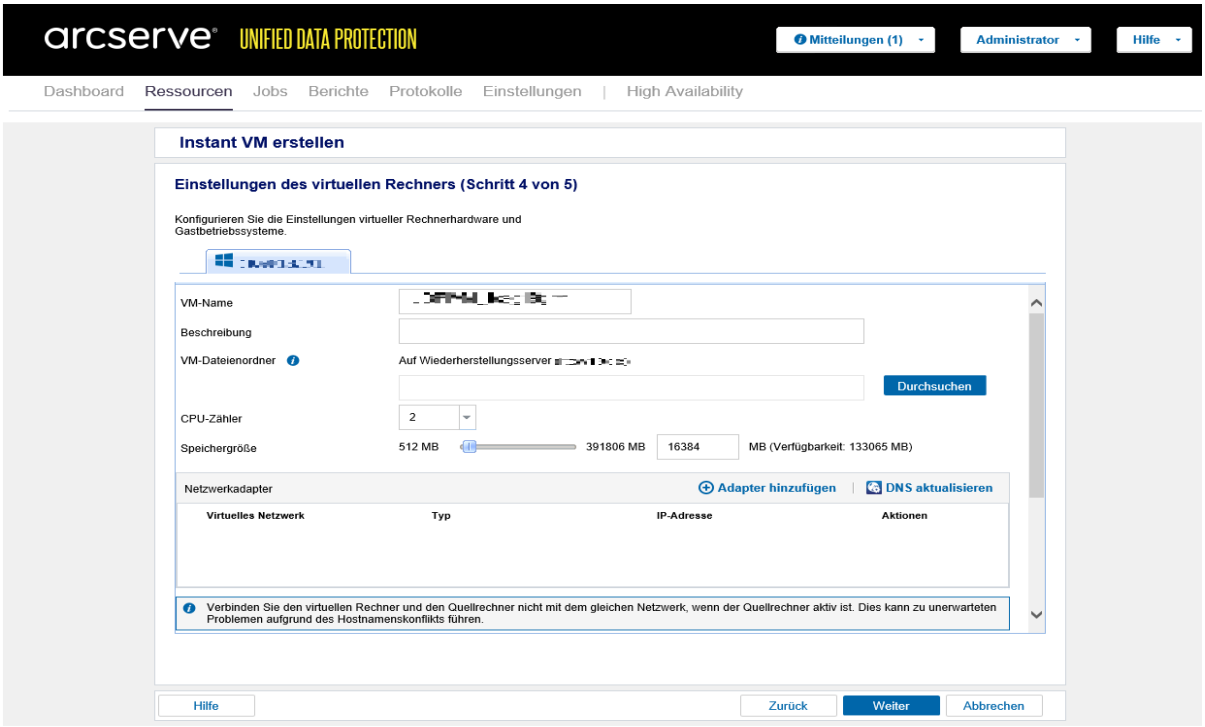
Konfigurieren der Einstellungen von virtuellen Rechnern

Dieser Abschnitt enthält Informationen zum Konfigurieren der Einstellungen von virtuellen Rechnern für die Erstellung einer Instant VM.

Der Bildschirm "Einstellungen der virtuellen Rechner" enthält für jeden ausgewählten Knoten einen eigenen Abschnitt mit den Konfigurationsdetails. In jedem Abschnitt können Sie die Details angeben, die zum Erstellen der Instant VM benötigt werden.

Gehen Sie wie folgt vor:

1. Klicken Sie im Fenster "Einstellungen der virtuellen Rechner" auf den VM-Knoten, den Sie konfigurieren möchten.



2. Führen Sie auf dem ausgewählten VM-Knoten die folgenden Schritte aus:

   - Geben Sie für "VM-Name" den Namen der Instant VM ein. Der Name des Quellknotens mit einem Präfix ist der Standardname der Instant VM.
   - (Optional) Geben Sie unter "Beschreibung" die Beschreibung für die Instant VM nach Bedarf ein.
   - Klicken Sie für "VM-Dateiordner" auf die Schaltfläche **Durchsuchen**, um den Speicherort des Ordners für die Instant VM auf dem Wiederherstellungsserver auszuwählen. Sie können im Dialogfeld "VM-Dateiordner" auch einen neuen Ordner erstellen.

     Hinweis: Die Option "VM-Dateiordner" ist nur für Windows-VM-Knoten verfügbar. Für Linux-VM-Knoten können Sie den verfügbaren Datenspeicher in der Drop-down-Liste "VM-Dateidatenspeicher" auswählen.
   - Wählen Sie für "CPU-Anzahl" die Anzahl der CPUs für die Instant VM aus.
   - Geben Sie unter "Speichergröße" die Größe des Arbeitsspeichers für die Instant VM ein.

     Hinweis: Sie können die Speichergröße für die Instant VM auch mit dem Schieberegler festlegen.
   - Gehen Sie für "Netzwerkadapter" wie folgt vor:

Adapter hinzufügen

Sie können mehrere Netzwerkadapter hinzufügen. Nach dem Hinzufügen eines Netzwerkadapters können Sie den Netzwerkadapter in der Spalte Aktionen bearbeiten und löschen.

Hinweis: Für eine Linux-Instant-VM können Sie mindestens eine virtuelle Netzwerkkarte verwenden, um eine Verbindung zum Linux-Sicherungsserver herzustellen.

Gehen Sie wie folgt vor, um einen Netzwerkadapter hinzuzufügen:

a. Klicken Sie im Abschnitt "Netzwerkadapter" auf **Adapter hinzufügen**.

   Das Dialogfeld "Netzwerkadapter hinzufügen" wird angezeigt.

b. Geben Sie im Dialogfeld "Netzwerkadapter hinzufügen" die folgenden Details ein, und klicken Sie auf **OK**.

   - **Virtuelles Netzwerk:** Wählen Sie im Drop-down-Menü "Virtuelles Netzwerk" das gewünschte virtuelle Netzwerk aus.
   - **Adaptertyp:** Wählen Sie im Drop-down-Menü "Adaptertyp" den Adaptertyp aus.
   - **TCP-/IP-Einstellungen:** Wählen Sie im Drop-down-Menü "TCP-/IP-Einstellungen" je nach Bedarf die Option **Quelle (Automatisch)** oder **Benutzerdefinierte IP-/Gateway-/DNS-/WINS-Einstellungen** aus.

     Hinweis: Wenn Sie die Option "Benutzerdefinierte IP-/Gateway-/DNS-/WINS-Einstellungen" auswählen, klicken Sie auf "Adresse hinzufügen", um die TCP/IP-Details manuell anzugeben.

Der Netzwerkadapter wird hinzugefügt.

DNS aktualisieren

Wenn Sie im Netzwerkadapter und Quellrechner einer Domäne bereits eine IP-Adresse und DNS-Adresse angegeben haben, können Sie das DNS folgendermaßen aktualisieren:

Hinweis: Diese Funktion steht nur für Windows-Instant VMs zur Verfügung.

a. Klicken Sie im Abschnitt "Netzwerkadapter" auf **DNS aktualisieren**.

b. Um einen DNS-Aktualisierungsdatensatz hinzuzufügen, klicken Sie auf **DNS-Adresse hinzufügen**.

Hinweise:

- Sie können den DNS-Aktualisierungsdatensatz entfernen. Klicken Sie zum Entfernen auf **Entfernen**.
- Um die Reihenfolge der Datensätze anzupassen, klicken Sie auf die Nach-oben- und Nach-unten-Schaltfläche.

c. Wählen Sie eine DNS-Adresse und eine IP-Adresse in der Drop-down-Liste aus, und klicken Sie dann auf **OK**.

d. Geben Sie die TTL (Zeit bis Ablauf) an.

e. Geben Sie die DNS-Authentifizierung an.

Geben Sie für den Microsoft-DNS-Server den Benutzernamen und das Kennwort ein. Für BIND-Server müssen Sie den vollständigen Pfadnamen, einschließlich des Dateinamens der Schlüsseldatei im Wiederherstellungsserver, angeben.

- Gehen Sie für "Erweiterte Einstellungen" wie folgt vor:
  - Überprüfen Sie den freien Speicherplatz der VM-Dateiordnerkapazität.

    Hinweis: Das Kontrollkästchen **Freien Speicherplatz der VM-Dateiordnerkapazität überwachen** ist standardmäßig aktiviert. Die Kapazitätsleiste wird auf der Seite "Instant VMs" in Gelb angezeigt, wenn der freie Speicherplatz der VM-Dateiordnerkapazität unter dem Schwellenwert liegt. Der Standardschwellenwert ist 3 %. Sie können den Wert nach Bedarf ändern.
  - Aktivieren Sie das Kontrollkästchen **Geben Sie den Datenträger-Controller-Typ für den virtuellen Rechner an**, und wählen Sie den Typ des Datenträger-Controllers für den virtuellen Rechner in der Drop-down-Liste aus.

Hinweis: Das Kontrollkästchen **Geben Sie den Datenträger-Controller-Typ für den virtuellen Rechner an** ist verfügbar, wenn Sie **VMware vSphere** als Speicherort für die VM ausgewählt haben. Die Instant VM wird erstellt, wobei der angegebene Datenträger-Controller in VMware angewendet wird.

- Um die Aktualisierungen virtueller Datenträger an den VMware-Datenspeicher umzuleiten, gehen Sie folgendermaßen vor:

  a. Aktivieren Sie das Kontrollkästchen **Aktualisierungen virtueller Datenträger an den VMware-Datenspeicher umleiten**.

  Hinweis: Das Kontrollkästchen **Aktualisierungen virtueller Datenträger an den VMware-Datenspeicher umleiten** ist nur verfügbar, wenn Sie VMware vSphere als VM-Speicherort auswählen.

  b. Wählen Sie in der Drop-down-Liste den gewünschten VMware-Datenspeicher aus.

  Die Aktualisierungen des virtuellen Datenträgers werden an den ausgewählten VMware-Datenspeicher umgeleitet.

- Um den Instant VM-Hostnamen zu ändern, gehen Sie folgendermaßen vor:

  a. Klicken Sie auf das Kontrollkästchen **Hostnamen ändern**.

  Der Bildschirm wird mit den neuen Feldern aktualisiert.

  b. Geben Sie im Feld "Neuer Hostname" den neuen Hostnamen nach Bedarf ein.

  c. Wenn sich der Quellrechner in einer Domäne befindet, geben Sie die folgenden Details nach Bedarf an:

  - **Benutzerkonto:** Geben Sie das Benutzerkonto ein.
  - **Kennwort:** Geben Sie das Kennwort ein.
  - **Kennwort bestätigen:** Geben Sie das Kennwort zur Bestätigung erneut ein.

  Hinweis: Wenn sich der Quellrechner in einer Domäne befindet, müssen Sie über die erforderlichen Kontoberechtigungen verfügen, um den Hostnamen in der Domäne zu ändern.

- (Optional) Aktivieren Sie für eine Linux-Instant VM das Kontrollkästchen **Daten nach Start von Instant VM automatisch wiederherstellen**, um die automatische Wiederherstellung von Daten zu aktivieren, wenn das Instant VM-Ziel gestartet wird.

  Beim Standardverhalten der Linux-Instant VM werden zuerst die notwendigen Daten wiederhergestellt. Anschließend wird die VM gestartet. Wenn die Option nicht aktiviert ist, werden die verbleibenden Daten beim Start der VM nicht wiederhergestellt, auch wenn sie als normale VM verwendet wird. Wenn die Option aktiviert ist, werden die verbleibenden Daten auf dem Back-End wiederhergestellt, sobald Sie die VM verwenden. Sie können das Instant VM-Ziel auch dauerhaft beibehalten, wenn die Datenwiederherstellung abgeschlossen ist.

  Hinweis: Wenn der Status der Linux-Instant VM-Ziels "Ausgeschaltet" lautet, schlägt der Instant VM-Job fehl. Wenn dieser Wiederherstellungspunkt zusammengeführt wird, kann die Linux-Instant VM nicht eingeschaltet werden.

3. Klicken Sie auf **Weiter**.

   Das Fenster "Zusammenfassung" wird angezeigt.

Führen Sie den letzten Schritt aus: Überprüfen der Zusammenfassung

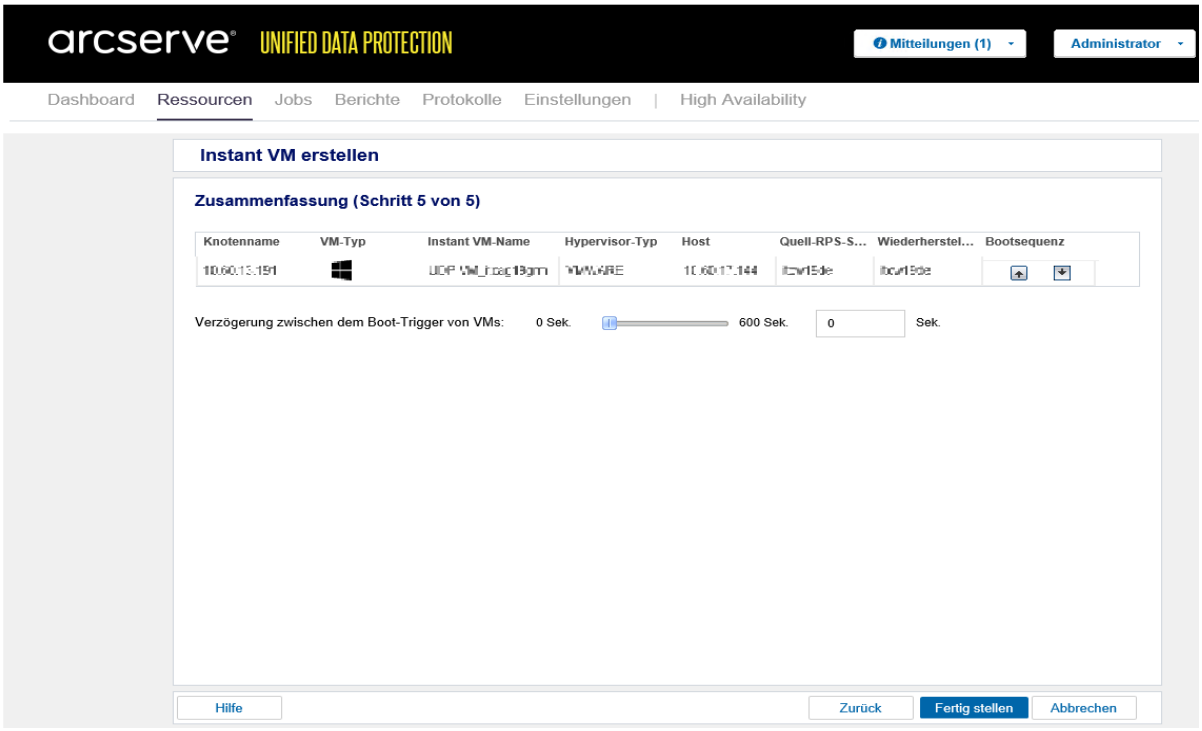
Überprüfen der Zusammenfassung

Dies ist der letzte Schritt der Erstellung von gleichzeitigen Instant VMs. Dieser Abschnitt enthält Informationen zum Überprüfen der Zusammenfassung, zum Anpassen der Bootsequenz und zum Festlegen einer Verzögerung zwischen dem Boot-Trigger von VMs.

Im Bildschirm "Zusammenfassung" wird die Liste der ausgewählten Knoten mit Details wie VM-Name, VM-Typ, Instant VM-Name, Hypervisor-Typ, Host, Quell-RPS, Wiederherstellungsserver und Bootsequenz angezeigt. Sie können die Details überprüfen und die VMs in der gewünschten Bootreihenfolge priorisieren.

Gehen Sie wie folgt vor:

1. Führen Sie im Fenster "Zusammenfassung" die folgenden Schritte aus:



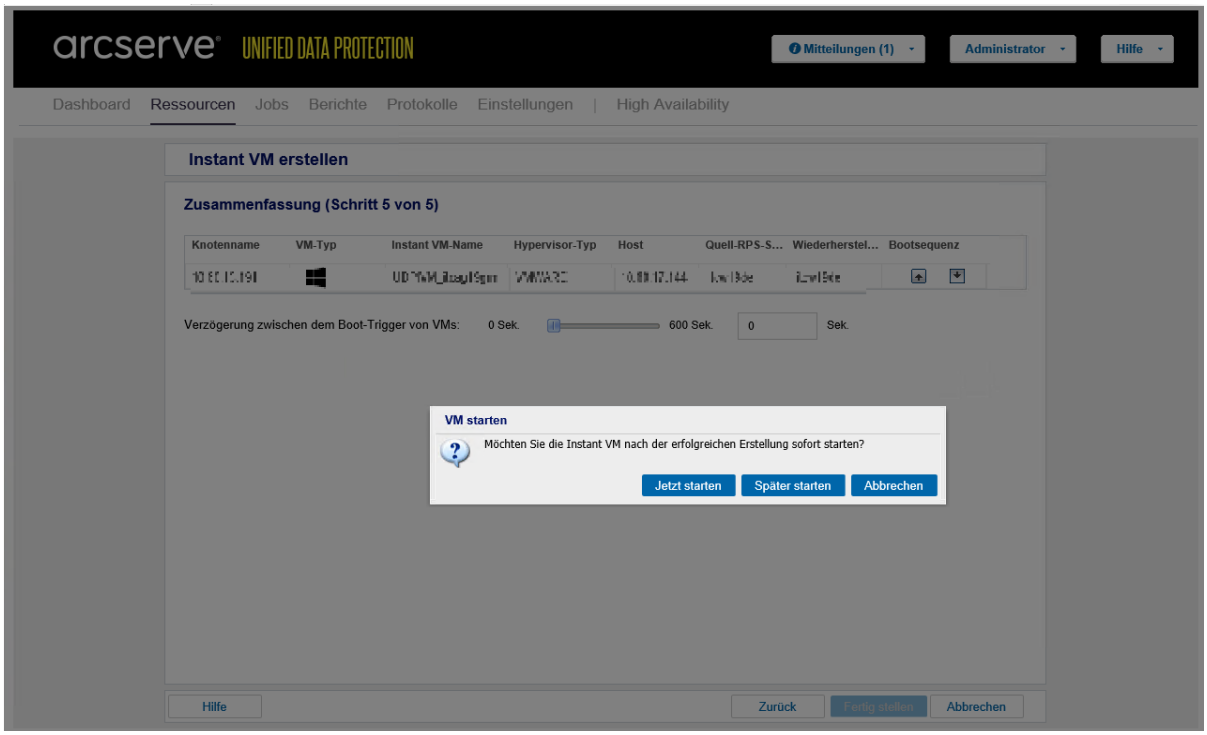
   - Klicken Sie in der Liste der Knoten für die Option "Bootsequenz" jedes Knotens auf die Nach-oben- oder Nach-unten-Schaltfläche, um die Bootsequenz der VM zu priorisieren.
   - Geben Sie für "Verzögerung zwischen dem Boot-Trigger von VMs" die Verzögerungszeit im Bereich zwischen 0 und 600 Sekunden ein.

     Hinweis: Sie können die Verzögerungszeit auch mit dem Schieberegler festlegen.

2. Klicken Sie auf **Fertig stellen**.

   Das Dialogfeld "VM starten" wird geöffnet.

3. Wählen Sie im Dialogfeld "VM starten" eine der folgenden Optionen aus:



- **Jetzt starten:** Erstellt gleichzeitige Instant VMs. Nachdem die gleichzeitigen Instant VMs erstellt wurden, startet die Konsole die VMs automatisch.
- **Später starten:** Erstellt gleichzeitige Instant VMs. Nachdem die gleichzeitigen Instant VMs erstellt wurden, können Sie die VMs manuell starten.
- **Abbrechen:** Sie kehren zur Seite "Instant VM erstellen" zurück, ohne gleichzeitige Instant-VMs zu erstellen.

Gleichzeitige Instant VMs werden erstellt.

Konfigurieren von gleichzeitigen Virtual Standby-Rechnern

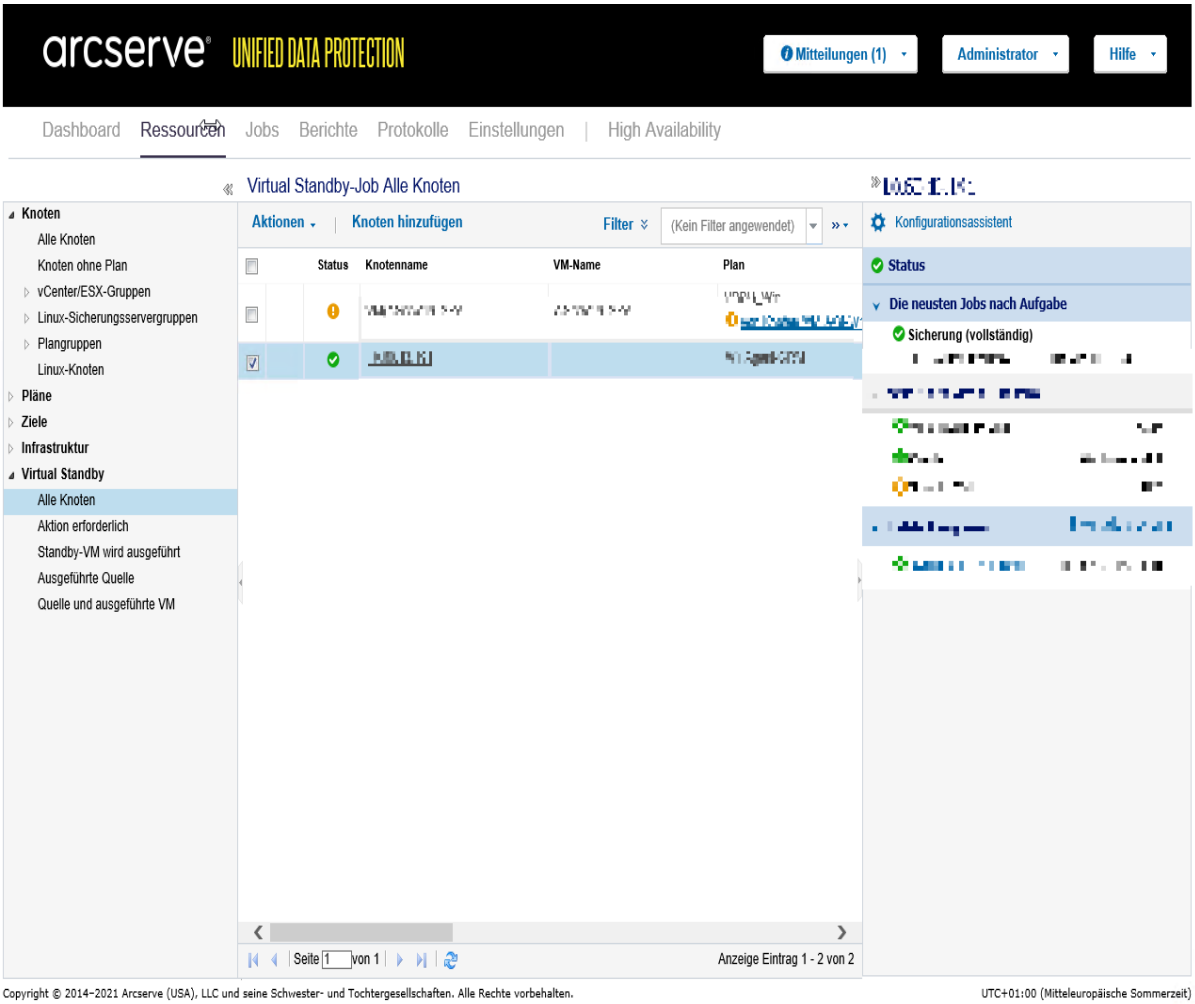
Dieser Abschnitt enthält Informationen zum Konfigurieren von gleichzeitigen Virtual Standby-Rechnern.

Sie können gleichzeitige Virtual Standby-Rechner über die Arcserve UDP-Konsole mithilfe des Dialogfelds "Standby-VM" konfigurieren.

Befolgen Sie diese Schritte:

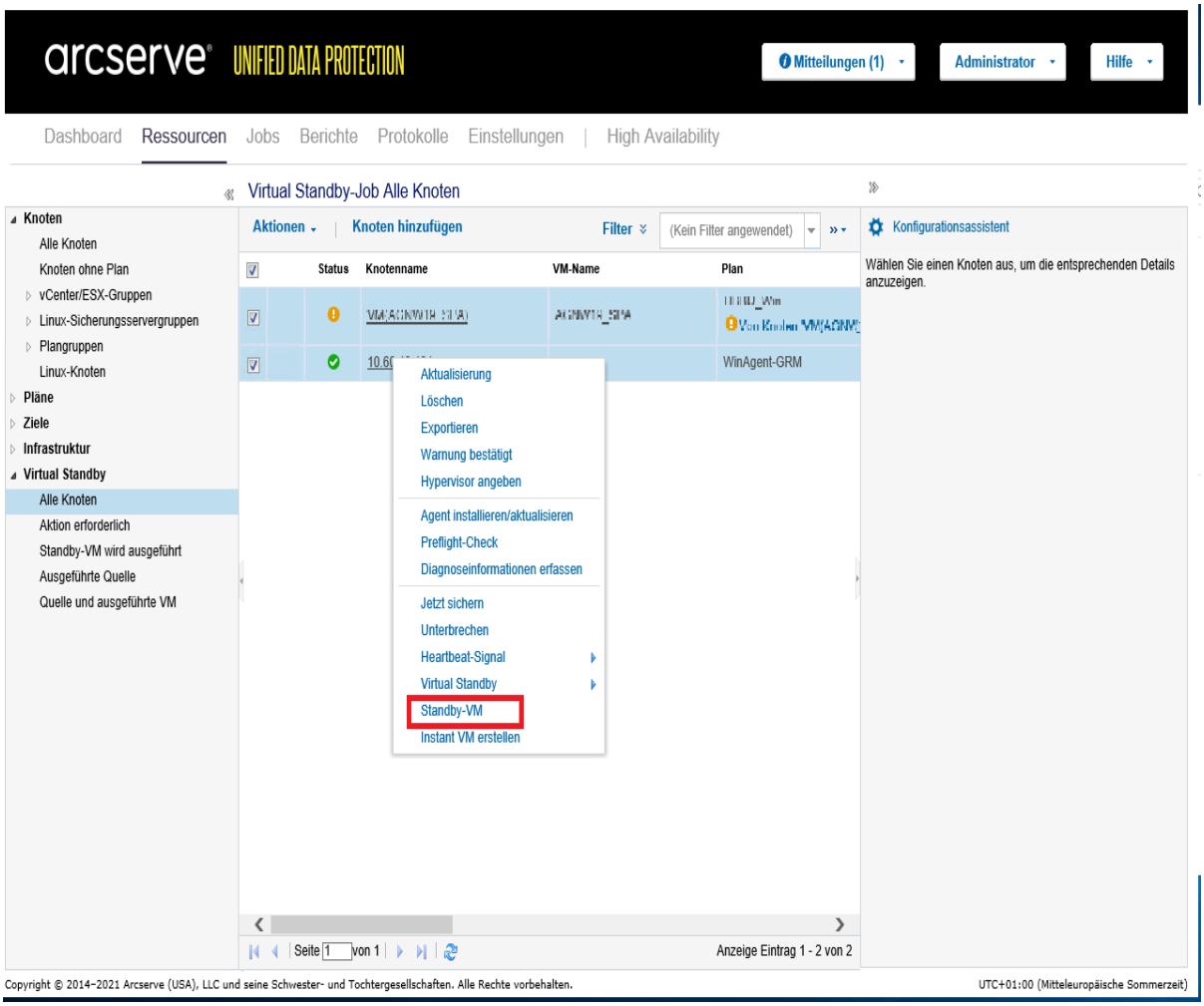
1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Klicken Sie auf der Seite der UDP-Konsole auf die Registerkarte **Ressourcen**.
3. Navigieren Sie im linken Fensterbereich zu **Knoten** > **Alle Knoten**.

   Die Liste der vorhandenen Knoten wird im mittleren Fensterbereich angezeigt.



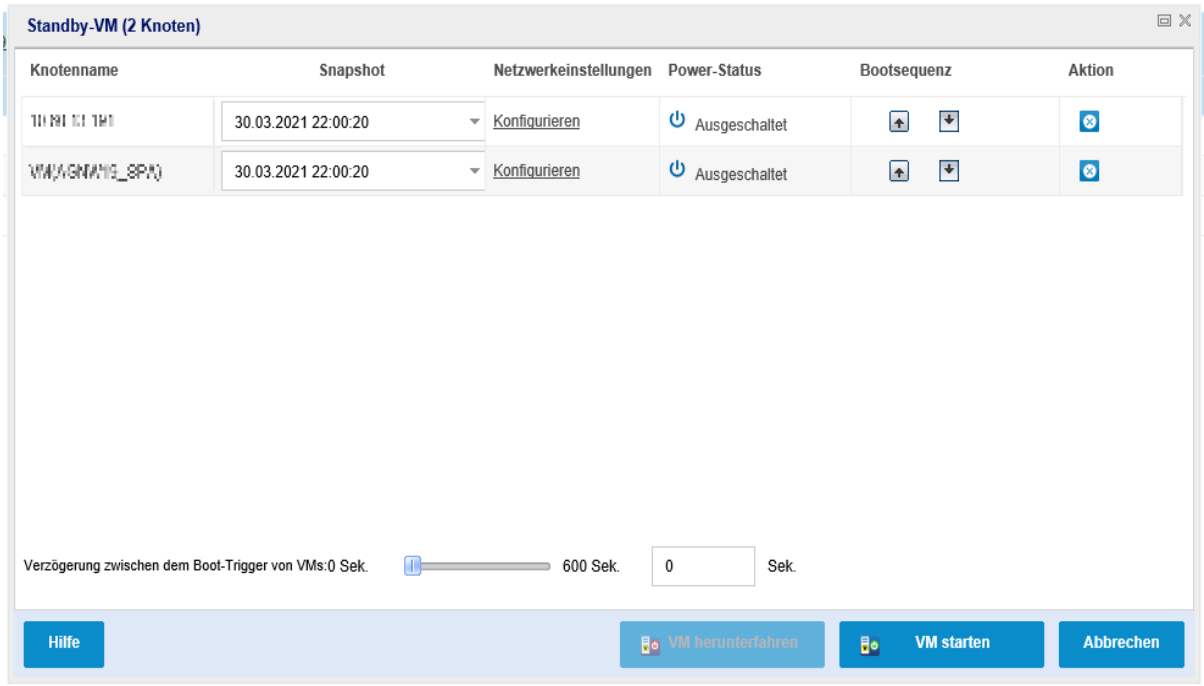
4. Wählen Sie einen oder mehrere Knoten aus, die bereits einem Plan zugeordnet sind.

   Hinweis: Wenn ein Knoten keinem Plan zugeordnet ist, wird die Option "Standby-VM" nicht angezeigt.



5. Klicken Sie mit der rechten Maustaste auf die ausgewählten Knoten, und wählen Sie dann die Option **Standby-VM** aus.

   Das Dialogfeld "Standby-VM" mit der Liste der ausgewählten Knoten wird angezeigt.



6. Führen Sie im Dialogfeld "Standby-VM" die folgenden Schritte aus:

   - **VM starten**

     Hinweis: Diese Option ist nur für ausgeschaltete Virtual Standby-Rechner aktiviert.

     Um virtuelle Rechner gleichzeitig zu starten, gehen Sie wie folgt vor:

     a. Führen Sie in der Liste der ausgewählten Knoten für jeden Knoten die folgenden Schritte aus:

        - Wählen Sie für "Snapshot" in der Drop-down-Liste das Datum und die Uhrzeit des Wiederherstellungspunkt-Snapshots aus.

          Hinweis: Die Snapshot-Details werden nur angezeigt, wenn der VSB-Job erfolgreich abgeschlossen wird.

        - Wählen Sie für "Netzwerkeinstellungen" den Link "Konfigurieren" aus. Weitere Informationen finden Sie unter Konfigurieren des Standby-VM-Netzwerks.

        - Klicken Sie für "Bootsequenz" auf die Nach-oben- oder Nach-unten-Schaltfläche, um die Bootsequenz der Standby-VM zu priorisieren.

        - Klicken Sie unter "Aktion" auf das blaue Kreuzsymbol, um den Knoten zu entfernen.

b. (Optional) Geben Sie für "Verzögerung zwischen dem Boot-Trigger von VMs" die Verzögerungszeit im Bereich zwischen 0 und 600 Sekunden ein.

   Hinweis: Sie können die Verzögerungszeit auch mit dem Schieberegler festlegen.

c. Klicken Sie auf **VM starten**.

   Die Standby-VMs werden gleichzeitig unter Verwendung der im Wiederherstellungspunkt-Snapshot enthaltenen Daten gestartet.

- **VM herunterfahren**

  Um die Virtual Standby-Rechner gleichzeitig herunterzufahren, klicken Sie auf **VM herunterfahren**.

  Hinweis: Diese Option ist nur für eingeschaltete Virtual Standby-Rechner aktiviert.

Kapitel 12: Verwenden eines Hardware-Snapshots für die Sicherung

In diesem Abschnitt werden die folgenden Themen behandelt:

Verwenden von Hardware-Snapshots für Sicherungen

Arcserve UDP bietet die Möglichkeit, Hardwarespeicher-Snapshots für die Sicherung zu nutzen. Sie können angeben, ob Sie einen Hardware-Snapshot verwenden möchten, wenn Sie einen Sicherungstask erstellen. Wenn Sie den Hardware-Snapshot auswählen, versucht Arcserve UDP zuerst, einen Hardware-Snapshot zu erstellen. Wenn der Hardware-Snapshot fehlschlägt, kehrt Arcserve UDP automatisch zum Software-Snapshot zurück, ohne dass der Sicherungsjob fehlschlägt.

Sie können den Hardware-Snapshot für die agentenbasierte Sicherung (physische Windows-Rechner) oder die hostbasierte agentenlose Sicherung (VMware- und Hyper-V) nutzen.

Unterstützte Speicher-Arrays:

- **NetApp Speicher-Array:** Arcserve UDP unterstützt einen Hardware-Snapshot für agentenbasierte Sicherung (physische Windows-Maschinen) und hostbasierte agentenlose Sicherung (VMware und Hyper-V).
- **Nimble Speicher-Array:** Arcserve UDP unterstützt Hardware-Snapshot für agentenbasierte Sicherung (physische Windows-Maschinen) und hostbasierte agentenlose Sicherung (VMware und Hyper-V).
- **HPE 3PAR storeserve-Array:** Arcserve UDP unterstützt einen Hardware-Snapshot für agentenbasierte Sicherung (physische Windows-Maschinen) und hostbasierte agentenlose Sicherung (VMware und Hyper-V).
- **Dell EMC Unity VSA Speicher-Array:** Arcserve UDP unterstützt Hardware-Snapshot für agentenbasierte Sicherung (physische Windows-Maschinen) und hostbasierte agentenlose Sicherung (Hyper-V).

Der nächste Schritt

- Verwenden von Hardware-Snapshots für die agentenlose VMware-Sicherung
- Verwenden von Hardware-Snapshots für die agentenlose Hyper-V-Sicherung
- Verwenden von Hardware-Snapshots für die agentenbasierte Sicherung
- Überprüfen, ob die Sicherung Hardware-Snapshots verwendet hat

Verwenden von Hardware-Snapshots für die agentenlose VMware-Sicherung

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

   Für NetApp-Snapshots

   - Arcserve UDP unterstützt NetApp iSCSI//FC LUNs und NetApp NFS Volume Exporte, die als Datenspeicher konfiguriert sind. iSCSI, FC und NFS müssen bestimmte Bedingungen erfüllen, um den Hardware-Snapshot verwenden zu können.

     Hinweise für den NetApp iSCSI/FC-Support für VMware

     Hinweise für den NFS-Support für VMware

   - Fügen Sie zum Erstellen eines Hardware-Snapshots für VMware das Speicher-Array zur Konsole hinzu. Weitere Informationen zum Hinzufügen eines Speicher-Arrays finden Sie unter Hinzufügen eines Speicher-Arrays.
   - Um einen Hardware-Snapshot zu verwenden, wird für NetApp-Speicher-Arrays mit Data ONTAP im 7-Mode und Cluster-Mode eine FlexClone-Lizenz empfohlen.

   Hinweis: Weitere Informationen zur Konfiguration von NetApp finden Sie in der NetApp Dokumentation oder wenden Sie sich an das NetApp Support Team.

   HPE 3PAR-Hardware-Snapshot:

   - Damit der VMware-VM-Hardware-Snapshot unterstützt wird, muss HP RMC das HPE 3PAR-Speicher-Array verwalten.
   - Das Speicher-Array muss über eine Virtual Copy-Lizenz verfügen.

     Unterstützte Protokolle für VMware-Hardware-Snapshot: FC und iSCSI
   - Fügen Sie zum Erstellen eines Hardware-Snapshots für VMware das Speicher-Array zur Konsole hinzu. Weitere Informationen zum Hinzufügen eines Speicher-Arrays finden Sie unter Hinzufügen eines Speicher-Arrays.

   Nimble-Hardware-Snapshots:

   - Unterstützte Protokolle für VMware-Hardware-Snapshot: FC und iSCSI
   - Fügen Sie zum Erstellen eines Hardware-Snapshots für VMware das Speicher-Array zur Konsole hinzu. Weitere Informationen zum Hinzufügen eines Speicher-Arrays finden Sie unter Hinzufügen eines Speicher-Arrays

     Hinweise zu Nimble-Speicher bei aktivierter CHAP-Authentifizierung

2. Melden Sie sich bei der Konsole an, und erstellen Sie einen Sicherungsplan.

   Hinweis: Weitere Informationen zur Erstellung eines agentenlosen Sicherungsplans finden Sie unter So erstellen Sie einen hostbasierten agentenlosen Sicherungsplan.

3. Stellen Sie sicher, dass Sie auf der Registerkarte **Erweitert** die Option **So oft wie möglich Hardware-Snapshot verwenden** ausgewählt haben.

   Hinweis: Um eine Sicherung nur aus einem Hardware-Snapshot (nicht aus einem Software-Snapshot) durchzuführen, bietet Arcserve UDP den folgenden Registrierungsschlüssel: *FallbackToSWSnapshot =0(dword)*

   Sie können diesen Registrierungsschlüssel für einen bestimmten Knoten sowie alle Knoten anwenden.

   - Um einen bestimmten Knoten zu beantragen, erstellen Sie die Registrierung unter HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\(Nodeid).

     Hinweis: (Nodeid) wird nur nach einer Sicherung erstellt.

   - Um alle Knoten zu beantragen, erstellen Sie die Registrierung unter HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll.

   Wichtig! Wenn der Unterschlüssel "AFBackupDll" nicht verfügbar ist, müssen Sie den Unterschlüssel *AFBackupDll* unter engine als Engine\AFBackupDll\ manuell hinzufügen und dann *DWORD FallbackToSWSnapshot* unter *AFBackupDll* hinzufügen.

4. **Speichern Sie den Plan, und übergeben Sie den Sicherungsjob.**

   Der Sicherungsjob wird mit dem Hardware-Snapshot ausgeführt.

Hinweise für den NetApp iSCSI/FC-Support für VMware

Arcserve UDP unterstützt Hardware-Snapshots für VMware-VMs nur dann, wenn das zugrunde liegende Speicher-Array ein NetApp-Speicher-Array ist.

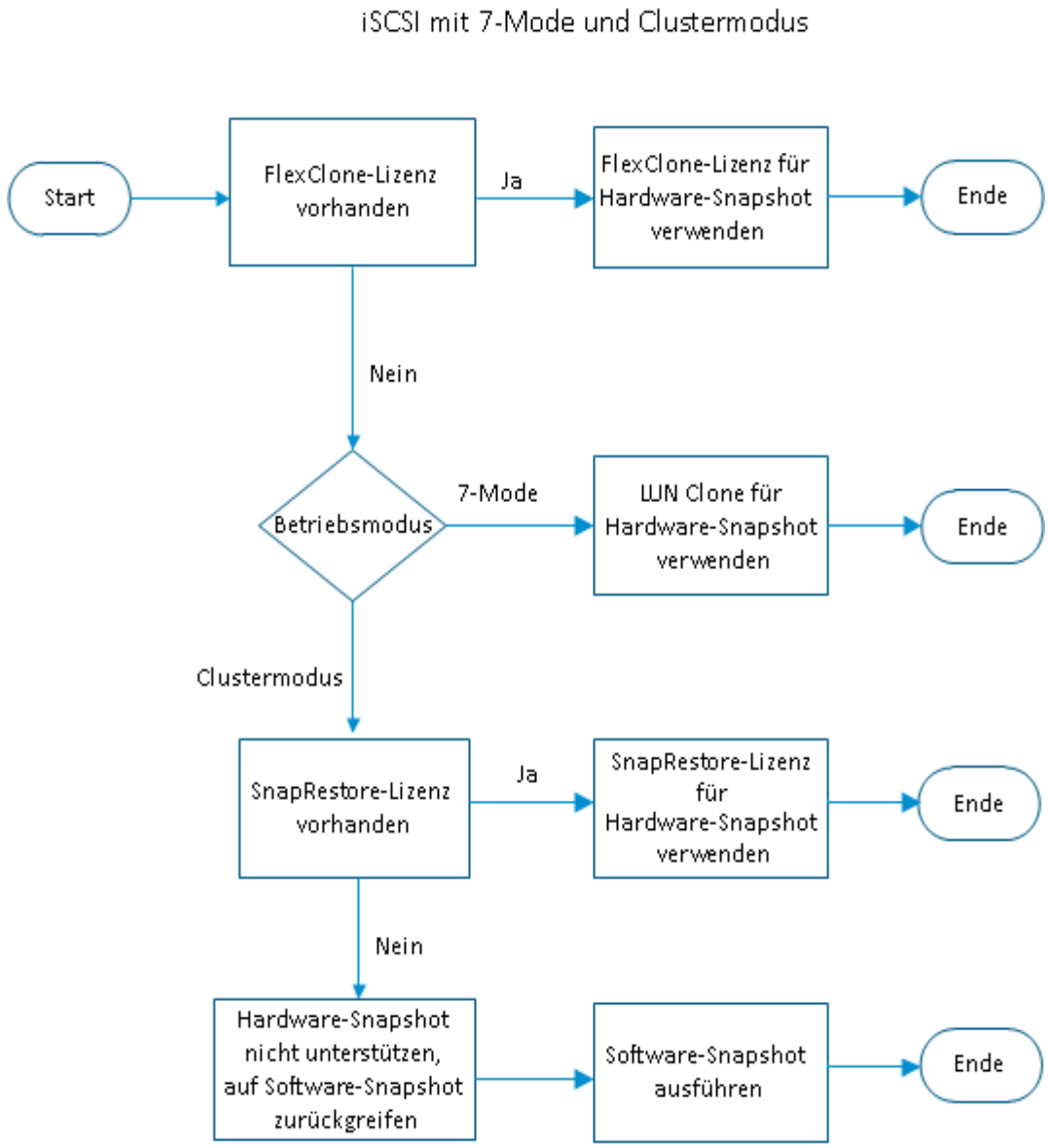
NetApp im 7-Mode

Wenn das NetApp-Speichersystem im 7-Mode ausgeführt wird, ist es nicht notwendig, zusätzliche Lizenzen zu installieren, um Hardware-Snapshots verwenden zu können. Es wird jedoch empfohlen, eine FlexClone-Lizenz zu installieren.

NetApp im Cluster-Modus

Wenn das NetApp-Speichersystem im Cluster-Modus (C-Mode) ausgeführt wird, müssen Sie über eine FlexClone- oder SnapRestore-Lizenz verfügen, damit Sie Hardware-Snapshots verwenden können.

Im folgenden Flussdiagramm werden die Bedingungen für Hardware-Snapshots für NetApp iSCSI/FC mit VMware erläutert:



Einschränkungen eines LUN-Klons

Bei einem herkömmlichen LUN-Klon kann der Sicherungs-Snapshot in einigen Fällen während der Bereinigung nicht gelöscht werden. Eine LUN ist in der Regel im Dateisystem als Datei vorhanden. Ein Snapshot erfasst daher diese Datei. Wenn Sie einen LUN-Klon erstellen, wird im Dateisystem eine weitere Datei erstellt. Daher erfasst der nächste Snapshot die ursprüngliche Datei und die doppelt erstellte Datei. Wenn mehrere Snapshots erstellt werden, wird der LUN-Klon ein Teil der Snapshot-Kette. Wenn Sie nun einen Snapshot löschen möchten, wird der Snapshot nicht gelöscht, da er sich auf einen LUN-Klon bezieht, der wiederum zu einem anderen Snapshot gehört. In solchen Fällen können Sie einen Snapshot erst dann löschen, wenn Sie den LUN-Klon und alle Snapshots, die sich auf diesen LUN-Klon beziehen, gelöscht haben. Als Folge davon können Ihre Aufbewahrungsrichtlinie für geplante Snapshots beeinträchtigt werden.

Um diese Situation zu vermeiden, installieren Sie die FlexClone-Lizenz auf dem NetApp-Speichersystem. Arcserve UDP verwendet dann die FlexClone-Technologie zum Klonen von LUNs.

Registrierungsschlüssel für SnapRestore

Wenn Sie die SnapRestore-Lizenz verwenden, benötigen LUNs abhängig von der Größe der LUN und der Umgebung längere Zeit. Dies ist darauf zurückzuführen, dass das Löschen eines Snapshots länger dauert, da der Snapshot mit der Wiederherstellung der LUN beschäftigt ist. Arcserve UDP verfügt nicht über einen Mechanismus, mit dem der Fortschritt der Wiederherstellung einer LUN überwacht werden kann. Daher verwendet Arcserve UDP den Wiederholungsmechanismus zum Löschen des Snapshots.

Arcserve UDP stellt zwei Registrierungsschlüssel bereit (**DeleteRetryTimeoutInMins** und **DeleteRetryCount**), die Sie verwenden können, um die Leistung beim Löschen von Snapshots je nach Größe der LUN und der Umgebung zu verbessern. Die Registrierungsschlüssel befinden sich im folgenden Speicherort:

SOFTWARE\Arcserve\Unified Data Protection\Engine

DeleteRetryTimeoutInMins

Gibt das Zeitlimit (in Minuten) zum Löschen eines Snapshots an. Wenn Sie nur über SnapRestore und nicht über die FlexClone-Lizenz verfügen, dauert das Löschen von Snapshots wahrscheinlich sehr lange. Über den Registrierungsschlüssel können Sie benutzerdefinierte Werte angeben. Es wird jedoch empfohlen, die FlexClone-Lizenz zu verwenden.

Wenn das Zeitlimit zum Beispiel zwei Minuten beträgt, wartet der UDP-Agent zwei Minuten, bis NetApp den Snapshot löscht, bevor der Löschbefehl bei der nächsten Wiederholung an das NetApp-Speicher-Array gesendet wird. Dieser Registrierungsschlüssel wird zusammen mit dem Schlüssel **DeleteRetryCount** verwendet.

Standardwert: 1 (in Minuten)

Typ: REG_SZ

DeleteRetryCount

Gibt die Anzahl der Wiederholungen an, um einen Snapshot zu löschen.

Wenn die Anzahl der Wiederholungen zum Beispiel fünf beträgt, versucht der UDP-Agent fünfmal, den Snapshot-Löschbefehl an das NetApp-Speicher-Array zu senden. Wenn der Befehl zum Löschen des Snapshots fünfmal gesendet wurde und der Snapshot noch immer vorhanden ist, müssen Sie den Snapshot manuell löschen. Außerdem müssen Sie die Anzahl der Wiederholungsversuche entsprechend erhöhen, sodass dieses Problem bei der

nächsten Sicherung nicht mehr auftritt. Dieser Registrierungsschlüssel wird in Verbindung mit dem Schlüssel **DeleteRetryTimeoutInMins** verwendet.

Standardwert: 30

Typ: REG_SZ

Registrierungsschlüssel für das Deaktivieren der Reservierung von LUN-Speicherplatz

Wenn während der Sicherung mithilfe eines Hardware-Snapshots ein LUN geklont wird, wird die Reservierung von Speicherplatz standardmäßig vom Quell-LUN vererbt. Arcserve UDP enthält einen Registrierungsschlüssel, den Sie verwenden können, um die Reservierung von Speicherplatz zu deaktivieren. Die Registrierungsschlüssel befinden sich am folgenden Speicherort:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

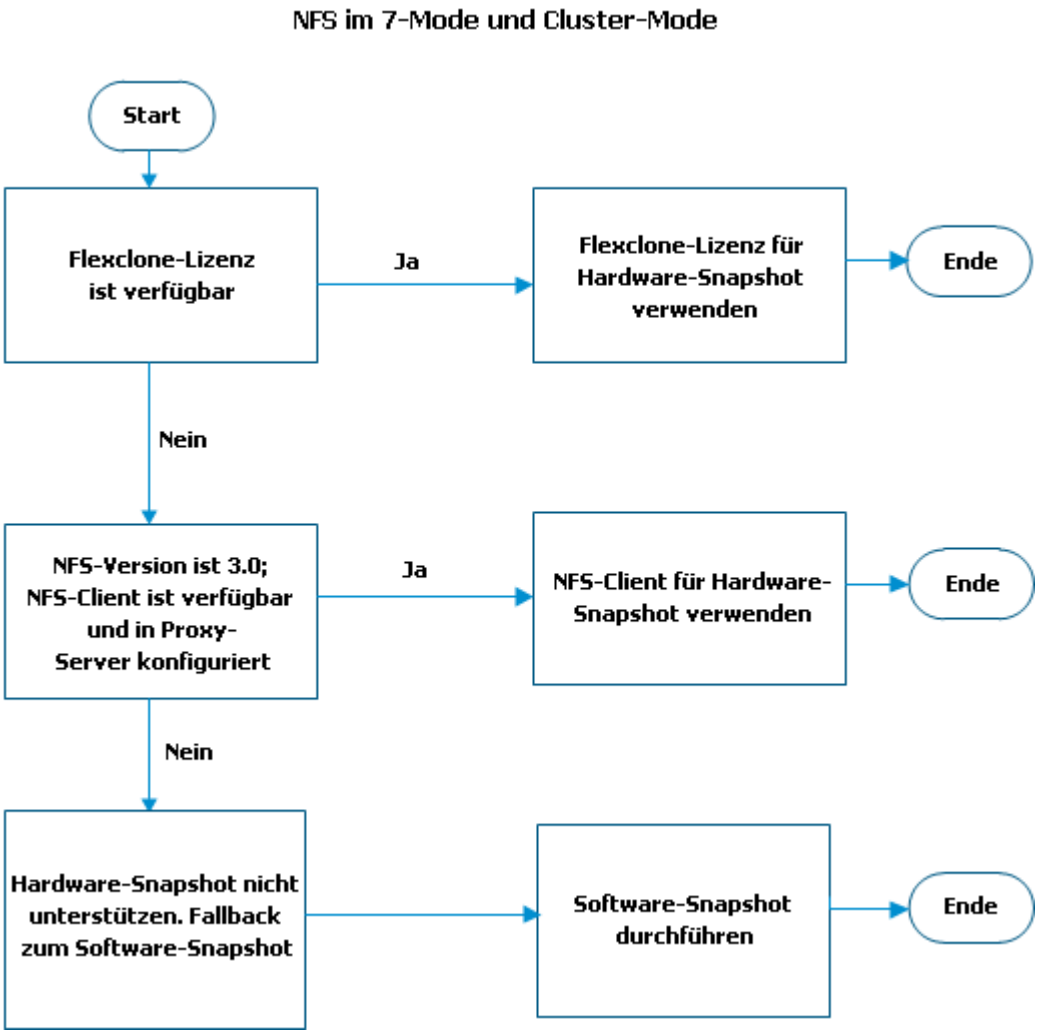
DisableLunSpaceReservation = 1

Gibt an, dass die Reservierungen von LUN-Speicherplatz deaktiviert werden.

Hinweis: Diese Option gilt nur, wenn eine FlexClone-Lizenz angewendet wird.

Hinweise für den NFS-Support für VMware

Im folgenden Flussdiagramm werden die Bedingungen für Hardware-Snapshots für NetApp NFS mit VMware erläutert:



Arcserve UDP unterstützt Hardware-Snapshots für Datenspeicher der NFS Version 3.0. Um Hardware-Snapshots zu verwenden, muss auf dem Sicherungs-Proxy der Microsoft-NFS-Client installiert und konfiguriert sein.

Die folgende Tabelle enthält die NFS-Versionen, die VMware-VMs und Arcserve UDP unterstützen. Stellen Sie sicher, dass Sie über die richtige NFS-Version mit der entsprechenden VMware-Version verfügen.

VMware-Versionen	NFS-Versionen, die VMware unterstützt	NFS-Versionen, die Arcserve UDP für Hardware-Snapshots für FlexClone unterstützt	NFS-Versionen, die Arcserve UDP für Hardware-Snapshots für den Windows NFS Client unterstützt
VMware 6.0	Unterstützt NFS	Unterstützt NFS 3.0 und	Unterstützt nur NFS 3.0 und

und höher	3.0 und 4.1	4.1	muss die Voraussetzungen erfüllen
VMware-Versionen, die älter sind als 6.0	Unterstützt nur NFS 3.0	Unterstützt NFS 3.0	Unterstützt nur NFS 3.0 und muss die Voraussetzungen erfüllen

Voraussetzungen für NFS 3.0

- Wenn die FlexClone-Lizenz nicht vorhanden ist, müssen auf der NetApp-Appliance die folgenden Versionen von OnTAP installiert sein, damit Hardware-Snapshots von VMDK-Dateien, die auf NFS 3.0-Datenspeichern gehostet werden, unterstützt werden können:
  - Alle Data ONTAP 7-Mode-Systeme werden unterstützt.
  - Clustered Data ONTAP 8.2-Versionen ab Version 8.2.3 werden unterstützt. Außerdem werden Clustered Data ONTAP 8.3-Versionen ab Version 8.3.1 unterstützt.
  - Standardmäßig ist die Unterstützung für den Windows NFS v3-Client deaktiviert. Um sie auf SVMs zu aktivieren, verwenden Sie den folgenden Befehl:

  vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled

- Auf dem Sicherungs-Proxy, mit dem die VMware-VM gesichert wird, sollte der Microsoft-NFS-Client installiert und konfiguriert sein. Der Sicherungs-Proxy sollte Zugriff auf die NFS-Freigabe habe. Informationen zur manuellen Installation des NFS-Clients auf dem Server finden Sie unter So installieren Sie den Microsoft-NFS-Client manuell auf einem Windows-Server.
- Sie müssen den Microsoft-NFS-Client-Dienst auf dem Proxy-Server nach der Bereitstellung des agentenlosen Sicherungsplans neu starten. Sie müssen den Dienst nur beim ersten Mal neu starten, da die Planbereitstellung nur zu einigen Änderungen bezüglich des NFS-Clients auf dem Proxy-Server führt.

So installieren Sie den Microsoft-NFS-Client manuell auf einem Windows-Server

Gehen Sie folgendermaßen vor, um den Microsoft-NFS-Client manuell auf einem Windows-Server zu installieren.

1. Melden Sie sich beim Windows-Server an.
2. Öffnen Sie den Server-Manager, und klicken Sie auf "Verwalten".
3. Klicken Sie auf "Rollen und Features hinzufügen".
4. Klicken Sie im Dialogfeld "Bevor Sie beginnen" auf "Weiter".
5. Wählen Sie im Dialogfeld "Installationstyp wählen" die rollenbasierte oder funktionsbasierte Installationsmethode aus, und klicken Sie auf "Weiter".
6. Wenn Sie auf den lokalen Server installieren möchten, klicken Sie im Dialogfeld "Zielserver wählen" auf "Weiter". Wählen Sie andernfalls aus der Serverpoolliste einen Server aus.
7. Klicken Sie im Dialogfeld "Serverrollen auswählen" auf "Weiter".
8. Scrollen Sie im Dialogfeld "Funktionen wählen" in der Liste der verfügbaren Funktionen nach unten, und aktivieren Sie das Kontrollkästchen "Client für NFS".
9. Klicken Sie auf "Weiter".
10. Überprüfen Sie im Dialogfeld "Installationsauswahl bestätigen" Ihre Auswahl, und klicken Sie auf "Installieren".
11. Wenn die Installation abgeschlossen ist, überprüfen Sie die Ergebnisse, und klicken Sie auf "Schließen".

Hinweise zu Nimble-Speicher bei aktivierter CHAP-Authentifizierung

Sie können Hardware-Snapshots sichern, wenn für Nimble-Speicher CHAP-Authentifizierung aktiviert ist.

Hinweis: CHAP-Authentifizierung wird unter ESXi 5.0 nicht unterstützt, da diese ESXi-Version nicht über SQLite verfügt.

Die folgenden Voraussetzungen müssen erfüllt werden:

Voraussetzungen

Wichtig: Die Voraussetzungen gelten nur, wenn Sie möchten, dass der hostbasierte agentenlose Sicherungsjob SAN als Transportmodus verwendet.

- Aktivieren Sie SSH auf ESXi, auf dem Nimble-Speicher mit CHAP-Authentifizierung konfiguriert ist.
- Überprüfen Sie, ob der Proxy-Rechner über die zur Konfiguration von iSCSI-Zielgeräten nötige iscsicli-Befehlszeile verfügt.
- Stellen Sie die Ausführungsrichtlinie auf dem Proxy-Rechner auf "RemoteSigned" ein, um die PowerShell-Skripte auszuführen. Verwenden Sie den folgenden Befehl:

  Set-ExecutionPolicy RemoteSigned
- Speichern Sie ESXi-Anmeldeinformationen über ein PowerShell-Skript, für das der Nimble-Speicher mit CHAP-Authentifizierung konfiguriert ist.

  Führen Sie diese Schritte aus, um die ESXi-Anmeldeinformationen zu speichern:

  - Führen Sie das PowerShell-Skript "StoreESXCredentials.ps1" von der PowerShell auf dem Proxy aus.

    Sie werden aufgefordert, Details zur IP-Adresse, zum Benutzernamen und zum Kennwort einzugeben.
  - Geben Sie alle drei Parameter ein.

    Die Anmeldeinformationen werden in einer CSV-Datei ("ESXCredentials.csv") gespeichert, und das Kennwort wird verschlüsselt.

  Gehen Sie wie folgt vor, um das PowerShell-Skript zu finden:

  - Melden Sie sich bei dem Proxy-Rechner an, und öffnen Sie die PowerShell.
  - Navigieren Sie zum folgenden Verzeichnis:

Hinweis: Der Pfad ändert sich je nach Installationsverzeichnis.

C:\Programme\Arcserve\Unified Data Protection\Engine\BIN

- Führen Sie das PowerShell-Skript wie im Nachfolgenden gezeigt aus:

  PS C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN>
  .\StoreESXCredentials.ps1

Verwenden von Hardware-Snapshots für die agentenlose Hyper-V-Sicherung

Wichtig!Hyper-V Agentless Backup verwendet Hardware-Snapshot nur, wenn sich alle Festplatten der VM auf Hardware-Snapshot-kompatiblen Volumes befinden. Andernfalls verwendet die Sicherung einen Software-Snapshot.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:
   - Installieren Sie einen VSS-Hardwareanbieter (z. B. NetApp) auf den Hyper-V-Servern. Installieren Sie den VSS-Hardwareanbieter zur Unterstützung des übertragbaren Snapshots auf dem Sicherungs-Proxy-Server. Die typische Konfiguration eines VSS-Hardwareanbieters umfasst:
     - Angeben eines Servers, der die LUN steuert
     - Angeben der Anmeldeinformationen des Datenträger-Arrays für den Zugriff auf das Datenträger-Array

     Hinweis: Weitere Informationen zur Konfiguration des VSS-Hardwareanbieters erhalten Sie bei Ihrem Hardwareanbieter.
   - Auf dem Hyper-V-Server und dem Proxy-Server muss jeweils eine ähnliche Betriebssystemversion installiert sein.
   - Wenn der Hyper-V-Server zu einem Cluster gehört, sollte der Proxy-Server nicht Teil des Hyper-V-Clusters sein.
2. Melden Sie sich bei der Konsole an, und erstellen Sie einen Sicherungsplan.

   Hinweis: Weitere Informationen zur Erstellung eines agentenlosen Sicherungsplans finden Sie unter So erstellen Sie einen hostbasierten agentenlosen Sicherungsplan.
3. Stellen Sie sicher, dass Sie auf der Registerkarte **Erweitert** die Option **So oft wie möglich Hardware-Snapshot verwenden** ausgewählt haben.

   Hinweis: Um eine Sicherung nur aus einem Hardware-Snapshot (nicht aus einem Software-Snapshot) durchzuführen, bietet Arcserve UDP den folgenden Registrierungsschlüssel: *FallbackToSWSnapshot =0(dword)*

   Sie können diesen Registrierungsschlüssel für einen bestimmten Knoten sowie alle Knoten anwenden.
   - Um einen bestimmten Knoten zu beantragen, erstellen Sie die Registrierung unter HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\(Nodeid).

     Hinweis: (Nodeid) wird nur nach einer Sicherung erstellt.

- Um alle Knoten zu beantragen, erstellen Sie die Registrierung unter HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll.

Wichtig! Wenn der Unterschlüssel "AFBackupDll" nicht verfügbar ist, müssen Sie den Unterschlüssel *AFBackupDll* unter engine als Engine\AFBackupDll\ manuell hinzufügen und dann *DWORD FallbackToSWSnapshot* unter *AFBackupDll* hinzufügen.

4. **Speichern** Sie den Plan und **Übermitteln** Sie den Sicherungsjob.

   Der Sicherungsjob wird mit dem Speicher-Snapshot ausgeführt.

Verwenden von Hardware-Snapshots für die agentenbasierte Sicherung

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

   - Installieren Sie einen VSS-Hardwareanbieter, der Hardware-Snapshots auf den Arcserve UDP-Agenten unterstützt. Die typische Konfiguration eines VSS-Hardwareanbieters umfasst:

     - Angeben eines Servers, der die LUN steuert.
     - Angeben der Anmeldeinformationen des Datenträger-Arrays für den Zugriff auf das Datenträger-Array.

     Hinweis: Weitere Informationen zur Konfiguration des VSS-Hardwareanbieters erhalten Sie beim Hersteller des Hardwareanbieters.

2. Melden Sie sich bei der Konsole an, und erstellen Sie einen Sicherungsplan.

   Hinweis: Weitere Informationen zum Erstellen eines agentenbasierten Plans für Windows finden Sie unter So erstellen Sie einen Sicherungsplan für Windows.

3. Stellen Sie sicher, dass Sie auf der Registerkarte **Erweitert** die Option **So oft wie möglich Hardware-Snapshot verwenden** ausgewählt haben.

4. Speichern Sie den Plan, und übergeben Sie den Sicherungsjob.

   Der Sicherungsjob wird mit dem Speicher-Snapshot ausgeführt.

Überprüfen, ob die Sicherung Hardware-Snapshots verwendet hat

Wenn die Voraussetzungen für einen Hardware-Snapshot nicht erfüllt sind, kehrt Arcserve UDP automatisch zum Software-Snapshot zurück, ohne dass der Sicherungsjob fehlschlägt. Wenn der Hardware-Snapshot fehlschlägt, wird das Ereignis in den Aktivitätsprotokollen aufgezeichnet.

Überprüfen Sie die Protokollmeldungen, um sicherzustellen, dass die Sicherung den Hardware-Snapshot verwendet hat.

Gehen Sie wie folgt vor:

1. Navigieren Sie zum folgenden Pfad:

   <Installationsordner>\Arcserve\Unified Data Protection\Engine\Logs

2. Öffnen Sie die entsprechende Datei für die jeweilige Job-ID.

   Wenn die Job-ID z. B. JW002 lautet, navigieren Sie zum Ordner **Protokolle**, und öffnen Sie die Datei JW002.

3. Überprüfen Sie die Nachrichten in der Datei, um zu überprüfen, ob die Sicherung den Speicher-Snapshot verwendet hat.

   Sie haben erfolgreich den Speicher-Snapshot für eine Sicherung verwendet.

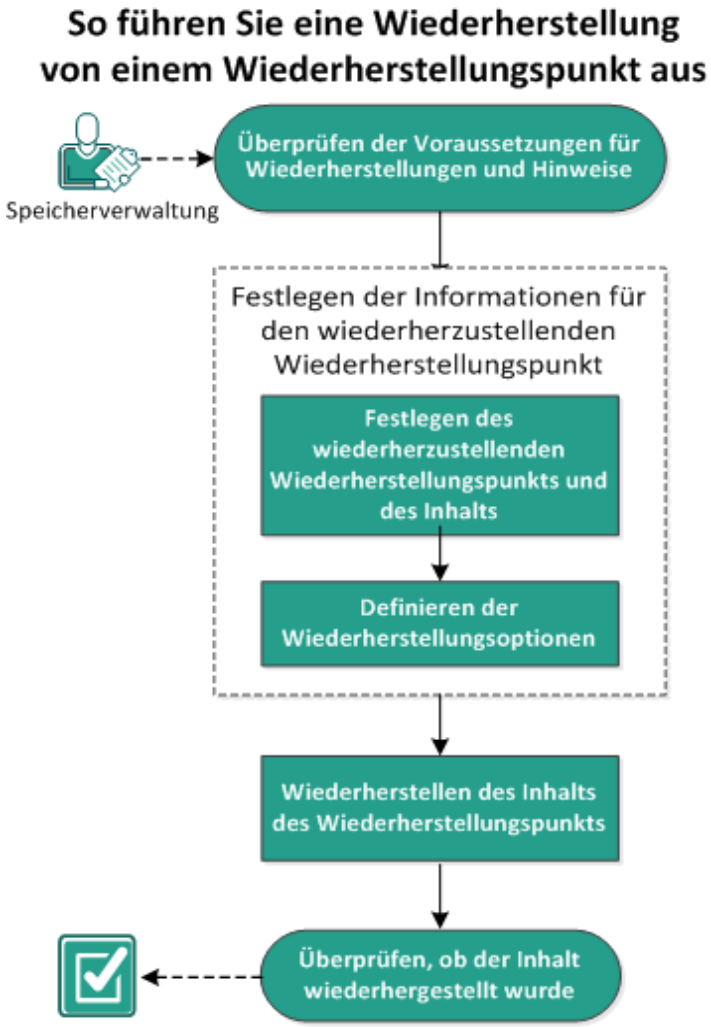
Kapitel 13: Wiederherstellen von geschützten Daten

In diesem Abschnitt werden die folgenden Themen behandelt:

So führen Sie eine Wiederherstellung von einem Wiederherstellungspunkt aus

Jedes Mal, wenn Arcserve UDP eine erfolgreiche Sicherung ausführt, wird gleichzeitig ein Snapshot-Image Ihrer Sicherung (ein Wiederherstellungspunkt) erstellt. Diese Sammlung an Wiederherstellungspunkten ermöglicht es Ihnen, das Sicherungs-Image, das Sie wiederherstellen möchten, zu finden und genau anzugeben. Wenn Sie zu einem späteren Zeitpunkt den Verdacht haben, dass gesicherte Informationen verloren gegangen, korrupt oder nicht zuverlässig sein könnten, können Sie diese Informationen suchen und aus einer früheren Version wiederherstellen, deren Qualität außer Frage steht.

Das folgende Diagramm veranschaulicht den Prozess für das Wiederherstellen von einem Wiederherstellungspunkt aus:



Führen Sie die folgenden Aufgaben aus, um von einem Wiederherstellungspunkt aus wiederherzustellen:

1. Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise
2. Festlegen der Informationen für den wiederherzustellenden Wiederherstellungspunkt
    a. Festlegen des wiederherzustellenden Wiederherstellungspunkts und des Inhalts
    b. Definieren der Wiederherstellungsoptionen
3. Wiederherstellen des Inhalts des Wiederherstellungspunkts
4. Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Wiederherstellung ausführen:

- Sie haben mindestens einen Wiederherstellungspunkt zur Wiederherstellung zur Verfügung.
- Sie haben ein gültiges und zugreifbares Wiederherstellungspunktziel, von dem aus Sie den Inhalt des Wiederherstellungspunkts wiederherstellen können.
- Sie haben einen gültigen und zugreifbaren Zielspeicherort, auf dem Sie den Inhalt des Wiederherstellungspunkts wiederherstellen können.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Überprüfen Sie die folgenden Wiederherstellungshinweise:

- Wenn die Wiederherstellung auf einem Remote-Ziel erfolgt und alle Laufwerksbuchstaben (A - Z) besetzt sind, gelingt die Wiederherstellung auf einem Remote-Pfad nicht. Arcserve UDP Agent (Windows) benötigt einen Laufwerksbuchstaben, um den Pfad des Remote-Ziels zu laden.
- (Optional) Erfahren Sie, wie die Wiederherstellung funktioniert. Weitere Informationen erhalten Sie unter Funktionsweise von Wiederherstellungen auf Dateiebene.
- (Optional) Überprüfen Sie die Dateien, die während der Wiederherstellung übersprungen wurden. Weitere Informationen finden Sie unter "Dateien, die während der Wiederherstellung übersprungen wurden".
- Wenn Sie versuchen, eine optimierte Sicherungssitzung auf einem nichtleeren Volume (unoptimierte Wiederherstellung) wiederherzustellen, kann der Wiederherstellungsjob mehr Zeit kosten als die geschätzte Zeit, die im Job-Monitor angezeigt wird. Die Datenmenge, die bearbeitet wird, und die vergangene Zeit können größer werden auf der Basis der Daten, die auf dem Volume optimiert werden.

Beispiel:

Die Sicherungsvolumegröße beträgt 100 GB und nach Optimierung ist die Volumegröße auf 50 GB reduziert.

Wenn Sie eine unoptimierte Wiederherstellung dieses Volume ausführen, zeigt der Wiederherstellungsjob-Monitor 100 % an, nachdem er 50 GB wiederhergestellt hat, aber es dauert länger, um die ganzen 100 GB wiederherzustellen.

- Folgende Aktivitätsprotokollmeldung wird angezeigt, wenn die Systemdateien wiederhergestellt werden:

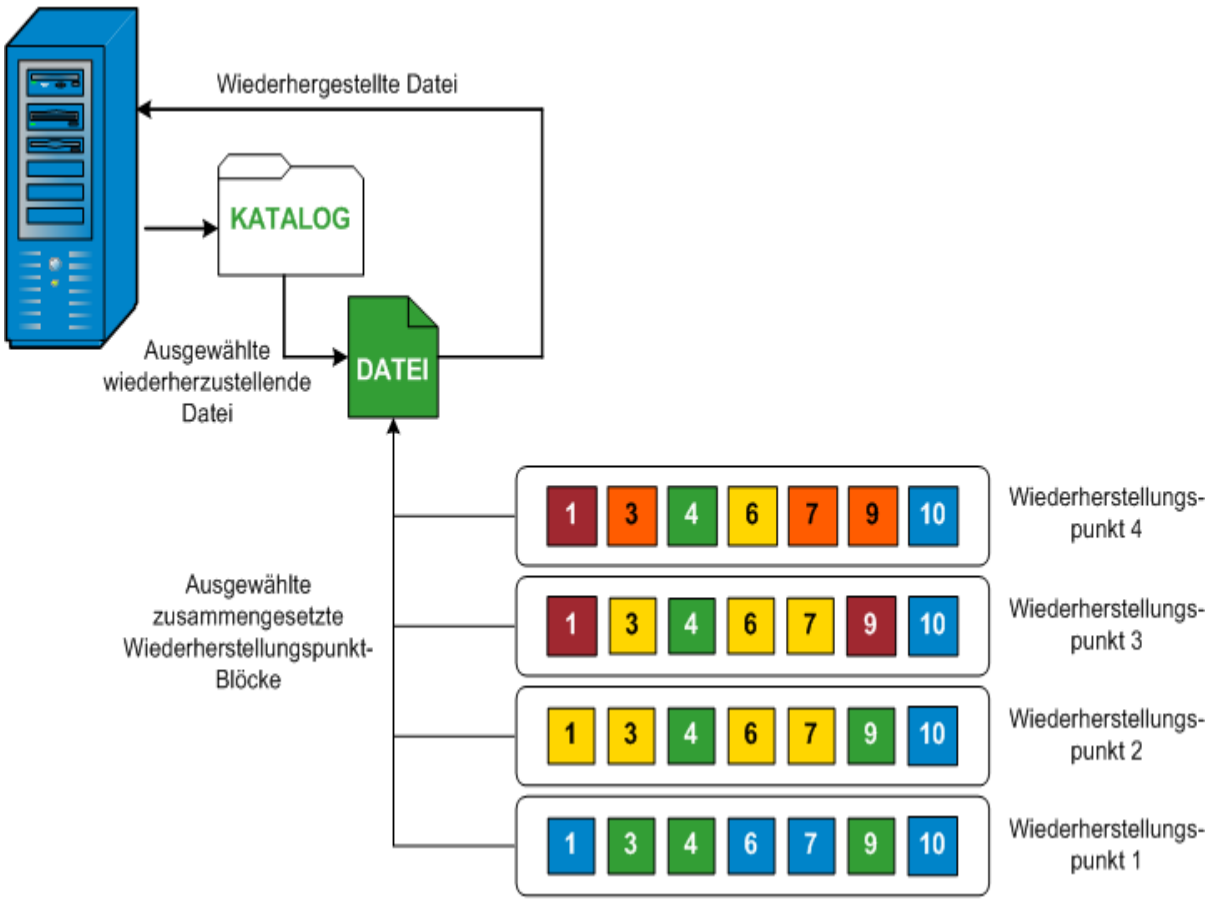
  "Systemdateien wurden übersprungen. Im Bedarfsfall können Sie die Option "Bare-Metal-Recovery (BMR)" verwenden, um sie wiederherzustellen."

Funktionsweise von Wiederherstellungen auf Dateiebene

Bei einer Sicherung auf Blockebene besteht jede gesicherte Datei aus mehreren erfassten Blöcken, die sie definieren. Zusätzlich wird eine Katalogdatei mit einer Liste der gesicherten Dateien, der einzelnen Blöcke, die für jede Datei verwendet wurden, und der Wiederherstellungspunkte, die für diese Datei zur Verfügung stehen, erstellt. Wenn Sie eine bestimmte Datei wiederherstellen möchten, können Sie Ihre Sicherung durchsuchen, um die Datei und den Wiederherstellungspunkt auszuwählen. Arcserve UDP erfasst die Versionen der Blöcke, die für den Wiederherstellungspunkt der ausgewählten Datei verwendet wurden, fasst sie zusammen und stellt die Datei wieder her.

Hinweis: Sie können auch Wiederherstellungen ohne Katalogdateien von katalogLosen Sicherungs-Wiederherstellungspunkten ausführen.

Das folgende Ablaufschema veranschaulicht den Prozess, mit dem Arcserve UDP eine spezifische Datei wiederherstellt:



Dateien, die während der Wiederherstellung übersprungen wurden

Bei Wiederherstellungen mit Arcserve UDP Agent (Windows) werden bestimmte Dateien möglicherweise absichtlich übersprungen.

Die Dateien und Ordner in der folgenden Tabelle werden während einer Wiederherstellung übersprungen, wenn die folgenden zwei Bedingungen vorhanden sind:

- Dateien werden übersprungen, wenn solche Dateien vor der Wiederherstellung vorhanden sind und die Konfliktoption "Vorhandene Dateien überspringen" ist.
- Dateien und Ordner, die in der folgenden Tabelle aufgelistet sind, werden übersprungen, weil sie keine wichtige Komponente für Windows oder Arcserve UDP Agent (Windows) sind.

BS	Ordner oder Speicherort	Datei oder Ordnername	Bemerkungen
Alle	Stammordner von jedem Volume	CAVolTrc.dat	Wird von dem Arcserve UDP-Treiber für die Nachverfolgung verwendet.
		cavoltrcsnapshot.dat	
		System Volume Information*	Wird verwendet, um Dateien/Ordner von einem Windows-System zu speichern, zum Beispiel Volume-Schattenkopie-Dateien.
		RECYCLER*	Wird nur auf NTFS-Partitionen verwendet. Es enthält einen Papierkorb für jeden Benutzer, der sich beim Computer anmeldet, sortiert nach Sicherheitskennung (SID).
		$Recycle.Bin*	Wenn Sie eine Datei in Windows NT Explorer oder im Arbeitsplatz löschen, dann wird die Datei im Papierkorb gespeichert, bis Sie den Papierkorb leeren oder die Datei wiederherstellen.
	Alle Ordner enthalten Bilddateien	Thumbs.db	Speichert Miniaturansicht -Bilder für Windows Explorer Miniaturansicht.
	Stammordner des Volume	PageFile.sys	Windows-Auslagerungsdatei des virtuellen Speichers.
		Hiberfil.sys	Ruhezustanddatei wird verwendet, um die Systemdaten zu speichern, wenn ein Computer in den Ruhezustand geht.

Die folgenden Dateien und Ordner werden nur übersprungen, wenn Sie eine Wiederherstellung am ursprünglichen Speicherort durchführen:

BS	Ordner oder Speicherort	Datei oder	Bemerkung

		Ordnername	
Alle	Der Ordner ist im Wertdatensatz hier angegeben: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Alle Dateien/Ordner (rekursiv)	Der Ordner enthält eine zwischengespeicherte DLL-Datei, die für SFC (System File Checker) verwendet wird, und die Inhalte des Verzeichnisses des System-DLL-Cache werden mithilfe von SFC neu erstellt.
	%SystemRoot%\SYSTEM32\dllCache		
	Stammordner von quorum_device	MSCS*	Wird für Microsoft Cluster Server verwendet.
	%SystemRoot%\SYSTEM32\	perf?00?.dat	Leistungsdaten, die vom Windows-Leistungsindikator verwendet werden.
		perf?00?.bak	
		CATROOT*	Wird für WFP (Windows File Protection) verwendet. Es werden digitale Signaturen der Betriebssystemteminstallationen (wie z. B. DLL, EXE, SYS, OCX usw.) erfasst, um sie vor Löschung oder vor Ersatz von älteren Versionen zu schützen.
	%SystemRoot%\inetsrv\	metabase.bin	Binäre Metabasis-Datei von früheren IIS-Versionen vor 6.0.
	Datei oder Ordner, der im Wert angegeben ist, mit Ausnahme von "Gemeinsamer SIS-Speicher" unter	Alle Dateien/Ordner	Dateien und Ordner sollten nicht

	"HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup"	(rekursiv)	gesichert und nicht wiederhergestellt werden. Weitere Informationen finden Sie unter Link.
XP W2-003	System-Volume	NTLDR	Der Haupt-Boot-Loader.
		BOOT.INI	Enthält die Boot-Konfiguration (falls nicht vorhanden, wird NTLDR standardmäßig auf \Windows auf der ersten Partition der ersten Festplatte gesetzt).
		NTDETECT.COM	Ist erforderlich, um ein NT-basiertes BS zu starten. Erkennt grundlegende Hardware-Informationen, die für einen erfolgreichen Start erforderlich sind.
Vista und höher	Stammordner des System-Volume	boot*	Boot-Ordner für Windows.
		bootmgr	Datei "Windows-Start-Manager"
		EFI\Microsoft\Boot*	Wird für EFI-Boot verwendet.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Speichert ETW-Ablaufverfolgungsdateien (mit der Erweiterung .etl) für Ablaufverfolgungssitzungen

			der Ereignisse in Echtzeit.
		con-fig\RegBack*	Sicherung der aktuellen Regis-trierungstabelle.
Win-8 und höh-er	System-Volume	swapfile.sys	Systemcontroller-Datei, nor-malerweise ca. 256 MB. Wird von Anwendungen im Metro-Stil ver-wendet, die nicht in die her-kömmlichen Paging-Merkmale (wie z. B. Ver-wendungsmuster, Wachstum, Reser-vierung von Spei-cherplatz) von pagefile.sys pas-sen.
		BOOTNXT	Wird verwendet, um von einem BS aus zu starten, das nicht Windows 8 ist. Wird erstellt, wenn die Start-optionen aktiviert werden, und wird von Windows aktualisiert.

Das Aktivitätsprotokoll stellt folgende Informationen bereit:

- Datums- und Uhrzeitinformationen: jobxxxx Systemdateien wurden über-sprungen. Sie können bei Bedarf die Bare-Metal-Recovery-Option (BMR) ver-wenden, um sie wiederherzustellen.
- Datums- und Uhrzeitinformationen: jobxxxx Dateien oder Verzeichnisse wur-den übersprungen. Übersprungene Dateien oder Verzeichnisse finden Sie hier: C:\Programme\Arcserve\Unified Data Protection\Engine\Logs\Restore-<JJJJMMTT>-<hhmmss>-<Prozess-ID>-<Job-ID>.log.

Festlegen der Informationen für den wiederherzustellenden Wiederherstellungspunkt

Arcserve UDP bietet eine Option zur Wiederherstellung von Daten von einem Wiederherstellungspunkt. Das Ziel eines Wiederherstellungsjobs besteht darin, schnell zu erkennen, welche Daten benötigt werden, und sie vom entsprechenden Sicherungsdatenträger abzurufen. Für jeden Wiederherstellungsjob ist eine Quelle und ein Ziel erforderlich.

Der Prozess für das Wiederherstellen von einem Wiederherstellungspunkt aus verläuft folgendermaßen:

1. Festlegen des wiederherzustellenden Wiederherstellungspunkts und des Inhalts
2. Definieren der Wiederherstellungsoptionen

Festlegen des wiederherzustellenden Wiederherstellungspunkts und des Inhalts

Dieser Abschnitt enthält Informationen über die Vorgehensweise zum Angeben des Wiederherstellungspunkts und des wiederherzustellenden Inhalts.

Gehen Sie wie folgt vor:

1. Verwenden Sie eines der folgenden Verfahren, um auf das Dialogfeld zur Auswahl der Wiederherstellungsmethoden zuzugreifen:

   Über die Arcserve UDP-Konsole:

   a. Melden Sie sich bei der Arcserve UDP-Konsole an.

   b. Navigieren Sie zu **Ressourcen** > **Knoten** > **Alle Knoten**.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   c. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie dann **Wiederherstellen** aus.

      Sie werden automatisch bei der Konsole des Agentenknotens angemeldet, und das Dialogfeld "Wiederherstellen" wird geöffnet.

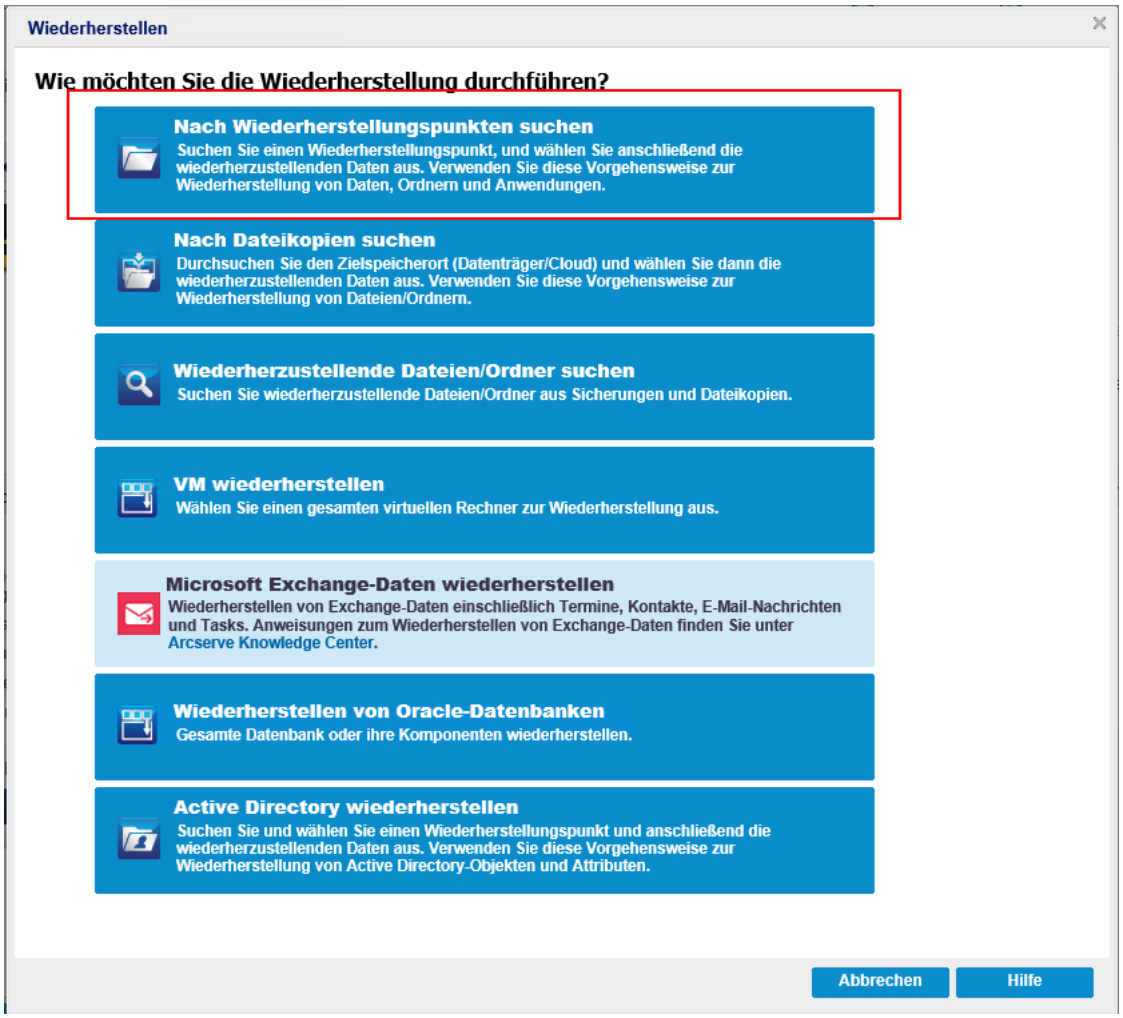
   In Arcserve UDP Agent (Windows):

   a. Melden Sie sich bei Arcserve UDP Agent (Windows) an.

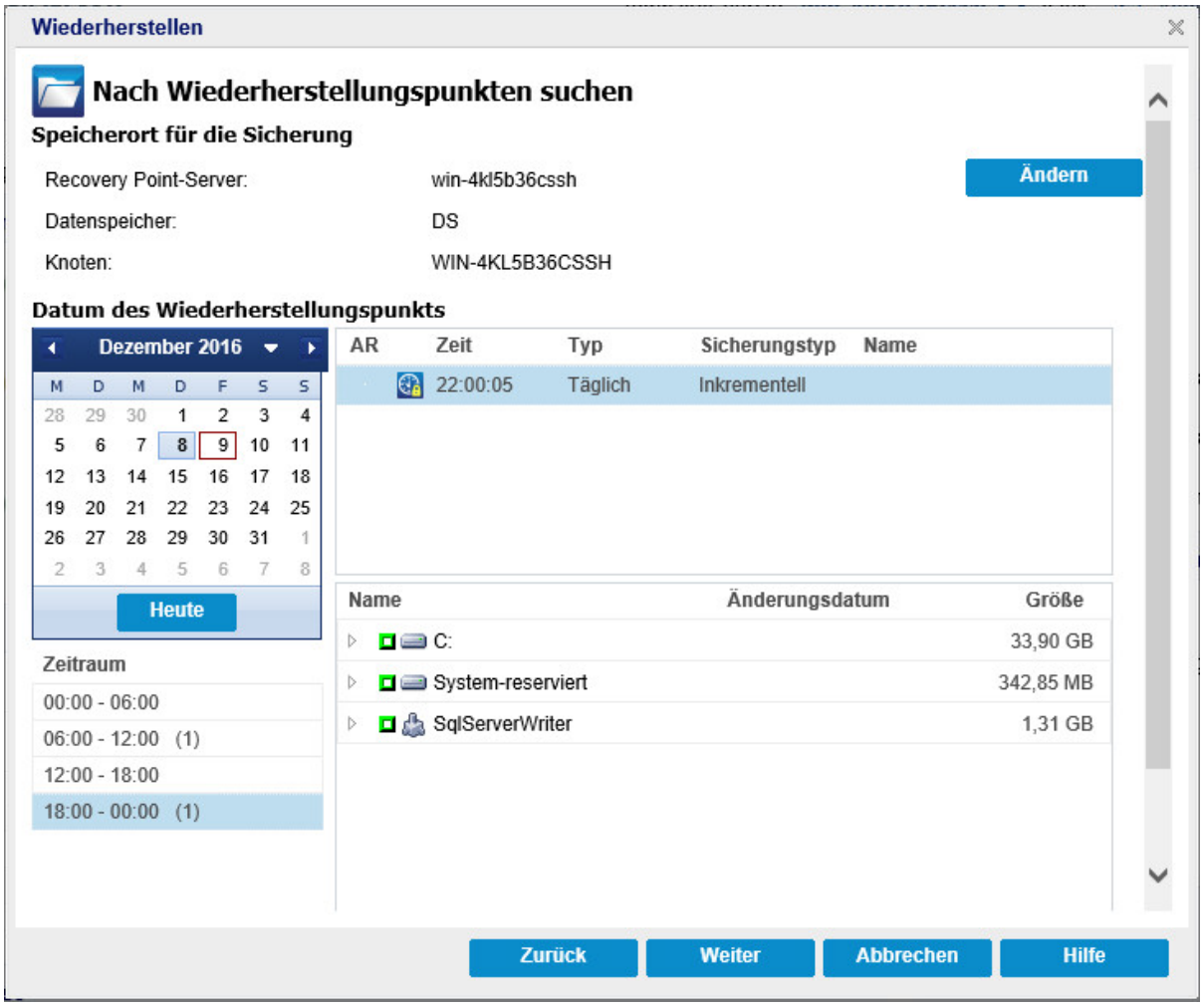
   b. Wählen Sie auf der Startseite **Wiederherstellen** aus.

      Das Dialogfeld Wiederherstellen wird geöffnet.

2. Klicken Sie im Dialogfeld "Wiederherstellen" auf **Nach Wiederherstellungspunkten suchen**.



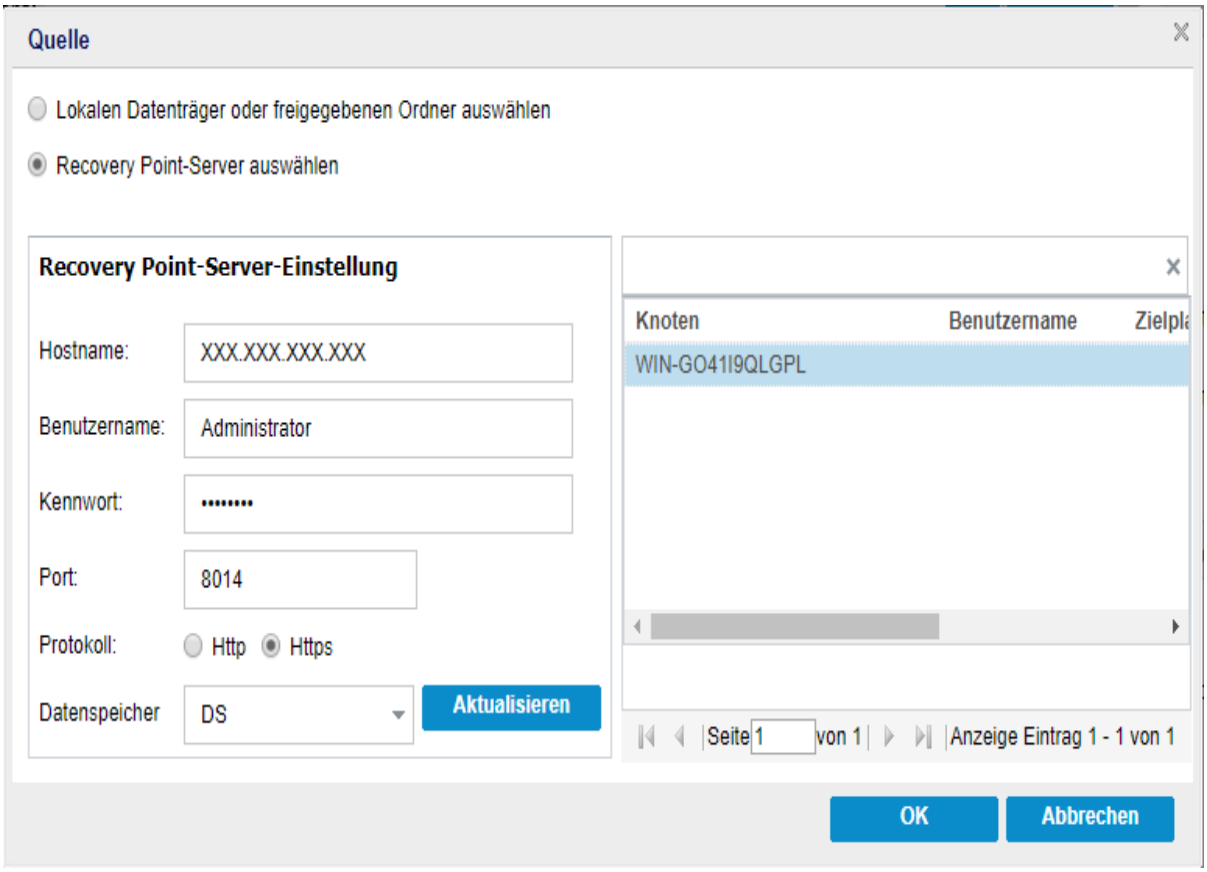
3. Gehen Sie auf der Seite "Nach Wiederherstellungspunkten suchen" folgendermaßen vor:



a. Klicken Sie auf **Ändern**, um den Speicherort für die Sicherung zu aktualisieren.

   Das Dialogfeld Quelle wird geöffnet.

b. Wählen Sie im Dialogfeld "Quelle" einen der folgenden Speicherorte für die Sicherung aus, und klicken Sie dann auf **OK**:



Lokalen Datenträger oder freigegebenen Ordner auswählen

1. Legen Sie den Speicherort fest, unter dem Ihre Sicherungs-Images gespeichert werden, und wählen Sie die entsprechende Sicherungsquelle aus.
2. Um die Verbindung zum angegebenen Speicherort zu überprüfen, klicken Sie auf die Schaltfläche mit dem grünen Pfeil. Falls erforderlich, geben Sie den Benutzernamen und das Kennwort für den Zugriff auf diesen Quellspeicherort ein.

   Das Dialogfeld "Speicherort für die Sicherung auswählen" wird geöffnet.
3. Wählen Sie den Ordner aus, in dem die Wiederherstellungspunkte gespeichert sind, und klicken Sie dann auf **OK**.

   Das Dialogfeld "Speicherort für die Sicherung auswählen" wird geschlossen, und der Sicherungsspeicherort wird im Dialogfeld "Quelle" angezeigt.

   Die Wiederherstellungspunkte werden im Dialogfeld Nach Wiederherstellungspunkten suchen aufgelistet.

Auswählen des Recovery Point-Servers

1. Geben Sie die Details für die Einstellungen des Recovery Point Servers an, und klicken Sie dann auf **Aktualisieren**.

   Alle Agenten werden in der Spalte "Data Protection Agent" im Dialogfeld Quelle aufgelistet.

2. Wählen Sie den Agenten in der angezeigten Liste aus.

   Die Wiederherstellungspunkte werden im Dialogfeld "Nach Wiederherstellungspunkten suchen" aufgelistet.

c. Geben Sie das Datum des Sicherungs-Images an, das Sie wiederherstellen möchten.

   Alle Daten, die Wiederherstellungspunkte für die angegebene Sicherungsquelle enthalten, werden grün hervorgehoben.

   Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp (vollständige Sicherung, Zuwachssicherung oder Überprüfungssicherung) und der Name der Sicherung angezeigt.

d. Wählen Sie einen wiederherzustellenden Wiederherstellungspunkt aus.

   Der Sicherungsinhalt (einschließlich aller Anwendungen) für die ausgewählten Wiederherstellungspunkte wird angezeigt.

   Hinweis: Wenn eine Uhr mit einem Schlosssymbol angezeigt wird, bedeutet dies, dass der Wiederherstellungspunkt verschlüsselte Informationen enthält und möglicherweise ein Kennwort zur Wiederherstellung benötigt wird.

e. Wählen Sie den wiederherzustellenden Inhalt aus.

   - Bei einer Wiederherstellung auf Volume-Ebene können Sie angeben, ob das gesamte Volume oder ausgewählte Dateien/Ordner wiederhergestellt werden sollen.
   - Bei einer Wiederherstellung auf Anwendungsebene können Sie festlegen, ob die gesamte Anwendung, oder ausgewählte Komponenten, Datenbanken, Instanzen etc. wiederhergestellt werden sollen.

4. Klicken Sie auf **Weiter**.

   Das Dialogfeld Wiederherstellungsoptionen wird geöffnet.

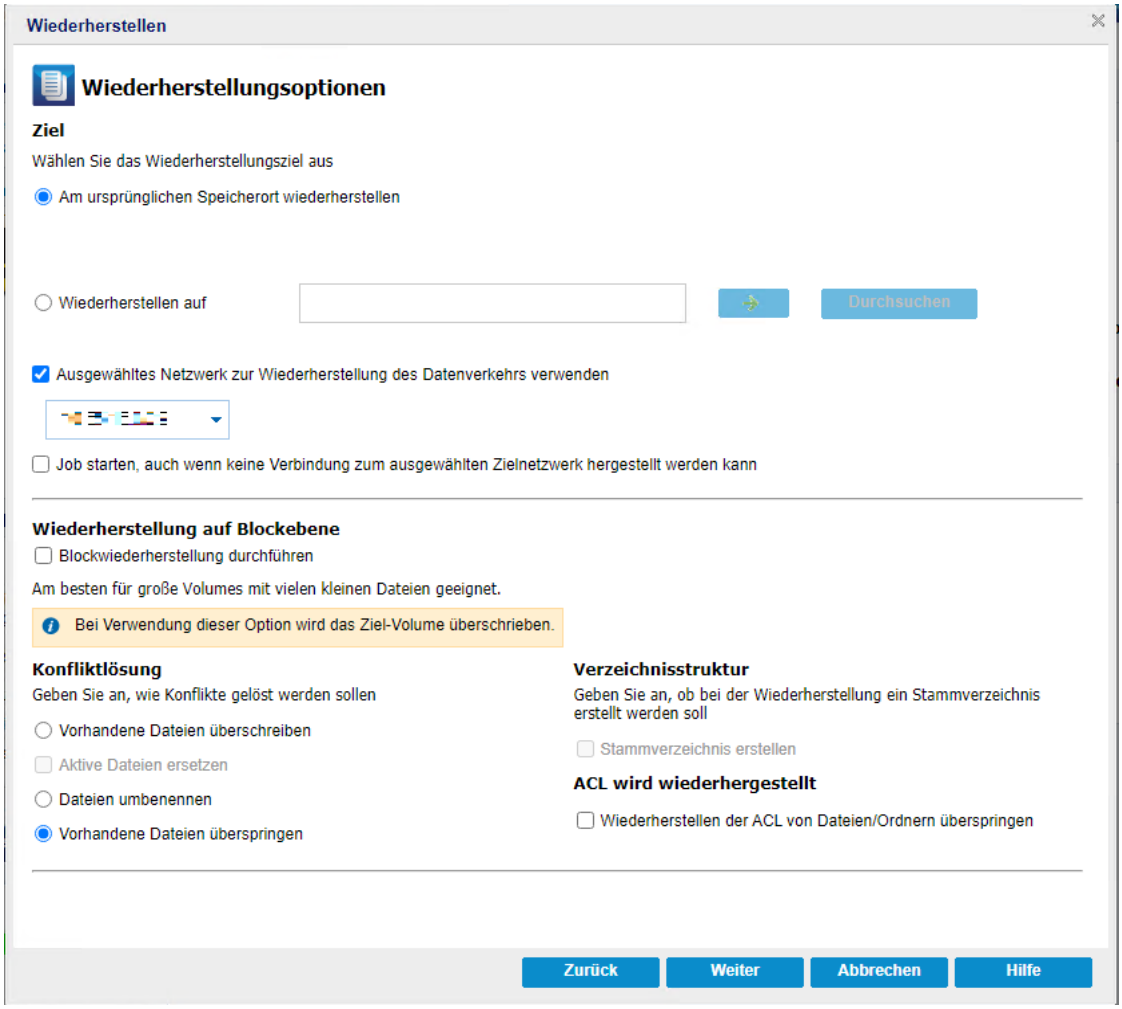
   Wiederherstellungspunkt und wiederherzustellender Inhalt werden festgelegt.

Definieren der Wiederherstellungsoptionen

Nachdem Sie Wiederherstellungspunkt und wiederherzustellenden Inhalt festgelegt haben, definieren Sie die Kopieroptionen für den ausgewählten Wiederherstellungspunkt. In diesem Abschnitt wird erläutert, wie Sie die Wiederherstellungsoptionen für den ausgewählten Wiederherstellungspunkt definieren.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld Wiederherstellungsoptionen das Wiederherstellungsziel aus.



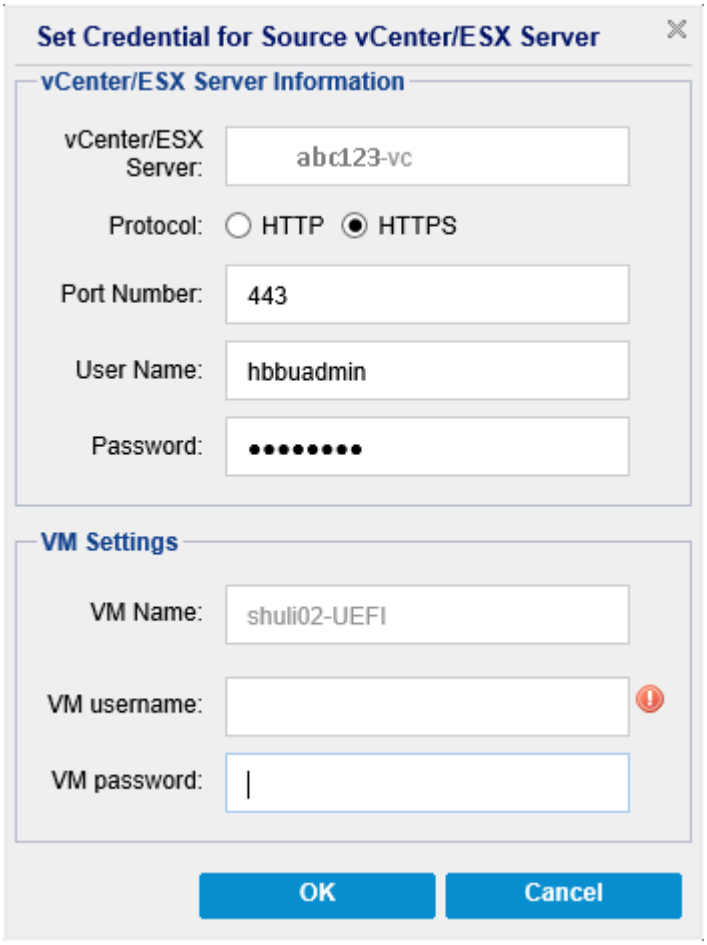
Es sind folgende Zieloptionen verfügbar:

Am ursprünglichen Speicherort wiederherstellen

Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

Hinweis: Wenn Sie die Recovery Point-Sicherung mithilfe der hostbasierten agentenlosen Sicherung durchgeführt haben, wird die Datei bei der Wiederherstellung am ursprünglichen Speicherort auf dem virtuellen Rechner wiederhergestellt. In diesem Fall wird ein Dialogfeld geöffnet. Sie können die Anmeldeinformationen des Hypervisors und des Betriebssystems des virtuellen Rechners eingeben.

Für VMware-VM:



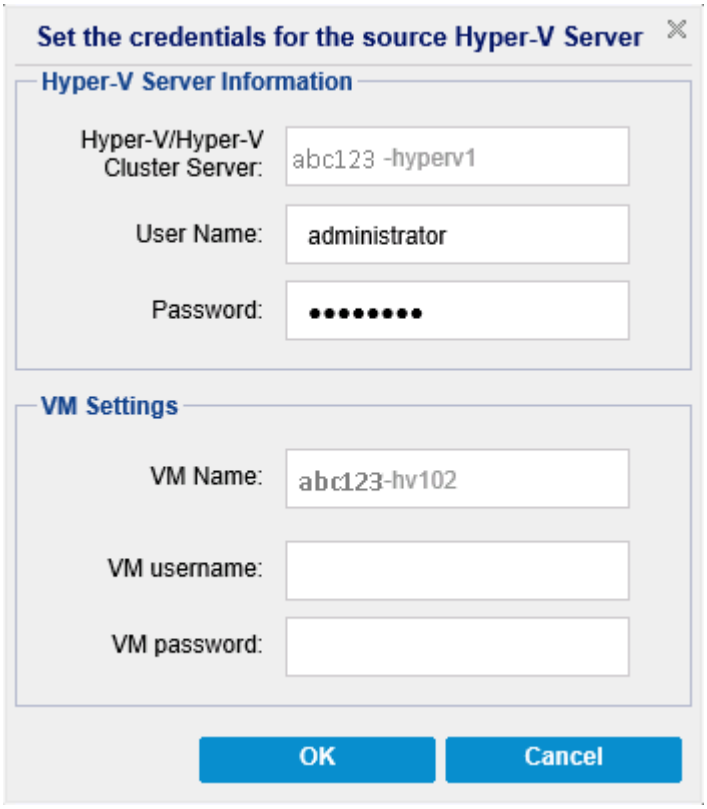
Hinweis: Um Dateien innerhalb der VM zu erstellen oder zu schreiben, beachten Sie die folgenden Anforderungen für die Einstellungen und die Kontoberechtigung des virtuellen Rechners:

- VMware-Tools ist installiert und wird ausgeführt.
- Firewall muss Datei- und Druckerfreigabe zulassen.
- Das Konto ist ein integrierter lokaler Administrator, integrierter Domänenadministrator oder ein Domänenkonto, das Mitglied der lokalen Administratorengruppe ist. Wenn andere Konten verwendet werden, gehen Sie folgendermaßen vor:

- Deaktivieren Sie den Remote-Zugriff auf UAC. Informationen zum Deaktivieren des Remote-Zugriffs auf UAC finden Sie in Importieren von virtuellen Rechnern mit einem zusätzlichen Administratorkonto.
- Deaktivieren Sie UAC in der lokalen Sicherheitsrichtlinie, indem Sie die Einstellung zur Ausführung aller Administratoren im Administrator-Genehmigungsmodus unter secpol.msc-> lokale Richtlinien-> Sicherheitsoptionen deaktivieren. (Secpol.msc ist der Editor für Sicherheitsrichtlinien von Microsoft).

  Wichtig! Versuchen Sie nicht, die UAC im Dialogfeld "Einstellungen zur Benutzerkontensteuerung" zu deaktivieren, das über die Systemsteuerung geöffnet wird.

Für Hyper-V-VM:



Hinweis: Um Dateien innerhalb der VM zu erstellen oder zu schreiben, beachten Sie die folgenden Anforderungen für die Einstellungen und die Kontoberechtigung des virtuellen Rechners:

- Hyper-V-Integrationsdienste sind installiert und werden ausgeführt.

- Firewall muss Datei- und Druckerfreigabe zulassen.
- Das Konto ist ein integrierter lokaler Administrator, integrierter Domänenadministrator oder ein Domänenkonto, das Mitglied der lokalen Administratorengruppe ist. Wenn andere Konten verwendet werden, deaktivieren Sie den Remote-Zugriff auf UAC. Informationen zum Deaktivieren des Remote-Zugriffs auf UAC finden Sie in Importieren von virtuellen Rechnern mit einem zusätzlichen Administratorkonto.
- Wenn das VM-Gast-BS Clientversion-Windows (z. B. Windows 10) ist, muss Firewall manuell so konfiguriert werden, dass Windows-Verwaltungsinstrumentation (WMI) zugelassen wird.

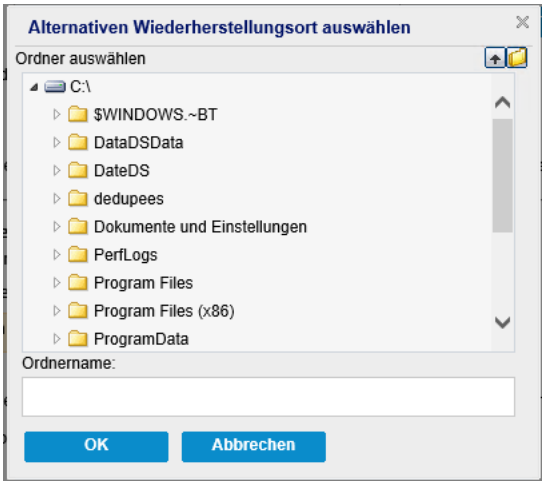
Wiederherstellen auf

Stellt am angegebenen Speicherort wieder her. Gehen Sie folgendermaßen vor, um die Daten am angegebenen Speicherort wiederherzustellen:

- Klicken Sie auf **Durchsuchen**, um das Ziel anzugeben.

  Das Dialogfeld "Alternativen Wiederherstellungsort auswählen" wird angezeigt.

- Wählen Sie den vorhandenen Ordner aus, oder erstellen Sie einen neuen Ordner nach Bedarf, und klicken Sie dann auf **OK**.



- Um die Verbindung zum angegebenen Speicherort zu überprüfen, klicken Sie auf die Schaltfläche mit dem grünen Pfeil. Falls erforderlich, geben Sie den Benutzernamen und das Kennwort ein, um Zugriff auf diesen Speicherort zu erhalten.

2. (Optional) Um die Kommunikation zwischen Windows-Agent und Recovery Point Server zu aktivieren, aktivieren Sie das Kontrollkästchen **Ausgewähltes Netzwerk**

für Wiederherstellungsdatenverkehr verwenden, und wählen Sie dann das Netzwerk in der Drop-down-Liste aus.

Hinweise:

- Um den Sicherungsjob mit dem verfügbaren Netzwerk oder dem Standardnetzwerk fortzusetzen, falls das ausgewählte Sicherungsnetzwerk nicht zugänglich ist, aktivieren Sie das Kontrollkästchen **Führen Sie den Job weiter aus, selbst wenn keine Verbindung zum ausgewählten Sicherungsnetzwerk hergestellt werden kann**.
- Um die Einschränkung für den SMB-Multichannel zu definieren, sodass die Datenübertragung nur über das ausgewählte Netzwerk übertragen wird, aktivieren Sie das Kontrollkästchen **Dediziertes Ethernet verwenden, wenn der aktuelle Computer SMB Multichannel ermöglicht**.

  Diese Option ist nicht standardmäßig verfügbar. Um diese Option zu aktivieren, erstellen Sie die Zeichenfolgenregistrierung *UseDedicatedEthernet* im folgenden Pfad, und legen Sie dann den Registrierungswert auf 1 fest:

  SOFTWARE\Arcserve\Unified Data Protection\Engine

  - Wenn Sie einen Wiederherstellungsjob über die Seite "Knoten" ausführen, erstellen Sie einen Registrierungsschlüssel auf dem Sicherungs-Proxy.
  - Wenn Sie einen Wiederherstellungsjob vom normalen Agenten mithilfe der RPS-Sicherungssitzung ausführen, erstellen Sie einen Registrierungsschlüssel auf dem normalen Agenten.

3. Um den Durchsatz beim Wiederherstellen eines großen Volumes mit vielen kleinen Dateien zu verbessern, wählen Sie ein Volume aus, und klicken Sie dann unter "Wiederherstellung auf Blockebene" auf das Kontrollkästchen **Blockwiederherstellung durchführen**. Andere Optionen werden deaktiviert, und eine Benachrichtigung wird angezeigt. Um mit der Wiederherstellung der Blockebene fortzufahren, klicken Sie auf **OK**.

Hinweis: Die Daten werden auf dem aktuellen UDP-Agent-Computer wiederhergestellt, und das Zielvolume wird überschrieben. Auf das Zielvolume kann während des Wiederherstellungsauftrags nicht zugegriffen werden.

4. Legen Sie die Option für die Konfliktlösung fest, die von Arcserve UDP ausgeführt werden soll, wenn während der Wiederherstellung Konflikte auftreten.

   Es sind folgende Optionen verfügbar:

   Vorhandene Dateien überschreiben

   Überschreibt (ersetzt) alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind. Alle Objekte werden aus den Sicherungsdateien wiederhergestellt, unabhängig davon, ob sie auf Ihrem Rechner vorhanden sind.

   Aktive Dateien ersetzen

   Ersetzt alle aktiven Dateien nach einem Neustart. Wenn Arcserve UDP Agent (Windows) während eines Wiederherstellungsversuchs entdeckt, dass die vorhandene Datei gerade verwendet wird oder gerade auf sie zugegriffen wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

   Diese Option ist nur verfügbar, wenn Sie die Option **Vorhandene Dateien überschreiben** auswählen.

   Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien im Wiederherstellungsprozess übersprungen.

   Dateien umbenennen

   Erstellt eine neue Datei, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit demselben Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten sind dann in einer neuen Datei wiederhergestellt.

   Vorhandene Dateien überspringen

   Überspringt alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, und überschreibt (ersetzt) sie nicht. Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

   Standard: Vorhandene Dateien überspringen

5. Wenn Sie während der Wiederherstellung ein Stammverzeichnis erstellen möchten, aktivieren Sie unter "Verzeichnisstruktur" das Kontrollkästchen **Stammverzeichnis erstellen**.

Das Kontrollkästchen **Stammverzeichnis erstellen** legt fest, dass Arcserve UDP eine ggf. vorhandene Stammverzeichnisstruktur des erfassten Sicherungs-Images im Zielpfad der Wiederherstellung neu erstellt.

Wenn diese Option nicht ausgewählt wird, wird die Datei oder der Ordner direkt im Zielordner wiederhergestellt.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt" und "C:\Ordner1\Unterordner2\B.txt" erfasst und als Wiederherstellungsziel "D:\Wiederherstellen" ausgewählt.

- Wenn Sie die Wiederherstellung der Dateien "A.txt" und "B.txt" einzeln festgelegt haben, werden die Dateien in "D:\Wiederherstellen\A.txt" und "D:\Wiederherstellen\B.txt" wiederhergestellt (das Stammverzeichnis über der ausgewählten Dateiebene wird nicht wiederhergestellt).
- Wenn Sie eine Wiederherstellung auf "Unterordner2"-Ebene auswählen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Unterordner2\A.txt" und "D:\Wiederherstellen\Unterordner2\B.txt" (das Stammverzeichnis über der ausgewählten Ordnerebene wird nicht wiederhergestellt).

Wenn diese Option ausgewählt wird, wird der gesamte Stammverzeichnispfad für die Dateien/Ordner (einschließlich des Volume-Namens) im Zielordner neu erstellt. Wenn Dateien/Ordner vom selben Volume-Name wiederhergestellt werden sollen, ist dieser Volume-Name nicht im Wiederherstellungsziel-Stammverzeichnispfad enthalten. Wenn Dateien/Ordner von einem anderen Volume-Name wiederhergestellt werden sollen, enthält der Wiederherstellungsziel-Stammverzeichnispfad diesen Volume-Namen.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt", "C:\Ordner1\Unterordner2\B.txt" und E:\Ordner3\Unterordner4\C.txt erfasst und bei der Wiederherstellung "D:\Wiederherstellen" als Wiederherstellungsziel ausgewählt.

- Wenn Sie nur die Datei "A.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Ordner1\Unterordner2\A.txt" (das gesamte Stammverzeichnis wird ohne den Volume-Namen erneut erstellt).
- Wenn Sie die Dateien "A.txt" und "C.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\C\Ordner1\Unterordner2\A.txt" und "D:\Wiederherstellen\ E\Ordner3\Unterordner4\C.txt" (das gesamte Stammverzeichnis wird mit dem Volume-Namen erneut erstellt).

6. Um die ursprüngliche Berechtigung für wiederhergestellte Dateien/Ordner zu überspringen, aktivieren Sie unter "ACL wird wiederhergestellt" das Kontrollkästchen **Wiederherstellen der ACL von Dateien/Ordnern überspringen**. Bei Auswahl dieser Option können Sie stattdessen die Berechtigungen des Zielordners erben. Wenn Sie

diese Option nicht auswählen, werden die ursprünglichen Berechtigungen beibehalten.

7. Geben Sie ggf. im Feld **Sicherungsverschlüsselung oder Schutzkennwort** das Sicherungsverschlüsselungskennwort an, wenn die Daten, die Sie wiederherstellen möchten, verschlüsselt sind.

   Es ist kein Kennwort erforderlich, wenn Sie versuchen, die Wiederherstellung über denselben Arcserve UDP Agent (Windows)-Rechner durchzuführen, auf dem die verschlüsselte Sicherung ausgeführt wurde. Wenn Sie jedoch versuchen, die Wiederherstellung über einen anderen Arcserve UDP Agent (Windows)-Rechner durchzuführen, ist ein Kennwort erforderlich.

   Hinweis: Wenn eine Uhr mit einem Schlosssymbol angezeigt wird, bedeutet dies, dass der Wiederherstellungspunkt verschlüsselte Informationen enthält und möglicherweise ein Kennwort zur Wiederherstellung benötigt wird.

8. Klicken Sie auf **Weiter**.

   Die Seite "Wiederherstellungs-Übersicht" wird geöffnet.

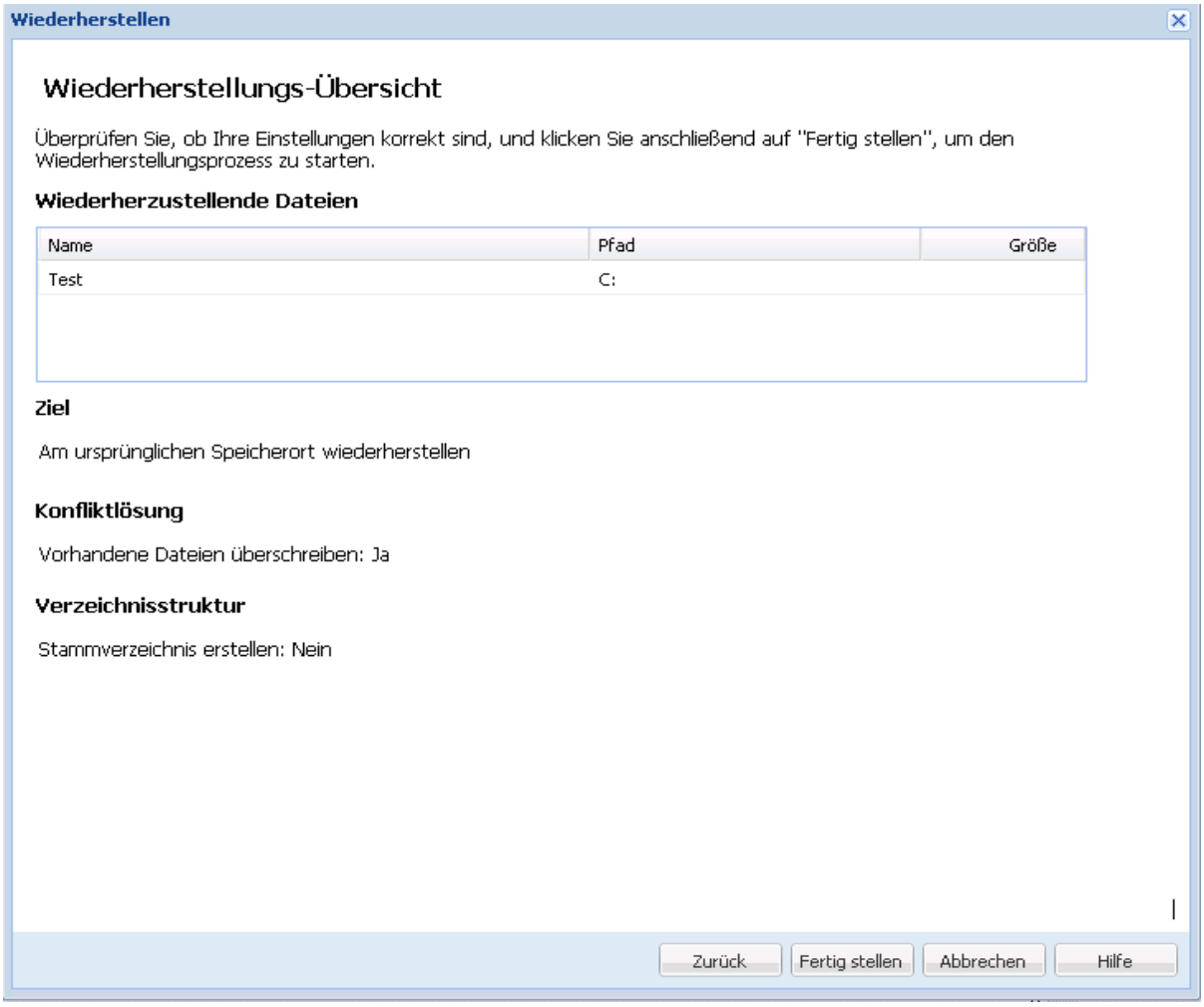
   Die Wiederherstellungsoptionen sind für die Wiederherstellung von einem Wiederherstellungspunkt aus festgelegt.

Wiederherstellen des Inhalts des Wiederherstellungspunkts

Nachdem Sie die Wiederherstellungsoptionen definiert haben, überprüfen Sie, dass Ihre Einstellungen korrekt sind, und bestätigen Sie den Wiederherstellungsprozess. Die Seite "Wiederherstellungs-Übersicht" ist hilfreich, um sämtliche Wiederherstellungsoptionen, die Sie festgelegt haben, zu überprüfen und bei Bedarf zu ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Informationen im Dialogfeld Wiederherstellungsübersicht, um die Richtigkeit aller Wiederherstellungsoptionen und Einstellungen sicherzustellen.



2. Wählen Sie eine der folgenden Vorgehensweisen:

- Wenn die Übersichtsinformationen Fehler enthalten, klicken Sie auf **Zurück**, und ändern Sie die inkorrekten Einstellungen im entsprechenden Dialogfeld.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsprozess zu starten.

Der Wiederherstellungspunktinhalt wurde wiederhergestellt.

Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen Sie nach dem Abschluss der Wiederherstellung, ob der Inhalt auf dem angegebenen Ziel wiederhergestellt wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie in der Arcserve UDP-Konsole zu **Jobs** > **Jobs erfolgreich abgeschlossen**.

   Die Liste der abgeschlossenen Sicherungsjobs wird im mittleren Fensterbereich angezeigt.

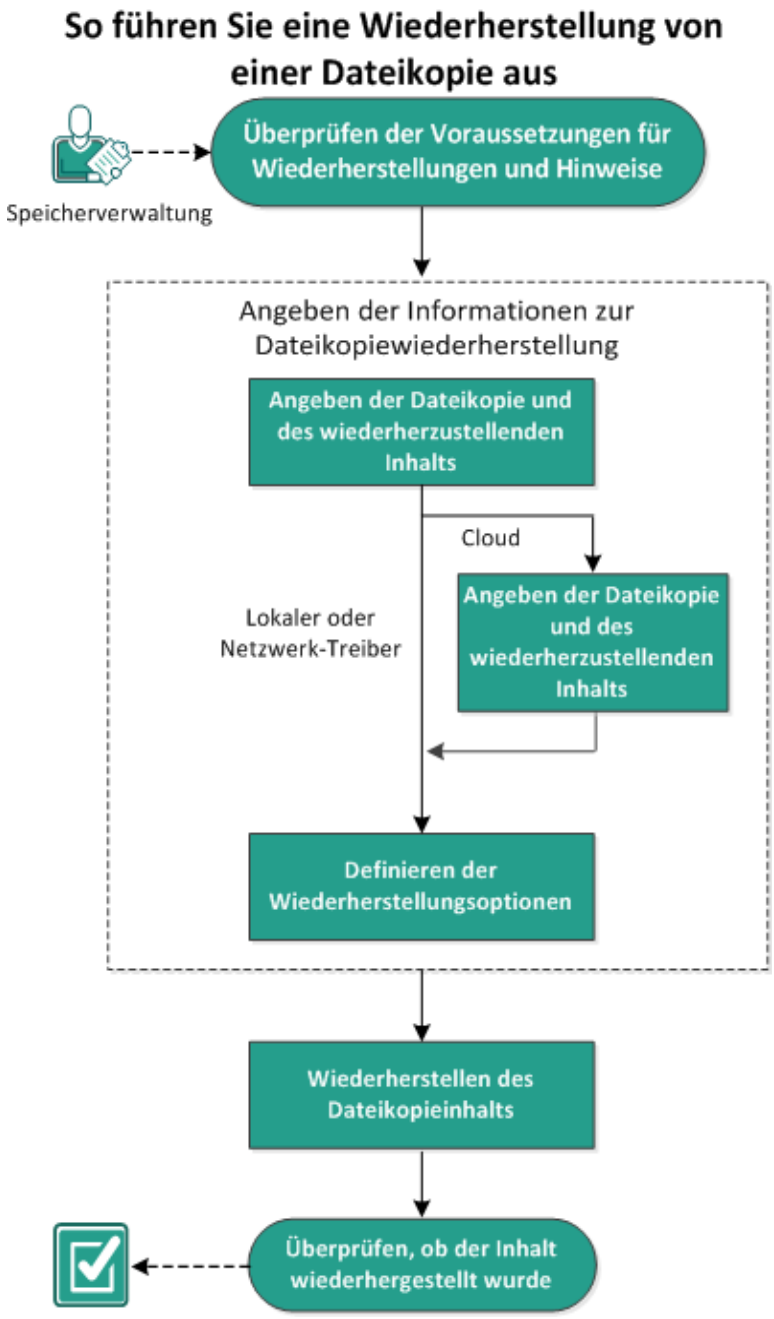
2. Klicken Sie auf den abgeschlossenen umgekehrten Replikationsjob. Der rechte Fensterbereich wird aktualisiert.
3. Klicken Sie unter "Jobdetails" auf den Hyperlink **Protokolle anzeigen**.
4. Überprüfen Sie den Inhalt, um den Wiederherstellungsjob zu bestätigen.

   Der wiederhergestellte Inhalt wurde erfolgreich überprüft.

So führen Sie eine Wiederherstellung von einer Dateikopie aus

Jedes Mal, wenn Arcserve UDP einen erfolgreichen Dateikopierjob ausführt, werden alle Dateien gesichert, die seit dem letzten erfolgreichen Dateikopierjob geändert wurden. Diese Wiederherstellungsmethode ermöglicht es Ihnen, die dateikopierten Daten zu durchsuchen und genau anzugeben, welche Datei Sie wiederherstellen möchten.

Das folgende Diagramm veranschaulicht den Prozess für das Wiederherstellen von einer Dateikopie aus:



Führen Sie die folgenden Aufgaben aus, um von einer Dateikopie aus wiederherzustellen:

1. Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise
2. Angeben der Informationen zur Dateikopiewiederherstellung
    a. Angeben der Dateikopie und des wiederherzustellenden Inhalts
        - Festlegen von Cloud-Konfigurationen für Wiederherstellungen
    b. Definieren der Wiederherstellungsoptionen

3. Wiederherstellen des Inhalts des Wiederherstellungspunkts
4. Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Wiederherstellung ausführen:

- Sie haben mindestens eine Dateikopie zur Wiederherstellung zur Verfügung.
- Sie haben ein gültiges und zugreifbares Dateikopieziel, von dem aus Sie den Dateikopieinhalt wiederherstellen können.
- Sie haben einen gültigen und zugreifbaren Zielspeicherort, auf dem Sie den Inhalt der Dateikopie wiederherstellen können.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Überprüfen Sie die folgenden Wiederherstellungshinweise:

- Arcserve UDP kann nur einen Wiederherstellungsjob zur gleichen Zeit ausführen. Wenn Sie versuchen, einen Wiederherstellungsjob manuell zu starten, während ein anderer Wiederherstellungsjob ausgeführt wird, öffnet sich eine Warnmeldung, die Sie darüber informiert, dass ein anderer Job ausgeführt wird, und Sie auffordert, es später erneut zu versuchen.
- Wenn die Wiederherstellung auf einem Remote-Ziel erfolgt und alle Laufwerksbuchstaben (A – Z) besetzt sind, gelingt die Wiederherstellung auf einem Remote-Pfad nicht. Arcserve UDP Agent (Windows) benötigt einen Laufwerksbuchstaben, um den Pfad des Remote-Ziels zu laden.
- Verbessern Sie die Dateikopie, um die Leistung zu optimieren:
  - Dateikopie kann gleichzeitig mehrere Chunks an das Ziel senden (ArchMultChunkIO)
  - Dateikopie kann mehr als eine Datei gleichzeitig vom Ziel kopieren (ThreadsForArchive).
  - Die Wiederherstellung von einer Dateikopie aus kann mehr als eine Datei gleichzeitig herunterladen (ThreadsForRestore).
  - Die Katalogsynchronisation verwendet mehrere Threads (ThreadForCatalogSync).

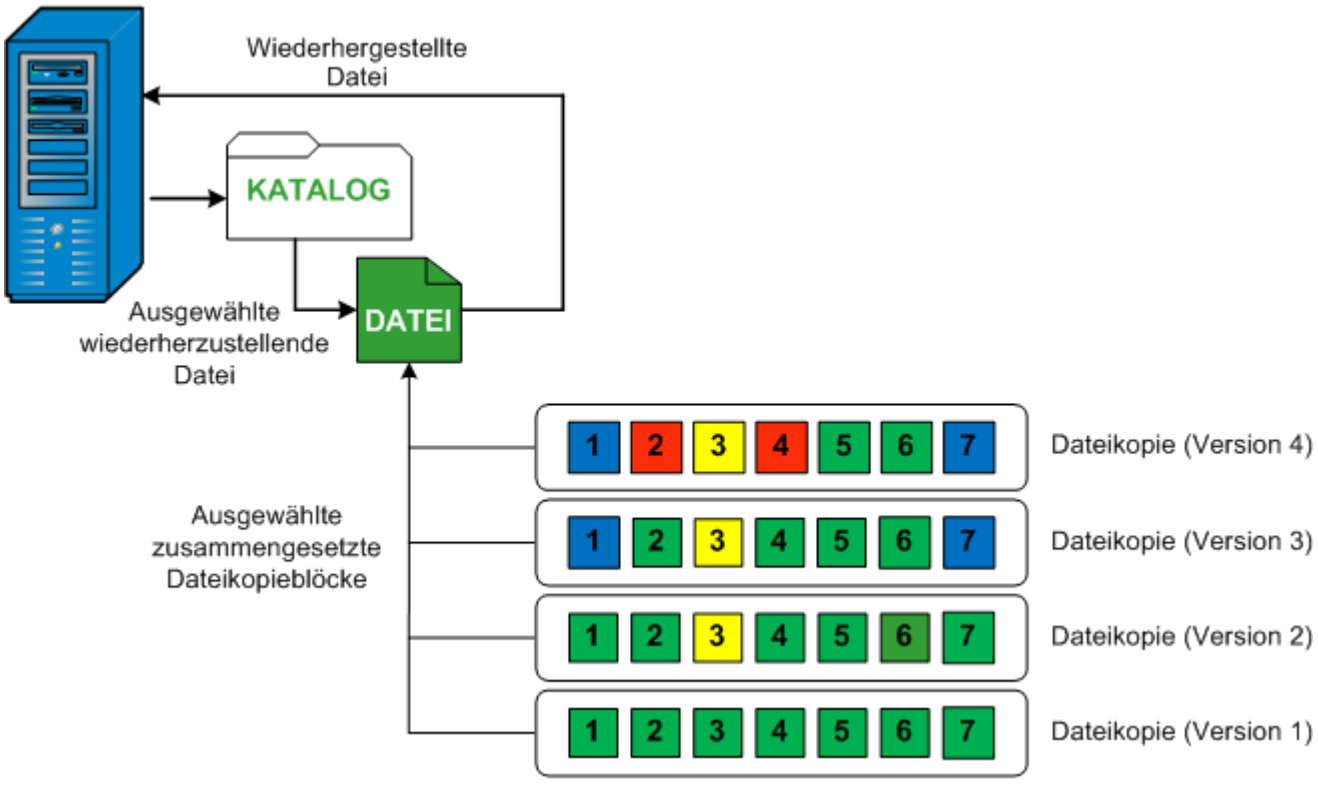
  Sie können die standardmäßigen Dateikopieregistrierungswerte durch Ändern des entsprechenden DWORD-Wertes ändern. Weitere Informationen finden Sie unter Konfigurieren der Dateikopieeinstellungen zur Optimierung der Leistung in der *Online-Hilfe zum Agenten für Windows*.

- (Optional) Erfahren Sie, wie die Wiederherstellung funktioniert. Weitere Informationen erhalten Sie unter Funktionsweise von Wiederherstellungen auf Dateiebene.

Funktionsweise von Wiederherstellungen auf Dateiebene

Während einer Dateikopie besteht jede gesicherte Datei aus einer Sammlung von Blöcken, die jeweils die spezifische Datei definieren. Für jede Version der gesicherten Datei wird eine Katalogdatei erstellt, zusammen mit den individuellen Blöcken, die für diese Dateien verwendet wurden. Wenn Sie eine bestimmte Datei wiederherstellen möchten, können Sie das System nach ihr durchsuchen und die Datei auswählen, die Sie wiederherstellen möchten, sowie die Dateikopieversionen, von denen aus Sie die Wiederherstellung ausführen möchten. Anschließend sammelt Arcserve UDP die Version der Blöcke, die für die Dateikopie der angegebenen Datei eingesetzt wurden, wodurch die Datei wieder zusammengefügt und wiederhergestellt wird.

Das folgende Ablaufschema veranschaulicht den Prozess, mit dem Arcserve UDP eine spezifische Datei wiederherstellt:



Angeben der Informationen zur Dateikopiewiederherstellung

Arcserve UDP bietet eine Option zur Wiederherstellung von Daten von einer Dateikopie. Das Ziel eines Wiederherstellungsjobs besteht darin, schnell zu erkennen, welche Daten benötigt werden, und sie vom entsprechenden Sicherungsdatenträger abzurufen. Für jeden Wiederherstellungsjob ist eine Quelle und ein Ziel erforderlich.

Der Prozess für das Wiederherstellen von einer Dateikopie aus verläuft folgendermaßen:

- Angeben der Dateikopie und des wiederherzustellenden Inhalts
- Definieren der Wiederherstellungsoptionen

Angeben der Dateikopie und des wiederherzustellenden Inhalts

Verwenden Sie die Option **Nach Dateikopien suchen**, um eine Wiederherstellung auf Basis einer Dateikopie durchzuführen. Diese Wiederherstellungsmethode ermöglicht es Ihnen, die dateikopierten Daten zu durchsuchen und genau anzugeben, welche Datei Sie wiederherstellen möchten.

Gehen Sie wie folgt vor:

1. Verwenden Sie eine der folgenden Vorgangsweisen, um auf das Dialogfeld zur Auswahl der Wiederherstellungsmethoden zuzugreifen:

   In Arcserve UDP:

   a. Melden Sie sich bei Arcserve UDP an.

   b. Klicken Sie auf die Registerkarte **Ressourcen**.

   c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

   e. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

      Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

      Hinweis: Sie werden automatisch im Agentenknoten angemeldet, und das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird im Agentenknoten geöffnet.

   In Arcserve UDP Agent (Windows):

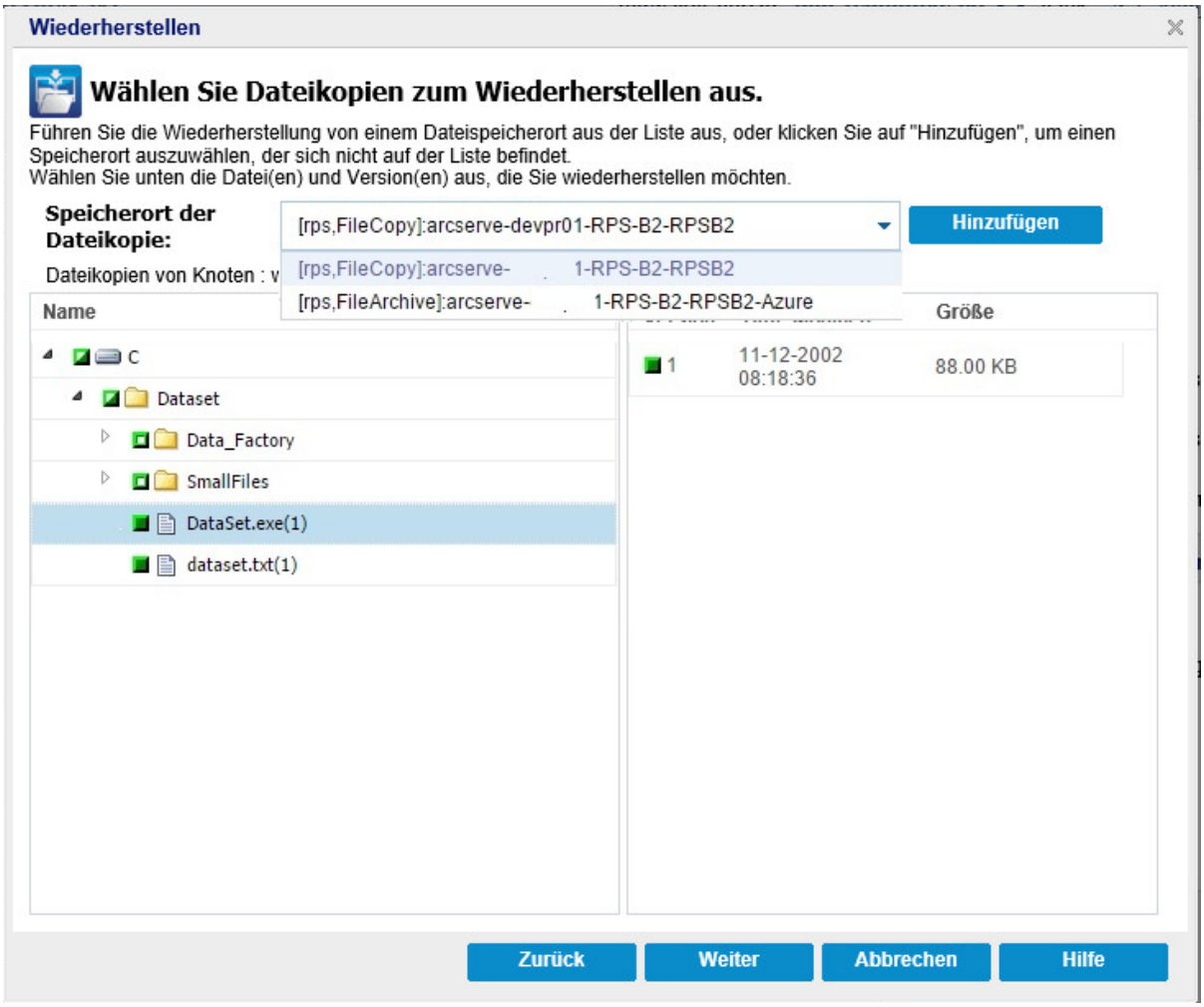
   a. Melden Sie sich bei Arcserve UDP Agent (Windows) an.

   b. Wählen auf der Startseite **Wiederherstellen** aus.

   Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

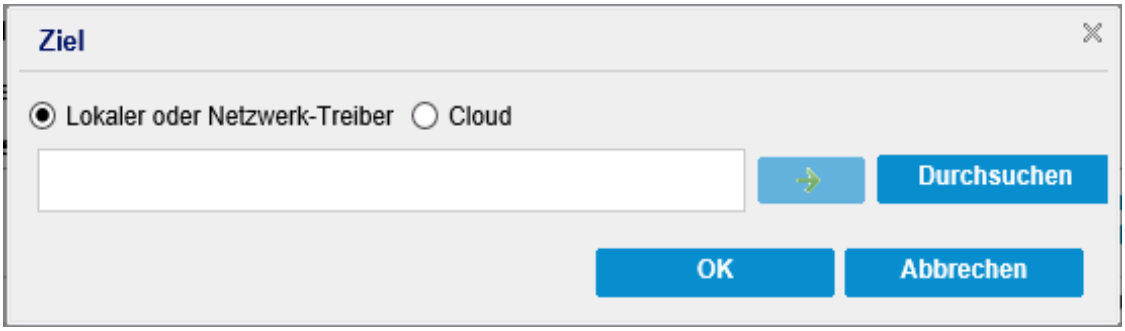
2. Klicken Sie auf die Option **Nach Dateikopien suchen**.

   Das Dialogfeld **Wiederherstellen** wird geöffnet. Das Ziel, das im Feld **Wiederherstellen von** angezeigt wird, ist das konfigurierte Standardziel für die **Dateikopie**.



3. Bei Bedarf können Sie auf **Hinzufügen** klicken, um einen alternativen Speicherort zu suchen, an dem Ihre Dateikopie-Images gespeichert werden sollen.

   Das **Ziel**-Dialogfeld wird geöffnet und zeigt verfügbare alternative Zieloptionen an.



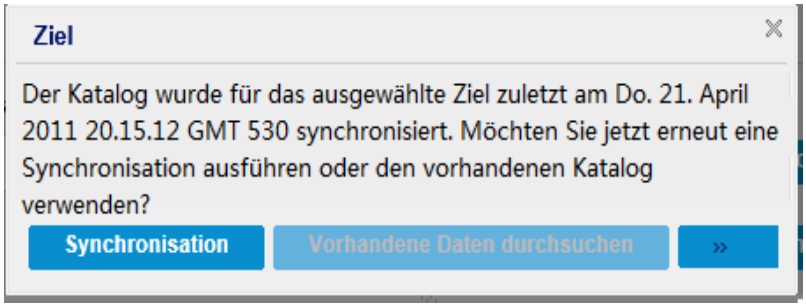
Lokales Laufwerk oder Netzwerklaufwerk

Das Dialogfeld **Speicherort für die Sicherung auswählen** wird geöffnet. Sie können einen alternativen Speicherort für Ihr lokales Laufwerk oder Netzwerklaufwerk suchen und auswählen.

Cloud

Das Dialogfeld **Cloud-Konfiguration** wird geöffnet. Hier können Sie auf einen alternativen Cloud-Speicherort zugreifen und ihn auswählen. Weitere Informationen über dieses Dialogfeld finden Sie unter "Festlegen der Cloud-Konfiguration für Wiederherstellungen".

Wenn Sie das Ziel in einen alternativen Speicherort ändern, wird unabhängig davon, ob Sie eine Wiederherstellung von einem **lokalen Laufwerk oder Netzwerklaufwerk** oder aus der **Cloud** ausgewählt haben, ein Pop-up-Dialogfeld angezeigt, in dem Sie angeben müssen, ob Sie eine neue Katalogsynchronisation durchführen oder aus dem vorhandenen Katalog lesen möchten.



- Wenn Sie zum ersten Mal eine Katalogsynchronisation durchführen, wird die Schaltfläche **Vorhandene Daten durchsuchen** deaktiviert, da der Dateikopiekatalog nicht lokal vorhanden ist.
- Wenn zuvor bereits eine Katalogsynchronisation durchgeführt wurde, zeigt dieses Dialogfeld Details über die letzte Katalogsynchronisation von diesem Ziel an. Wenn seit dem angezeigten Zeitpunkt mehrere Dateikopiejobs durchgeführt wurden, ist Ihr Katalog möglicherweise nicht synchronisiert. Sie können die Option **Synchronisieren** auswählen, um sicherzustellen, dass Ihr Dateikopiekatalog aktuell ist.

  1. Klicken Sie auf **Synchronisieren**, um den Dateikopiekatalog vom angegebenen Dateikopieziel auf Ihren lokalen Rechner herunterzuladen, um den Suchvorgang zu beschleunigen.

  2. Klicken Sie auf **Vorhandene Daten durchsuchen**, um den lokal verfügbaren Dateikopiekatalog zu verwenden und ihn nicht erneut herunterzuladen bzw. zu synchronisieren.

4. Geben Sie im linken Bereich die Daten der Dateikopie an, die wiederhergestellt werden sollen. Sie können Ordner oder Dateien der Dateikopie auswählen, die wiederhergestellt werden sollen.

   Wenn Sie eine individuelle Datei zur Wiederherstellung auswählen, werden alle kopierten Versionen dieser Datei im rechten Bereich angezeigt. Wenn mehrere Versionen verfügbar sind, müssen Sie auswählen, welche Version der Dateikopie Sie wiederherstellen möchten.

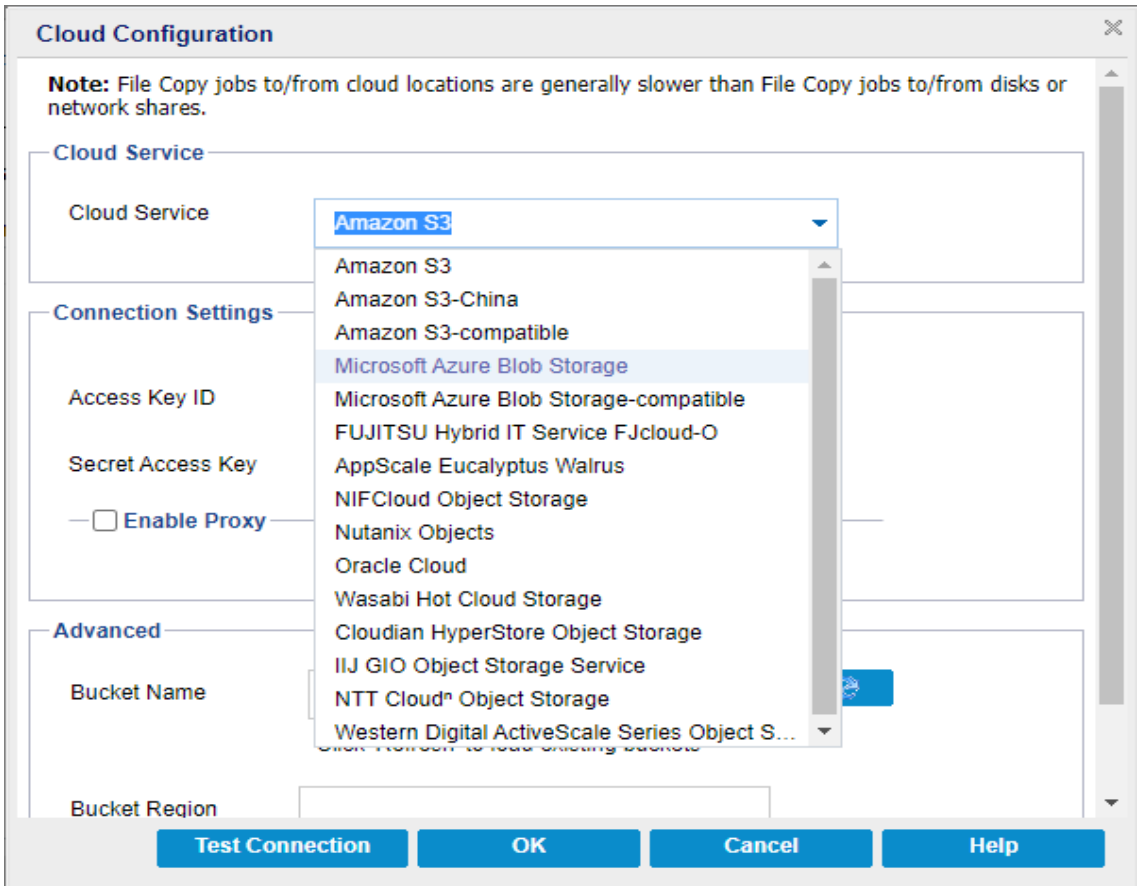
5. Nachdem Sie den Dateikopieordner oder die Dateiversion für die Wiederherstellung ausgewählt haben, klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet.

   Dateikopie und wiederherzustellender Inhalt sind nun festgelegt.

Festlegen von Cloud-Konfiguration für Wiederherstellungen

Hinweis: Der folgende Vorgang gilt nur, wenn Sie eine Datei bzw. einen Ordner von einem Cloud-Dateikopie- oder -Dateiarchivspeicherort wiederherstellen.



Die verfügbaren Optionen sind "Amazon S3", "Amazon S3-kompatibel", "Windows Azure", "Windows Azure-kompatibel", "FUJITSU Hybrid IT Service FJcloud-O" und "Eucalyptus-Walrus". (Amazon S3 ist der Standardanbieter).

Hinweis: Wenn Sie Eucalyptus Walrus als Cloud-Anbieter für Ihre Dateikopie verwenden, können Sie Dateien kopieren, deren gesamte Pfadlänge größer ist als 170 Zeichen.

Die Konfigurationsoptionen für jeden Cloud-Anbieter sind ähnlich (mit etwas unterschiedlicher Terminologie), und alle Unterschiede werden beschrieben.

1. Klicken Sie von der Option**Nach Dateikopien suchen** oder **Wiederherzustellende Dateien/Ordner suchen** auf **Hinzufügen** .

   Das Dialogfeld **Ziel** wird geöffnet.

2. Wählen Sie **Cloud** aus und klicken Sie auf **Durchsuchen**.

Das Dialogfeld **Cloud-Konfiguration** wird geöffnet.

3. Geben Sie die folgenden Details ein:

Speichername

Gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Speichernamen haben.

Speicherdienst

Wählen Sie den Dienst aus der Drop-down-Liste aus. Die Konfigurationsoption variiert je nach ausgewähltem Speicherdienst.

Zugriffsschlüssel-ID/Kontoname/Abfrage-ID

Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

Für dieses Feld verwendet Amazon S3 die Zugriffsschlüssel-ID, Windows Azure und FUJITSU Hybrid IT Service FJcloud-O verwenden den Kontonamen, und Eucalyptus-Walrus verwendet die Abfrage-ID.

Geheimer Zugriffsschlüssel/Geheimschlüssel

Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Bewahren Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

Für dieses Feld verwendet Amazon S3 den geheimen Zugriffsschlüssel. Windows Azure, FUJITSU Hybrid IT Service FJcloud-O und Eucalyptus-Walrus verwenden einen geheimen Schlüssel.

Proxy-Einstellungen

Legt die Proxy-Server-Einstellungen fest. Wählen Sie **Über einen Proxy-Server verbinden**, um diese Option zu aktivieren. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Sie müssen dann die entsprechenden Authentifizierungsinformationen (Domänenname\Benutzername

und Kennwort) angeben, die zur Verwendung des Proxy-Servers erforderlich sind.

Hinweis: Die Proxy-Fähigkeit ist für Eucalyptus-Walrus nicht verfügbar.

Bucket-Name/Container

Alle Dateien und Ordner, die zum Cloud-Anbieter verschoben oder kopiert wurden, werden in Ihren Buckets (oder Containern) gespeichert und organisiert. Buckets sind wie Container für Ihre Dateien und werden verwendet, um Objekte zu gruppieren und gemeinsam zu verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

Für dieses Feld verwenden Amazon S3 und Eucalyptus-Walrus den Bucket-Namen. Windows Azure und FUJITSU Hybrid IT Service FJcloud-O verwenden Container.

Hinweis: Für die restlichen Schritte können, soweit nicht anders angegeben, alle Verweise zu den Buckets auch auf die Container angewendet werden.

Bucket-Region

Bezieht sich auf die Region des Buckets in Amazon und FUJITSU Hybrid IT Service FJcloud-O.

Vertragsnummer

Bezieht sich auf die Nummer Ihres Vertrages für FUJITSU Hybrid IT Service FJcloud-O.

Projekt-ID

Bezieht sich auf die von FUJITSU Hybrid IT Service FJcloud-O generierte ID des Projekts.

"Reduced Redundancy Storage" aktivieren

Nur bei Amazon S3 können Sie mit dieser Option "Reduced Redundancy Storage" (RRS) aktivieren. RRS ist eine Speicheroption innerhalb von Amazon S3, die Ihnen hilft, durch das Speichern von unkritischen, reproduzierbaren Daten auf niedrigeren Redundanzniveaus als dem Amazon S3s Standard-Speicher Kosten zu sparen. Sowohl die Standardoption als auch die RRS-Option speichern Daten in mehreren Einrichtungen und auf mehreren Geräten. Allerdings werden die Daten mit RRS weniger oft repliziert, sodass die Kosten geringer sind. Sie sollten die gleiche Latenz und den gleichen Durchsatz erhalten, indem Sie entweder den Standardspeicher von Amazon S3 oder RRS verwenden. Standardmäßig ist diese Option nicht aktiviert (Amazon S3 verwendet die standardmäßige Speicheroption).

4. Klicken Sie auf **Verbindung testen**, um die Verbindung zum angegebenen Cloud-Speicherort zu überprüfen.
5. Klicken Sie auf **OK**.

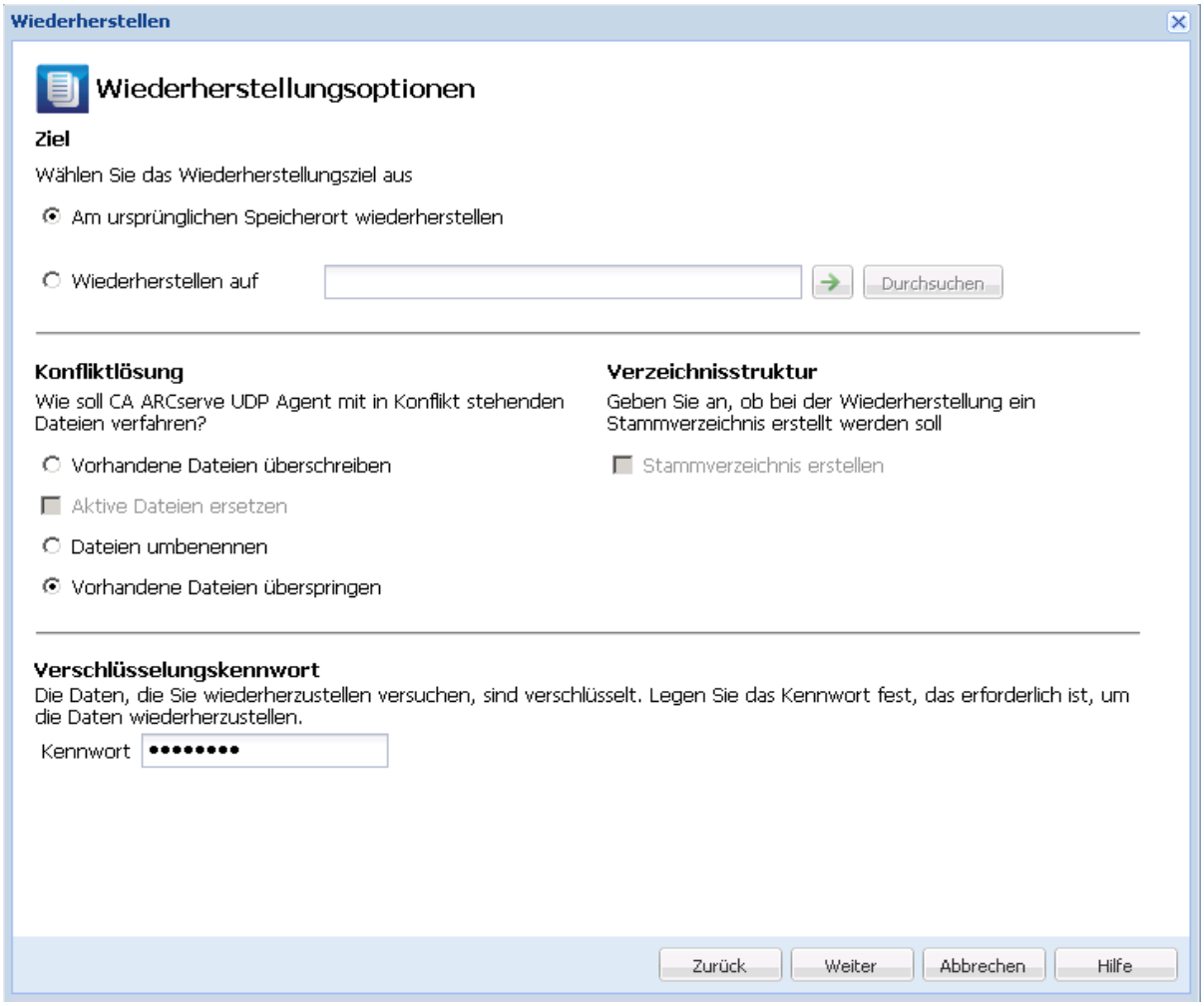
   Das Cloud-Konto wird zur Konsole hinzugefügt.

Definieren der Wiederherstellungsoptionen

Nachdem Sie die Informationen für die Dateikopiewiederherstellung angegeben haben, legen Sie die Kopieoptionen für die ausgewählte Dateikopie und den Inhalt fest.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Wiederherstellungsoptionen** das Wiederherstellungsziel aus.



Es sind folgende Zieloptionen verfügbar:

Am ursprünglichen Speicherort wiederherstellen

Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

Wiederherstellen auf

Stellt am angegebenen Speicherort wieder her. Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.

2. Legen Sie die Option für die **Konfliktlösung** fest, die von Arcserve UDP ausgeführt werden soll, wenn während der Wiederherstellung Konflikte auftreten.

   Es sind folgende Optionen verfügbar:

   Vorhandene Dateien überschreiben

   Überschreibt (ersetzt) alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind. Alle Objekte werden aus den Sicherungsdateien wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.

   Aktive Dateien ersetzen

   Ersetzt alle aktiven Dateien nach einem Neustart. Wenn Arcserve UDP Agent (Windows) während eines Wiederherstellungsversuchs entdeckt, dass die vorhandene Datei gerade verwendet wird oder gerade auf sie zugegriffen wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

   Diese Option ist nur verfügbar, wenn Sie die Option **Vorhandene Dateien überschreiben** auswählen.

   Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien im Wiederherstellungsprozess übersprungen.

   Dateien umbenennen

   Erstellt eine neue Datei, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit demselben Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten sind dann in einer neuen Datei wiederhergestellt.

   Vorhandene Dateien überspringen

   Überspringt alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, und überschreibt (ersetzt) sie nicht. Es werden nur Objekte aus den

Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

Standard: Vorhandene Dateien überspringen

3. Geben Sie die **Verzeichnisstruktur** an, um während der Wiederherstellung ein Stammverzeichnis zu erstellen.

Stammverzeichnis erstellen

Legt fest, dass Arcserve UDP die Stammverzeichnisstruktur des erfassten Sicherungs-Images, soweit vorhanden, am Zielpfad wiederherstellt.

Wenn diese Option nicht ausgewählt wird, wird die Datei oder der Ordner direkt im Zielordner wiederhergestellt.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt" und "C:\Ordner1\Unterordner2\B.txt" erfasst und als Wiederherstellungsziel "D:\Wiederherstellen" ausgewählt.

- Wenn Sie die Wiederherstellung der Dateien "A.txt" und "B.txt" einzeln festgelegt haben, werden die Dateien in "D:\Wiederherstellen\A.txt" und "D:\Wiederherstellen\B.txt" wiederhergestellt (das Stammverzeichnis über der ausgewählten Dateiebene wird nicht wiederhergestellt).
- Wenn Sie eine Wiederherstellung auf "Unterordner2"-Ebene auswählen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Unterordner2\A.txt" und "D:\Wiederherstellen\Unterordner2\B.txt" (das Stammverzeichnis über der ausgewählten Ordnerebene wird nicht wiederhergestellt).

Wenn diese Option ausgewählt ist, wird der gesamte Stammverzeichnispfad für die Dateien/Ordner (einschließlich des Volume-Namens) im Zielordner neu erstellt. Wenn Dateien/Ordner vom selben Volume-Name wiederhergestellt werden sollen, ist dieser Volume-Name nicht im Wiederherstellungsziel-Stammverzeichnispfad enthalten. Wenn Dateien/Ordner von einem anderen Volume-Name wiederhergestellt werden sollen, enthält der Wiederherstellungsziel-Stammverzeichnispfad diesen Volume-Namen.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt", "C:\Ordner1\Unterordner2\B.txt" und E:\Ordner3\Unterordner4\C.txt erfasst, und bei der Wiederherstellung "D:\Wiederherstellen" als Wiederherstellungsziel ausgewählt.

- Wenn Sie nur die Datei "A.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Ordner1\Unterordner2\A.txt" (das gesamte Stammverzeichnis wird ohne den Volume-Namen erneut erstellt).

- Wenn Sie die Dateien "A.txt" und "C.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\C\Ordner1\Unterordner2\A.txt" und "D:\Wiederherstellen\ E\Ordner3\Unterordner4\C.txt" (das gesamte Stammverzeichnis wird mit dem Volume-Namen erneut erstellt).

4. Geben Sie das Verschlüsselungskennwort in **Verschlüsselungskennwort für Dateikopie** ein.
5. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsübersicht** wird geöffnet.

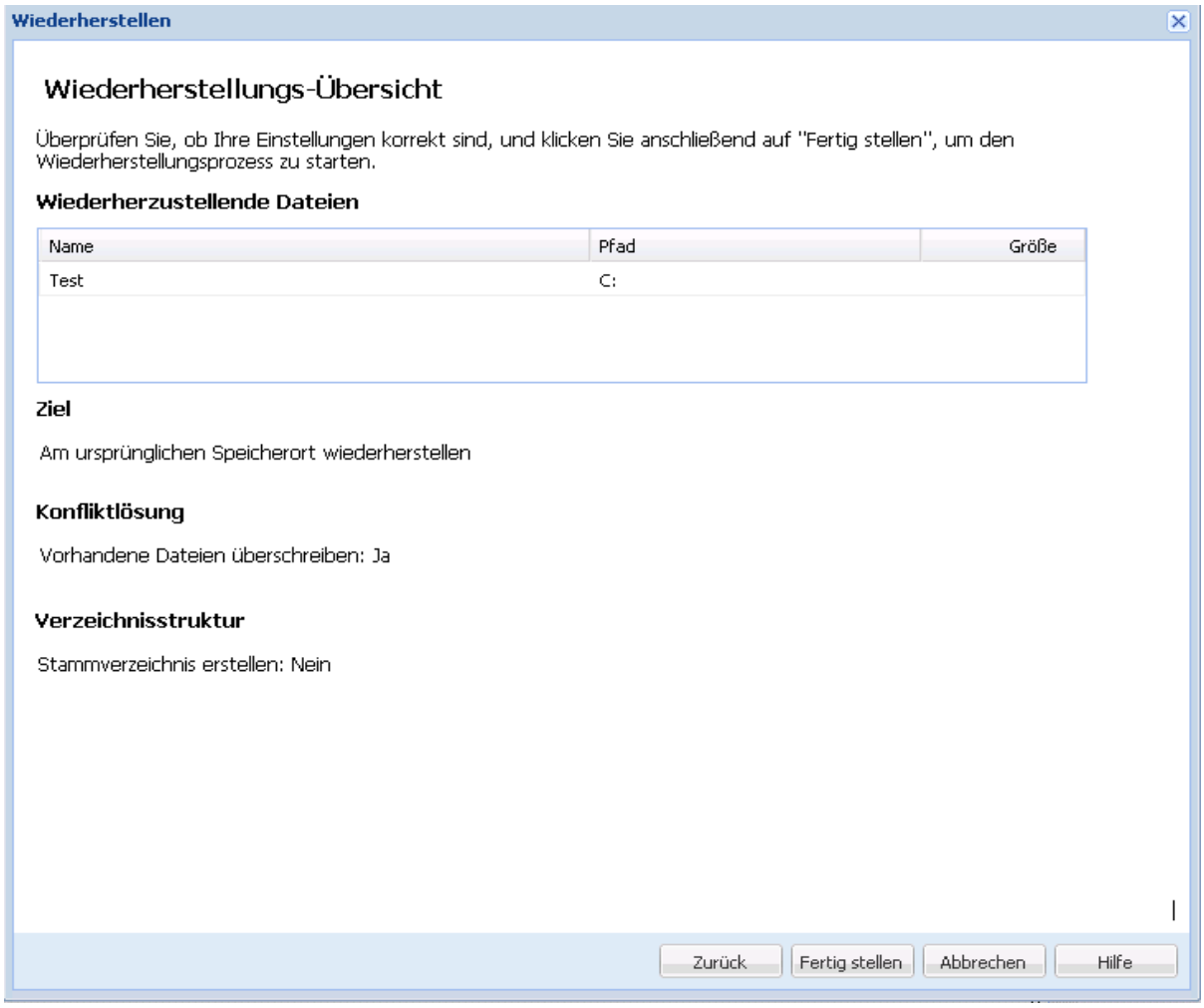
   Die Wiederherstellungsoptionen sind für die Wiederherstellung von einer Dateikopie aus festgelegt.

Wiederherstellen des Dateikopieinhalts

Nachdem Sie die Wiederherstellungsoptionen definiert haben, überprüfen Sie, dass Ihre Einstellungen korrekt sind, und bestätigen Sie den Wiederherstellungsprozess. Die **Wiederherstellungsübersicht** ist hilfreich, um sämtliche Wiederherstellungsoptionen, die Sie festgelegt haben, zu überprüfen und bei Bedarf zu ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Informationen im Dialogfeld **Wiederherstellungsübersicht**, um die Richtigkeit aller Wiederherstellungsoptionen und Einstellungen sicherzustellen.



- Wenn die Übersichtsinformationen Fehler enthalten, klicken Sie auf **Zurück**, und ändern Sie die inkorrekten Einstellungen im entsprechenden Dialogfeld.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsprozess zu starten.

Der Dateikopieinhalt wurde wieder hergestellt.

Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen Sie nach dem Abschluss der Wiederherstellung, dass der Inhalt auf dem angegebenen Ziel wiederhergestellt wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Wiederherstellungsziel, das Sie angegeben haben.

   Eine Liste mit Ordnern wird angezeigt.

2. Suchen Sie die Datei, in der Sie den Inhalt wiederhergestellt haben.

   Wenn Sie zum Beispiel auswählen, dass Datei **A.txt** am Wiederherstellungsziel als "D:\Restore" wiederhergestellt werden soll, navigieren Sie zu folgendem Speicherort:

   D:\Restore\A.txt

3. Überprüfen Sie den Inhalt, um den Wiederherstellungsjob zu bestätigen.

   Der wiederhergestellte Inhalt wurde erfolgreich überprüft.

Ausführen einer Wiederherstellung anhand von einer Dateikopie

Jedes Mal, wenn Arcserve UDP einen erfolgreichen Dateiarchivierungsjob ausführt, werden alle Dateien gesichert, die seit dem letzten erfolgreichen Datei-archivierungsjob geändert wurden. Diese Wiederherstellungsmethode ermöglicht es Ihnen, sich die archivierten Dateien anzuschauen und genau anzugeben, welche Datei Sie wiederherstellen möchten.

Der Vorgang der Wiederherstellung aus einem Dateiarchiv ist mit der Wie-derherstellung aus einer Dateikopie identisch.

Führen Sie die folgenden Aufgaben aus, um eine Wiederherstellung aus einer Datei-kopie durchzuführen:

1. Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise
2. Angeben der Informationen zur Dateikopiewiederherstellung
    a. Angeben der Dateikopie und des wiederherzustellenden Inhalts
        - Festlegen von Cloud-Konfigurationen für Wiederherstellungen
    b. Definieren der Wiederherstellungsoptionen
3. Wiederherstellen des Inhalts des Wiederherstellungspunkts
4. Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Wiederherstellung ausführen:

- Sie haben mindestens eine Dateikopie zur Wiederherstellung zur Verfügung.
- Sie haben ein gültiges und zugreifbares Dateikopieziel, von dem aus Sie den Dateikopieinhalt wiederherstellen können.
- Sie haben einen gültigen und zugreifbaren Zielspeicherort, auf dem Sie den Inhalt der Dateikopie wiederherstellen können.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Überprüfen Sie die folgenden Wiederherstellungshinweise:

- Arcserve UDP kann nur einen Wiederherstellungsjob zur gleichen Zeit ausführen. Wenn Sie versuchen, einen Wiederherstellungsjob manuell zu starten, während ein anderer Wiederherstellungsjob ausgeführt wird, öffnet sich eine Warnmeldung, die Sie darüber informiert, dass ein anderer Job ausgeführt wird, und Sie auffordert, es später erneut zu versuchen.
- Wenn die Wiederherstellung auf einem Remote-Ziel erfolgt und alle Laufwerksbuchstaben (A – Z) besetzt sind, gelingt die Wiederherstellung auf einem Remote-Pfad nicht. Arcserve UDP Agent (Windows) benötigt einen Laufwerksbuchstaben, um den Pfad des Remote-Ziels zu laden.
- Verbessern Sie die Dateikopie, um die Leistung zu optimieren:
  - Dateikopie kann gleichzeitig mehrere Chunks an das Ziel senden (ArchMultChunkIO)
  - Dateikopie kann mehr als eine Datei gleichzeitig vom Ziel kopieren (ThreadsForArchive).
  - Die Wiederherstellung von einer Dateikopie aus kann mehr als eine Datei gleichzeitig herunterladen (ThreadsForRestore).
  - Die Katalogsynchronisation verwendet mehrere Threads (ThreadForCatalogSync).

  Sie können die standardmäßigen Dateikopieregistrierungswerte durch Ändern des entsprechenden DWORD-Wertes ändern. Weitere Informationen finden Sie unter Konfigurieren der Dateikopieeinstellungen zur Optimierung der Leistung in der *Online-Hilfe zum Agenten für Windows*.

- (Optional) Erfahren Sie, wie die Wiederherstellung funktioniert. Weitere Informationen erhalten Sie unter Funktionsweise von Wiederherstellungen auf Dateiebene.

Angeben der Informationen zur Dateikopiewiederherstellung

Arcserve UDP bietet eine Option zur Wiederherstellung von Daten von einer Dateikopie. Das Ziel eines Wiederherstellungsjobs besteht darin, schnell zu erkennen, welche Daten benötigt werden, und sie vom entsprechenden Sicherungsdatenträger abzurufen. Für jeden Wiederherstellungsjob ist eine Quelle und ein Ziel erforderlich.

Der Prozess für das Wiederherstellen von einer Dateikopie aus verläuft folgendermaßen:

- Angeben der Dateikopie und des wiederherzustellenden Inhalts
- Definieren der Wiederherstellungsoptionen

Angeben der Dateikopie und des wiederherzustellenden Inhalts

Verwenden Sie die Option **Nach Dateikopien suchen**, um eine Wiederherstellung auf Basis einer Dateikopie durchzuführen. Diese Wiederherstellungsmethode ermöglicht es Ihnen, die dateikopierten Daten zu durchsuchen und genau anzugeben, welche Datei Sie wiederherstellen möchten.

Gehen Sie wie folgt vor:

1. Verwenden Sie eine der folgenden Vorgangsweisen, um auf das Dialogfeld zur Auswahl der Wiederherstellungsmethoden zuzugreifen:

   In Arcserve UDP:

   a. Melden Sie sich bei Arcserve UDP an.

   b. Klicken Sie auf die Registerkarte **Ressourcen**.

   c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

   e. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

      Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

      Hinweis: Sie werden automatisch im Agentenknoten angemeldet, und das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird im Agentenknoten geöffnet.

   In Arcserve UDP Agent (Windows):

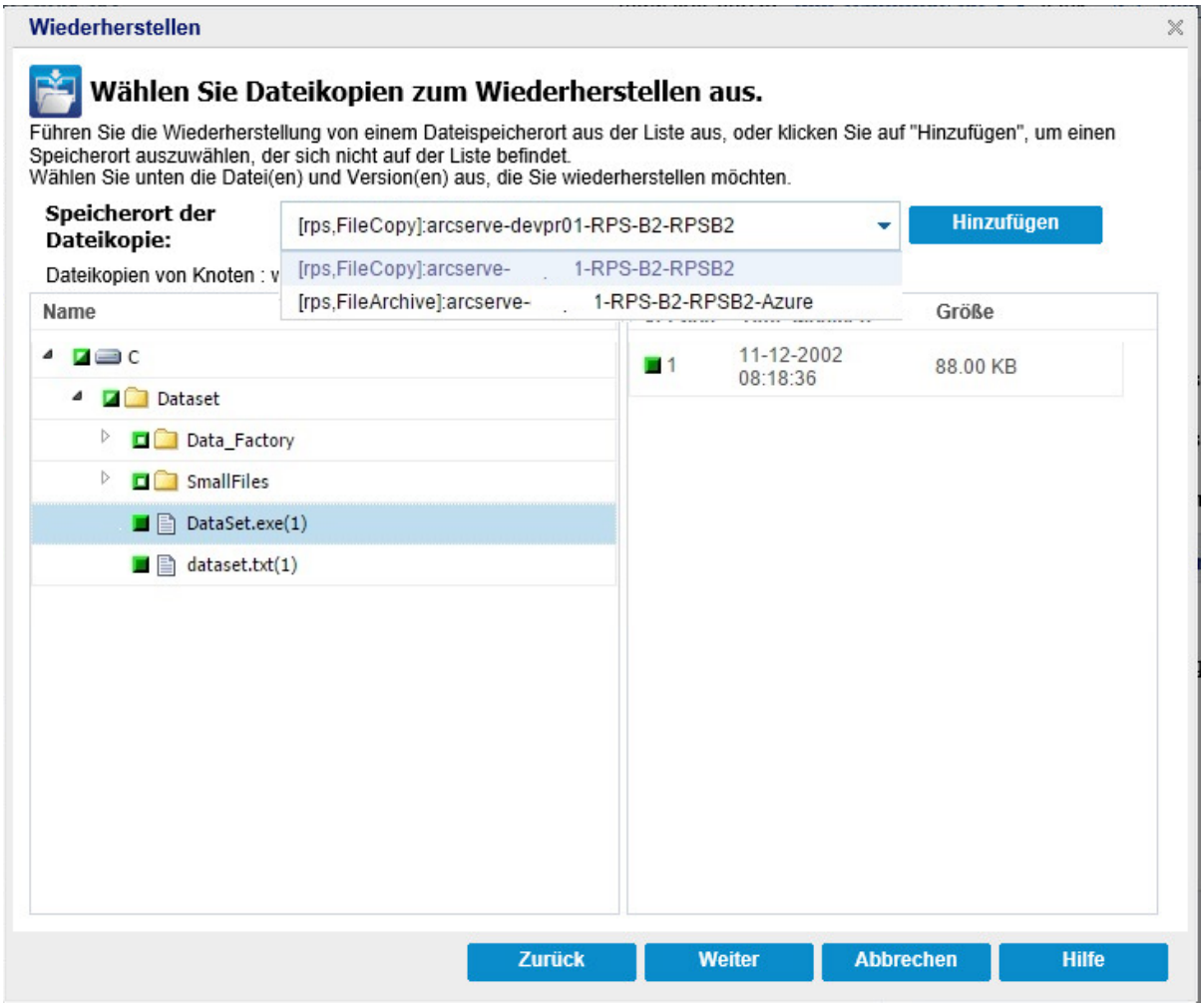
   a. Melden Sie sich bei Arcserve UDP Agent (Windows) an.

   b. Wählen auf der Startseite **Wiederherstellen** aus.

   Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

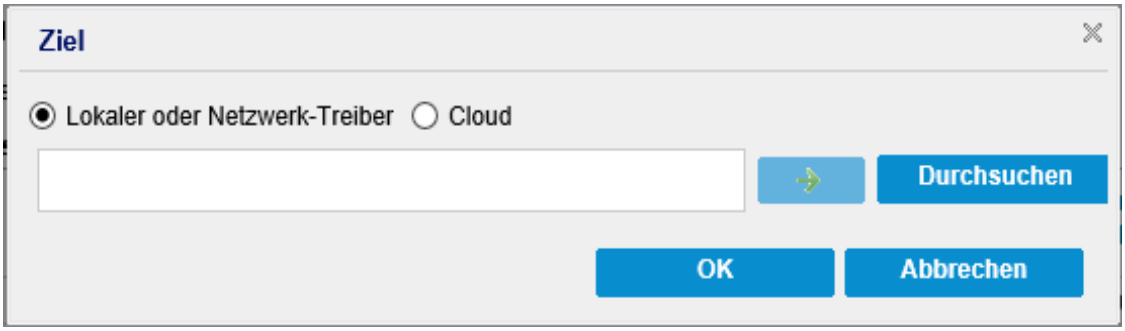
2. Klicken Sie auf die Option **Nach Dateikopien suchen**.

   Das Dialogfeld **Wiederherstellen** wird geöffnet. Das Ziel, das im Feld **Wiederherstellen von** angezeigt wird, ist das konfigurierte Standardziel für die **Dateikopie**.



3. Bei Bedarf können Sie auf **Hinzufügen** klicken, um einen alternativen Speicherort zu suchen, an dem Ihre Dateikopie-Images gespeichert werden sollen.

   Das **Ziel**-Dialogfeld wird geöffnet und zeigt verfügbare alternative Zieloptionen an.



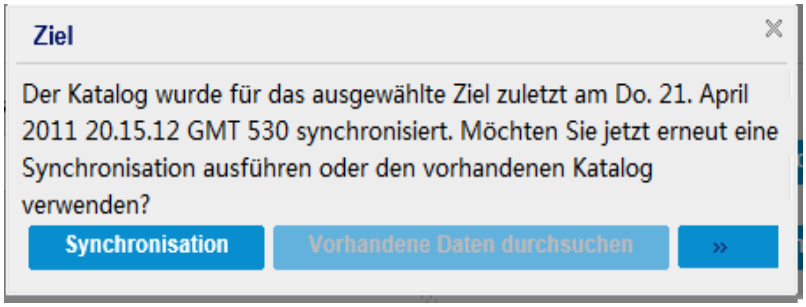
Lokales Laufwerk oder Netzwerklaufwerk

Das Dialogfeld **Speicherort für die Sicherung auswählen** wird geöffnet. Sie können einen alternativen Speicherort für Ihr lokales Laufwerk oder Netzwerklaufwerk suchen und auswählen.

Cloud

Das Dialogfeld **Cloud-Konfiguration** wird geöffnet. Hier können Sie auf einen alternativen Cloud-Speicherort zugreifen und ihn auswählen. Weitere Informationen über dieses Dialogfeld finden Sie unter "Festlegen der Cloud-Konfiguration für Wiederherstellungen".

Wenn Sie das Ziel in einen alternativen Speicherort ändern, wird unabhängig davon, ob Sie eine Wiederherstellung von einem **lokalen Laufwerk oder Netzwerklaufwerk** oder aus der **Cloud** ausgewählt haben, ein Pop-up-Dialogfeld angezeigt, in dem Sie angeben müssen, ob Sie eine neue Katalogsynchronisation durchführen oder aus dem vorhandenen Katalog lesen möchten.



- Wenn Sie zum ersten Mal eine Katalogsynchronisation durchführen, wird die Schaltfläche **Vorhandene Daten durchsuchen** deaktiviert, da der Dateikopiekatalog nicht lokal vorhanden ist.
- Wenn zuvor bereits eine Katalogsynchronisation durchgeführt wurde, zeigt dieses Dialogfeld Details über die letzte Katalogsynchronisation von diesem Ziel an. Wenn seit dem angezeigten Zeitpunkt mehrere Dateikopiejobs durchgeführt wurden, ist Ihr Katalog möglicherweise nicht synchronisiert. Sie können die Option **Synchronisieren** auswählen, um sicherzustellen, dass Ihr Dateikopiekatalog aktuell ist.

  1. Klicken Sie auf **Synchronisieren**, um den Dateikopiekatalog vom angegebenen Dateikopieziel auf Ihren lokalen Rechner herunterzuladen, um den Suchvorgang zu beschleunigen.

  2. Klicken Sie auf **Vorhandene Daten durchsuchen**, um den lokal verfügbaren Dateikopiekatalog zu verwenden und ihn nicht erneut herunterzuladen bzw. zu synchronisieren.

4. Geben Sie im linken Bereich die Daten der Dateikopie an, die wiederhergestellt werden sollen. Sie können Ordner oder Dateien der Dateikopie auswählen, die wiederhergestellt werden sollen.

   Wenn Sie eine individuelle Datei zur Wiederherstellung auswählen, werden alle kopierten Versionen dieser Datei im rechten Bereich angezeigt. Wenn mehrere Versionen verfügbar sind, müssen Sie auswählen, welche Version der Dateikopie Sie wiederherstellen möchten.

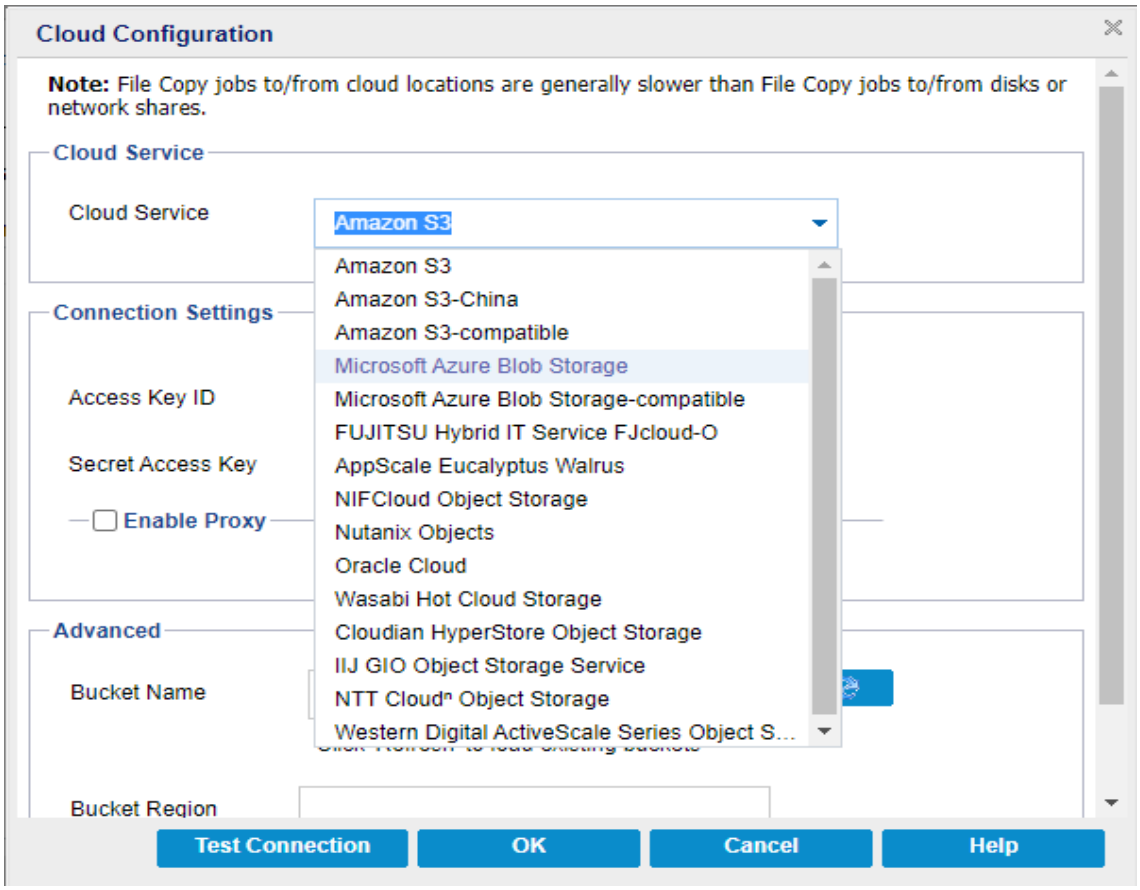
5. Nachdem Sie den Dateikopieordner oder die Dateiversion für die Wiederherstellung ausgewählt haben, klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet.

   Dateikopie und wiederherzustellender Inhalt sind nun festgelegt.

Festlegen von Cloud-Konfiguration für Wiederherstellungen

Hinweis: Der folgende Vorgang gilt nur, wenn Sie eine Datei bzw. einen Ordner von einem Cloud-Dateikopie- oder -Dateiarchivspeicherort wiederherstellen.



Die verfügbaren Optionen sind "Amazon S3", "Amazon S3-kompatibel", "Windows Azure", "Windows Azure-kompatibel", "FUJITSU Hybrid IT Service FJcloud-O" und "Eucalyptus-Walrus". (Amazon S3 ist der Standardanbieter).

Hinweis: Wenn Sie Eucalyptus Walrus als Cloud-Anbieter für Ihre Dateikopie verwenden, können Sie Dateien kopieren, deren gesamte Pfadlänge größer ist als 170 Zeichen.

Die Konfigurationsoptionen für jeden Cloud-Anbieter sind ähnlich (mit etwas unterschiedlicher Terminologie), und alle Unterschiede werden beschrieben.

1. Klicken Sie von der Option**Nach Dateikopien suchen** oder **Wiederherzustellende Dateien/Ordner suchen** auf **Hinzufügen** .

   Das Dialogfeld **Ziel** wird geöffnet.

2. Wählen Sie **Cloud** aus und klicken Sie auf **Durchsuchen**.

Das Dialogfeld **Cloud-Konfiguration** wird geöffnet.

3. Geben Sie die folgenden Details ein:

Speichername

Gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Speichernamen haben.

Speicherdienst

Wählen Sie den Dienst aus der Drop-down-Liste aus. Die Konfigurationsoption variiert je nach ausgewähltem Speicherdienst.

Zugriffsschlüssel-ID/Kontoname/Abfrage-ID

Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

Für dieses Feld verwendet Amazon S3 die Zugriffsschlüssel-ID, Windows Azure und FUJITSU Hybrid IT Service FJcloud-O verwenden den Kontonamen, und Eucalyptus-Walrus verwendet die Abfrage-ID.

Geheimer Zugriffsschlüssel/Geheimschlüssel

Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Bewahren Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

Für dieses Feld verwendet Amazon S3 den geheimen Zugriffsschlüssel. Windows Azure, FUJITSU Hybrid IT Service FJcloud-O und Eucalyptus-Walrus verwenden einen geheimen Schlüssel.

Proxy-Einstellungen

Legt die Proxy-Server-Einstellungen fest. Wählen Sie **Über einen Proxy-Server verbinden**, um diese Option zu aktivieren. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Sie müssen dann die entsprechenden Authentifizierungsinformationen (Domänenname\Benutzername

und Kennwort) angeben, die zur Verwendung des Proxy-Servers erforderlich sind.

Hinweis: Die Proxy-Fähigkeit ist für Eucalyptus-Walrus nicht verfügbar.

Bucket-Name/Container

Alle Dateien und Ordner, die zum Cloud-Anbieter verschoben oder kopiert wurden, werden in Ihren Buckets (oder Containern) gespeichert und organisiert. Buckets sind wie Container für Ihre Dateien und werden verwendet, um Objekte zu gruppieren und gemeinsam zu verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

Für dieses Feld verwenden Amazon S3 und Eucalyptus-Walrus den Bucket-Namen. Windows Azure und FUJITSU Hybrid IT Service FJcloud-O verwenden Container.

Hinweis: Für die restlichen Schritte können, soweit nicht anders angegeben, alle Verweise zu den Buckets auch auf die Container angewendet werden.

Bucket-Region

Bezieht sich auf die Region des Buckets in Amazon und FUJITSU Hybrid IT Service FJcloud-O.

Vertragsnummer

Bezieht sich auf die Nummer Ihres Vertrages für FUJITSU Hybrid IT Service FJcloud-O.

Projekt-ID

Bezieht sich auf die von FUJITSU Hybrid IT Service FJcloud-O generierte ID des Projekts.

"Reduced Redundancy Storage" aktivieren

Nur bei Amazon S3 können Sie mit dieser Option "Reduced Redundancy Storage" (RRS) aktivieren. RRS ist eine Speicheroption innerhalb von Amazon S3, die Ihnen hilft, durch das Speichern von unkritischen, reproduzierbaren Daten auf niedrigeren Redundanzniveaus als dem Amazon S3s Standard-Speicher Kosten zu sparen. Sowohl die Standardoption als auch die RRS-Option speichern Daten in mehreren Einrichtungen und auf mehreren Geräten. Allerdings werden die Daten mit RRS weniger oft repliziert, sodass die Kosten geringer sind. Sie sollten die gleiche Latenz und den gleichen Durchsatz erhalten, indem Sie entweder den Standardspeicher von Amazon S3 oder RRS verwenden. Standardmäßig ist diese Option nicht aktiviert (Amazon S3 verwendet die standardmäßige Speicheroption).

4. Klicken Sie auf **Verbindung testen**, um die Verbindung zum angegebenen Cloud-Speicherort zu überprüfen.
5. Klicken Sie auf **OK**.

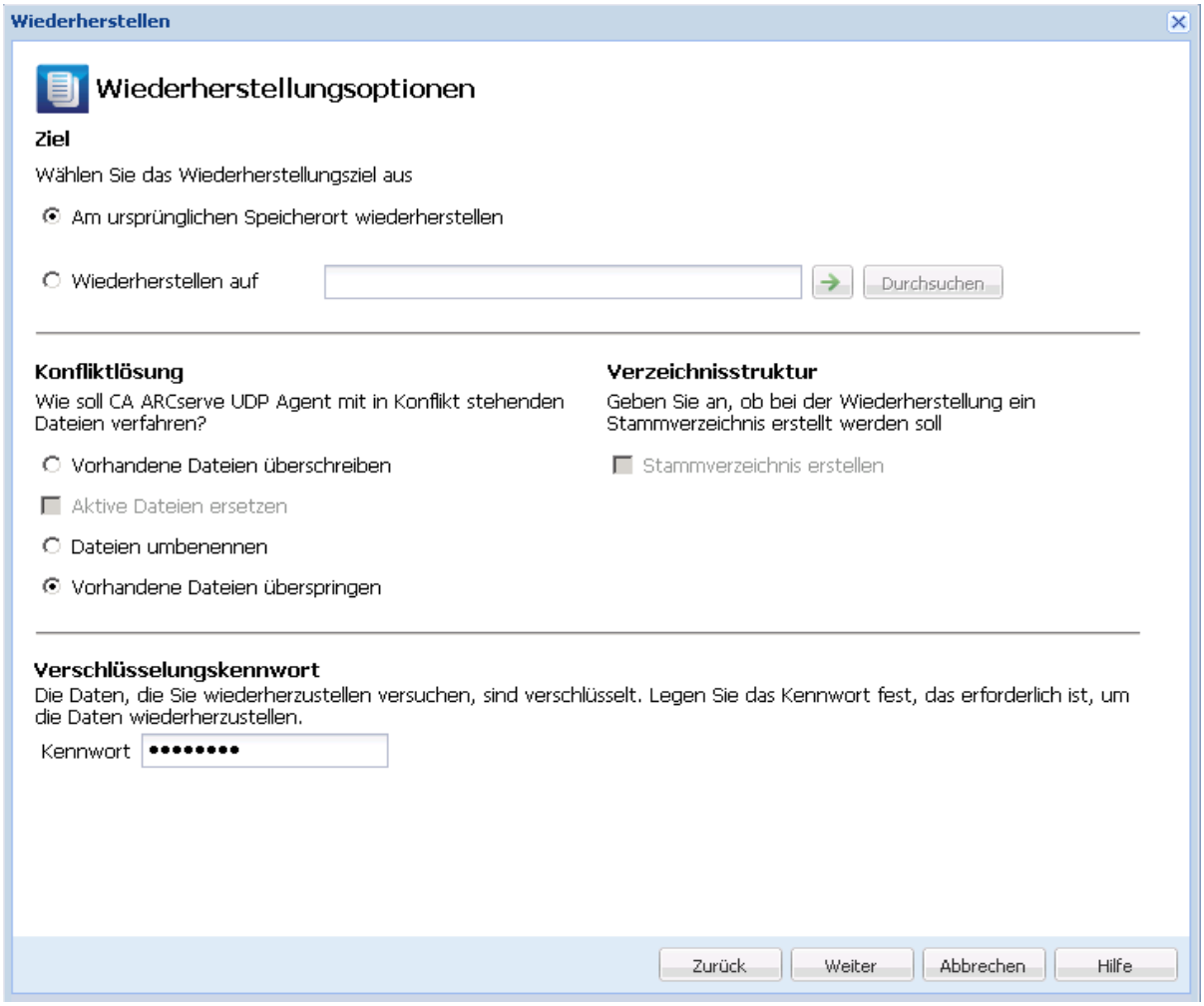
   Das Cloud-Konto wird zur Konsole hinzugefügt.

Definieren der Wiederherstellungsoptionen

Nachdem Sie die Informationen für die Dateikopiewiederherstellung angegeben haben, legen Sie die Kopieoptionen für die ausgewählte Dateikopie und den Inhalt fest.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Wiederherstellungsoptionen** das Wiederherstellungsziel aus.



Es sind folgende Zieloptionen verfügbar:

Am ursprünglichen Speicherort wiederherstellen

Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

Wiederherstellen auf

Stellt am angegebenen Speicherort wieder her. Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.

2. Legen Sie die Option für die **Konfliktlösung** fest, die von Arcserve UDP ausgeführt werden soll, wenn während der Wiederherstellung Konflikte auftreten.

   Es sind folgende Optionen verfügbar:

   Vorhandene Dateien überschreiben

   Überschreibt (ersetzt) alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind. Alle Objekte werden aus den Sicherungsdateien wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.

   Aktive Dateien ersetzen

   Ersetzt alle aktiven Dateien nach einem Neustart. Wenn Arcserve UDP Agent (Windows) während eines Wiederherstellungsversuchs entdeckt, dass die vorhandene Datei gerade verwendet wird oder gerade auf sie zugegriffen wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

   Diese Option ist nur verfügbar, wenn Sie die Option **Vorhandene Dateien überschreiben** auswählen.

   Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien im Wiederherstellungsprozess übersprungen.

   Dateien umbenennen

   Erstellt eine neue Datei, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit demselben Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten sind dann in einer neuen Datei wiederhergestellt.

   Vorhandene Dateien überspringen

   Überspringt alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, und überschreibt (ersetzt) sie nicht. Es werden nur Objekte aus den

Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

Standard: Vorhandene Dateien überspringen

3. Geben Sie die **Verzeichnisstruktur** an, um während der Wiederherstellung ein Stammverzeichnis zu erstellen.

Stammverzeichnis erstellen

Legt fest, dass Arcserve UDP die Stammverzeichnisstruktur des erfassten Sicherungs-Images, soweit vorhanden, am Zielpfad wiederherstellt.

Wenn diese Option nicht ausgewählt wird, wird die Datei oder der Ordner direkt im Zielordner wiederhergestellt.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt" und "C:\Ordner1\Unterordner2\B.txt" erfasst und als Wiederherstellungsziel "D:\Wiederherstellen" ausgewählt.

- Wenn Sie die Wiederherstellung der Dateien "A.txt" und "B.txt" einzeln festgelegt haben, werden die Dateien in "D:\Wiederherstellen\A.txt" und "D:\Wiederherstellen\B.txt" wiederhergestellt (das Stammverzeichnis über der ausgewählten Dateiebene wird nicht wiederhergestellt).
- Wenn Sie eine Wiederherstellung auf "Unterordner2"-Ebene auswählen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Unterordner2\A.txt" und "D:\Wiederherstellen\Unterordner2\B.txt" (das Stammverzeichnis über der ausgewählten Ordnerebene wird nicht wiederhergestellt).

Wenn diese Option ausgewählt ist, wird der gesamte Stammverzeichnispfad für die Dateien/Ordner (einschließlich des Volume-Namens) im Zielordner neu erstellt. Wenn Dateien/Ordner vom selben Volume-Name wiederhergestellt werden sollen, ist dieser Volume-Name nicht im Wiederherstellungsziel-Stammverzeichnispfad enthalten. Wenn Dateien/Ordner von einem anderen Volume-Name wiederhergestellt werden sollen, enthält der Wiederherstellungsziel-Stammverzeichnispfad diesen Volume-Namen.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt", "C:\Ordner1\Unterordner2\B.txt" und E:\Ordner3\Unterordner4\C.txt erfasst, und bei der Wiederherstellung "D:\Wiederherstellen" als Wiederherstellungsziel ausgewählt.

- Wenn Sie nur die Datei "A.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Ordner1\Unterordner2\A.txt" (das gesamte Stammverzeichnis wird ohne den Volume-Namen erneut erstellt).

- Wenn Sie die Dateien "A.txt" und "C.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\C\Ordner1\Unterordner2\A.txt" und "D:\Wiederherstellen\ E\Ordner3\Unterordner4\C.txt" (das gesamte Stammverzeichnis wird mit dem Volume-Namen erneut erstellt).

4. Geben Sie das Verschlüsselungskennwort in **Verschlüsselungskennwort für Dateikopie** ein.
5. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsübersicht** wird geöffnet.

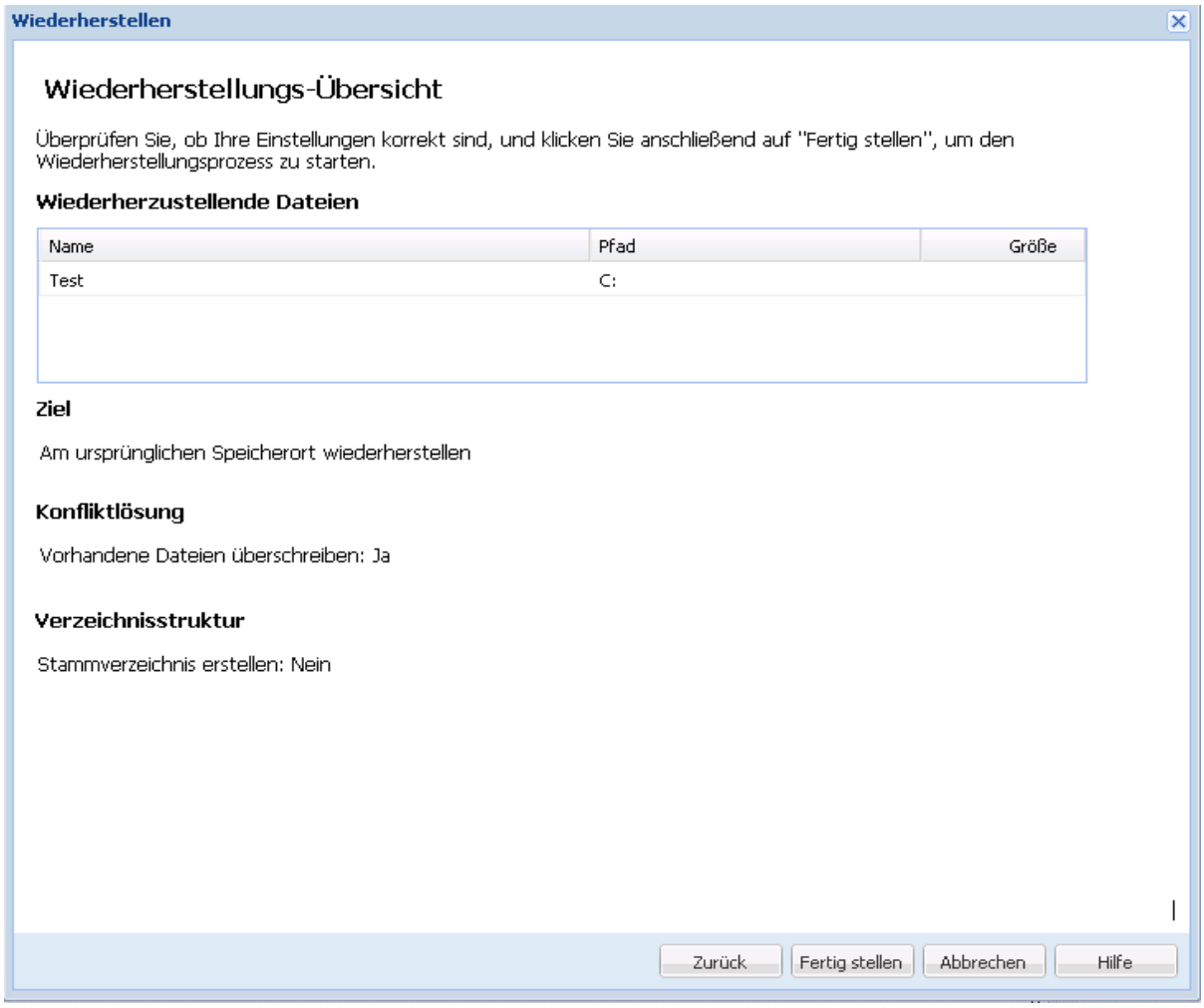
   Die Wiederherstellungsoptionen sind für die Wiederherstellung von einer Dateikopie aus festgelegt.

Wiederherstellen des Inhalts des Wiederherstellungspunkts

Nachdem Sie die Wiederherstellungsoptionen definiert haben, überprüfen Sie, dass Ihre Einstellungen korrekt sind, und bestätigen Sie den Wiederherstellungsprozess. Die **Wiederherstellungsübersicht** ist hilfreich, um sämtliche Wiederherstellungsoptionen, die Sie festgelegt haben, zu überprüfen und bei Bedarf zu ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Informationen im Dialogfeld **Wiederherstellungsübersicht**, um die Richtigkeit aller Wiederherstellungsoptionen und Einstellungen sicherzustellen.



- Wenn die Übersichtsinformationen Fehler enthalten, klicken Sie auf **Zurück**, und ändern Sie die inkorrekten Einstellungen im entsprechenden Dialogfeld.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsprozess zu starten.

Der Dateikopieinhalt wurde wieder hergestellt.

Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen Sie nach dem Abschluss der Wiederherstellung, dass der Inhalt auf dem angegebenen Ziel wiederhergestellt wurde.

Gehen Sie wie folgt vor:

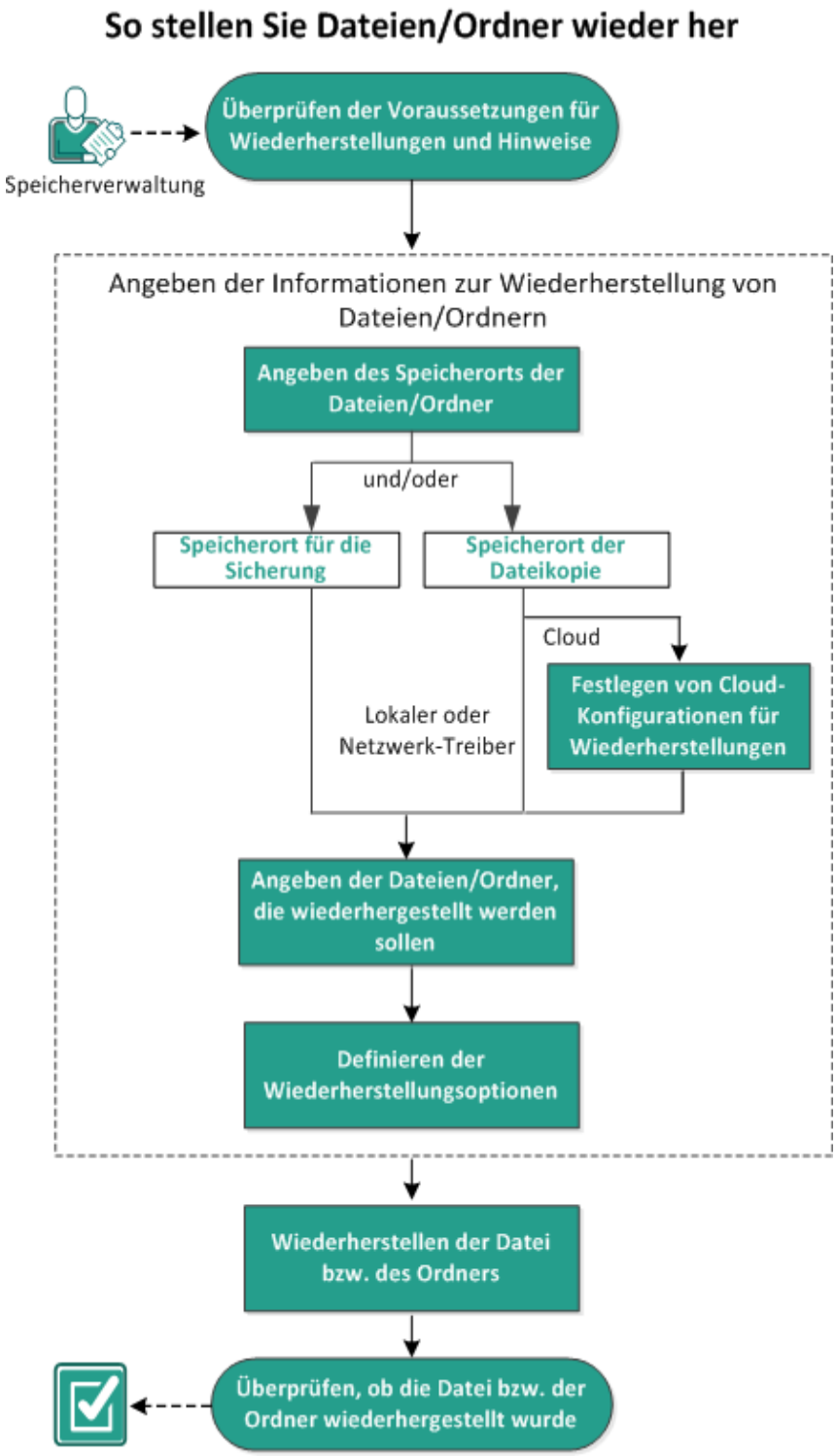
1. Melden Sie sich beim Zielpostfach an.
2. Überprüfen Sie das Postfachelement, das Sie wiederhergestellt haben.
3. Überprüfen die wiederhergestellten Inhalte.

   Der wiederhergestellte Inhalt wurde erfolgreich überprüft.

So stellen Sie Dateien/Ordner wieder her

Bei jeder erfolgreichen Arcserve UDP-Sicherung werden alle gesicherten Dateien/Ordner zum Snapshot-Image der Sicherung hinzugefügt. Mit dieser Wiederherstellungsmethode können Sie genau festlegen, welche Dateien/Ordner wiederhergestellt werden sollen.

Folgendes Diagramm veranschaulicht den Prozess zur Wiederherstellung von bestimmten Dateien/Ordnern:



Führen Sie folgende Aufgaben aus, um Dateien/Ordner wiederherzustellen:

1. Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise
2. Angeben der Informationen zur Wiederherstellung von Dateien/Ordnern

a. Angeben des Speicherorts der Dateien/Ordner
    - Festlegen von Cloud-Konfigurationen für Wiederherstellungen
b. Angeben der Dateien/Ordner, die wiederhergestellt werden sollen
c. Definieren der Wiederherstellungsoptionen

3. Wiederherstellen der Datei bzw. des Ordners
4. Überprüfen, ob die Datei bzw. der Ordner wiederhergestellt wurde

Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Wiederherstellung ausführen:

- Sie haben mindestens eine Sicherung oder eine Dateikopie der Version zur Wiederherstellung zur Verfügung.
- Sie haben ein gültiges und zugreifbares Sicherungs- oder Dateikopieziel, von dem aus Sie den Sicherungs- oder Dateikopieinhalt wiederherstellen können.
- Sie haben einen gültigen und zugreifbaren Zielspeicherort, auf dem Sie den Inhalt der Sicherung oder Dateikopie wiederherstellen können.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Überprüfen Sie die folgenden Wiederherstellungshinweise:

- Um bei einem Wiederherstellungspunkt, für den kein Dateisystemkatalog erstellt wurde, sicherzustellen, dass Sie wiederherzustellende Dateien/Ordner über die Benutzeroberfläche suchen und auswählen können, sollte dem Konto bzw. der Gruppe vor der Erstellung der Sicherung Lese-und Schreibzugriff für alle Ordner/Dateien auf allen Volumes gewährt werden.

  Damit Arcserve UDP Agent (Windows) eine Sicherung, für die kein Dateisystemkatalog erstellt wurde, durchsuchen kann, muss das lokale System (SYSTEM) oder die integrierte Administratorengruppe (BUILTIN\Administrators) zur ACL der Ordner hinzugefügt werden. Anderenfalls kann Arcserve UDP Agent (Windows) die Ordner nicht über die Wiederherstellungs-Benutzeroberfläche durchsuchen.

- (Optional) Erfahren Sie, wie die Wiederherstellung funktioniert. Weitere Informationen erhalten Sie unter Funktionsweise von Wiederherstellungen auf Dateiebene.

  Hinweis: Der Prozess für das Wiederherstellen von einem Speicherort der Dateikopie ähnelt dem Wiederherstellen von einem Speicherort für die Sicherung.

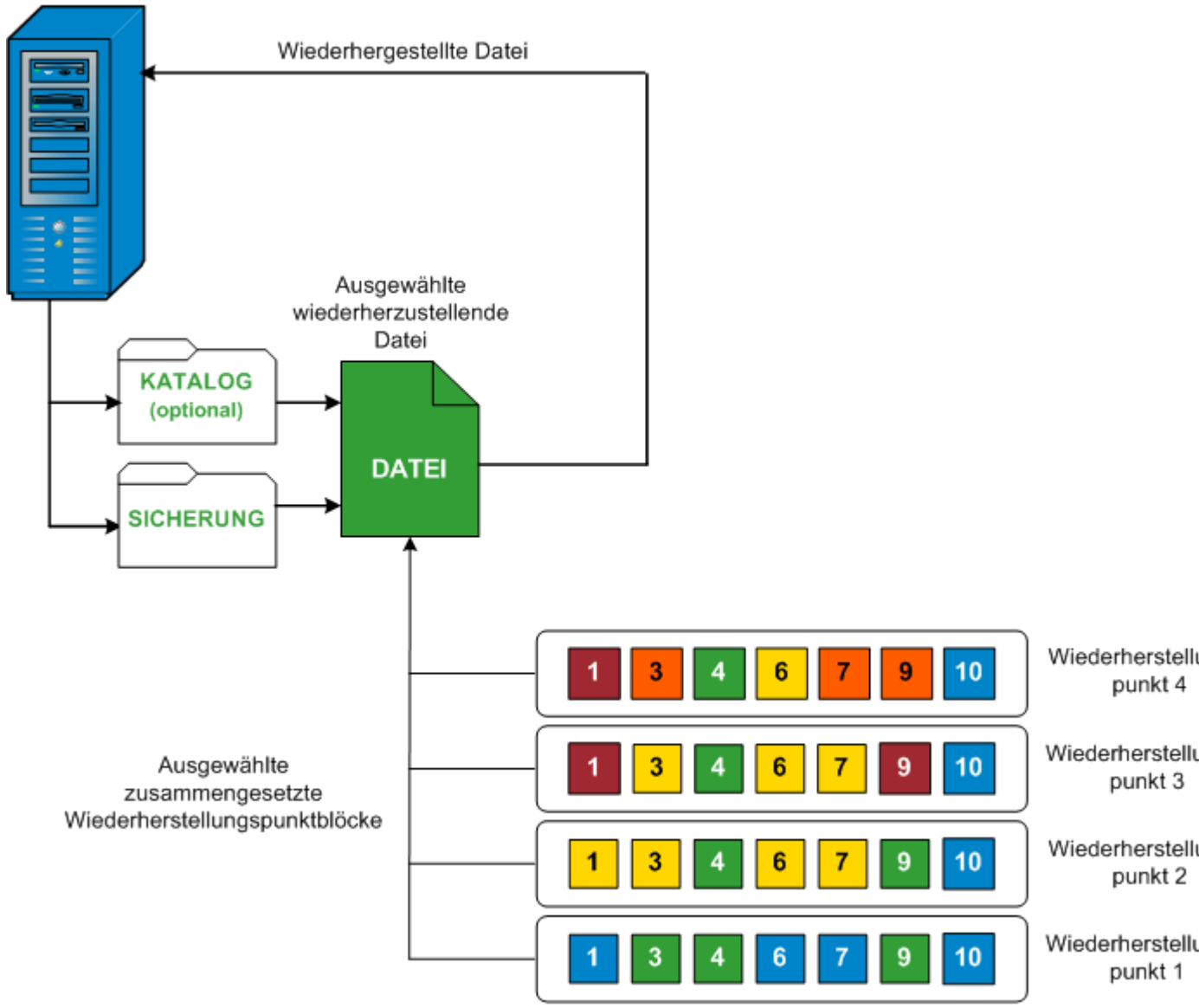
- (Optional) Überprüfen Sie die Dateien, die während der Wiederherstellung übersprungen wurden. Weitere Informationen finden Sie unter "Dateien, die während der Wiederherstellung übersprungen wurden".

Funktionsweise von Wiederherstellungen auf Dateiebene

Bei einer Sicherung auf Blockebene besteht jede gesicherte Datei aus mehreren erfassten Blöcken, die sie definieren. Wenn Sie eine bestimmte Datei wiederherstellen möchten, können Sie Ihre Sicherung durchsuchen, um die Datei und den Wiederherstellungspunkt auszuwählen. Arcserve UDP Agent (Windows) erfasst dann die Versionen der Blöcke, die für den Wiederherstellungspunkt der ausgewählten Datei verwendet wurden, fasst sie zusammen und stellt die Datei wieder her.

Hinweis: Wenn Sie Ihre Sicherungseinstellungen angeben, können Sie eine Option auswählen, um während der Sicherung einen Dateikatalog zu erstellen. Dieser Dateikatalog lässt Sie die Sicherungssitzungen bei der Wiederherstellung schneller durchsuchen. Wenn Sie vorziehen, während der Sicherung keinen Katalog zu erstellen, kann er zu einem späteren Zeitpunkt erstellt werden.

Das folgende Ablaufschema veranschaulicht den Prozess, mit dem Arcserve UDP eine spezifische Datei wiederherstellt.


Wiederhergestellte Datei
Ausgewählte wiederherzustellende Datei
KATALOG (optional)
SICHERUNG
DATEI
Ausgewählte zusammengesetzte Wiederherstellungspunktblöcke
1 3 4 6 7 9 10
Wiederherstellu punkt 4
1 3 4 6 7 9 10
Wiederherstellu punkt 3
1 3 4 6 7 9 10
Wiederherstellu punkt 2
1 3 4 6 7 9 10
Wiederherstellu punkt 1

Dateien, die während der Wiederherstellung übersprungen wurden

Bei Wiederherstellungen mit Arcserve UDP Agent (Windows) werden bestimmte Dateien möglicherweise absichtlich übersprungen.

Die Dateien und Ordner in der folgenden Tabelle werden während einer Wiederherstellung übersprungen, wenn die folgenden zwei Bedingungen vorhanden sind:

- Dateien werden übersprungen, wenn solche Dateien vor der Wiederherstellung vorhanden sind und die Konfliktoption "Vorhandene Dateien überspringen" ist.
- Dateien und Ordner, die in der folgenden Tabelle aufgelistet sind, werden übersprungen, weil sie keine wichtige Komponente für Windows oder Arcserve UDP Agent (Windows) sind.

BS	Ordner oder Speicherort	Datei oder Ordnername	Bemerkungen
Alle	Stammordner von jedem Volume	CAVolTrc.dat	Wird von dem Arcserve UDP-Treiber für die Nachverfolgung verwendet.
		cavoltrcsnapshot.dat	
		System Volume Information*	Wird verwendet, um Dateien/Ordner von einem Windows-System zu speichern, zum Beispiel Volume-Schattenkopie-Dateien.
		RECYCLER*	Wird nur auf NTFS-Partitionen verwendet. Es enthält einen Papierkorb für jeden Benutzer, der sich beim Computer anmeldet, sortiert nach Sicherheitskennung (SID).
		$Recycle.Bin*	Wenn Sie eine Datei in Windows NT Explorer oder im Arbeitsplatz löschen, dann wird die Datei im Papierkorb gespeichert, bis Sie den Papierkorb leeren oder die Datei wiederherstellen.
	Alle Ordner enthalten Bilddateien	Thumbs.db	Speichert Miniaturansicht -Bilder für Windows Explorer Miniaturansicht.
	Stammordner des Volume	PageFile.sys	Windows-Auslagerungsdatei des virtuellen Speichers.
		Hiberfil.sys	Ruhezustanddatei wird verwendet, um die Systemdaten zu speichern, wenn ein Computer in den Ruhezustand geht.

Die folgenden Dateien und Ordner werden nur übersprungen, wenn Sie eine Wiederherstellung am ursprünglichen Speicherort durchführen:

BS	Ordner oder Speicherort	Datei oder	Bemerkung

		Ordnername	
Alle	Der Ordner ist im Wertdatensatz hier angegeben: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Alle Dateien/Ordner (rekursiv)	Der Ordner enthält eine zwischengespeicherte DLL-Datei, die für SFC (System File Checker) verwendet wird, und die Inhalte des Verzeichnisses des System-DLL-Cache werden mithilfe von SFC neu erstellt.
	%SystemRoot%\SYSTEM32\dllCache		
	Stammordner von quorum_device	MSCS*	Wird für Microsoft Cluster Server verwendet.
	%SystemRoot%\SYSTEM32\	perf?00?.dat	Leistungsdaten, die vom Windows-Leistungsindikator verwendet werden.
		perf?00?.bak	
		CATROOT*	Wird für WFP (Windows File Protection) verwendet. Es werden digitale Signaturen der Betriebssystemteminstallationen (wie z. B. DLL, EXE, SYS, OCX usw.) erfasst, um sie vor Löschung oder vor Ersatz von älteren Versionen zu schützen.
	%SystemRoot%\inetsrv\	metabase.bin	Binäre Metabasis-Datei von früheren IIS-Versionen vor 6.0.
	Datei oder Ordner, der im Wert angegeben ist, mit Ausnahme von "Gemeinsamer SIS-Speicher" unter	Alle Dateien/Ordner	Dateien und Ordner sollten nicht

	"HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup"	(rekursiv)	gesichert und nicht wiederhergestellt werden. Weitere Informationen finden Sie unter Link.
XP W2-003	System-Volume	NTLDR	Der Haupt-Boot-Loader.
		BOOT.INI	Enthält die Boot-Konfiguration (falls nicht vorhanden, wird NTLDR standardmäßig auf \Windows auf der ersten Partition der ersten Festplatte gesetzt).
		NTDETECT.COM	Ist erforderlich, um ein NT-basiertes BS zu starten. Erkennt grundlegende Hardware-Informationen, die für einen erfolgreichen Start erforderlich sind.
Vista und höher	Stammordner des System-Volume	boot*	Boot-Ordner für Windows.
		bootmgr	Datei "Windows-Start-Manager"
		EFI\Microsoft\Boot*	Wird für EFI-Boot verwendet.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Speichert ETW-Ablaufverfolgungsdateien (mit der Erweiterung .etl) für Ablaufverfolgungssitzungen

			der Ereignisse in Echtzeit.
		con-fig\RegBack*	Sicherung der aktuellen Regis-trierungstabelle.
Win-8 und höh-er	System-Volume	swapfile.sys	Systemcontroller-Datei, nor-malerweise ca. 256 MB. Wird von Anwendungen im Metro-Stil ver-wendet, die nicht in die her-kömmlichen Paging-Merkmale (wie z. B. Ver-wendungsmuster, Wachstum, Reser-vierung von Spei-cherplatz) von pagefile.sys pas-sen.
		BOOTNXT	Wird verwendet, um von einem BS aus zu starten, das nicht Windows 8 ist. Wird erstellt, wenn die Start-optionen aktiviert werden, und wird von Windows aktualisiert.

Das Aktivitätsprotokoll stellt folgende Informationen bereit:

- Datums- und Uhrzeitinformationen: jobxxxx Systemdateien wurden über-sprungen. Sie können bei Bedarf die Bare-Metal-Recovery-Option (BMR) ver-wenden, um sie wiederherzustellen.
- Datums- und Uhrzeitinformationen: jobxxxx Dateien oder Verzeichnisse wur-den übersprungen. Übersprungene Dateien oder Verzeichnisse finden Sie hier: C:\Programme\Arcserve\Unified Data Protection\Engine\Logs\Restore-<JJJJMMTT>-<hhmmss>-<Prozess-ID>-<Job-ID>.log.

Angeben der Informationen zur Wiederherstellung von Dateien/Ordnern

Arcserve UDP stellt eine Option bereit, mit der Sie eine bestimmte Datei oder einen bestimmten Ordner suchen und wiederherstellen können. Das Ziel eines Wiederherstellungsjobs besteht darin, schnell zu erkennen, welche Daten benötigt werden, und sie vom entsprechenden Sicherungsdatenträger abzurufen. Für jeden Wiederherstellungsjob ist eine Quelle und ein Ziel erforderlich.

Der Prozess für das Wiederherstellen durch Suchen nach Dateien/Ordnern verläuft folgendermaßen:

1. Angeben des Speicherorts der Dateien/Ordner
    - Festlegen von Cloud-Konfigurationen für Wiederherstellungen
2. Angeben der Dateien/Ordner, die wiederhergestellt werden sollen
3. Definieren der Wiederherstellungsoptionen

Angeben des Speicherorts der Dateien/Ordner

Verwenden Sie die Option **Wiederherzustellende Dateien/Ordner suchen**, um Dateien und Ordner wiederherzustellen. Mit dieser Wiederherstellungsmethode können Sie genau festlegen, welche Dateien oder Ordner wiederhergestellt werden sollen.

Gehen Sie wie folgt vor:

1. Verwenden Sie eine der folgenden Vorgangsweisen, um auf das Dialogfeld zur Auswahl der Wiederherstellungsmethoden zuzugreifen:

   In Arcserve UDP:

   a. Melden Sie sich bei Arcserve UDP an.

   b. Klicken Sie auf die Registerkarte **Ressourcen**.

   c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

   e. Klicken Sie bei den Drop-down-Optionen unter **Aktionen** auf **Wiederherstellen**.

      Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

      Hinweis: Sie werden automatisch beim Agentenknoten angemeldet, und das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird im Agentenknoten geöffnet.

   In Arcserve UDP Agent (Windows):

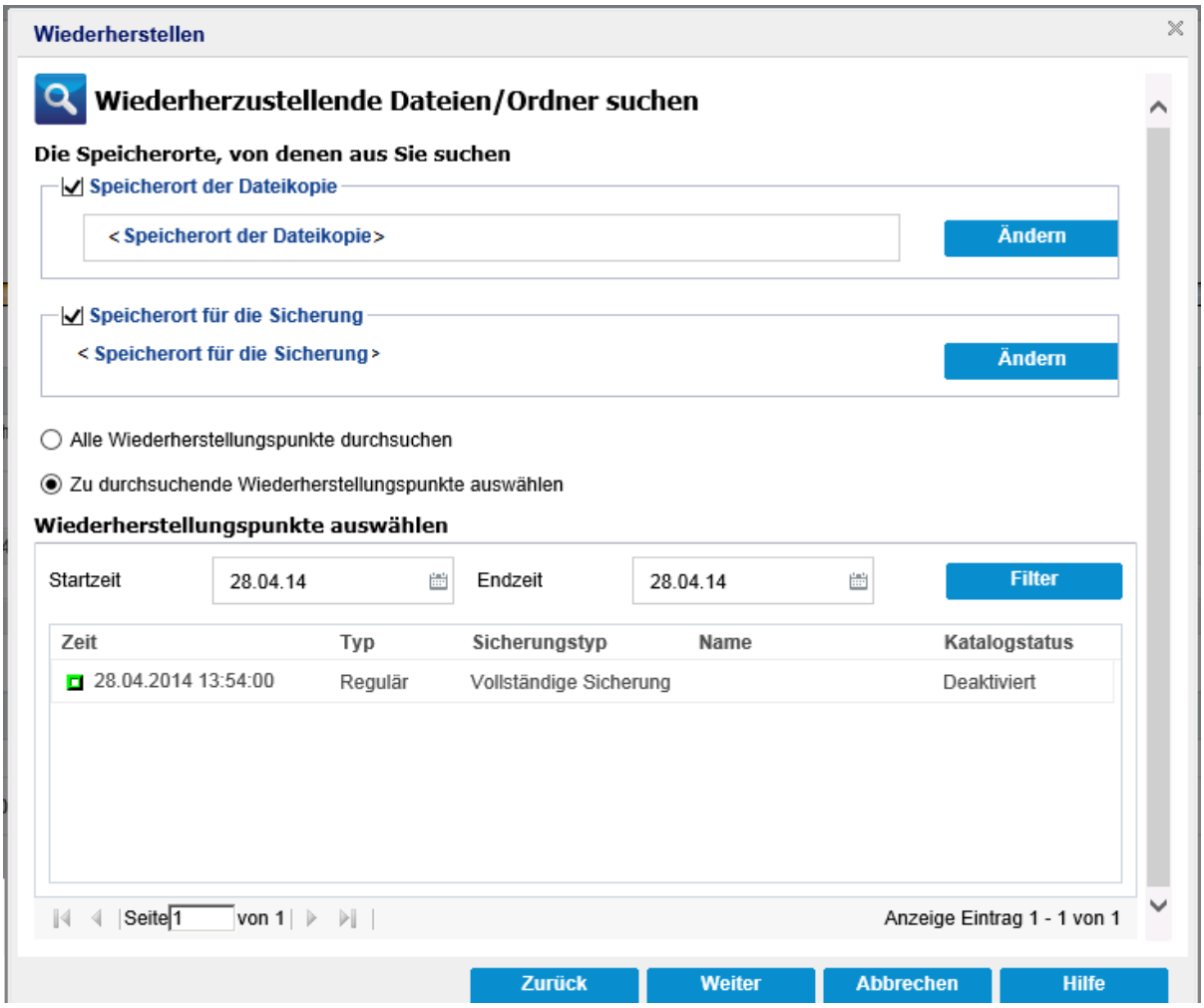
   a. Melden Sie sich bei Arcserve UDP Agent (Windows) an.

   b. Wählen auf der Startseite **Wiederherstellen** aus.

   Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

2. Klicken Sie auf die Option **Wiederherzustellende Dateien/Ordner suchen**.

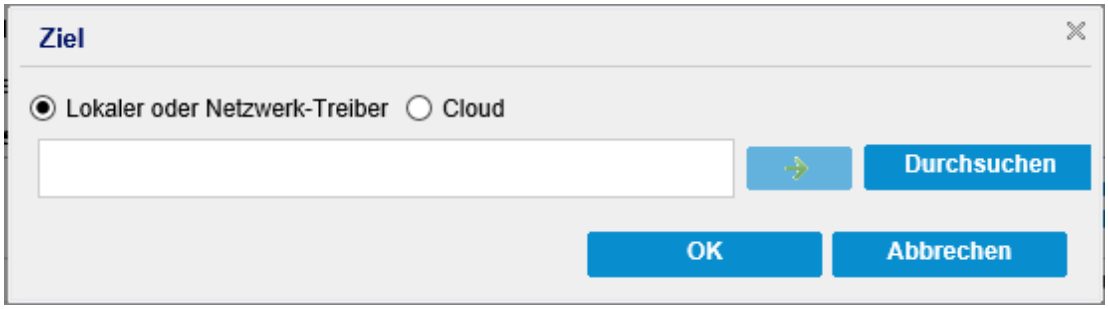
   Das Dialogfeld **Wiederherzustellende Dateien/Ordner suchen** wird geöffnet.



3. Aktivieren Sie das Kontrollkästchen **Speicherort der Dateikopie**, und klicken Sie auf die Schaltfläche **Ändern**, um den Speicherort auf das Ziel zu setzen, an dem Ihre Dateikopie-Images gespeichert sind.

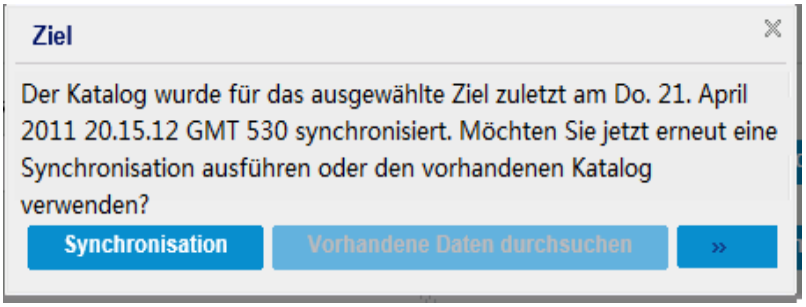
   Das Dialogfeld **Ziel** wird geöffnet. Hier können Sie **Lokales Laufwerk oder Netzwerklaufwerk** oder **Cloud** auswählen.

   Hinweis: Standardmäßig wird in den Feldern **Speicherort für die Sicherung** und **Speicherort der Dateikopie** der Pfad angezeigt, der jeweils für die aktuellsten Sicherungs- bzw. Dateikopieziele verwendet wird.



- Wenn Sie **Lokaler oder Netzwerk-Treiber** auswählen, können Sie entweder einen Speicherort angeben oder den Speicherort suchen, in dem Ihre Dateikopie-Images gespeichert sind.
- Klicken Sie auf das grüne Pfeilsymbol für die Validierung, um zu überprüfen, ob ein ordnungsgemäßer Zugriff auf den Speicherort der Sicherungsquelle besteht.
- Wenn Sie **Cloud** auswählen, können Sie entweder einen Cloud-Speicherort angeben oder auf die Schaltfläche **Konfigurieren** klicken, um das Dialogfeld **Cloud-Konfiguration** anzuzeigen. Weitere Informationen finden Sie unter Festlegen von Cloud-Konfigurationen für Wiederherstellungen.

  Wenn Sie das Ziel in einen alternativen Speicherort ändern, wird unabhängig davon, ob Sie eine Wiederherstellung von einem **lokalen Laufwerk oder Netzwerklaufwerk** oder aus der **Cloud** ausgewählt haben, ein Pop-up-Dialogfeld angezeigt, in dem Sie angeben müssen, ob Sie eine neue Katalogsynchronisation durchführen oder aus dem vorhandenen Katalog lesen möchten.



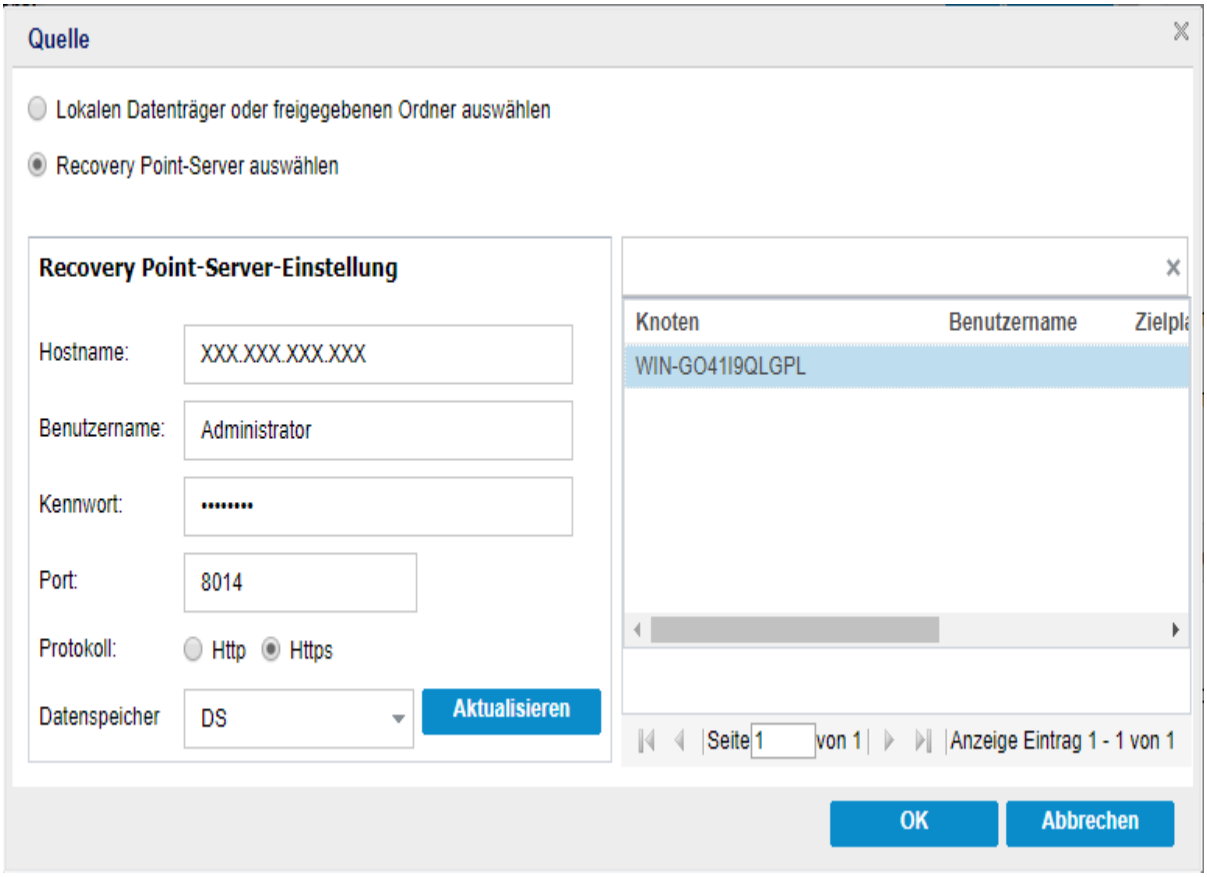
  - Wenn Sie zum ersten Mal eine Katalogsynchronisation durchführen, wird die Schaltfläche **Vorhandene Daten durchsuchen** deaktiviert, da der Dateikopiekatalog nicht lokal vorhanden ist.
  - Wenn zuvor bereits eine Katalogsynchronisation durchgeführt wurde, zeigt dieses Dialogfeld Details über die letzte Katalogsynchronisation von diesem Ziel an. Wenn seit dem angezeigten Zeitpunkt mehrere Dateikopiejobs durchgeführt wurden, ist Ihr Katalog möglicherweise nicht synchronisiert. Sie können die Option **Synchronisieren** auswählen, um sicherzustellen, dass Ihr Dateikopiekatalog aktuell ist.

    1. Klicken Sie auf **Synchronisieren**, um den Dateikopiekatalog vom angegebenen Dateikopieziel auf Ihren lokalen Rechner herunterzuladen, um den Suchvorgang zu beschleunigen.

    2. Klicken Sie auf **Vorhandene Daten durchsuchen**, um den lokal verfügbaren Dateikopiekatalog zu verwenden und ihn nicht erneut herunterzuladen bzw. zu synchronisieren.

4. Aktivieren Sie das Kontrollkästchen **Speicherort für die Sicherung**, und klicken Sie auf **Ändern**, um den Speicherort für die Sicherung zu ändern.

   Das Dialogfeld **Quelle**, in dem Sie den Sicherungsspeicherort auswählen können, wird geöffnet.



5. Wählen Sie im Dialogfeld **Quelle** eine der folgenden Optionen aus:

   Lokalen Datenträger oder freigegebenen Ordner auswählen

   a. Legen Sie den Speicherort fest, unter dem Ihre Sicherungs-Images gespeichert werden, und wählen Sie die entsprechende Sicherungsquelle aus.

      Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Quellspeicherort zu erhalten.

      Das Dialogfeld **Speicherort für die Sicherung auswählen** wird geöffnet.

   b. Wählen Sie den Ordner, in dem die Wiederherstellungspunkte gespeichert sind, aus, und klicken Sie auf **OK**.

      Das Dialogfeld **Speicherort für die Sicherung auswählen** wird geschlossen, und der Sicherungsspeicherort wird im Dialogfeld **Quelle** angezeigt.

c. Klicken Sie auf **OK**.

Die Wiederherstellungspunkte werden im Dialogfeld **Wiederherzustellende Dateien/Ordner suchen** aufgelistet.

Auswählen des Recovery Point Servers

a. Geben Sie die Details für die **Einstellungen des Recovery Point Servers** an, und klicken Sie auf **Aktualisieren**.

Alle Agenten werden in der Spalte **Data Protection Agent** im Dialogfeld **Quelle** aufgelistet.

b. Wählen Sie den Agenten aus der angezeigten Liste aus, und klicken Sie auf **OK**.

Die Wiederherstellungspunkte werden im Dialogfeld **Wiederherzustellende Dateien/Ordner suchen** aufgelistet.

Hinweis: Wenn Sie einen anderen Agenten auswählen und wenn die Wiederherstellungspunkte verschlüsselt sind, dann müssen Sie das Verschlüsselungskennwort angeben, wenn Sie danach gefragt werden.

6. Aktivieren Sie eine der folgenden Optionen, um Wiederherstellungspunkte zu suchen:

Alle Wiederherstellungspunkte durchsuchen

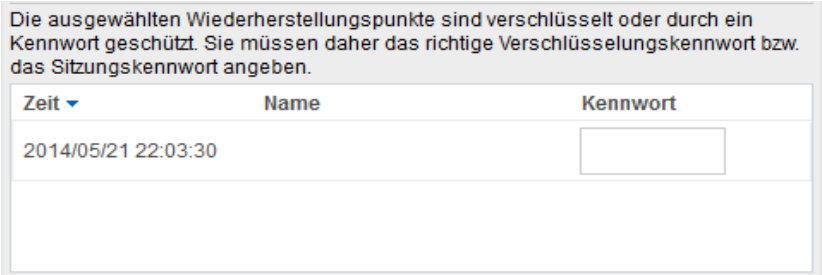
Sucht die Datei oder den Ordner in allen Wiederherstellungspunkten, die im angegebenen Speicherort gespeichert sind. Sie müssen die Datei oder den Ordner, die bzw. den Sie finden möchten, im Dialogfeld **Wiederherzustellende Dateien/Ordner suchen** angeben.

Zu durchsuchende Wiederherstellungspunkte auswählen

Zeigt die Wiederherstellungspunkte zwischen dem angegebenen Zeitraum an. Sie können die Startzeit und Endzeit angeben und anschließend den Wiederherstellungspunkt aus dem angegebenen Zeitraum auswählen.

7. Wählen Sie den Wiederherstellungspunkt aus, und klicken Sie auf **Weiter**.

Hinweis: Wenn Sie im Dialogfeld **Quelle** einen anderen Agenten ausgewählt haben und die Wiederherstellungspunkte verschlüsselt sind, wird das Verschlüsselungsdialogfeld geöffnet. Geben Sie das Kennwort ein, und klicken Sie auf **OK**.



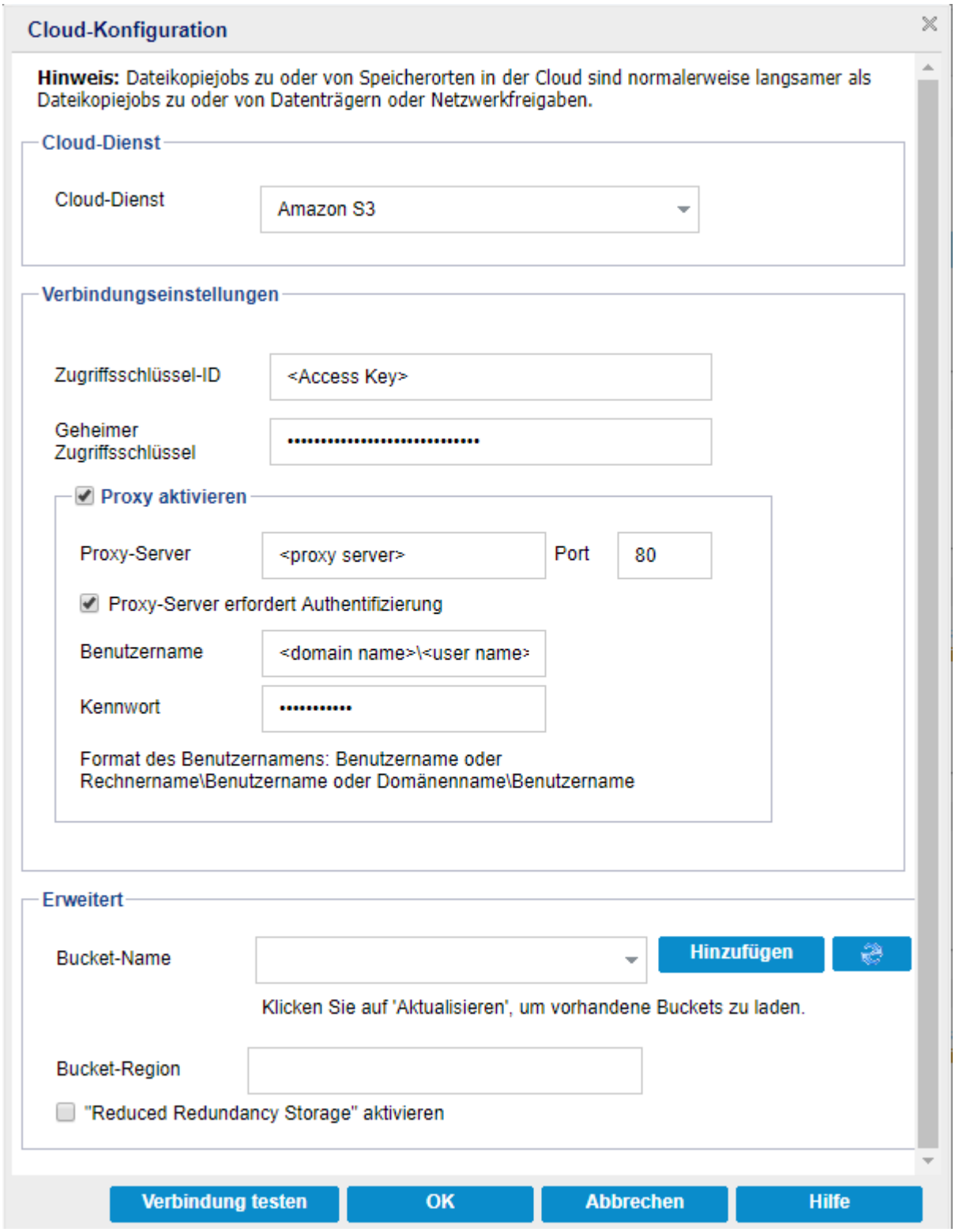
Das Dialogfeld **Wiederherzustellende Dateien/Ordner suchen** wird geöffnet.

Der Speicherort für die **Sicherung oder Dateikopie** ist angegeben.

Festlegen von Cloud-Konfiguration für Wiederherstellungen

Hinweis: Der folgende Vorgang gilt nur, wenn Sie eine Datei bzw. einen Ordner von einem Cloud-Dateikopiespeicherort wiederherstellen.

Klicken Sie in den Optionen **Nach Dateikopien suchen** oder **Wiederherzustellende Dateien/Ordner suchen** auf die Schaltfläche **Konfigurieren**, um das Dialogfeld **Cloud-Konfiguration** anzuzeigen.



Gehen Sie wie folgt vor:

1. Verwenden Sie das Drop-down-Menü im Dialogfeld **Cloud-Konfiguration**, um auszuwählen, von welchem Cloud-Anbietertyp Sie die Wiederherstellung ausführen möchten. Die verfügbaren Optionen sind **Amazon S3**, **Windows Azure**, **FUJITSU**

Hybrid IT Service FJcloud-O und **Eucalyptus-Walrus**. (**Amazon S3** ist der Standardanbieter). Weitere Informationen zu Fujitsu Cloud (Windows Azure) und FUJITSU Hybrid IT Service FJcloud-O finden Sie unter Übersicht und Registrierung.

Hinweis: Wenn der Pfad nach der Verschlüsselung des Bucket-Namens länger als 170 Zeichen ist, kann Eucalyptus-Walrus keine Dateien kopieren.

2. Legen Sie die **Konfigurationsoptionen** fest.

   Die Konfigurationsoptionen für jeden Cloud-Anbieter sind ähnlich (mit etwas unterschiedlicher Terminologie), und alle Unterschiede werden beschrieben.

   a. Geben Sie die **Verbindungseinstellungen** an:

      Anbieter-URL:

      Identifiziert die URL-Adresse des Cloud-Anbieters.

      Für Amazon S3 und Windows Azure wird die Anbieter-URL automatisch vorab aufgefüllt. Bei Eucalyptus-Walrus muss die Anbieter-URL mithilfe des angegebenen Formats manuell eingegeben werden.

      Zugriffsschlüssel-ID/Kontoname/Abfrage-ID

      Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

      Für dieses Feld verwendet Amazon S3 die Zugriffsschlüssel-ID, Windows Azure und FUJITSU Hybrid IT Service FJcloud-O verwenden den Kontonamen, und Eucalyptus-Walrus verwendet die Abfrage-ID.

      Geheimer Zugriffsschlüssel/Geheimschlüssel

      Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

      Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Ort aufbewahren. Bewahren Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

      Für dieses Feld verwendet Amazon S3 den geheimen Zugriffsschlüssel. Windows Azure, FUJITSU Hybrid IT Service FJcloud-O und Eucalyptus-Walrus verwenden einen geheimen Schlüssel.

      Proxy aktivieren

      Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-

Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Sie müssen dann die entsprechenden Authentifizierungsinformationen (Benutzername und Kennwort) angeben, die zur Verwendung des Proxy-Servers erforderlich sind.

(Proxy-Fähigkeit ist für Eucalyptus-Walrus nicht verfügbar).

b. Nehmen Sie die Eingaben unter **Erweiterte Einstellungen** vor:

Bucket-Name/Container

Alle Dateien und Ordner, die zum Cloud-Anbieter verschoben oder kopiert wurden, werden in Ihren Buckets (oder Containern) gespeichert und organisiert. Buckets sind wie Container für Ihre Dateien und werden verwendet, um Objekte zu gruppieren und gemeinsam zu verwalten. Jedes Objekt, das beim Cloud-Anbieter gespeichert wurde, wird in einem Bucket abgelegt.

Wählen Sie aus der Drop-down-Liste einen Bucket-Namen aus. Bei Bedarf können Sie auf die Schaltfläche **Aktualisieren** klicken, um die Liste der verfügbaren Buckets zu aktualisieren.

Für dieses Feld nutzen Amazon S3 und Eucalyptus-Walrus einen Bucket-Namen. Windows Azure und FUJITSU Hybrid IT Service FJcloud-O verwenden Container.

Bucket-Region

Bezieht sich auf die Region des Buckets in Amazon und FUJITSU Hybrid IT Service FJcloud-O.

Vertragsnummer

Bezieht sich auf die Nummer Ihres Vertrages für FUJITSU Hybrid IT Service FJcloud-O.

Projekt-ID

Bezieht sich auf die von FUJITSU Hybrid IT Service FJcloud-O generierte ID des Projekts.

"Reduced Redundancy Storage" aktivieren

Nur bei Amazon S3 können Sie mit dieser Option "Reduced Redundancy Storage" (RRS) aktivieren. RRS ist eine Speicheroption innerhalb von Amazon S3, die Ihnen hilft, durch das Speichern von unkritischen, reproduzierbaren Daten auf niedrigeren Redundanzniveaus als dem Amazon S3s Standard-Speicher Kosten zu sparen. Sowohl die Standardoption als auch die RRS-Option speichern Daten in mehreren Einrichtungen und auf

mehreren Geräten. Allerdings werden die Daten mit RRS weniger oft repliziert, sodass die Kosten geringer sind. Sie sollten die gleiche Latenz und den gleichen Durchsatz erhalten, indem Sie entweder den Standardspeicher von Amazon S3 oder RRS verwenden. Standardmäßig ist diese Option nicht aktiviert (Amazon S3 verwendet die standardmäßige Speicheroption).

3. Klicken Sie auf **Verbindung testen**, um die Verbindung zum angegebenen Cloud-Speicherort zu überprüfen.
4. Klicken Sie auf **OK**, um das Dialogfeld Cloud-Konfiguration zu verlassen.

Angeben der Dateien/Ordner, die wiederhergestellt werden sollen

Nachdem Sie den Speicherort für die Sicherung oder den Speicherort der Dateikopie angegeben haben, suchen Sie nach dem Datei- oder Ordnernamen, der wiederhergestellt werden soll. Wenn die Datei mehrere Versionen der Dateikopie hat, werden alle Versionen nach Datum geordnet aufgelistet (die letzte Version steht an erster Stelle).

Gehen Sie wie folgt vor:

1. Geben Sie im Dialogfeld **Wiederherzustellende Dateien/Ordner suchen** an, wonach Sie suchen (Name der Datei bzw. des Ordners für die Wiederherstellung).

   Hinweis: Das Feld **Dateiname** unterstützt die Suche nach vollständigen Namen und mit Platzhaltern. Wenn Ihnen der vollständige Dateiname nicht bekannt ist, können Sie die Abfrage vereinfachen, indem Sie die Platzhalter "*" und "?" im Feld "Dateiname" eingeben.

   Folgende Platzhalter für den Datei- oder Ordnernamen werden unterstützt:

   - Verwenden Sie den Asterisk, um null oder mehr Zeichen in einem Datei- oder Ordnernamen zu ersetzen.
   - Verwenden Sie das Fragezeichen, um ein einzelnes Zeichen in einem Datei- oder Ordnernamen zu ersetzen.

   Beispiel: Wenn Sie *.txt angeben, werden alle Dateien mit einer .txt-Dateierweiterung in den Suchergebnissen angezeigt.

2. (Optional) Geben Sie einen Pfad an, um Ihre Suche zu filtern, und geben Sie an, ob Unterverzeichnisse in die Suche eingeschlossen werden sollen.

3. Klicken Sie auf **Suchen**, um die Suchergebnisse aufzurufen.

   Die Suchergebnisse werden angezeigt. Wenn die gesuchte Datei mehrere Versionen der Dateikopie hat, werden alle Versionen nach Datum geordnet aufgelistet (die letzte Version steht an erster Stelle). Es wird auch angezeigt, ob die gesuchte Datei gesichert oder kopiert wurde.

4. Wählen Sie die Version (das Vorkommnis) der Dateien oder Ordner aus, die Sie wiederherstellen möchten, und klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet.

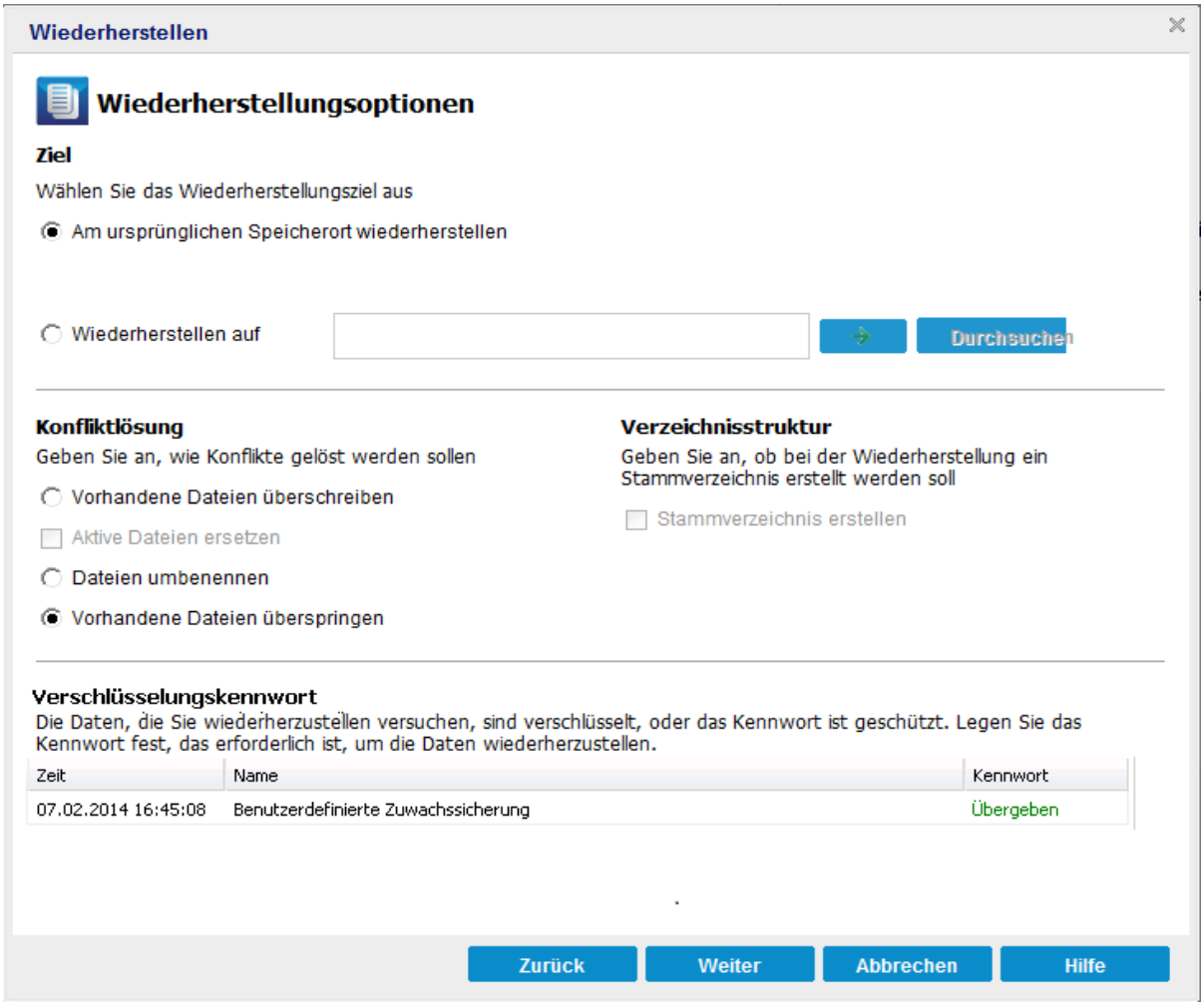
   Der wiederherzustellende Datei-/Ordnername ist angegeben.

Definieren der Wiederherstellungsoptionen

Nachdem Sie die wiederherzustellenden Dateien oder Ordner angegeben haben, legen Sie die Wiederherstellungsoptionen für die ausgewählte Datei oder den ausgewählten Ordner fest.

Gehen Sie wie folgt vor:

1. Geben Sie das Wiederherstellungsziel im Dialogfeld **Wiederherstellungsoptionen** an.



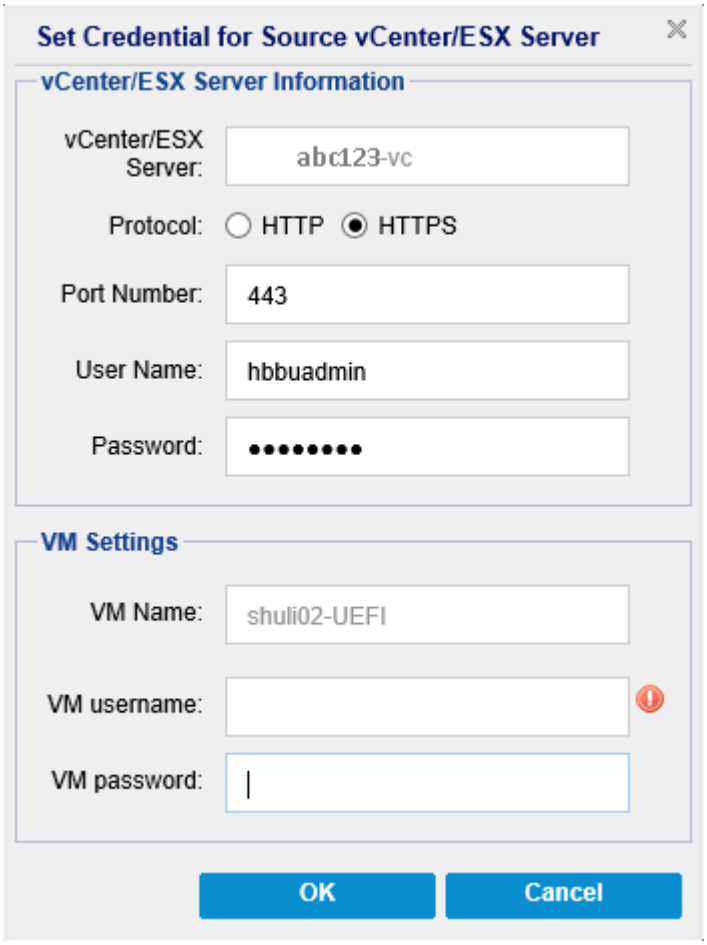
Es sind folgende Zieloptionen verfügbar:

Am ursprünglichen Speicherort wiederherstellen

Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

Hinweis: Wenn Sie die Recovery Point-Sicherung mithilfe der hostbasierten agentenlosen Sicherung durchgeführt haben, wird die Datei bei der Wiederherstellung am ursprünglichen Speicherort auf dem virtuellen Rechner wiederhergestellt. In diesem Fall wird ein Dialogfeld geöffnet. Sie können die Anmeldeinformationen des Hypervisors und des Betriebssystems des virtuellen Rechners eingeben.

Für VMware-VM:



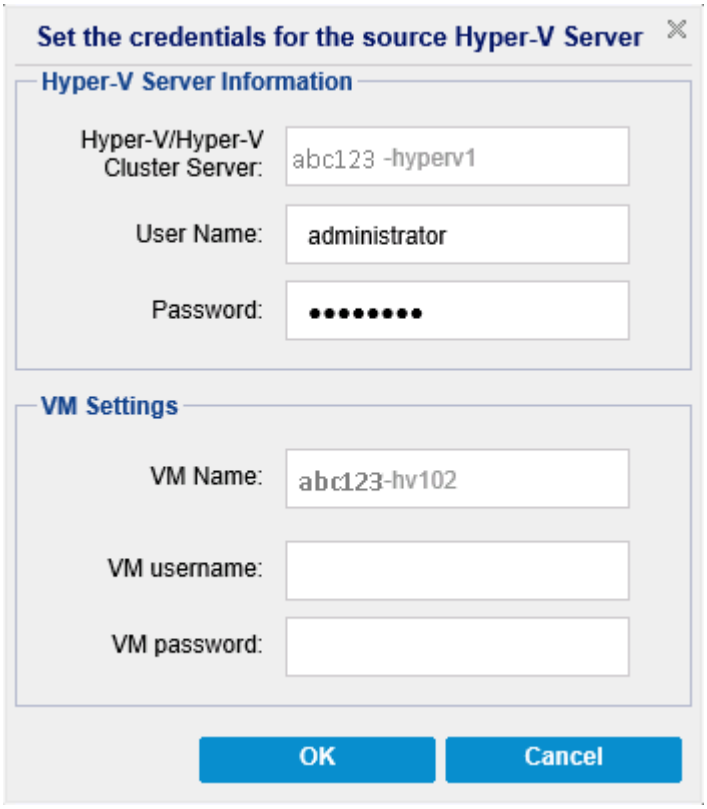
Hinweis: Um Dateien innerhalb des virtuellen Rechners zu erstellen und schreiben zu können, beachten Sie die folgenden Anforderungen für die Einstellungen und die Kontoberechtigung des virtuellen Rechners:

- VMware-Tools ist installiert und wird ausgeführt.
- Firewall muss Datei- und Druckerfreigabe zulassen.

- Das Konto ist ein integrierter lokaler Administrator, integrierter Domänenadministrator oder ein Domänenkonto, das Mitglied der lokalen Administratorengruppe ist. Wenn andere Konten verwendet werden:
  - Deaktivieren Sie den Remote-Zugriff auf UAC. Informationen zum Deaktivieren des Remote-Zugriffs auf UAC finden Sie in Importieren von virtuellen Rechnern mit einem zusätzlichen Administratorkonto.
  - Deaktivieren Sie UAC in der lokalen Sicherheitsrichtlinie, indem Sie die Einstellung zur Ausführung aller Administratoren im Administrator-Genehmigungsmodus unter secpol.msc-> lokale Richtlinien-> Sicherheitsoptionen deaktivieren. (Secpol.msc ist der Editor für Sicherheitsrichtlinien von Microsoft).

    Wichtig: Versuchen Sie nicht, die UAC im Dialogfeld "Einstellungen zur Benutzerkontensteuerung" zu deaktivieren, das über die Systemsteuerung geöffnet wird.

Für Hyper-V-VM:

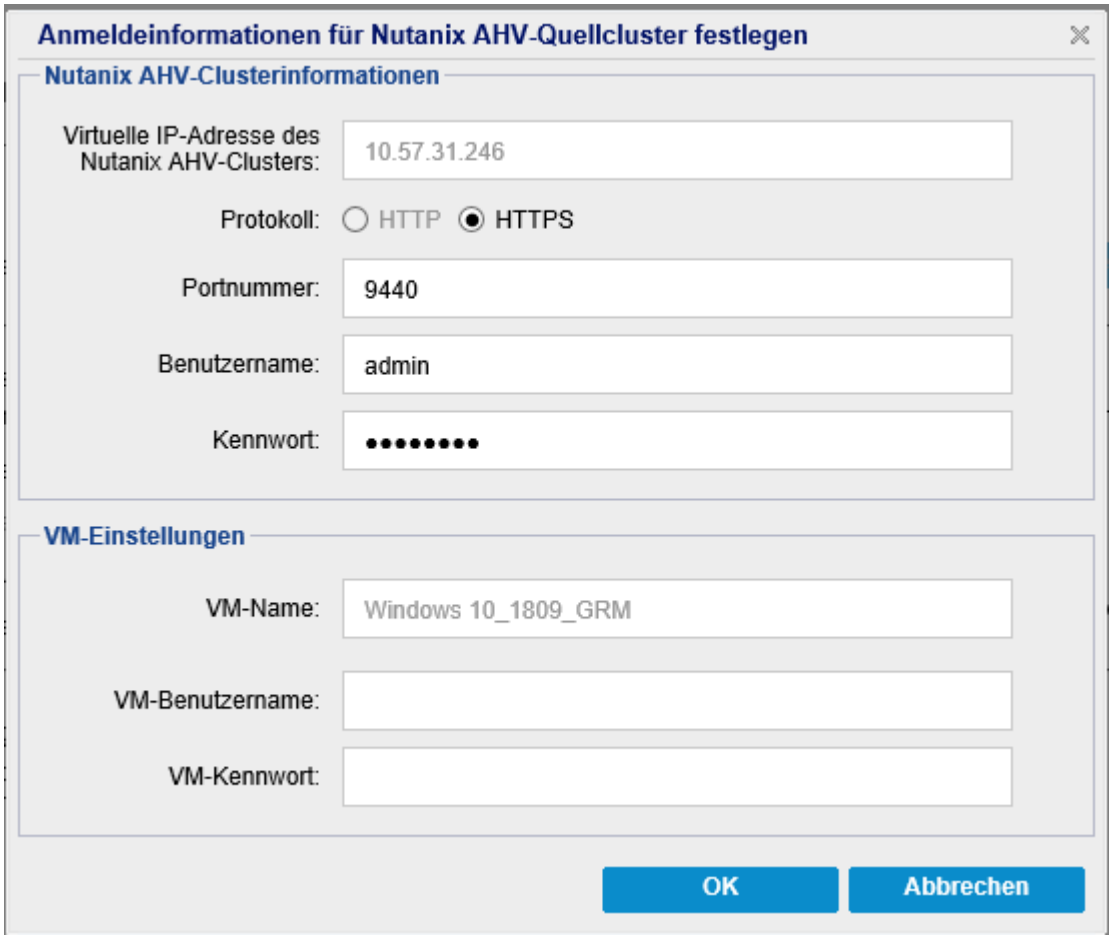


Hinweis: Um Dateien innerhalb des virtuellen Rechners zu erstellen und schreiben zu können, beachten Sie die folgenden Anforderungen für die Einstellungen und die Kontoberechtigung des virtuellen Rechners:

- Hyper-V-Integrationsdienste sind installiert und werden ausgeführt.
- Firewall muss Datei- und Druckerfreigabe zulassen.
- Das Konto ist ein integrierter lokaler Administrator, integrierter Domänenadministrator oder ein Domänenkonto, das Mitglied der lokalen Administratorengruppe ist. Wenn andere Konten verwendet werden:

  Deaktivieren Sie den Remote-Zugriff auf UAC. Informationen zum Deaktivieren des Remote-Zugriffs auf UAC finden Sie in Importieren von virtuellen Rechnern mit einem zusätzlichen Administratorkonto.
- Wenn das VM-Gast-BS Clientversion-Windows (z. B. Windows 10) ist, muss Firewall manuell so konfiguriert werden, dass Windows-Verwaltungsinstrumentation (WMI) zugelassen wird.

Für Nutanix VM



Hinweise: Um Dateien innerhalb der VM erstellen oder schreiben zu können, beachten Sie die folgenden Anforderungen an die Einstellungen und Kontenberechtigungen der virtuellen Maschine:

- Firewall muss Datei- und Druckerfreigabe zulassen.
- Das Konto ist ein integrierter lokaler Administrator, integrierter Domänenadministrator oder ein Domänenkonto, das Mitglied der lokalen Administratorengruppe ist. Wenn andere Konten verwendet werden:

  Deaktivieren Sie den Remote-Zugriff auf UAC. Informationen zum Deaktivieren des Remote-Zugriffs auf UAC finden Sie in Importieren von virtuellen Rechnern mit einem zusätzlichen Administratorkonto.
- Die Firewall muss Windows Management Instrumentation(WMI) erlauben.

Wiederherstellen auf

Stellt am angegebenen Speicherort wieder her. Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.

2. Legen Sie die Option für die **Konfliktlösung** fest, die von Arcserve UDP ausgeführt werden soll, wenn während der Wiederherstellung Konflikte auftreten.

   Es sind folgende Optionen verfügbar:

   Vorhandene Dateien überschreiben

   Überschreibt (ersetzt) alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind. Alle Objekte werden aus den Sicherungsdateien wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.

   Aktive Dateien ersetzen

   Ersetzt alle aktiven Dateien nach einem Neustart. Wenn Arcserve UDP Agent (Windows) während eines Wiederherstellungsversuchs entdeckt, dass die vorhandene Datei gerade verwendet wird oder gerade auf sie zugegriffen wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

   Diese Option ist nur verfügbar, wenn Sie die Option **Vorhandene Dateien überschreiben** auswählen.

   Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien im Wiederherstellungsprozess übersprungen.

   Dateien umbenennen

Erstellt eine neue Datei, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit demselben Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten sind dann in einer neuen Datei wiederhergestellt.

Vorhandene Dateien überspringen

Überspringt alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, und überschreibt (ersetzt) sie nicht. Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

Standard: Vorhandene Dateien überspringen

3. Geben Sie die **Verzeichnisstruktur** an, um während der Wiederherstellung ein Stammverzeichnis zu erstellen.

Stammverzeichnis erstellen

Legt fest, dass Arcserve UDP die Stammverzeichnisstruktur des erfassten Sicherungs-Images, soweit vorhanden, am Zielpfad wiederherstellt.

Wenn diese Option nicht ausgewählt wird, wird die Datei oder der Ordner direkt im Zielordner wiederhergestellt.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt" und "C:\Ordner1\Unterordner2\B.txt" erfasst und als Wiederherstellungsziel "D:\Wiederherstellen" ausgewählt.

- Wenn Sie die Wiederherstellung der Dateien "A.txt" und "B.txt" einzeln festgelegt haben, werden die Dateien in "D:\Wiederherstellen\A.txt" und "D:\Wiederherstellen\B.txt" wiederhergestellt (das Stammverzeichnis über der ausgewählten Dateiebene wird nicht wiederhergestellt).
- Wenn Sie eine Wiederherstellung auf "Unterordner2"-Ebene auswählen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Unterordner2\A.txt" und "D:\Wiederherstellen\Unterordner2\B.txt" (das Stammverzeichnis über der ausgewählten Ordnerebene wird nicht wiederhergestellt).

Wenn diese Option ausgewählt ist, wird der gesamte Stammverzeichnispfad für die Dateien/Ordner (einschließlich des Volume-Namens) im Zielordner neu erstellt. Wenn Dateien/Ordner vom selben Volume-Name wiederhergestellt werden sollen, ist dieser Volume-Name nicht im Wiederherstellungsziel-Stammverzeichnispfad enthalten. Wenn Dateien/Ordner von einem anderen Volume-Name wiederhergestellt werden sollen, enthält der Wiederherstellungsziel-Stammverzeichnispfad diesen Volume-Namen.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt", "C:\Ordner1\Unterordner2\B.txt" und

E:\Ordner3\Unterordner4\C.txt erfasst, und bei der Wiederherstellung "D:\Wiederherstellen" als Wiederherstellungsziel ausgewählt.

- Wenn Sie nur die Datei "A.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Ordner1\Unterordner2\A.txt" (das gesamte Stammverzeichnis wird ohne den Volume-Namen erneut erstellt).
- Wenn Sie die Dateien "A.txt" und "C.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\C\Ordner1\Unterordner2\A.txt" und "D:\Wiederherstellen\ E\Ordner3\Unterordner4\C.txt" (das gesamte Stammverzeichnis wird mit dem Volume-Namen erneut erstellt).

4. Das **Verschlüsselungskennwort** für das Dateikopieziel wird automatisch geladen. Wenn Sie ein alternatives Ziel für die Wiederherstellung auswählen, müssen Sie das Kennwort manuell eingeben.
5. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsübersicht** wird geöffnet.

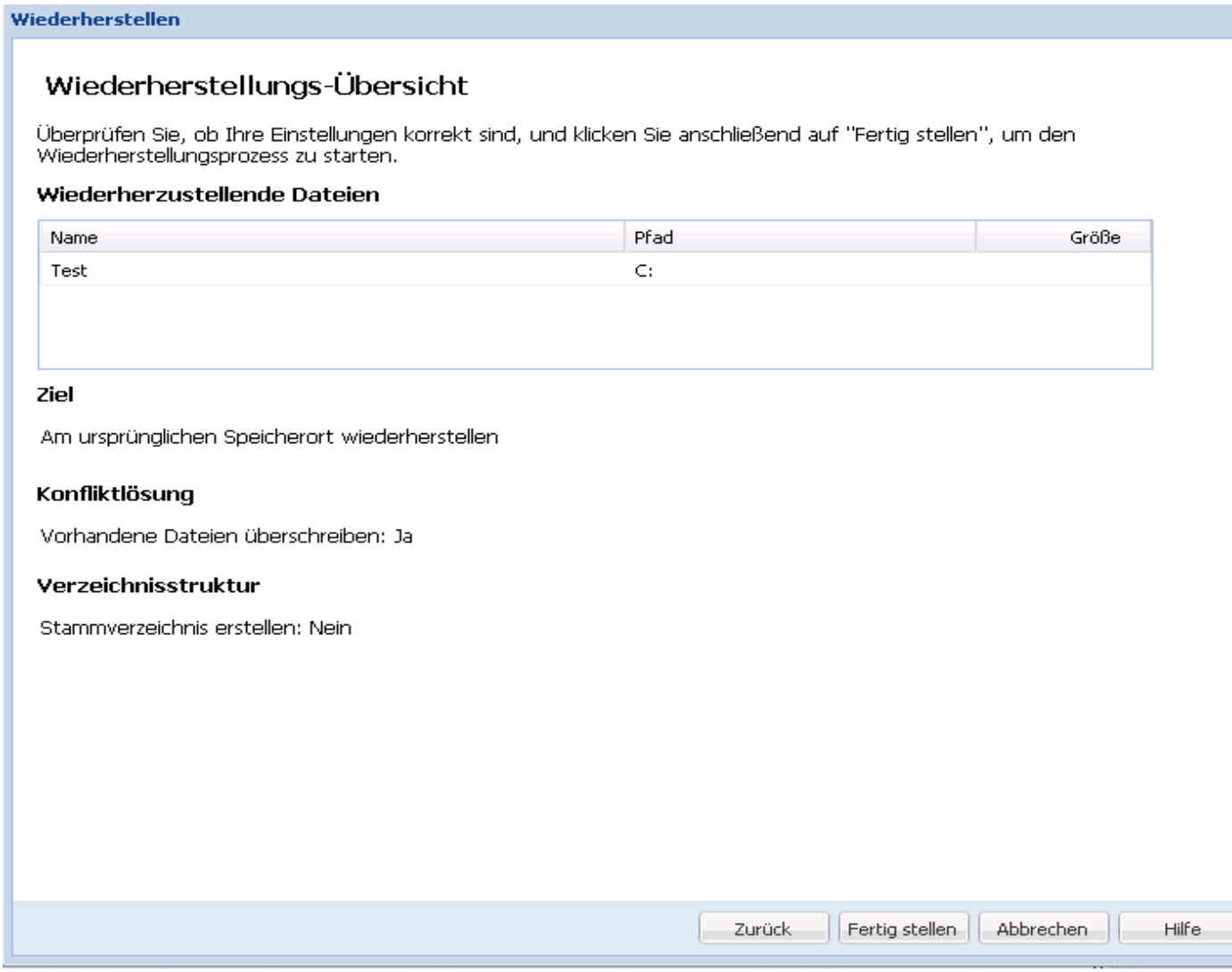
   Die Wiederherstellungsoptionen sind für die Wiederherstellung der angegebenen Dateien/Ordner festgelegt.

Wiederherstellen der Datei bzw. des Ordners

Das Dialogfeld **Wiederherstellungs-Übersicht** ist hilfreich, um alle Wiederherstellungsoptionen zu überprüfen, die Sie zuvor festgelegt haben, und sie bei Bedarf zu ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die angezeigten Informationen im Dialogfeld **Wiederherstellungs-Übersicht**, um die Richtigkeit aller Wiederherstellungsoptionen und Einstellungen sicherzustellen.



- Wenn die Übersichtsinformationen Fehler enthalten, klicken Sie auf **Zurück**, und ändern Sie die inkorrekten Einstellungen im entsprechenden Dialogfeld.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsprozess zu starten.

Die angegebenen Dateien/Ordner sind wiederhergestellt.

Überprüfen, ob die Datei bzw. der Ordner wiederhergestellt wurde

Überprüfen Sie nach dem Abschluss der Wiederherstellung, ob die Dateien/Ordner im angegebenen Ziel wiederhergestellt wurden.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Wiederherstellungsziel, das Sie angegeben haben.

   Eine Liste mit Ordnern wird angezeigt.

2. Suchen Sie die Datei, in der Sie den Inhalt wiederhergestellt haben.

   Wenn Sie zum Beispiel auswählen, dass Datei A.txt am Wiederherstellungsziel als "D:\Restore" wiederhergestellt werden soll, navigieren Sie zu folgendem Speicherort:

   D:\Restore\A.txt.

3. Überprüfen Sie den Inhalt der wiederhergestellten Dateien/Ordner.

   Der wiederhergestellte Inhalt wurde erfolgreich überprüft.

Ausführen einer Bare-Metal-Recovery mithilfe einer Virtual Standby-VM oder Instant VM

Eine Bare-Metal-Recovery ist eine Wiederherstellung Ihres Computersystems "von Null", einschließlich des Betriebssystems und Softwareanwendungen, mit einer darauffolgenden Wiederherstellung von Daten und Einstellungen. Durch eine Bare-Metal-Recovery können Sie Ihren Rechner mit minimalem Aufwand vollständig wiederherstellen. Dies ist sogar auf einer anderen Hardware möglich. BMR ist möglich, da Arcserve UDP Agent (Windows) während der Sicherung auf Blockebene nicht nur Daten, sondern auch Informationen erfasst werden, die sich auf folgende Anwendungen beziehen:

- Betriebssystem
- Installierte Anwendungen
- Konfigurationseinstellungen
- Erforderliche Treiber

  Alle Informationen, die für eine vollständige Systemwiederherstellung "von Null" benötigt werden, werden in mehreren Blöcken gesichert und im Sicherungsziel gespeichert.

Verwenden Sie eine der folgenden Methoden, um eine BMR von einem virtuellen Rechner auszuführen:

- Stellen Sie eine direkte Verbindung mit dem ESX-Server über die IP-Adresse her.
- Fügen Sie die richtige DNS-Einstellung auf Ihrem BMR-Rechner hinzu, und lösen Sie den Hostnamen in die IP-Adresse auf.

Gehen Sie folgt vor, um eine BMR mithilfe einer Virtual Standby VM oder Instant VM auszuführen:

1. Überprüfen der Voraussetzungen und Hinweise für BMR
2. Definieren der BMR-Optionen
   - Wiederherstellen mit einer Hyper-V-basierten Virtual Standby VM oder Instant VM
   - Wiederherstellen mit einer VMware-basierten Virtual Standby VM oder Instant VM
   - Ausführen von BMR im Expressmodus
   - Ausführen von BMR im erweiterten Modus
3. Überprüfen des Erfolgs der BMR

4. BMR-Referenzinformationen
5. Beheben von BMR-Problemen

Überprüfen der Voraussetzungen und Hinweise für BMR

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine BMR ausführen:

- Sie müssen über eines der folgenden Images verfügen:
  - Ein auf eine CD/DVD gebranntes erstelltes ISO-Image für BMR
  - Ein auf einen tragbaren USB-Stick gebranntes erstelltes ISO-Image für BMR

  Hinweis: Mit Arcserve UDP Agent (Windows) können Sie mithilfe eines Bootkit-Hilfsprogramms ein WinPE-Image und ein Arcserve UDP Agent (Windows)-Image miteinander verbinden, um ein BMR-ISO-Image zu erstellen. Dieses ISO-Image wird auf einen startfähigen Datenträger gebrannt. Sie können beide startfähigen Datenträger (CD/DVD oder USB-Stick) verwenden, um das neue Computersystem zu initialisieren und den Bare Metal Recovery-Prozess zu starten. Um sicherzustellen, dass Ihr gespeichertes Image immer die aktuellste Version ist, erstellen Sie jedes Mal ein neues ISO-Image, wenn Sie Arcserve UDP Agent (Windows) aktualisieren.
- Sie müssen über mindestens eine vollständige Sicherung verfügen.
- Auf dem virtuellen Rechner und auf dem Quellserver, den Sie wiederherstellen, muss mindestens 1 GB RAM installiert sein.
- Um virtuelle VMware-Rechner zu virtuellen VMware-Rechnern wiederherzustellen, die auf das Verhalten eines physischen Servers konfiguriert wurden, stellen Sie sicher, dass die Anwendung "VMware Tools" auf dem virtuellen Rechner des Ziels installiert ist.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Überprüfen Sie die folgenden Wiederherstellungshinweise:

- Der Prozess der Bare-Metal-Recovery ist bei den beiden Arten der Erstellung des Bootkit-Images praktisch identisch.

  Hinweis: Der BMR-Prozess kann keine Speicherplätze erstellen. Wenn der Quellrechner Speicherplätze hat, können Sie im Zuge der BMR keine Speicherplätze am Zielrechner erstellen. Sie können diese Volumes als normale Datenträger/Volumes wiederherstellen oder vor der Ausführung der BMR manuell Speicherplätze erstellen, um Daten in diesen Speicherplätzen wiederherzustellen.

- Dynamische Datenträger werden nur auf Datenträgerebene wiederhergestellt. Wenn Ihre Daten auf einem lokalen Volume eines dynamischen Datenträgers gesichert sind, können Sie diesen dynamischen Datenträger während der Bare-Metal-Recovery nicht wiederherstellen. Um in diesem Szenario eine Wiederherstellung während der BMR durchzuführen, müssen Sie eine der folgenden Aufgaben ausführen, und dann eine BMR vom kopierten Wiederherstellungspunkt aus durchführen:
  - Führen Sie eine Sicherung auf einem Volume oder auf einem anderen Laufwerk durch.
  - Führen Sie eine Sicherung auf der Remote-Freigabe durch.
  - Kopieren Sie einen Wiederherstellungspunkt in einen anderen Speicherort.

  Hinweis: Wenn Sie die BMR bei mehreren dynamischen Datenträgern ausführen, kann die BMR wegen unerwarteter Fehler fehlschlagen (z. B. Fehler beim Starten, unerkannte dynamische Volumes usw.). Wenn dies auftritt, sollten Sie nur den Systemdatenträger mithilfe von BMR wiederherstellen, und dann können Sie nach dem Rechnerneustart die anderen dynamischen Volumes auf einer normalen Umgebung wiederherstellen.
- Wenn Sie versuchen, eine BMR auf einer Hyper-V-VM mit einem 4 KB-Datenträger auszuführen, fügen Sie diesen 4 KB-Datenträger zum SCSI-Controller hinzu. Wenn Sie ihn der IDE-Steuerung hinzufügen, dann wird der Datenträger im Windows PE-System nicht erkannt.
- (Optional) Überprüfen Sie die BMR-Referenzinformationen. Weitere Informationen finden Sie in den folgenden Themen:
  - Funktionsweise von Bare-Metal-Recovery
  - Betriebssysteme, die UEFI/BIOS-Konvertierung unterstützen
  - Verwalten des Menüs von BMR-Vorgängen

Überprüfen Sie die folgenden Hinweise:

- Wenn Sie auf eine neuere Version oder ein Update von Arcserve UDP aktualisieren, müssen Sie das BMR-ISO-Image mithilfe der entsprechenden Windows AIK oder ADK-Ebene erneut erstellen, um die neuesten Funktionen und Fehlerkorrekturen unterstützen zu können. Nachdem eine BMR-ISO-Image erstellt wurde, kann jedoch die ISO-Datei für die gleiche BS-Stufe verwendet werden. Für folgende BS-Stufen können Sie das gleiche ISO-Image verwenden:
  - Mithilfe von Windows 7 WAIK erstelltes ISO-Image – funktioniert auf Windows 2003, Vista, 2008, 2008R2
  - Mithilfe von Windows 8/8.1 ADK erstelltes ISO-Image – funktioniert auf Windows 8, 8.1, Server 2012, Server 2012 R2

- Mithilfe von Windows 10 ADK erstelltes ISO-Image – funktioniert auf Windows 10

Definieren der BMR-Optionen

Bevor Sie den BMR-Prozess initiieren, müssen Sie eine Reihe von vorbereitenden BMR-Optionen angeben.

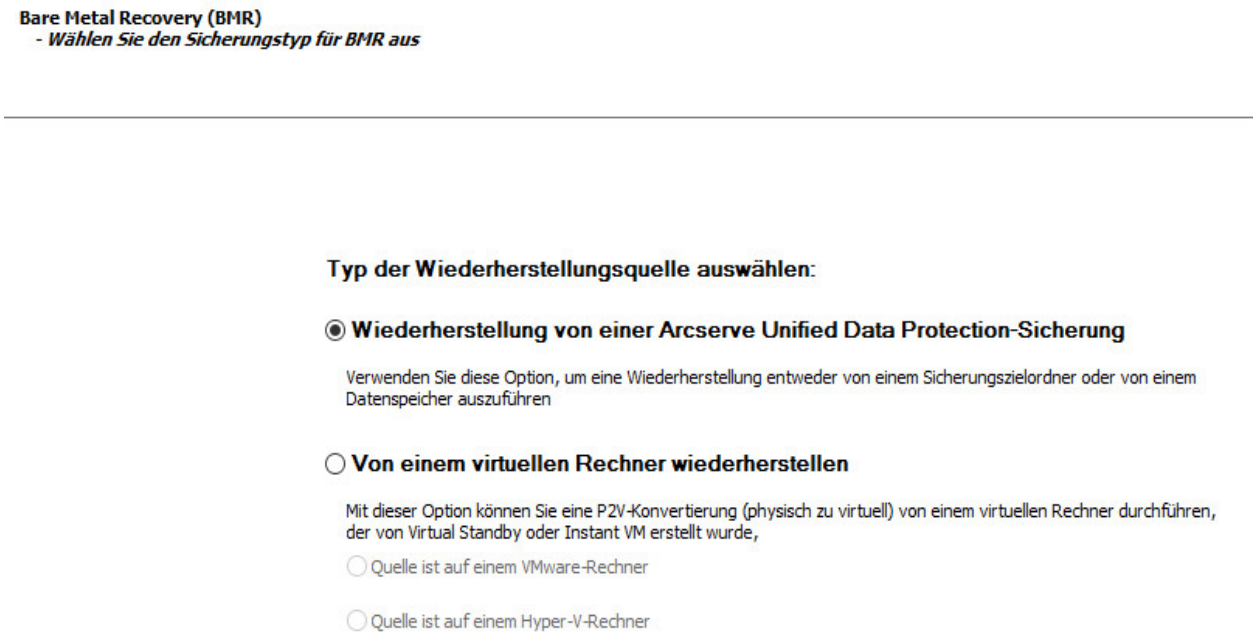
Gehen Sie wie folgt vor:

1. Legen Sie den Datenträger ein, auf dem das Bootkit-Image gespeichert ist, und starten Sie den Computer.
   - Wenn Sie ein auf eine CD/DVD gebranntes ISO-Image für BMR verwenden, legen Sie die CD/DVD ein.
   - Wenn Sie ein auf einen USB-Stick gebranntes ISO-Image für BMR verwenden, legen Sie den Stick ein.

   Der Bildschirm des **BIOS Setup-Hilfsprogramms** wird angezeigt.
2. Wählen Sie im Bildschirm des **BIOS Setup-Hilfsprogramms** die Option für CD-ROM-Laufwerk oder USB aus, um den Startprozess zu initiieren. Wählen Sie eine Architektur (x86 oder x64) aus, und drücken Sie die **Eingabetaste**, um fortzufahren.

   Der Arcserve UDP Agent (Windows)-Bildschirm zur Sprachauswahl wird angezeigt.
3. Wählen Sie eine Sprache aus, und klicken Sie auf **Weiter**, um fortzufahren.

Die Bare-Metal-Recovery wird gestartet und der erste Bildschirm des BMR-Assistenten wird angezeigt.



Im Bildschirm des BMR-Assistenten können Sie den BMR-Typ, den Sie ausführen möchten, auswählen:

- **Wiederherstellung von einer Arcserve Unified Data Protection-Sicherung**

  Verwenden Sie diese Option, um eine Wiederherstellung entweder von einem Sicherungszielordner oder von einem Datenspeicher auszuführen.

  Mit dieser Option können Sie Daten wiederherstellen, die mithilfe von Arcserve UDP Agent (Windows) gesichert wurden. Diese Option wird in Verbindung mit Sicherungssitzungen verwendet, die mit Arcserve UDP Agent (Windows) oder mit der Arcserve UDP-Anwendung für hostbasierte VM-Sicherung ausgeführt werden.

  Weitere Informationen finden Sie in der Online-Hilfe unter So führen Sie eine Bare-Metal-Recovery mithilfe einer Sicherung aus.

- **Wiederherstellen aus einer Virtual Standby-VM**

  Verwenden Sie diese Option, um eine V2P-Wiederherstellung (virtuell-zu-physisch) von einer Virtual Standby-VM oder Instant VM auszuführen. Virtuell-zu-physisch (V2P) ist ein Begriff, der sich auf das Migrieren eines Betriebssystems (BS), von Anwendungsprogrammen und von Daten von einem virtuellen Rechner oder von einer Datenträgerpartition zur Hauptfestplatte eines Computers bezieht. Beim Ziel kann es sich um einen oder mehrere Computer handeln.

- **Quelle ist auf einem VMware-Rechner**

  Ermöglicht es Ihnen, Daten für einen Rechner wiederherzustellen, für den eine virtuelle Konvertierung in einen virtuellen VMware-Rechner durchgeführt wurde. Diese Option wird in Verbindung mit der Arcserve Central Virtual Standby- oder Instant VM-Anwendung verwendet.

  Hinweis: Mit dieser Option können Sie nur Daten wiederherstellen, wenn die virtuelle Konvertierung in eine VMDK-Datei (für VMware) mit Arcserve Central Virtual Standby oder Instant VM durchgeführt wurde.

  Wenn Sie diese Option auswählen, lesen Sie den Abschnitt Wiederherstellen mit einem virtuellen VMware-Virtual Standby-Rechner oder Instant VM, um mit diesem Vorgang fortzufahren.

- **Quelle ist auf einem Hyper-V-Rechner**

  Ermöglicht es Ihnen, Daten für einen Rechner wiederherzustellen, für den eine virtuelle Konvertierung in einen virtuellen Hyper-V-Rechner durchgeführt wurde. Diese Option wird in Verbindung mit der Arcserve Central Virtual Standby- oder Instant VM-Anwendung verwendet.

  Hinweis: Mit dieser Option können Sie nur Daten wiederherstellen, wenn die virtuelle Konvertierung in eine VHD-Datei (für Hyper-V) mit Arcserve Central Virtual Standby oder Instant VM durchgeführt wurde.

  Wenn Sie diese Option auswählen, lesen Sie die Informationen zum Wiederherstellen mit einem virtuellen Hyper-V Virtual Standby-Rechner oder Instant VM, um mit diesem Vorgang fortzufahren.

4. Wählen Sie **Wiederherstellen aus einem Virtual Standby-VM aus**. Wählen Sie eine der Quellen aus.

   Wenn Sie die Option **Quelle ist auf einem VMware-Rechner** auswählen, lesen Sie die Informationen zum Wiederherstellen mit einem virtuellen VMware-Virtual Standby-Rechner oder Instant VM, um mit diesem Vorgang fortzufahren.

   Wenn Sie die Option **Quelle ist auf einem Hyper-V-Rechner** auswählen, lesen Sie die Informationen zum Wiederherstellen mit einem virtuellen Hyper-V-Virtual Standby-Rechner oder Instant VM, um mit diesem Vorgang fortzufahren.

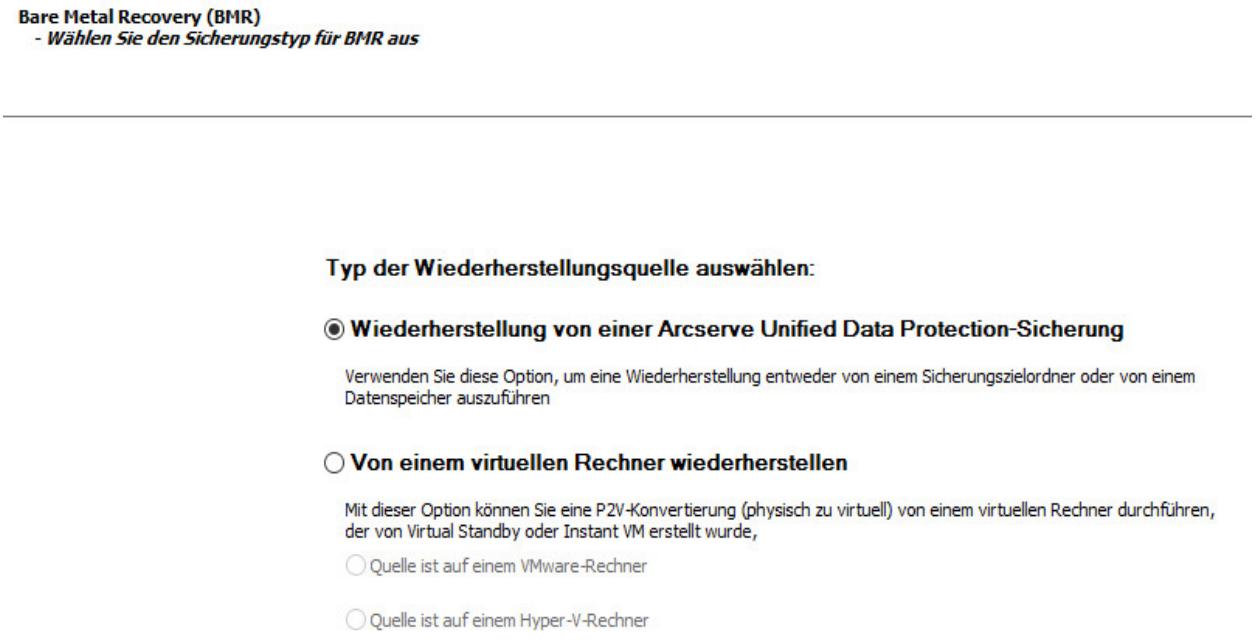
Wiederherstellen mit einer Hyper-V-basierten Virtual Standby-VM oder Instant VM

Mit Arcserve UDP Agent (Windows) können Sie eine V2P-Bare-Metal-Recovery (virtuell zu physisch) durchführen. Diese Funktion ermöglicht Ihnen die Ausführung von V2P-Wiederherstellungen vom aktuellsten Status eines virtuellen Standby-Rechners oder einer Instant VM und hilft Ihnen dabei, Verluste auf Ihrem Produktionsrechner zu reduzieren.

Gehen Sie wie folgt vor:

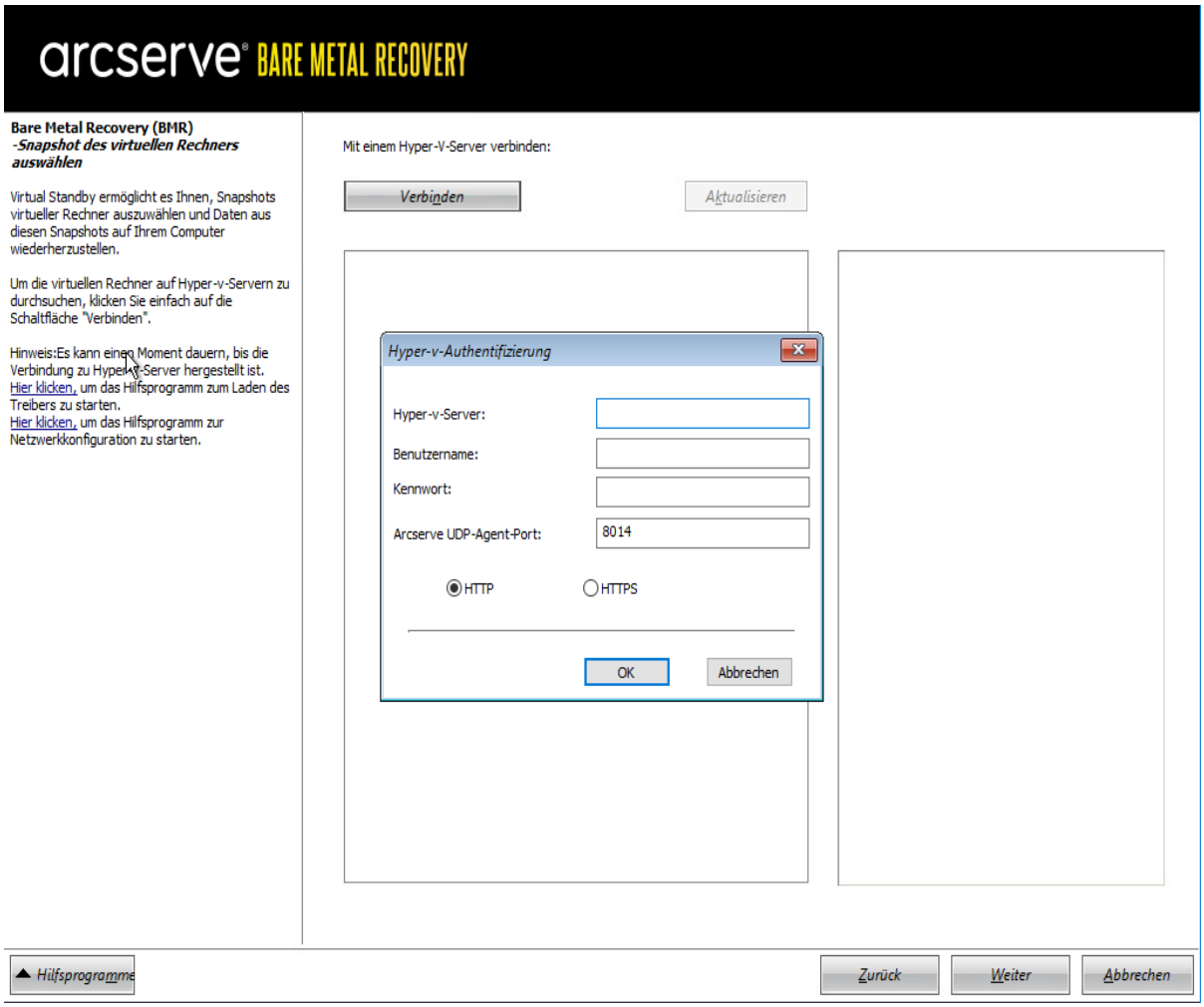
1. Wählen Sie im Assistentenfenster für den Typ der Bare-Metal-Recovery (BMR) die Optionen **Wiederherstellen aus einem Virtual Standby-VM** und **Quelle ist auf einem Hyper-V-Rechner** aus.

   Verwenden Sie diese Option, um eine V2P-Wiederherstellung (virtuell zu physisch) mithilfe von einem virtuellen Virtual Standby-Rechner oder Instant VM durchzuführen. "Virtuell-zu-physisch" bezeichnet das Migrieren von Betriebssystem (BS), Anwendungsprogrammen und Daten von einem virtuellen Rechner oder einer virtuellen Datenträgerpartition zur Hauptfestplatte eines Computers. Beim Ziel kann es sich um einen oder mehrere Computer handeln.



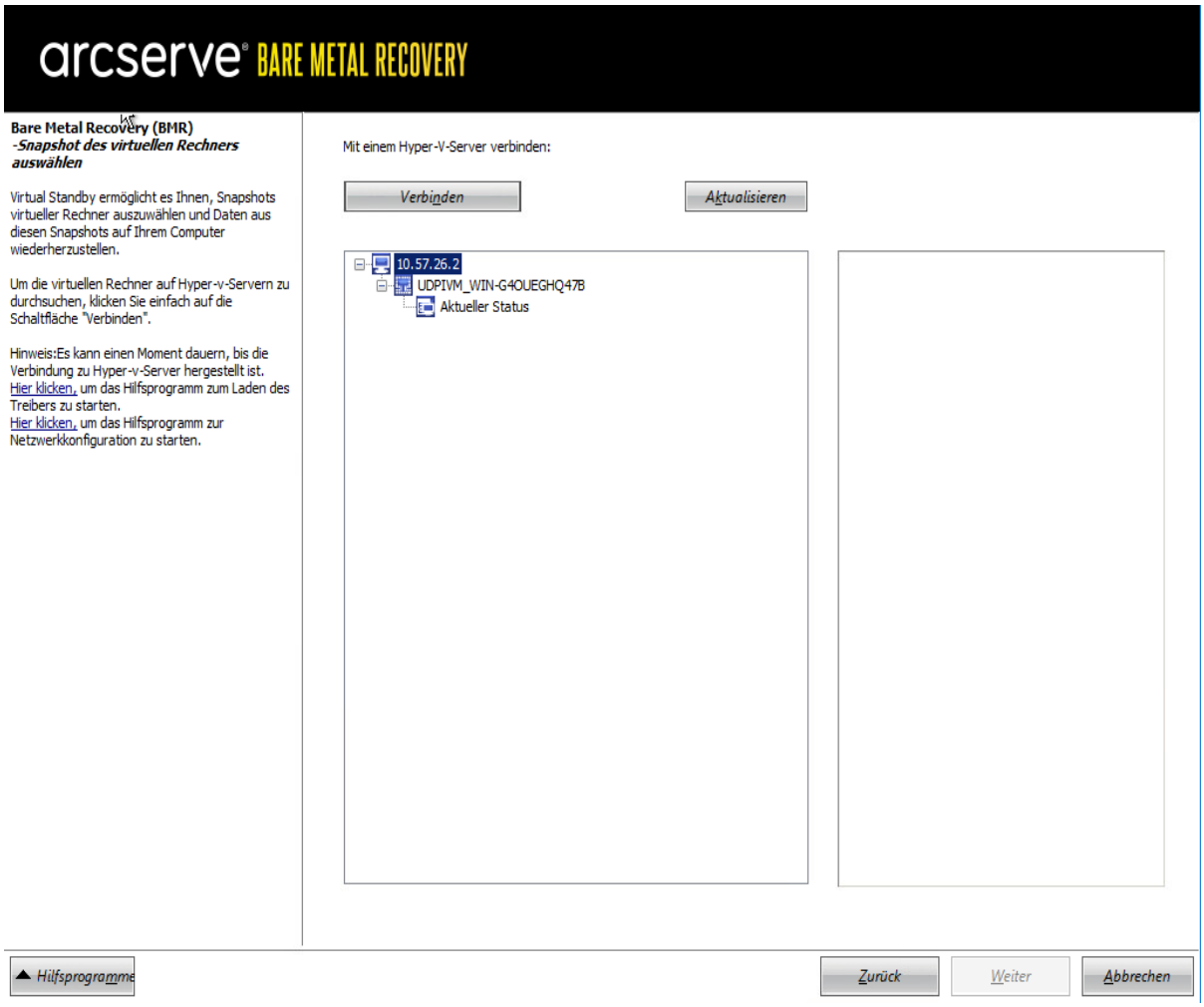
2. Klicken Sie auf **Weiter**.

   Der Bildschirm "Snapshot des virtuellen Rechners auswählen" wird mit dem Dialogfeld "Hyper-V-Authentifizierung" angezeigt, und Sie werden aufgefordert, Hyper-V-Serverdetails einzugeben.



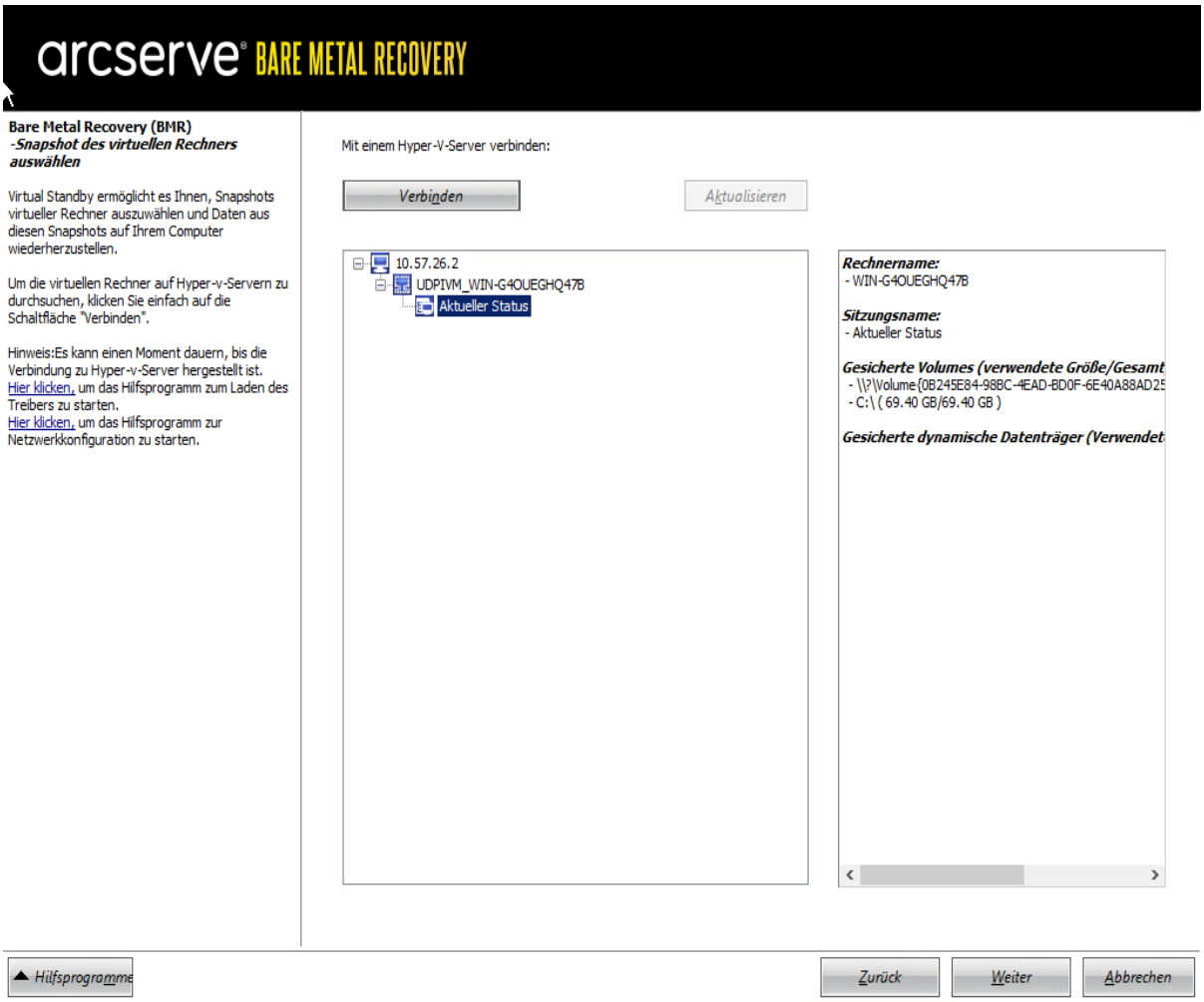
3. Geben Sie Authentifizierungsinformationen ein, und klicken Sie auf **OK**.

   Arcserve Unified Data Protection Agent für Windows entdeckt und zeigt den Hyper-V-Server mit einer Auflistung aller virtuellen Rechner an, die in den angegebenen Hyper-V-Server mithilfe von Arcserve Central Virtual Standby konvertiert werden.



4. Wählen Sie den virtuellen Rechner aus, der Wiederherstellungspunkt-Snapshots für Ihr Sicherungs-Image enthält.

   Die Sicherungssitzungen (Wiederherstellungspunkt-Snapshots) für den ausgewählten virtuellen Rechner werden angezeigt.



5. Wählen Sie die Sicherungssitzung des virtuellen Rechners (Wiederherstellungspunkt-Snapshot), die Sie wiederherstellen möchten.

   Die entsprechenden Details für den ausgewählten Wiederherstellungspunkt-Snapshot (Name des virtuellen Rechners, Name der Sicherungssitzung, gesicherte Volumes) werden im rechten Bereich angezeigt.

   Sie können einen der aufgelisteten Wiederherstellungspunkte auswählen oder **Aktueller Status** oder **Letzter Status** als Wiederherstellungspunkt verwenden.

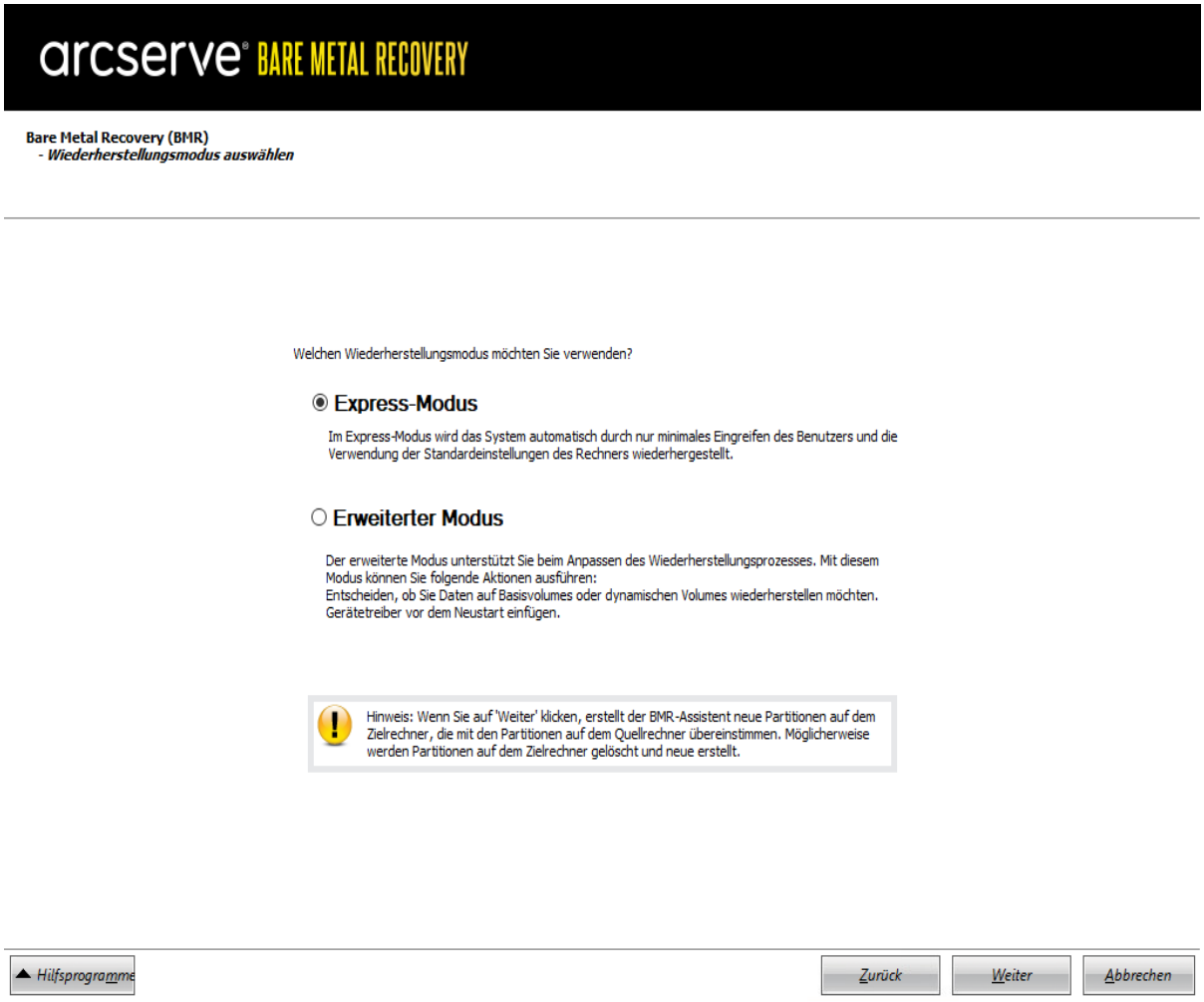
   - Wenn der virtuelle Rechner, von dem Sie eine Wiederherstellung durchführen, eingeschaltet ist, wird der Wiederherstellungspunkt **Aktueller Status** angezeigt.

     Hinweis: Wenn der virtuelle Rechner eingeschaltet ist, werden alle Datenänderungen auf dem virtuellen Rechner, die nach Beginn des BMR-Prozesses vorgenommen wurden, nicht wiederhergestellt.

- Wenn der virtuelle Rechner, von dem Sie eine Wiederherstellung durchführen, ausgeschaltet ist, wird der Wiederherstellungspunkt **Letzter Status** angezeigt.

6. Stellen Sie sicher, dass es sich um den gewünschten Wiederherstellungspunkt handelt, und klicken Sie auf **Weiter**.

   Im BMR-Assistenten werden die verfügbaren Wiederherstellungsmodi angezeigt.



   Es stehen die Optionen **Erweiterter Modus** und **Express-Modus** zur Verfügung.

   - Wenn Sie minimal in den Wiederherstellungsprozess eingreifen möchten, wählen Sie **Express-Modus**. Weitere Informationen finden Sie unter Ausführen von BMR im Express-Modus.
   - Wenn Sie den Wiederherstellungsprozess personalisieren möchten, wählen Sie **Erweiterter Modus**. Weitere Informationen finden Sie unter Ausführen von BMR im erweiterten Modus.

   Standard: Express-Modus.

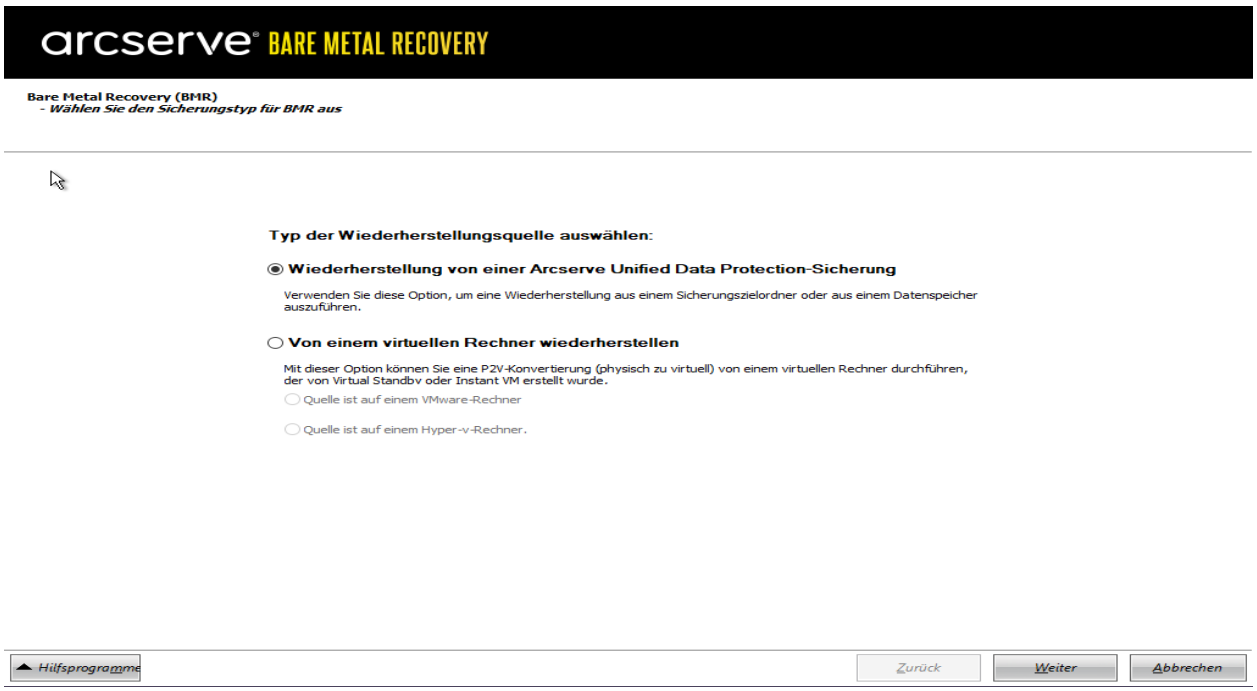
Wiederherstellen mit einer VMware-basierten Virtual Standby-VM oder Instant VM

Mit Arcserve UDP Agent (Windows) können Sie eine V2P-Bare-Metal-Recovery (virtuell zu physisch) durchführen. Diese Funktion ermöglicht Ihnen die Ausführung von Wiederherstellung von virtuellen auf physische Rechner vom aktuellsten Status des virtuellen Standby-Rechners und hilft Ihnen dabei, Verluste auf Ihrem Produktionsrechner zu reduzieren.

Gehen Sie wie folgt vor:

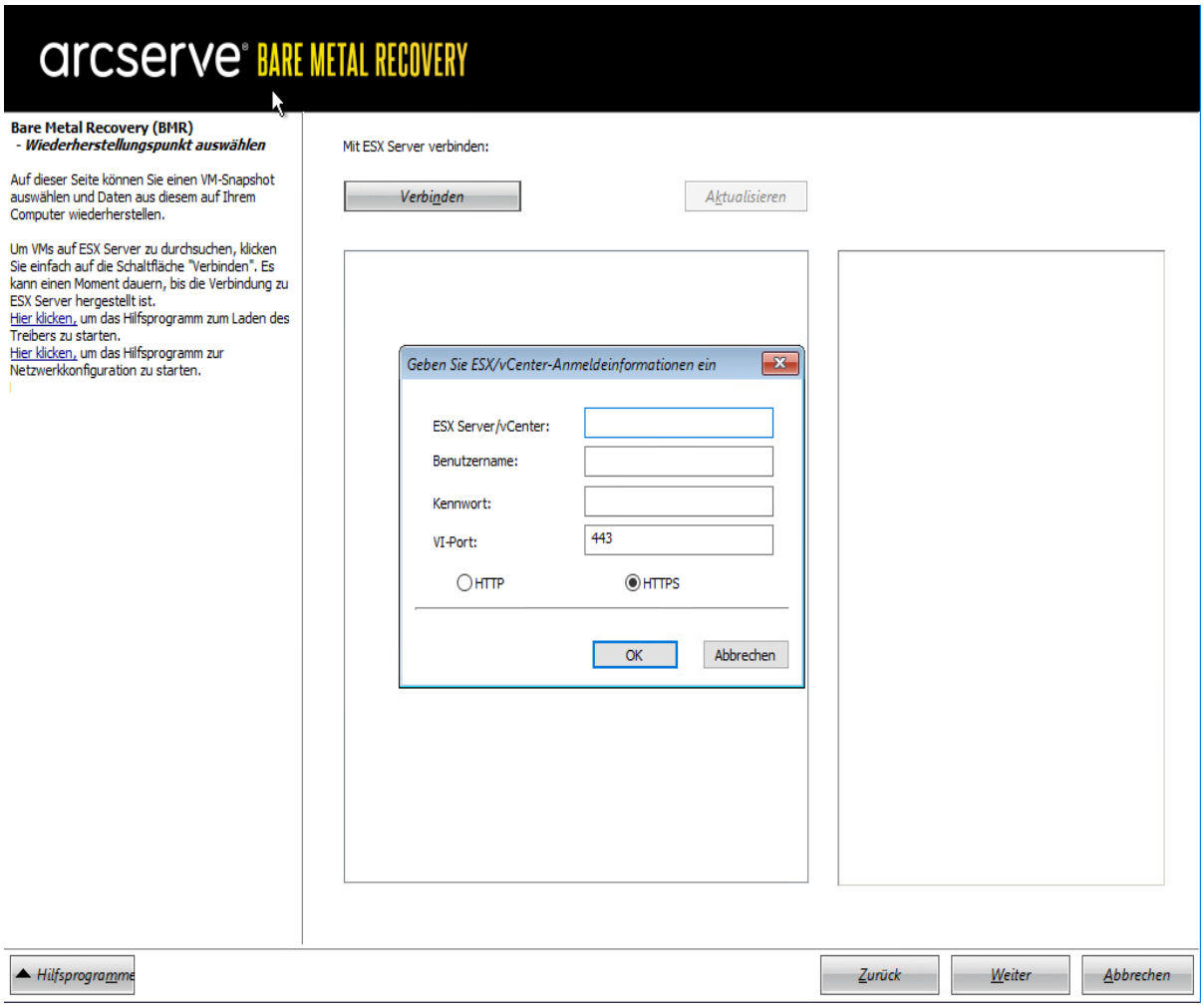
1. Wählen Sie im Assistentenfenster für den Typ der Bare-Metal-Recovery (BMR) die Optionen **Von einem virtuellen Rechner wiederherstellen** und **Quelle ist auf einem VMware-Rechner** aus.

   Verwenden Sie diese Option, um eine V2P-Wiederherstellung (virtuell zu physisch) mithilfe von einem virtuellen Virtual Standby-Rechner oder Instant VM durchzuführen. "Virtuell-zu-physisch" bezeichnet das Migrieren von Betriebssystem (BS), Anwendungsprogrammen und Daten von einem virtuellen Rechner oder einer virtuellen Datenträgerpartition zur Hauptfestplatte eines Computers. Beim Ziel kann es sich um einen oder mehrere Computer handeln.



2. Klicken Sie auf **Weiter**.

   Das Fenster **Wiederherstellungspunkt auswählen** wird mit dem Dialogfeld **ESX/VC-Anmeldeinformationen** angezeigt.



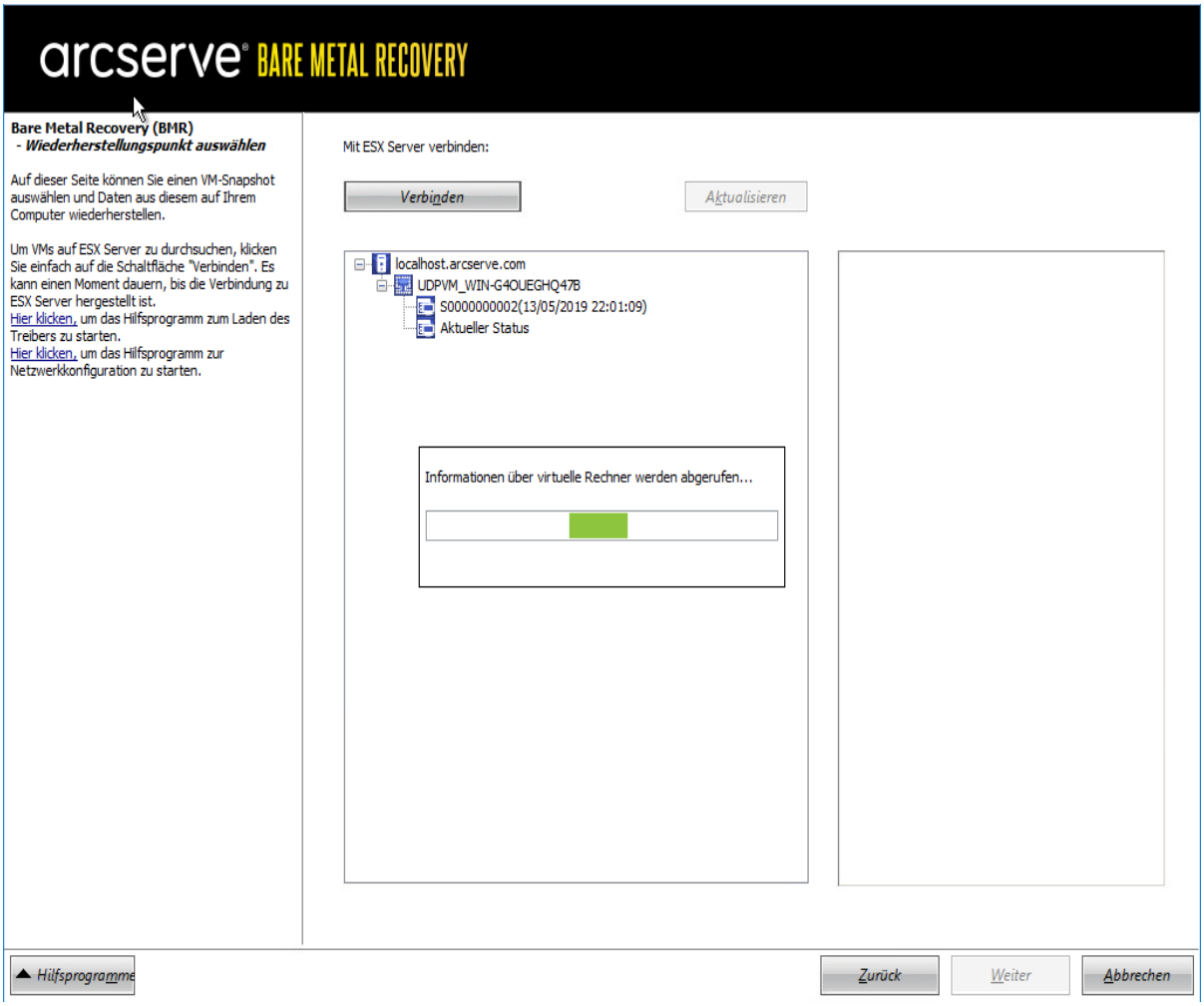
3. Geben Sie Anmeldeinformationen ein, und klicken Sie auf **OK**.

   Hinweis: Wenn Sie eine Verbindung mit vCenter herstellen, benötigen Sie keine Administratorrechte auf Ebene des vCenter-Servers, doch Sie müssen über Administratorrechte auf der Datencenter-Ebene verfügen. Außerdem müssen Sie folgende Berechtigungen auf vCenter-Serverebene haben:

   - Global, DisableMethods und EnableMethods
   - Global, Lizenz

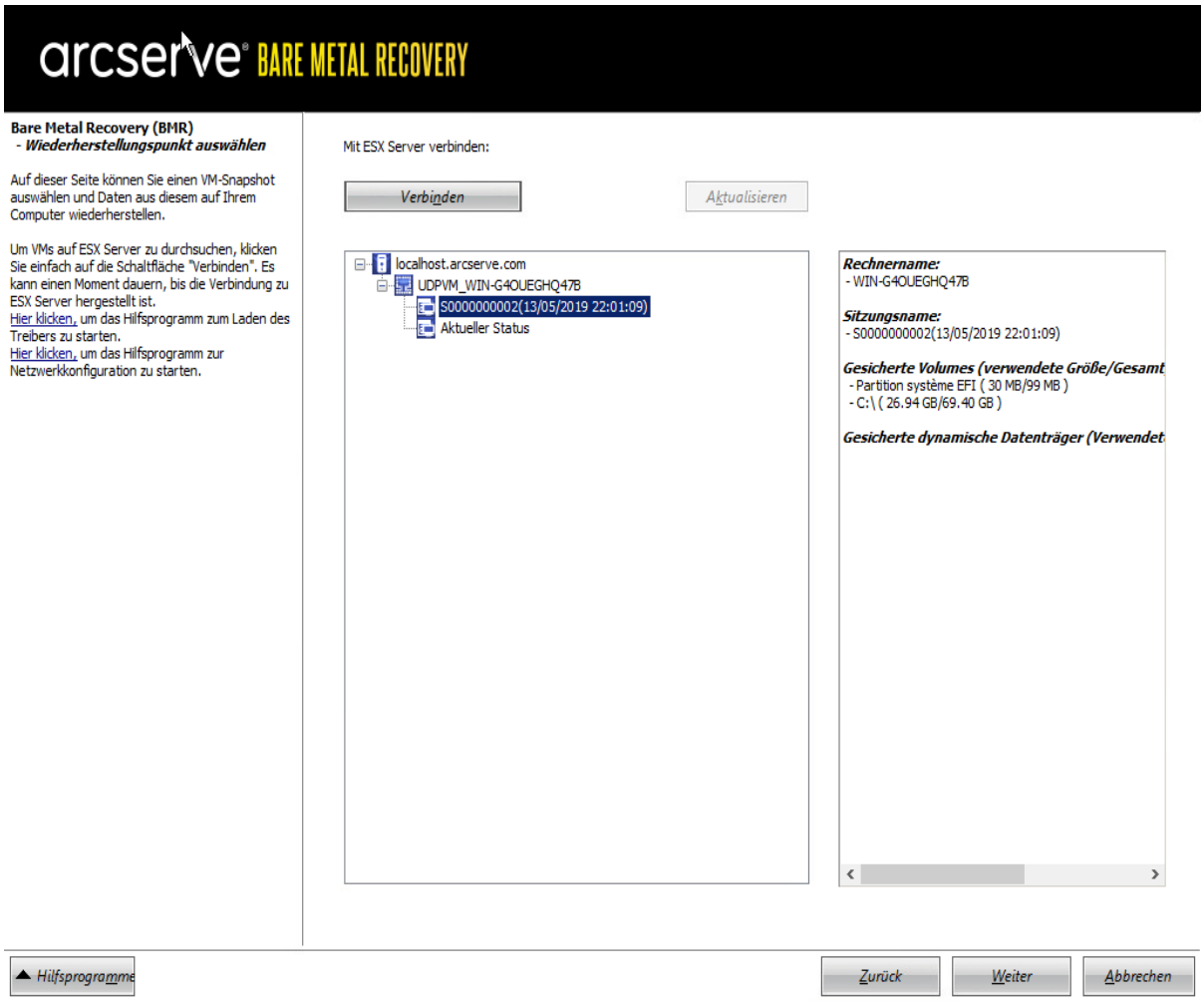
   Das Fenster **Wiederherstellungspunkt auswählen** wird angezeigt.

   Arcserve Unified Data Protection Agent für Windows ruft alle Wiederherstellungspunkt-Snapshots für den ausgewählten VMware-Server ab und zeigt den VMware-Server im linken Fensterbereich an. Die Anzeige enthält eine Auflistung aller virtuellen Rechner, die auf dem ausgewählten VMware-Server gehostet werden.



4. Wählen Sie den virtuellen Rechner aus, der Wiederherstellungspunkte für Ihr Sicherungs-Image enthält.

   Die Sicherungssitzungen (Wiederherstellungspunkt-Snapshots) für den ausgewählten virtuellen Rechner werden angezeigt.



5. Wählen Sie die Sicherungssitzung des virtuellen Rechners (Wiederherstellungspunkt-Snapshot) aus, die Sie wiederherstellen möchten.

   Die entsprechenden Details für den ausgewählten Wiederherstellungspunkt-Snapshot (Name des virtuellen Rechners, Name der Sicherungssitzung, gesicherte Volumes, gesicherte dynamische Datenträger) werden im rechten Bereich angezeigt.

   Sie können einen der aufgelisteten Wiederherstellungspunkte auswählen oder **Aktueller Status** oder **Letzter Status** als Wiederherstellungspunkt verwenden.

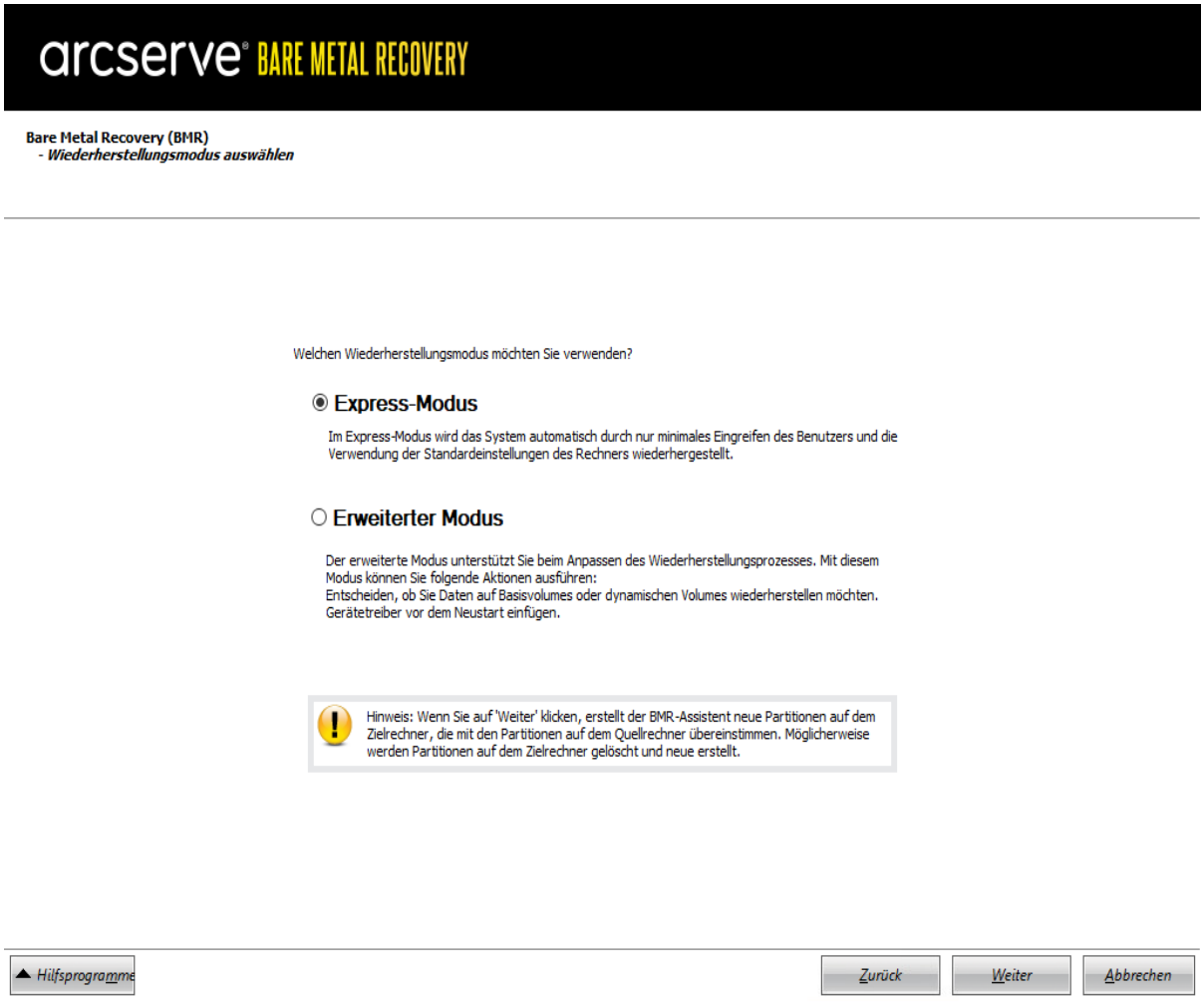
   - Wenn der virtuelle Rechner, von dem Sie eine Wiederherstellung durchführen, eingeschaltet ist, wird der Wiederherstellungspunkt **Aktueller Status** angezeigt.

     Hinweis: Wenn der virtuelle Rechner eingeschaltet ist, werden alle Datenänderungen auf dem virtuellen Rechner, die nach Beginn des BMR-Prozesses vorgenommen wurden, nicht wiederhergestellt.

- Wenn der virtuelle Rechner, von dem Sie eine Wiederherstellung durchführen, ausgeschaltet ist, wird der Wiederherstellungspunkt **Letzter Status** angezeigt.

6. Stellen Sie sicher, dass es sich um den gewünschten Wiederherstellungspunkt handelt, und klicken Sie auf **Weiter**.

   Im BMR-Assistenten werden die verfügbaren Wiederherstellungsmodi angezeigt.



Es stehen die Optionen **Erweiterter Modus** und **Express-Modus** zur Verfügung.

- Wenn Sie minimal in den Wiederherstellungsprozess eingreifen möchten, wählen Sie **Express-Modus**. Weitere Informationen finden Sie unter Ausführen von BMR im Express-Modus.
- Wenn Sie den Wiederherstellungsprozess personalisieren möchten, wählen Sie **Erweiterter Modus**. Weitere Informationen finden Sie unter Ausführen von BMR im erweiterten Modus.

Standard: Express-Modus.

Ausführen von BMR im Expressmodus

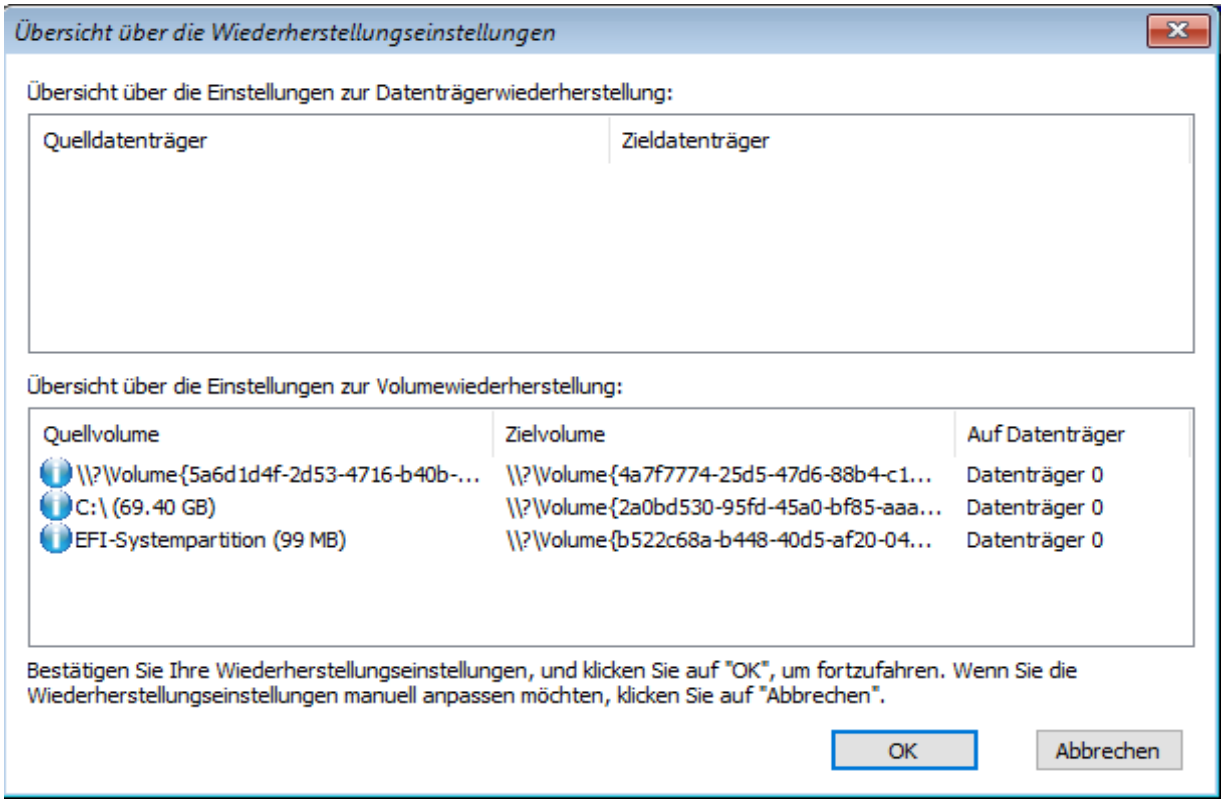
Der **Express-Modus** erfordert nur minimale Interaktion während des Wiederherstellungsprozesses.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Wiederherstellungsmodus auswählen Express-Modus** aus, und klicken Sie auf **Weiter**.

   Im Bildschirm **Übersicht über die Einstellungen zur Datenträgerwiederherstellung** wird eine Übersicht der wiederherzustellenden Volumes angezeigt.

   Hinweis: Die Laufwerkbuchstaben, die unten in der Spalte **Ziel-Volume** aufgelistet werden, werden von Windows Preinstallation Environment (WinPE) automatisch erstellt. Sie können von den Laufwerkbuchstaben der Spalte **Quell-Volume** abweichen. Auch wenn die Laufwerkbuchstaben nicht miteinander übereinstimmen werden die Daten im richtigen Volume ordnungsgemäß wiederhergestellt.



2. Nachdem Sie die Richtigkeit der Übersichtsinformationen überprüft haben, klicken Sie auf **OK**.

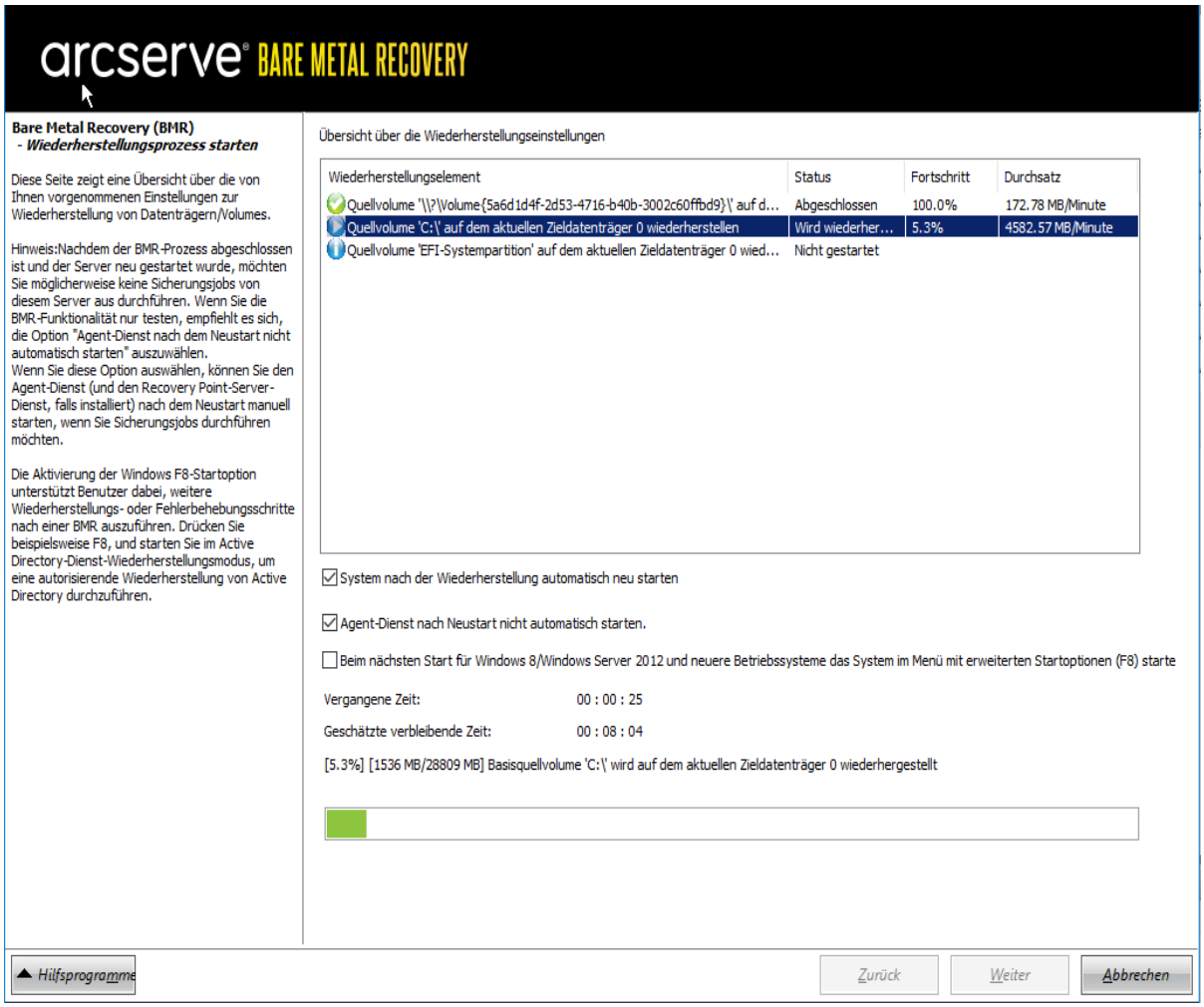
   Der Wiederherstellungsprozess beginnt. Im BMR-Assistenten wird der Wiederherstellungsstatus jedes Volume angezeigt.

- Dieser Vorgang kann je nach Größe des wiederherzustellenden Volumes eine Weile dauern.
- Sie stellen durch diesen Prozess sämtliche Informationen, die Sie für diesen Wiederherstellungspunkt gespeichert hatten, Block für Block wieder her und erstellen auf dem Zielrechner eine Kopie des Quellrechners.
- Standardmäßig ist die Option, die nach der Wiederherstellung einen automatischen Systemneustart festlegt, aktiviert. Wenn nötig, können Sie diese Option löschen und den Neustart zu einem späteren Zeitpunkt manuell durchführen.

  Wichtig: Wenn Sie eine verbindliche Wiederherstellung eines Active Directory nach einer BMR ausführen, müssen Sie die Option **System nach der Wiederherstellung automatisch neu starten** deaktivieren. Weitere Informationen finden Sie unter So führen Sie eine verbindliche Wiederherstellung eines Active Directory nach einer BMR aus.

  - Im Bedarfsfall können Sie "Agent-Dienst nach Neustart nicht automatisch starten" auswählen.

– Sie können den Vorgang auch jederzeit abbrechen.



3. Über das Menü **Hilfsprogramme** können Sie auf das BMR-**Aktivitätsprotokoll** zugreifen und es mithilfe der Option **Speichern** speichern.

   Der standardmäßige Speicherplatz für das Aktivitätsprotokoll ist folgender:

   X:\windows\system32\dr\log.

   Hinweis: Um Windows-bedingten Fehlern vorzubeugen, sollten Sie nicht die Option **Speichern unter** im Fenster des BMR-Aktivitätsprotokolls verwenden, um das Aktivitätsprotokoll auf Ihrem Desktop zu speichern oder einen Ordner auf Ihrem Desktop zu erstellen.

4. Wenn Sie die Wiederherstellung auf einer abweichenden Hardware durchführen (z. B. wenn der SCSI-/FC-Adapter, der zur Verbindung mit den Festplatten verwendet wurde, geändert wurde), und im ursprünglichen System kein kompatibler Treiber gefunden wird, wird die Seite "Treibereinfügung" angezeigt, über die Sie sich mit den benötigten Treibern versorgen können.

Sie können das System durchsuchen und einzufügende Treiber auswählen, sodass sogar ein Rechner mit anderer Hardware nach einer Bare-Metal-Recovery wiederhergestellt werden kann.

5. Nach Abschluss der Bare-Metal-Recovery wird eine Bestätigungsmeldung angezeigt.

Ausführen von BMR im erweiterten Modus

Im **erweiterten Modus** können Sie den Wiederherstellungsprozess benutzerdefiniert anpassen.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Wiederherstellungsmodus auswählen Erweiterter Modus** aus, und klicken Sie auf **Weiter**.

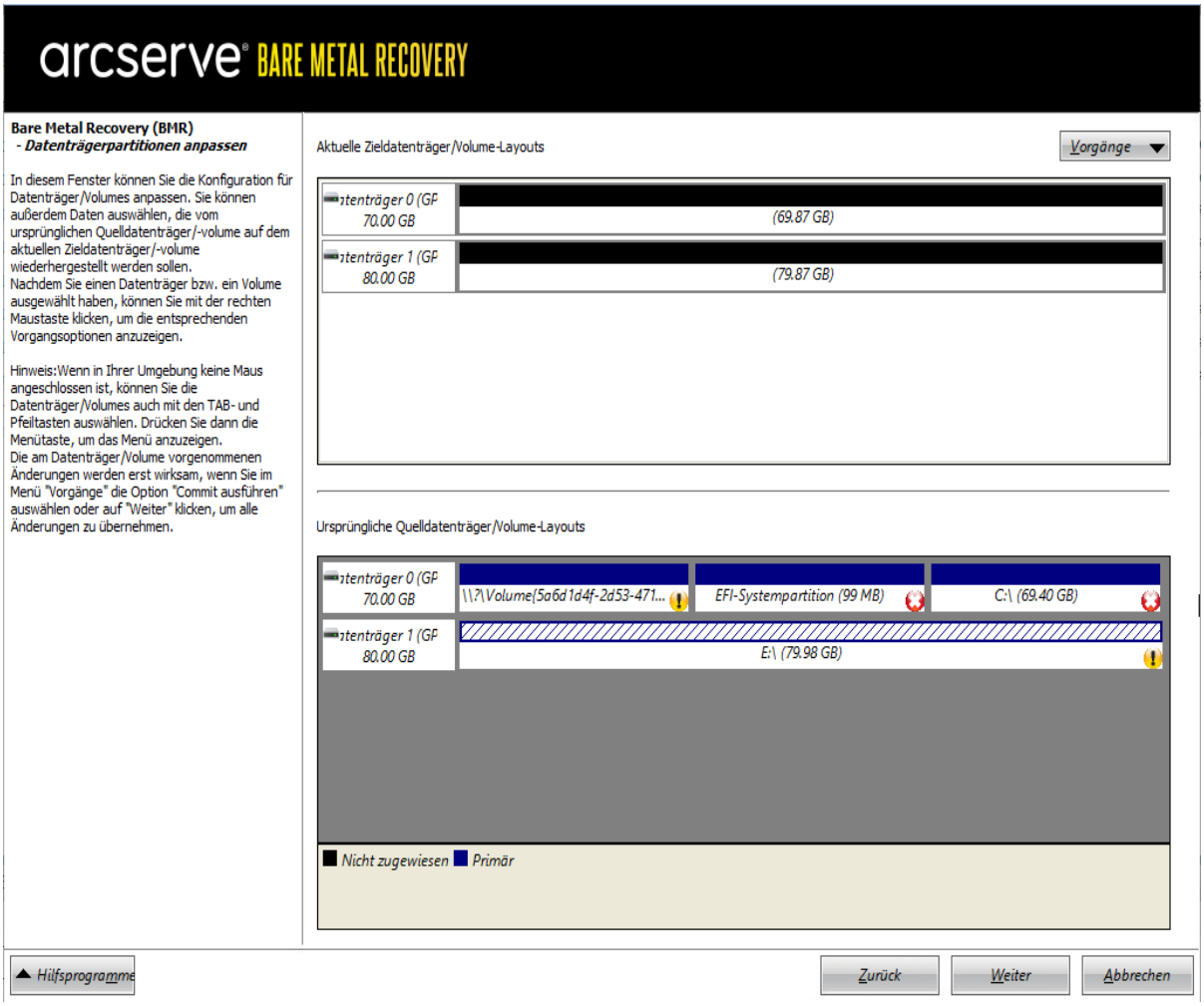
   Das BMR-Hilfsprogramm beginnt mit der Suche nach den wiederherzustellenden Rechnern und zeigt die entsprechenden Informationen zu Datenträgerpartitionen an.

   Im oberen Fensterbereich wird die Datenträgerkonfiguration des derzeitigen Rechners (Zielrechners) angezeigt. Im unteren Fensterbereich wird die Datenträgerkonfiguration angezeigt, die Sie am ursprünglichen Rechner (Quellrechner) eingestellt hatten.

   Wichtig! Ein rotes X-Symbol, das für ein Quell-Volume im unteren Bereich angezeigt wird, gibt an, dass dieses Volume Systeminformationen enthält und dem Zieldatenträger nicht zugewiesen (zugeordnet) wurde. Diese Systeminformationen müssen dem Zieldatenträger zugewiesen werden und während der Bare-Metal-Recovery wiederhergestellt werden. Anderenfalls schlägt der Neustart fehl.

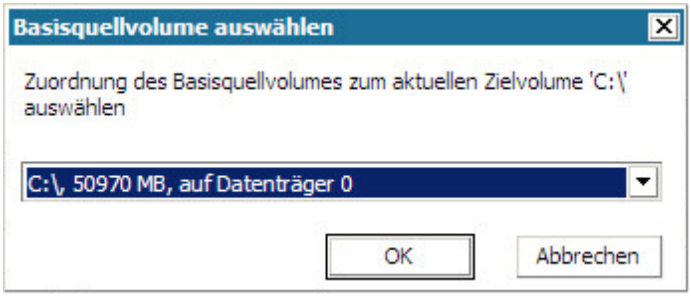
   Hinweis: Wenn Sie eine BMR ausführen und das System-Volume auf einem Datenträger wiederherstellen, der nicht als Startdatenträger konfiguriert ist, kann der Rechner nicht gestartet werden, nachdem BMR abgeschlossen wurde. Stellen Sie sicher, dass Sie das System-Volume auf einem ordnungsgemäß konfigurierten Startdatenträger wiederherstellen.

   Hinweis: Bei einer Wiederherstellung auf einem anderen Datenträger oder Volume muss die Kapazität des neuen Datenträgers gleich oder größer als die des ursprünglichen Datenträgers/Volumes sein. Datenträger-Größenänderung ist außerdem nur bei Basisdatenträgern möglich, nicht bei dynamischen Datenträgern.



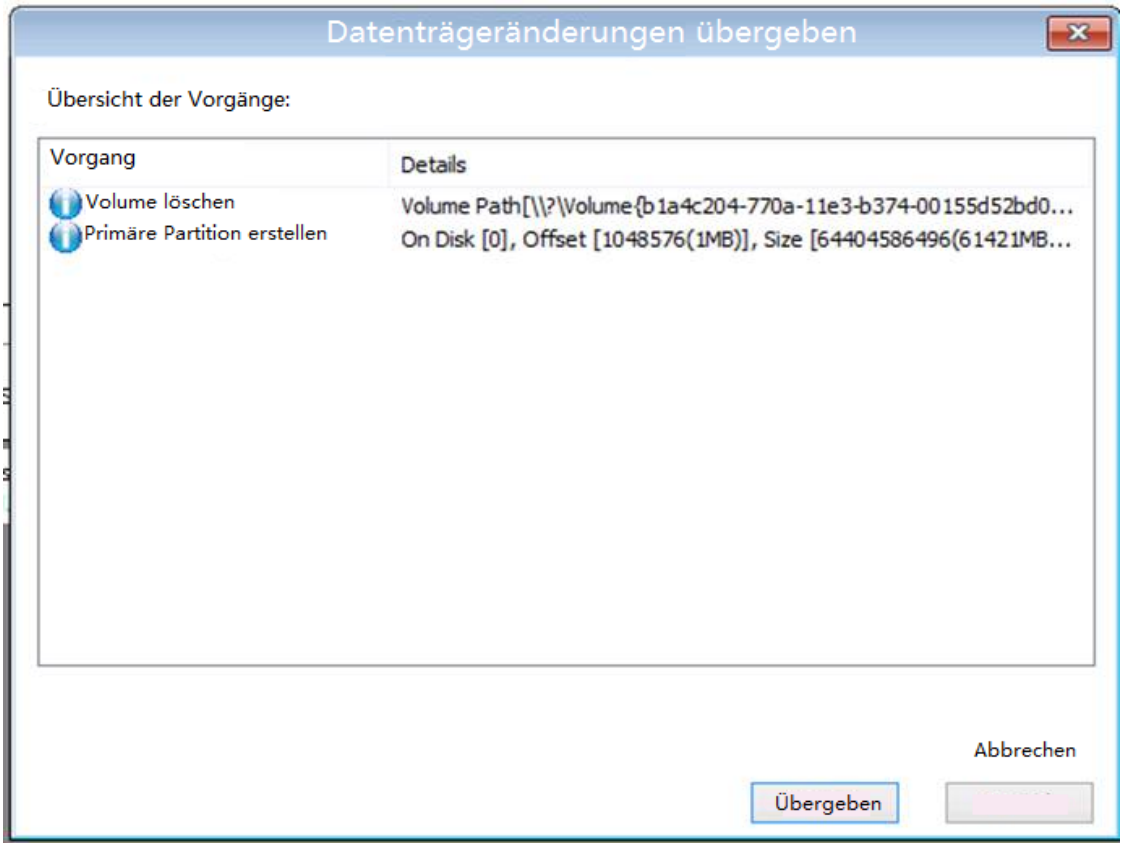
2. Wenn Ihnen die angezeigten aktuellen Datenträgerinformationen nicht richtig erscheinen, können Sie auf das Menü **Hilfsprogramm** zugreifen und nach fehlenden Treibern suchen.
3. Bei Bedarf können Sie im Fensterbereich des Zieldatenträgers/-Volume auf das Drop-down-Menü **Vorgänge** klicken, um die verfügbaren Optionen anzuzeigen. Weitere Informationen zu diesen Optionen finden Sie unter Verwalten des Menüs von BMR-Vorgängen.
4. Klicken Sie auf das entsprechende Ziel-Volume, und wählen Sie im Pop-up-Menü die Option **Volume zuordnen von** aus, um diesem Ziel-Volume ein Quell-Volume zuzuordnen.

   Das Dialogfeld **Basisquell-Volume auswählen** wird geöffnet.



5. Klicken Sie im Dialogfeld **Basisquell-Volume auswählen** auf das Drop-down-Menü, und wählen Sie das verfügbare Quell-Volume aus, um es dem ausgewählten Ziel-Volume zuzuordnen. Klicken Sie auf **OK**.
   - Im Ziel-Volume zeigt ein grünes hakenförmiges Symbol an, dass eine Zuordnung zu diesem Ziel-Volume durchgeführt wurde.
   - Im Quell-Volume zeigt ein rotes x-förmiges Symbol an, dass dieses Quell-Volume einem Ziel-Volume zugeordnet wurde.
6. Wenn Sie sicher sind, dass alle Volumes, die Sie wiederherstellen möchten, und alle Volumes, die Systeminformationen enthalten, zu einem Ziel-Volume zugeordnet sind, klicken Sie auf **Weiter**.

   Im Bildschirm "Datenträgeränderungen übergeben" wird eine Übersicht über die ausgewählten Vorgänge angezeigt. Für jedes neu erstellte Volume werden die entsprechenden Informationen angezeigt.



7. Nachdem Sie die Richtigkeit der Übersichtsinformationen überprüft haben, klicken Sie auf **Übergeben**. (Wenn die Informationen nicht richtig sind, klicken Sie auf **Abbrechen**).

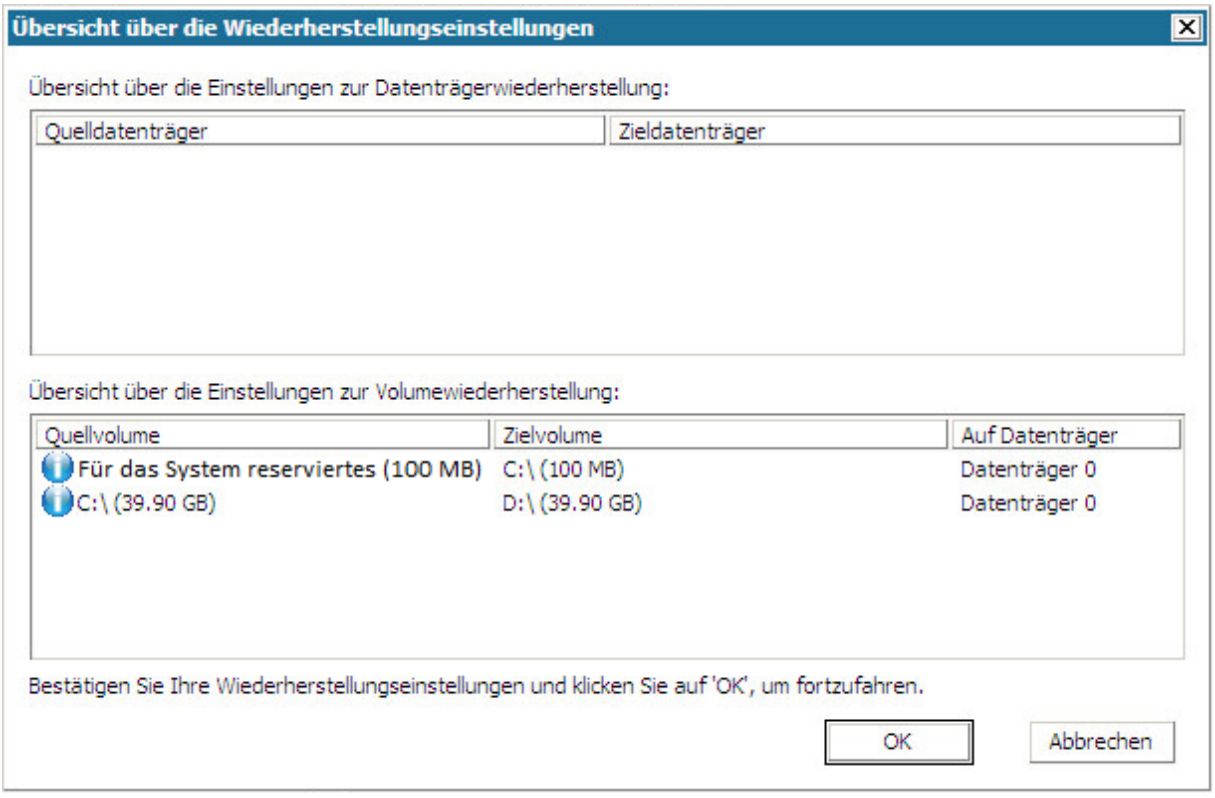
   Hinweis: Sämtliche Vorgänge, die die Festplatte betreffen, werden erst wirksam, wenn Sie sie übergeben haben.

   Auf dem Zielrechner werden die neuen Volumes erstellt und dem entsprechenden Quellrechner zugeordnet.

8. Wenn alle Änderungen abgeschlossen sind, klicken Sie auf **OK**.

   Im Bildschirm "Übersicht über die Einstellungen zur Datenträgerwiederherstellung" wird eine Übersicht der wiederherzustellenden Volumes angezeigt.

   Hinweis: Die Laufwerkbuchstaben, die unten in der Spalte "Ziel-Volume" aufgelistet werden, werden von Windows Preinstallation Environment (WinPE) automatisch erstellt. Sie können von den Laufwerkbuchstaben der Spalte "Quell-Volume" abweichen. Auch wenn die Laufwerkbuchstaben nicht miteinander übereinstimmen werden die Daten im richtigen Volume ordnungsgemäß wiederhergestellt.

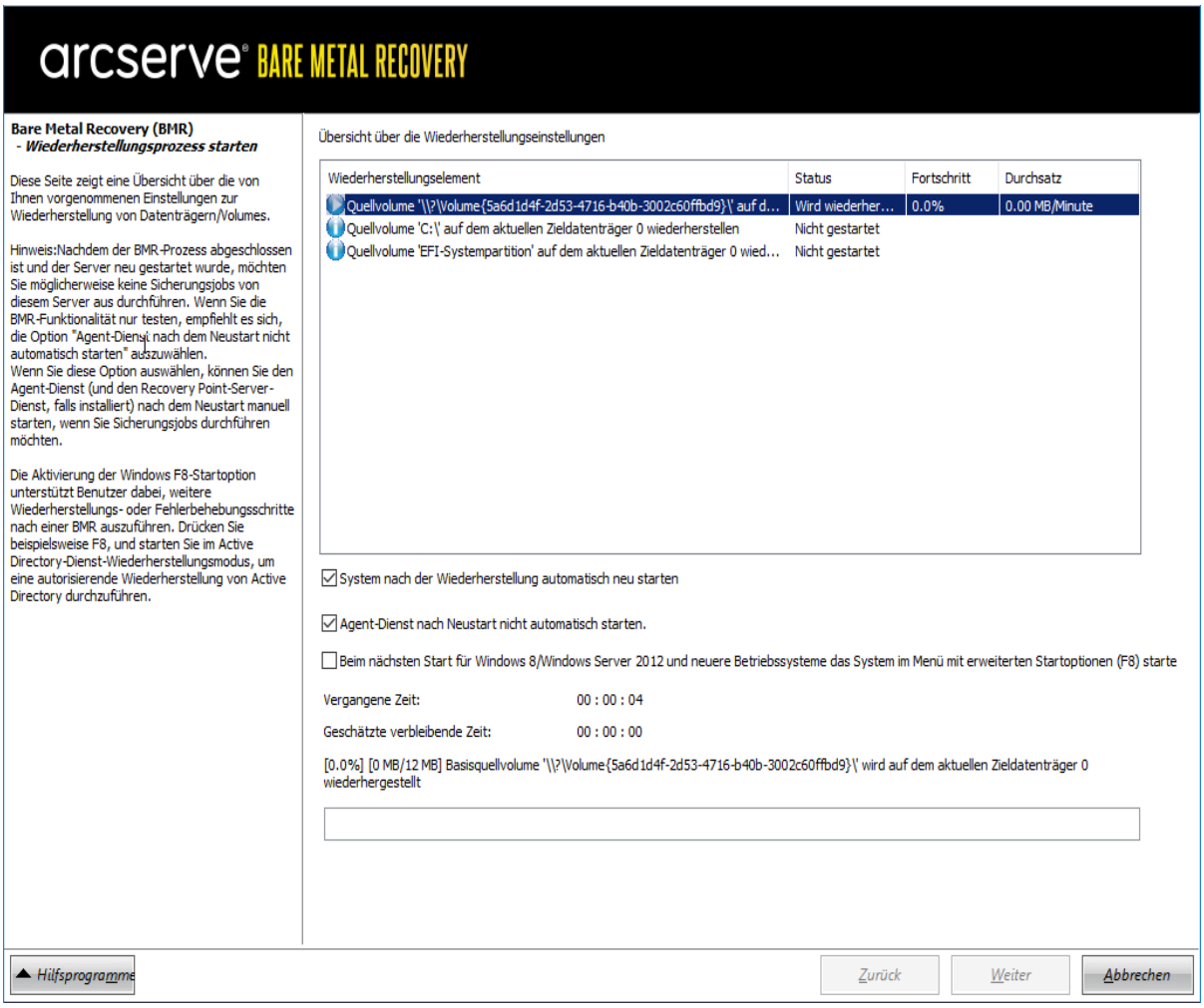


9. Nachdem Sie die Richtigkeit der Übersichtsinformationen überprüft haben, klicken Sie auf **OK**.

   Der Wiederherstellungsprozess beginnt. Im BMR-Assistenten wird der Wiederherstellungsstatus jedes Volume angezeigt.

- Dieser Vorgang kann, abhängig von der Größe des Volume, das wiederhergestellt wird, eine Weile dauern.
- Sie stellen durch diesen Prozess sämtliche Informationen, die Sie für diesen Wiederherstellungspunkt gespeichert hatten, Block für Block wieder her und erstellen auf dem Zielrechner eine Kopie des Quellrechners.
- Standardmäßig ist die Option, die nach der Wiederherstellung einen automatischen Systemneustart festlegt, aktiviert. Wenn nötig, können Sie diese Option löschen und den Neustart zu einem späteren Zeitpunkt manuell durchführen.

  Wichtig: Wenn Sie eine verbindliche Wiederherstellung eines Active Directory nach einer BMR ausführen, müssen Sie die Option **System nach der Wiederherstellung automatisch neu starten** deaktivieren. Weitere Informationen finden Sie unter So führen Sie eine verbindliche Wiederherstellung eines Active Directory nach einer BMR aus.
- Im Bedarfsfall können Sie "Agent-Dienst nach Neustart nicht automatisch starten" auswählen.
- Sie können den Vorgang auch jederzeit abbrechen.



10. Über das Menü **Hilfsprogramme** können Sie auf das BMR-**Aktivitätsprotokoll** zugreifen und es mithilfe der Option **Speichern** speichern.

    Der standardmäßige Speicherplatz für das Aktivitätsprotokoll ist folgender:

    X:\windows\system32\dr\log

    Hinweis: Um Windows-bedingten Fehlern vorzubeugen, sollten Sie nicht die Option **Speichern unter** im Fenster des BMR-Aktivitätsprotokolls verwenden, um das Aktivitätsprotokoll auf Ihrem Desktop zu speichern oder einen Ordner auf Ihrem Desktop zu erstellen.

11. Wenn Sie die Wiederherstellung auf einer abweichenden Hardware durchführen (z. B. wenn der SCSI-/FC-Adapter, der zur Verbindung mit den Festplatten verwendet wurde, geändert wurde), und im ursprünglichen System kein kompatibler Treiber gefunden wird, wird die Seite "Treibereinfügung" angezeigt, über die Sie sich mit den benötigten Treibern versorgen können.

Sie können das System durchsuchen und einzufügende Treiber auswählen, sodass sogar ein Rechner mit anderer Hardware nach einer Bare-Metal-Recovery wiederhergestellt werden kann.

12. Nach Abschluss der Bare-Metal-Recovery wird eine Bestätigungsmeldung angezeigt.

Überprüfen des Erfolgs der BMR

Um zu überprüfen, ob die BMR erfolgreich war, führen Sie die folgenden Tasks aus:

- Starten Sie das Betriebssystem neu.
- Überprüfen Sie, ob alle Systeme und Anwendungen ordnungsgemäß funktionieren.
- Überprüfen Sie, ob alle Netzwerkeinstellungen richtig konfiguriert sind.
- Überprüfen Sie, ob das BIOS so konfiguriert ist, dass der Start vom Datenträger, auf dem das Boot-Volume wiederhergestellt wurde, durchgeführt wird.
- Beachten Sie nach Abschluss der BMR die folgenden Bedingungen:
  - Die erste Sicherung, die nach der BMR ausgeführt wird, ist eine Überprüfungssicherung.
  - Wenn Sie auf abweichender Hardware wiederhergestellt haben, müssen Sie die Netzwerkadapter nach dem Neustart des Rechners möglicherweise manuell konfigurieren.

    Hinweis: Wenn der Rechner neu startet, wird möglicherweise ein Fenster mit einer Windows-Wiederherstellung nach einem Fehler geöffnet, das anzeigt, dass Windows nicht erfolgreich heruntergefahren ist. Wenn dies auftritt, können Sie diese Warnung beruhigt ignorieren und Windows ganz normal weiter starten.
  - Bei dynamischen Datenträgern können Sie den Offline-Status des Datenträgers über die Datenträgerverwaltung manuell in online umändern (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).
  - Sie können dynamische Volumes auf dynamischen Datenträgern, die aufgrund von Redundanz fehlgeschlagen sind, über die Datenträgerverwaltung manuell neu synchronisieren (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).

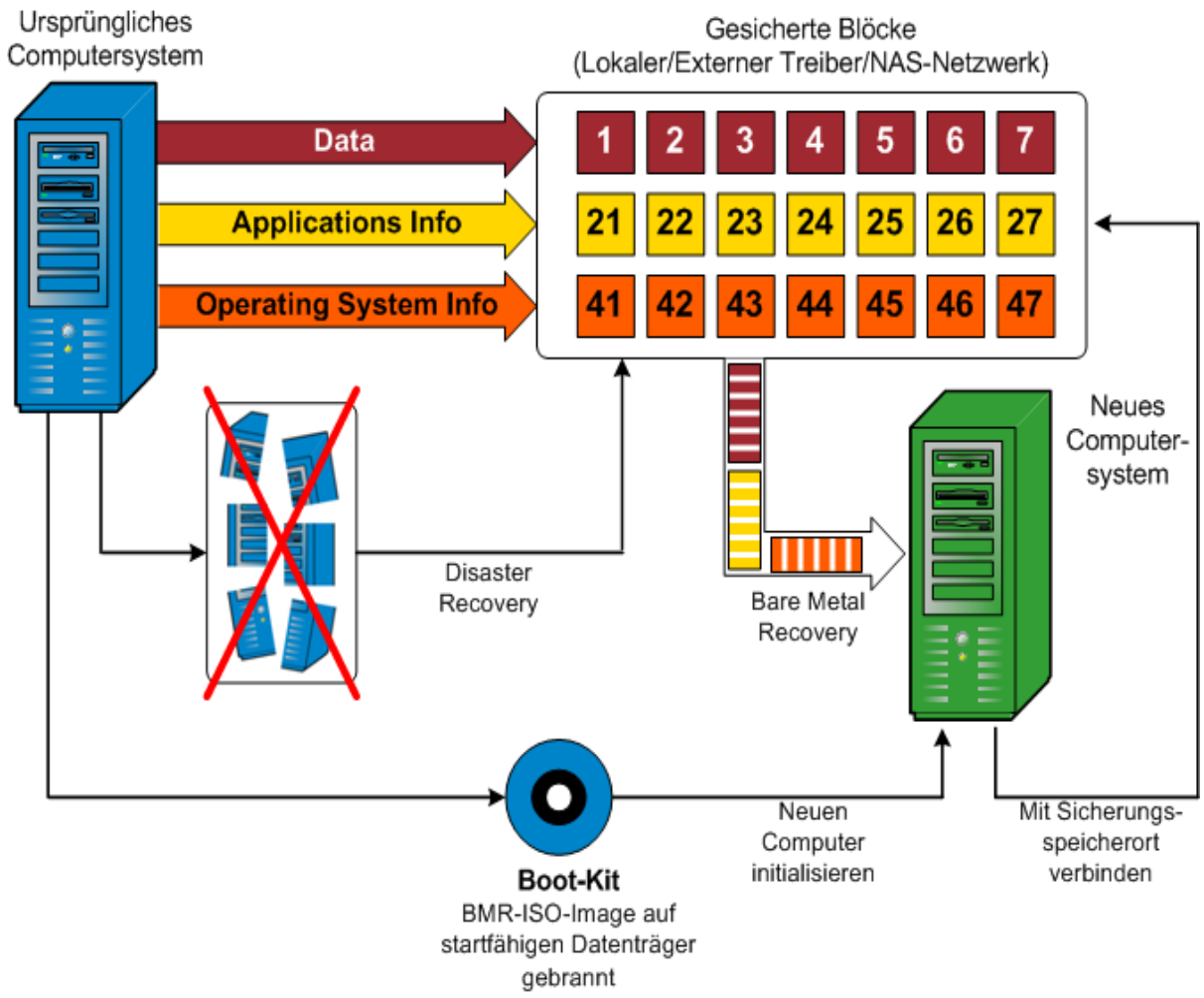
BMR-Referenzinformationen

- Funktionsweise von Bare-Metal-Recovery
- Betriebssysteme, die UEFI/BIOS-Konvertierung unterstützen
- Verwalten des Menüs von BMR-Vorgängen

Funktionsweise von Bare-Metal-Recovery

Bare-Metal-Recovery ist eine Wiederherstellung Ihres Computersystems "von Null", wobei Betriebssystem und Anwendungen neu installiert werden und Daten und Einstellungen wiederhergestellt werden. Die häufigsten Gründe für die Durchführung einer Bare-Metal-Recovery sind ein Festplattenausfall oder die Tatsache, dass eine Festplatte voll ist und ein Upgrade (eine Migration) auf eine größere Festplatte oder eine Migration zu neuerer Hardware erforderlich ist. Eine Bare-Metal-Recovery ist möglich, da Arcserve UDP Agent (Windows) während der Sicherung auf Blockebene nicht nur Daten, sondern auch sämtliche Informationen zum Betriebssystem sowie zu installierten Anwendungen, Konfigurationseinstellungen, benötigten Treibern usw. erfasst. Alle Informationen, die für eine vollständige Systemwiederherstellung "von Null" benötigt werden, werden in mehreren Blöcken gesichert und im Sicherungsziel gespeichert.

Hinweis: Dynamische Datenträger werden nur auf Datenträgerebene wiederhergestellt. Wenn Ihre Daten auf einem Volume eines dynamischen Datenträgers gesichert sind, können Sie diesen dynamischen Datenträger (einschließlich aller seiner Volumes) während der Bare-Metal-Recovery nicht wiederherstellen.



Bei einer Bare-Metal-Recovery initialisiert der Arcserve UDP Agent (Windows)-Startdatenträger das neue Computersystem und ermöglicht den Beginn der BMR. Zu Beginn der Bare-Metal-Recovery fordert Sie Arcserve UDP Agent (Windows) dazu auf, einen gültigen Speicherort auszuwählen oder anzugeben, von dem diese gesicherten Blöcke abgerufen werden sollen. Außerdem ist auch der Wiederherstellungspunkt für die Wiederherstellung anzugeben bzw. auszuwählen. Sie können auch aufgefordert werden, gültige Treiber für das neue System anzugeben. Sobald diese Verbindungs- und Konfigurationsinformationen angegeben sind, beginnt Arcserve UDP Agent (Windows) damit, das angegebene Sicherungs-Image vom Speicherort der Sicherung zu ziehen und alle gesicherten Blöcke im neuen System wiederherzustellen (leere Blöcke werden nicht wiederhergestellt). Wenn das Bare-Metal-Recovery-Image komplett wiederhergestellt ist, befindet sich der Rechner wieder im selben Status, in dem er sich beim Abschluss der letzten Sicherung befunden hat, und Arcserve UDP Agent (Windows)-Sicherungen können planmäßig fortgesetzt werden. (Die erste Sicherung nach Abschluss der Bare-Metal-Recovery ist eine Überprüfungssicherung).

Betriebssysteme, die UEFI/BIOS-Konvertierung unterstützen

Wenn entdeckt wird, dass das Betriebssystem Ihres Quellrechners nicht die gleiche Firmware wie Ihr System aufweist, werden Sie gefragt, ob Sie UEFI in ein BIOS-kompatibles System oder BIOS in ein UEFI-kompatibles System konvertieren möchten. Die folgende Tabelle listet alle Betriebssysteme und den Typ der unterstützten Konvertierung auf:

Betriebssystem (BS)	CPU	uEFI zu BIOS	BIOS zu uEFI
Windows Vista (kein SP)	x86	Nein	Nein
Windows Vista (kein SP)	x64	Nein	Nein
Windows Vista SP1	x86	Nein	Nein
Windows Vista SP1	x64	Ja	Ja
Windows Server 2008	x86	Nein	Nein
Windows Server 2008	x64	Ja	Ja
Windows Server 2008 R2	x64	Ja	Ja
Windows 7	x86	Nein	Nein
Windows 7	x64	Ja	Ja
Windows 8	x86	Nein	Nein
Windows 8	x64	Ja	Ja
Windows Server 2012	x64	Ja	Ja
Windows 8.1	x86	Nein	Nein
Windows 8.1	x64	Ja	Ja
Windows 10	x86	Nein	Nein
Windows 10	x64	Ja	Ja
Windows Server 2012 R2	x64	Ja	Ja
Windows Server 2016	x64	Ja	Ja
Windows Server 2019	x64	Ja	Ja

Verwalten des Menüs von BMR-Vorgängen

Das Menü von BMR-Vorgängen besteht aus den folgenden drei Arten von Vorgängen:

- Datenträgerspezifische Vorgänge
- Volume-/partitionsspezifische Vorgänge
- BMR-spezifische Vorgänge

Datenträgerspezifische Vorgänge:

Um datenträgerspezifische Vorgänge auszuführen, wählen Sie den Datenträger-Header aus, und klicken Sie auf **Vorgänge**.

Datenträger reinigen

Dieser Vorgang wird verwendet, um alle Partitionen eines Datenträgers zu bereinigen, und hat folgende Eigenschaften:

- Er ist eine alternative Methode, um alle Volumes von einem Datenträger zu löschen. Mit dem Vorgang **Datenträger reinigen** müssen Sie Volumes nicht einzeln hintereinander löschen.
- Er wird verwendet, um Nicht-Windows-Partitionen zu löschen. Aufgrund einer VDS-Einschränkung können Nicht-Windows-Partitionen nicht von der Benutzeroberfläche gelöscht werden, aber Sie können diesen Vorgang verwenden, um alle zu bereinigen.

  Hinweis: Während BMR können Sie – wenn der Zieldatenträger Nicht-Windows-Partitionen oder OEM-Partitionen hat – diese Partition nicht auswählen und nicht von der BMR-Benutzeroberfläche löschen. Üblicherweise würde dies auftreten, wenn Sie irgendwann Linux/UNIX auf dem Zieldatenträger installiert hatten. Gehen Sie folgendermaßen vor, um das Problem zu lösen:

- Wählen Sie den Datenträger-Header auf der BMR-Benutzeroberfläche aus, klicken Sie auf **Vorgänge**, und verwenden Sie den Vorgang **Datenträger reinigen**, um alle Partitionen auf dem Datenträger zu löschen.
- Öffnen Sie eine Eingabeaufforderung, und tippen Sie **Diskpart**, um die Diskpart-Befehlskonsole zu öffnen. Tippen Sie anschließend "select disk x", wobei "x" die Nummer des Datenträgers ist, und "clean", um alle Partitionen auf dem Datenträger zu löschen.

In MBR konvertieren

Dieser Vorgang wird verwendet, um einen Datenträger in MBR (Master Boot Record) zu konvertieren. Er ist nur verfügbar, wenn der ausgewählte

Datenträger ein GPT-Datenträger (GUID-Partitionstabelle) ist und keine Volumes auf diesem Datenträger vorhanden sind.

In GPT konvertieren

Dieser Vorgang wird verwendet, um einen Datenträger in GPT zu konvertieren. Er ist nur verfügbar, wenn der ausgewählte Datenträger ein MBR-Datenträger ist und keine Volumes auf diesem Datenträger vorhanden sind.

In "Basis" konvertieren

Dieser Vorgang wird verwendet, um einen Datenträger in einen Basisdatenträger zu konvertieren. Er ist nur verfügbar, wenn der ausgewählte Datenträger ein dynamischer Datenträger ist und keine Volumes auf diesem Datenträger vorhanden sind.

In "Dynamisch" konvertieren

Dieser Vorgang wird verwendet, um einen Datenträger in einen dynamischen Datenträger zu konvertieren. Er ist nur verfügbar, wenn der ausgewählte Datenträger ein Basisdatenträger ist.

Online-Datenträger

Dieser Vorgang wird verwendet, um einen Datenträger online zu stellen. Er ist nur verfügbar, wenn sich der ausgewählte Datenträger im Offline-Status befindet.

Datenträgereigenschaften

Dieser Vorgang wird verwendet, um detaillierte Datenträgereigenschaften anzuzeigen. Dieser Vorgang ist immer verfügbar. Wenn Sie ihn auswählen, wird ein Dialogfeld namens **Datenträgereigenschaften** angezeigt.

Volume-/partitionsspezifische Vorgänge:

Um Vorgänge für Volumes oder Partitionen auszuführen, wählen Sie den Textbereich des Datenträgers aus, und klicken Sie auf **Vorgänge**. Von diesem Menü aus können Sie neue Partitionen erstellen, um den Datenträgerpartitionen auf dem Quell-Volume zu entsprechen.

Primäre Partition erstellen

Dieser Vorgang wird verwendet, um eine Partition auf einem Basisdatenträger zu erstellen. Er ist nur verfügbar, wenn es sich beim ausgewählten Bereich um nicht zugeordneten Speicherplatz handelt.

Logische Partition erstellen

Dieser Vorgang wird verwendet, um eine logische Partition auf einem MBR-Basisdatenträger zu erstellen. Er ist nur verfügbar, wenn es sich beim ausgewählten Bereich um eine erweiterte Partition handelt.

Erweiterte Partition erstellen

Dieser Vorgang wird verwendet, um eine erweiterte Partition auf einem MBR--Basisdatenträger zu erstellen. Er ist nur verfügbar, wenn der Datenträger ein MBR-Datenträger ist und es sich beim ausgewählten Bereich um nicht zugeordneten Speicherplatz handelt.

Für das System reservierte Partition erstellen

Dieser Vorgang wird verwendet, um die für das System reservierte Partition auf einem BIOS-Firmwaresystem zu erstellen. Er erstellt eine Zuordnungsbeziehung mit der EFI-Systempartitionsquelle. Er ist nur verfügbar, wenn Sie ein UEFI-System in einem BIOS-System wiederherstellen.

Hinweis: Wenn Sie zu einem früheren Zeitpunkt UEFI in ein BIOS-kompatibles System konvertiert haben, verwenden Sie den Vorgang "Für das System reservierte Partition erstellen", um die Größe des Zieldatenträgers zu ändern.

EFI-Systempartition erstellen

Dieser Vorgang wird verwendet, um die EFI-Systempartition auf einem GPT-Basisdatenträger zu erstellen. Er ist nur verfügbar, wenn es sich bei der Firmware des Zielcomputers um UEFI handelt und der ausgewählte Datenträger ein GPT-Basisdatenträger ist.

Hinweis: Wenn Sie zu einem früheren Zeitpunkt BIOS in ein UEFI-kompatibles System konvertiert haben, verwenden Sie den Vorgang "EFI-Systempartition erstellen", um die Größe des Zieldatenträgers zu ändern.

Hinweis: In Systemen, die UEFI unterstützen, muss sich die Startpartition auf einer Festplatten mit GUID-Partitionstabellen (GPT) befinden. Wenn Sie einen MBR-Datenträger (Master Boot Record) verwenden, müssen Sie diesen Datenträger in einen GPT-Datenträger konvertieren und anschließend den Vorgang "EFI-Systempartition erstellen" verwenden, um die Größe des Zieldatenträgers zu ändern.

Größe des Volume ändern

Dieser Vorgang wird verwendet, um die Größe eines Volume zu ändern. Dies ist eine Alternative zu den Windows-Methoden "Volume erweitern" bzw. "Volume verkleinern". Er ist nur verfügbar, wenn es sich beim ausgewählten Bereich um eine gültige Datenträgerpartition handelt.

Volume löschen

Dieser Vorgang wird verwendet, um ein Volume zu löschen. Er ist nur verfügbar, wenn es sich beim ausgewählten Bereich um ein gültiges Volume handelt.

Erweiterte Partition löschen

Dieser Vorgang wird verwendet, um eine erweiterte Partition zu löschen. Er ist nur verfügbar, wenn es sich beim ausgewählten Bereich um eine erweiterte Partition handelt.

Volume-Eigenschaften

Dieser Vorgang wird verwendet, um detaillierte Volume-Eigenschaften anzuzeigen. Wenn Sie diesen Vorgang auswählen, wird ein Dialogfeld namens **Volume-Eigenschaften** angezeigt.

BMR-spezifische Vorgänge:

Diese Vorgänge sind spezifisch für BMR. Um BMR-Vorgänge auszuführen, wählen Sie den Header oder den Textbereich des Datenträgers aus, und klicken Sie auf **Vorgänge**.

Datenträger zuordnen von...

Dieser Vorgang wird verwendet, um eine Zuordnungsbeziehung zwischen dem Quelldatenträger und dem dynamischen Zieldatenträger zu erstellen. Er ist nur verfügbar, wenn der ausgewählte Datenträger ein dynamischer Datenträger ist.

Hinweis: Wenn Sie eine Zuordnung zu einem anderen Datenträger durchführen, muss die Kapazität jedes zugeordneten Ziel-Volume gleich oder größer als die des entsprechenden Quell-Volumes sein.

Volume zuordnen von...

Dieser Vorgang wird verwendet, um eine Zuordnungsbeziehung zwischen dem Quell-Volume und dem Basisziel-Volume zu erstellen. Er ist nur verfügbar, wenn das ausgewählte Volume ein Basis-Volume ist.

Hinweis: Wenn Sie eine Zuordnung zu einem anderen Datenträger durchführen, muss die Kapazität jedes zugeordneten Ziel-Volume gleich oder größer als die des entsprechenden Quell-Volumes sein.

Commit ausführen

Dieser Vorgang ist immer verfügbar. Alle Vorgänge werden zwischengespeichert und verursachen keine Änderungen des Zieldatenträgers, bis Sie den Vorgang **Commit ausführen** auswählen.

Zurücksetzen

Dieser Vorgang ist immer verfügbar. Der Vorgang **Zurücksetzen** wird verwendet, um Ihre Vorgänge aufzuheben und den Standardstatus des Datenträgerlayouts wiederherzustellen. Dieser Vorgang bereinigt alle zwischengespeicherten Vorgänge. Zurücksetzen bedeutet, die Informationen zu Quell- und Zieldatenträgerlayout neu aus der Konfigurationsdatei und

dem derzeitigen BS zu laden und alle vom Benutzer geänderten Informationen zum Datenträgerlayout zu verwerfen.

Beheben von BMR-Problemen

Wenn ein Problem erkannt wird, generiert Arcserve UDP Agent (Windows) eine Meldung, die Ihnen dabei hilft, das Problem zu identifizieren und zu beheben. Diese Meldungen sind im **Aktivitätsprotokoll** von Arcserve UDP Agent (Windows) enthalten, auf das über die Option **Protokolle anzeigen** auf der Startseite des Produkts zugegriffen werden kann. Wenn versucht wird, eine ungültige Aktion durchzuführen, zeigt Arcserve UDP Agent (Windows) außerdem üblicherweise eine Pop-up-Meldung an, damit Sie das Problem schnell identifizieren und lösen können.

- Langsamer Durchsatz während der BMR
- Nach der BMR werden dynamische Volumes nicht vom Betriebssystem erkannt
- Neustart von virtuellem Hyper-V-Rechner nach Bare-Metal-Recovery nicht möglich
- Neustart von virtuellem VMware-Rechner nach Bare-Metal-Recovery nicht möglich
- Server kann nicht gestartet werden, nachdem BMR ausgeführt wurde
- BMR-Job kann nicht an Recovery Point Server übergeben werden

Langsamer Durchsatz während der BMR

Dieses Problem wird kann durch SATA-Controller verursacht werden, bei denen "AHCI" aktiviert ist.

Während der BMR installiert Arcserve UDP Agent (Windows) Treiber für kritische unbekannte Geräte. Treiber, die bereits auf dem Gerät installiert sind, werden von Arcserve UDP Agent (Windows) nicht aktualisiert. Bei einigen Geräten verfügt Windows 7PE über die entsprechenden Treiber, die aber möglicherweise nicht die besten Treiber sind, was dazu führen kann, dass die BMR zu langsam ausgeführt wird.

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

- Überprüfen Sie, ob der Treiberordner die neuesten Laufwerktreiber enthält. Wenn dies der Fall ist und Sie eine Wiederherstellung auf dem ursprünglichen Rechner durchführen, installieren Sie den neuen Treiber aus dem Treiberordner. Wenn Sie eine Wiederherstellung auf einem alternativen Rechner durchführen, laden Sie aus dem Internet die aktuellsten Laufwerktreiber herunter und laden Sie sie, bevor Sie die Wiederherstellung der Daten starten. Um den Treiber zu laden, können Sie das Hilfsprogramm "drvload.exe" verwenden, das in Windows PE enthalten ist.
- Ändern Sie die Betriebsart des Gerätes von "AHCI" (Advanced Host Controller Interface) in Kompatibilitätsmodus. (Kompatibilitätsmodus gibt einen höheren Durchsatz an).

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Nach der BMR werden dynamische Volumes nicht vom Betriebssystem erkannt

Um dynamische Datenträger in einem konsistenten Status halten zu können, synchronisiert das Windows-Betriebssystem auf jedem dynamischen Datenträger automatisch die Metadaten des "Logical Disk Manager" (LDM). Wenn BMR einen dynamischen Datenträger wiederherstellt und ihn online stellt, werden die LDM-Metadaten auf diesem Datenträger automatisch vom Betriebssystem aktualisiert. Dies kann dazu führen, dass ein dynamisches Volume nicht vom Betriebssystem erkannt wird und nach dem Neustart fehlt.

Um dieses Problem zu beheben, sollten Sie bei einer BMR mit mehreren dynamischen Datenträgern keine Vorgänge vor der BMR durchführen, wie z. B. Volume reinigen oder löschen usw.

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Neustart von virtuellem Hyper-V-Rechner nach Bare-Metal-Recovery nicht möglich

Wenn Sie eine Bare-Metal-Recovery auf einem Hyper-V-Rechner durchgeführt haben, der aus mehr als einem mit einem Integrated Drive Electronics (IDE)-Controller verbundenen Datenträger besteht, und der Server nicht neu gestartet werden kann, führen Sie zur Fehlerbehebung folgenden Vorgang durch:

1. Stellen Sie sicher, dass der Datenträger, der das Systemvolume enthält, der Masterdatenträger ist.

   Das Hyper-V-BIOS sucht nach dem Systemvolume auf dem Masterdatenträger (Datenträger 1), der mit dem Masterkanal verbunden ist. Wenn das Systemvolume nicht auf dem Masterdatenträger gespeichert ist, startet der virtuelle Rechner nicht neu.

   Hinweis: Stellen Sie sicher, dass der Datenträger, der das Systemvolume enthält, mit einem IDE-Controller verbunden ist. Hyper-V kann nicht von einem SCSI-Datenträger gestartet werden.

2. Wenn nötig, ändern Sie die Hyper-V-Einstellungen. Verbinden Sie den Datenträger, der das Systemvolume enthält, mit dem IDE-Masterkanal, und starten Sie den virtuellen Rechner neu.

   Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Neustart von virtuellem VMware-Rechner nach Bare-Metal-Recovery nicht möglich

Wenn Sie eine Bare-Metal-Recovery auf einem VMware-Rechner durchgeführt haben, der aus mehr als einem mit einem Integrated Drive Electronics (IDE)-Controller oder einem SCSI-Adapter verbundenen Datenträger besteht, und der Server nicht neu gestartet werden kann, führen Sie zur Fehlerbehebung folgenden Vorgang durch:

1. Stellen Sie sicher, dass der Datenträger, der das Systemvolume enthält, der Masterdatenträger ist.

   Das VMware-BIOS sucht nach dem Systemvolume auf dem Masterdatenträger (Datenträger 0), der mit dem Masterkanal verbunden ist. Wenn sich das Systemvolume nicht auf dem Masterdatenträger befindet, startet der virtuelle Rechner nicht neu.

2. Wenn nötig, ändern Sie die VMware-Einstellungen. Verbinden Sie den Datenträger, der das Systemvolume enthält, mit dem IDE-Masterkanal, und starten Sie den virtuellen Rechner neu.

3. Wenn es sich um einen SCSI-Datenträger handelt, stellen Sie sicher, dass sich der Datenträger, der das Boot-Volume enthält, als erster mit dem SCSI-Adapter verbindet. Anderenfalls weisen Sie den Boot-Datenträger aus dem VMware-BIOS zu.

4. Da das VMware-BIOS während dem Starten nur acht Datenträger erkennt, stellen Sie sicher, dass sich der Datenträger mit dem Boot-Volume unter den letzten acht Datenträgern befindet. Wenn vor dem Datenträger mit dem Boot-Volume mehr als sieben Datenträger mit dem SCSI-Adapter verbunden sind, kann der virtuelle Rechner nicht gestartet werden.

   Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Der Server kann nicht gestartet werden, nachdem eine BMR ausgeführt wurde.

Problem

Wenn es sich beim Quellrechner um einen Active Directory-Server handelt, der eine BMR auf einen physischen Rechner mit abweichender Hardware oder auf einen virtuellen Rechner auf einem Hyper-V-Server ausführt, wird der Server nicht gestartet, und es wird ein blauer Bildschirm mit folgender Meldung angezeigt:

STOPP: c00002e2 Verzeichnisdienste konnten aufgrund von folgendem Fehler nicht gestartet werden: Ein Gerät, das an das System angehängt wurde, funktioniert nicht. Fehlerstatus: 0xc0000001.

Lösung

Starten Sie das System zur BMR-PE-Umgebung neu, benennen Sie alle *.log-Dateien im Ordner "C:\Windows\NTDS" um, und starten Sie das System neu. Benennen Sie zum Beispiel die Datei "edb.log" in "edb.log.old" um, und starten Sie das System neu.

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

BMR-Job kann nicht an Recovery Point Server übergeben werden

Bei einer Wiederherstellung von einem RPS-Server für denselben Knoten (Agent-Sicherung oder hostbasierte Sicherung) wird nur ein BMR-Job unterstützt. Dies wird vom Job-Monitor auf dem RPS-Server gesteuert.

Wenn der Rechner, auf dem der BMR-Job ausgeführt wird, unerwartet heruntergefahren oder neu gestartet wird, wartet der Job-Monitor auf der Seite des RPS-Servers 10 Minuten lang. Danach tritt eine Zeitüberschreitung ein. Während dieses Zeitraums können Sie für denselben Knoten über denselben RPS-Server keinen weiteren BMR-Job starten.

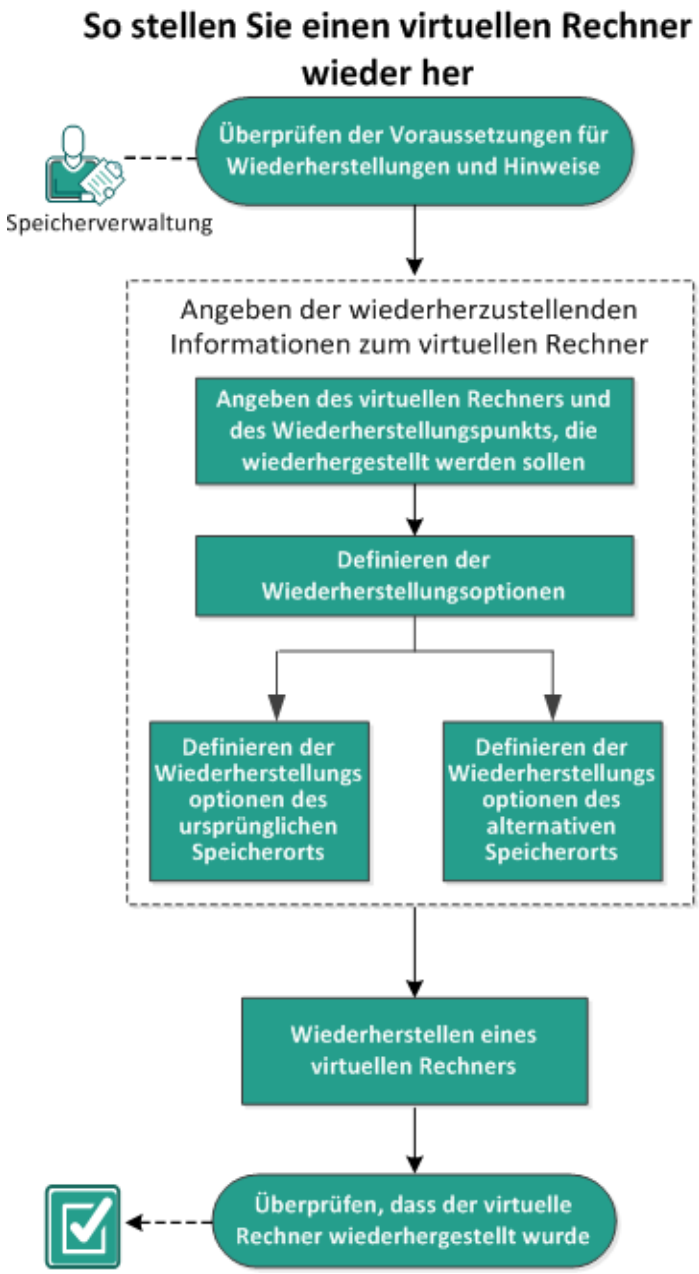
Wenn Sie die BMR über die BMR-Benutzeroberfläche abbrechen, tritt dieses Problem nicht auf.

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

So stellen Sie einen virtuellen Rechner wieder her

In Arcserve UDP können Sie die Option **VM wiederherstellen** verwenden, um einen virtuellen Rechner (VM) wiederherzustellen, den Sie zuvor über eine hostbasierte Sicherung und ohne Agent gesichert haben. Diese Methode ist hilfreich, um den gesamten virtuellen Rechner am ursprünglichen Speicherort oder an einem alternativen ESX- oder Hyper-V-Speicherort wiederherzustellen. Sie können die verfügbaren Wiederherstellungspunkte des virtuellen Rechners in einer Kalenderansicht durchsuchen, und Sie können auswählen, welchen Wiederherstellungspunkt Sie wiederherstellen möchten.

Folgendes Diagramm veranschaulicht den Prozess für das Wiederherstellen eines virtuellen Rechners aus:



Führen Sie folgende Aufgaben aus, um einen virtuellen Rechner wiederherzustellen:

1. Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise
2. Angeben der wiederherzustellenden Informationen zum virtuellen Rechner
    a. Angeben des virtuellen Rechners und des Wiederherstellungspunkts, die wiederhergestellt werden sollen
    b. Definieren der Wiederherstellungsoptionen

- Definieren der Wiederherstellungsoptionen des ursprünglichen Speicherorts
- Definieren der Wiederherstellungsoptionen des alternativen Speicherorts

3. Wiederherstellen eines virtuellen Rechners
4. Überprüfen, dass der virtuelle Rechner wiederhergestellt wurde

Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Wiederherstellung ausführen:

- Sie haben einen gültigen Wiederherstellungspunkt, von dem eine Wiederherstellung durchgeführt werden soll.
- Sie haben einen gültigen und zugreifbaren Virtual Center-, ESX- oder Hyper-V-Zielserver, um den virtuellen Rechner wiederherzustellen.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Überprüfen Sie die folgenden Wiederherstellungshinweise:

- Wenn als Ziel für "VM wiederherstellen" Windows Server 2008 R2 verwendet wird, sollte die Quell-VM für die Sicherung keine VHDx-Datenträger enthalten, da diese auf dem Hyper-V-Server (unter Windows Server 2008 R2) nicht unterstützt werden.
- Wenn als Ziel für "VM wiederherstellen" Windows Server 2008 R2 oder Win2012 verwendet wird, sollte es sich beim Subsystemtyp der Quell-VM für die Sicherung nicht um Generation 2 handeln. Dieser Typ wurde mit Windows Server 2012 R2 eingeführt und wird auf dem Hyper-V-Server (unter Windows Server 2012/2008 R2) nicht unterstützt.

Angeben der wiederherzustellenden Informationen zum virtuellen Rechner

Sie können einen kompletten virtuellen Rechner aus einem Wiederherstellungspunkt wiederherstellen.

Der Prozess für das Wiederherstellen eines virtuellen Rechners verläuft folgendermaßen:

1. Angeben des virtuellen Rechners und des Wiederherstellungspunkts, die wiederhergestellt werden sollen
2. Definieren der Wiederherstellungsoptionen
   - Definieren der Wiederherstellungsoptionen des ursprünglichen Speicherorts
   - Definieren der Wiederherstellungsoptionen des alternativen Speicherorts

Angeben des virtuellen Rechners und des Wiederherstellungspunkts, die wiederhergestellt werden sollen

Verwenden Sie die Option **VM wiederherstellen**, um einen virtuellen Rechner, den Sie zuvor gesichert haben, wiederherzustellen. Durch diese Methode wird ein virtueller Rechner von einem Arcserve UDP-Wiederherstellungspunkt auf einem ESX- oder Hyper-V-Server schnell und konsistent erstellt. Der wiederhergestellte virtuelle Rechner kann dann einfach gestartet werden, um den Wiederherstellungsvorgang abzuschließen.

Gehen Sie wie folgt vor:

1. Verwenden Sie eine der folgenden Vorgangsweisen, um auf das Dialogfeld zur Auswahl der Wiederherstellungsmethoden zuzugreifen:

   In Arcserve UDP:

   a. Melden Sie sich bei Arcserve UDP an.

   b. Klicken Sie auf die Registerkarte **Ressourcen**.

   c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

   e. Klicken Sie bei den Drop-down-Optionen unter **Aktionen** auf **Wiederherstellen**.

      Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

      Hinweis: Sie werden automatisch im Agentenknoten angemeldet, und das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird im Agentenknoten geöffnet.

   In Arcserve UDP Agent (Windows):

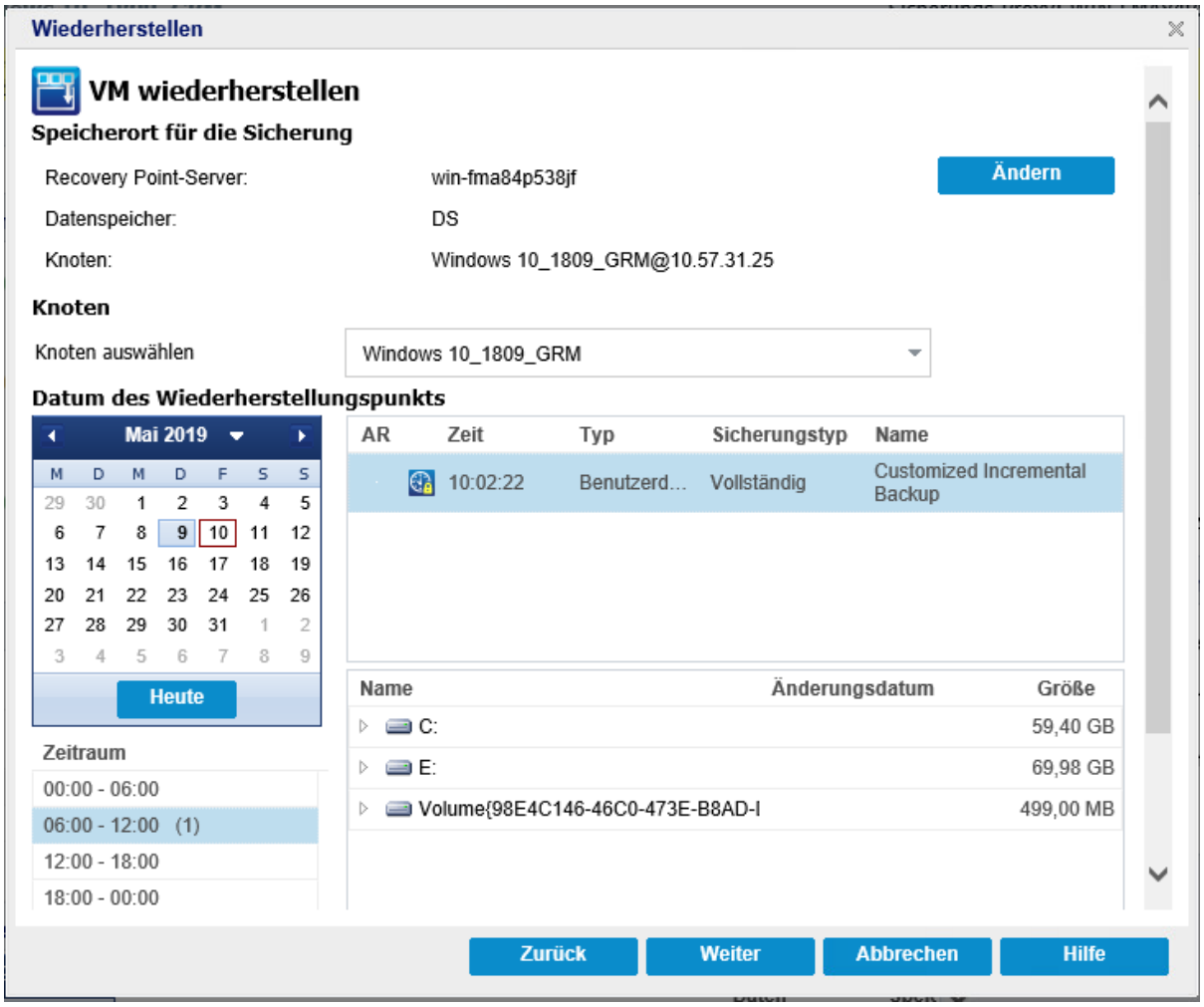
   a. Melden Sie sich bei Arcserve UDP Agent (Windows) an.

   b. Wählen auf der Startseite **Wiederherstellen** aus.

   Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

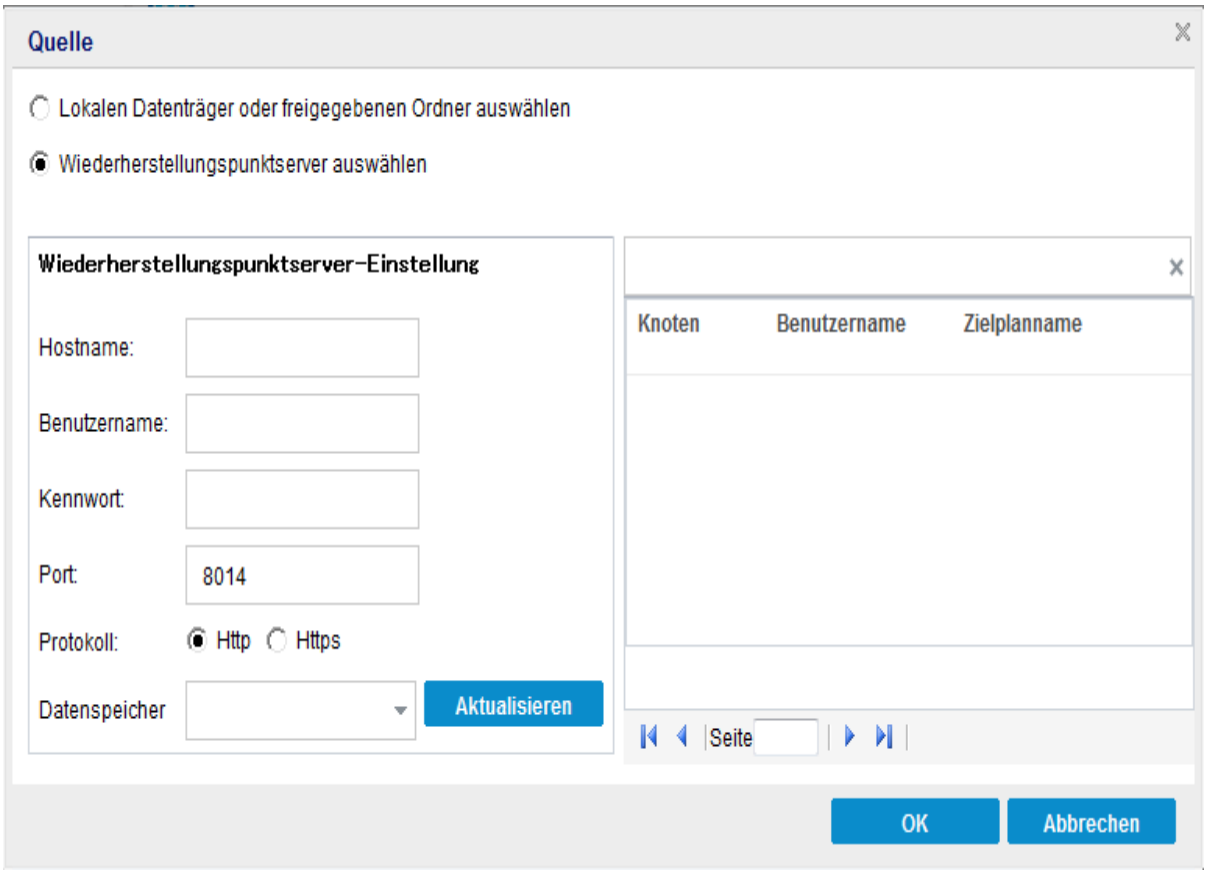
2. Klicken Sie auf die Option **VM wiederherstellen**.

   Das Dialogfeld **VM wiederherstellen** wird geöffnet.



3. Klicken Sie auf **Ändern**, um den Speicherort für die Sicherung zu ändern.

   Das Dialogfeld **Quelle** wird geöffnet. Sie können den Sicherungsspeicherort in diesem Dialogfeld auswählen.



4. Wählen Sie eine der folgenden Optionen:

   Lokalen Datenträger oder freigegebenen Ordner auswählen

   a. Legen Sie den Speicherort fest, unter dem Ihre Sicherungs-Images gespeichert werden, und wählen Sie die entsprechende Sicherungsquelle aus.

      Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Quellspeicherort zu erhalten.

      Das Dialogfeld **Speicherort für die Sicherung auswählen** wird geöffnet.

   b. Wählen Sie den Ordner, in dem die Wiederherstellungspunkte gespeichert sind, aus, und klicken Sie auf **OK**.

      Das Dialogfeld **Speicherort für die Sicherung auswählen** wird geschlossen, und der Sicherungsspeicherort wird im Dialogfeld **Quelle** angezeigt.

   c. Klicken Sie auf **OK**.

   Die Wiederherstellungspunkte werden im Dialogfeld **VM wiederherstellen** aufgelistet.

   Auswählen des Recovery Point Servers

a. Geben Sie die Details für die **Einstellungen des Recovery Point Servers** an, und klicken Sie auf **Aktualisieren**.

   Alle Knoten (Agenten/virtuelle Rechner) werden in der Spalte "Knoten" im Dialogfeld **Quelle** aufgelistet.

b. Wählen Sie den Knoten (Agenten/virtuelle Rechner) aus der angezeigten Liste aus, und klicken Sie auf **OK**.

   Die Wiederherstellungspunkte werden im Dialogfeld **VM wiederherstellen** aufgelistet.

5. Wählen Sie aus der Drop-down-Liste **Virtueller Rechner** den virtuellen Rechner aus, der wiederhergestellt werden soll.

   Die Kalenderansicht wird angezeigt und alle Daten, die Wiederherstellungspunkte für die angegebene Sicherungsquelle enthalten, werden grün hervorgehoben.

6. Geben Sie das Datum für das Image des virtuellen Rechners an, das Sie wiederherstellen möchten.

   Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp und Name der Sicherung angezeigt.

7. Wählen Sie einen wiederherzustellenden Wiederherstellungspunkt aus.

   Der Sicherungsinhalt (einschließlich aller Anwendungen) für die ausgewählten Wiederherstellungspunkte wird angezeigt. Wenn Sie einen virtuellen Rechner wiederherstellen, wird der gesamte Rechner wiederhergestellt. Dadurch können Sie individuelle Volumes, Ordner oder Dateien innerhalb des ausgewählten virtuellen Rechners anzeigen, aber nicht auswählen.

   Hinweis: Eine Uhr mit einem Sperrsymbol zeigt an, dass der Wiederherstellungspunkt verschlüsselte Informationen enthält und möglicherweise ein Kennwort zur Wiederherstellung benötigt.

8. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet.

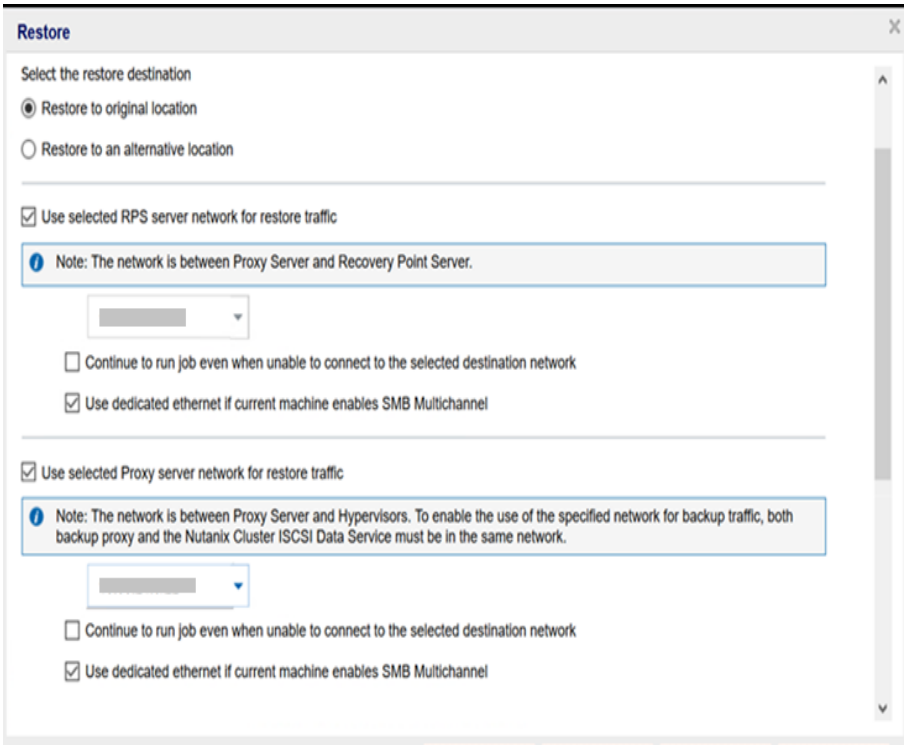
   Der virtuelle Rechner und der Wiederherstellungspunkt, die wiederhergestellt werden sollen, sind angegeben.

Definieren der Wiederherstellungsoptionen

Nachdem Sie den virtuellen Rechner und den Wiederherstellungspunkt, die wiederhergestellt werden sollen, angegeben haben, legen Sie die Wiederherstellungsoptionen für das ausgewählte Image des virtuellen Rechners fest.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld Wiederherstellungsoptionen das Wiederherstellungsziel aus.



Es sind folgende Zieloptionen verfügbar:

Am ursprünglichen Speicherort wiederherstellen

Stellt den virtuellen Rechner am gleichen Speicherort wieder her, an dem das Sicherungs-Image erstellt wurde. Standardmäßig ist diese Option aktiviert.

Weitere Informationen finden Sie unter Definieren der Wiederherstellungsoptionen des ursprünglichen Speicherorts.

Am alternativen Speicherort wiederherstellen

Stellt den virtuellen Rechner an einem anderen Speicherort wieder her, an dem das Sicherungs-Image erstellt wurde.

Weitere Informationen finden Sie unter Definieren der Wiederherstellungsoptionen des alternativen Speicherorts.

2. (Optional) Aktivieren Sie das Kontrollkästchen **Ausgewähltes RPS-Servernetzwerk für Wiederherstellungsdatenverkehr verwenden**, und gehen Sie dann wie folgt vor:

    a. Um die Kommunikation zwischen dem Windows-Proxy- und dem Wiederherstellungspunktserver zu aktivieren, wählen Sie das CIDR-Netzwerk in der Drop-down-Liste aus.

    b. Um die Einschränkung für den SMB-Multichannel zu definieren, sodass die Datenübertragung nur über das ausgewählte Netzwerk übertragen wird, aktivieren Sie das Kontrollkästchen **Dediziertes Ethernet verwenden, wenn der aktuelle Computer SMB Multichannel ermöglicht**.

    Hinweise:

    - Diese Option ist nicht standardmäßig verfügbar. Um diese Option zu aktivieren, erstellen Sie die Zeichenfolgenregistrierung *UseDedicatedEthernet* im folgenden Pfad, und legen Sie dann den Registrierungswert auf 1 fest:

      SOFTWARE\Arcserve\Unified Data Protection\Engine

    - Wenn Sie einen Wiederherstellungsjob über die Seite "Knoten" ausführen, erstellen Sie einen Registrierungsschlüssel auf dem Sicherungs-Proxy.

    - Wenn Sie einen Wiederherstellungsjob vom normalen Agenten mithilfe der RPS-Sicherungssitzung ausführen, erstellen Sie einen Registrierungsschlüssel auf dem normalen Agenten.

3. (Optional) Aktivieren Sie das Kontrollkästchen **Ausgewähltes Proxy-Server-Netzwerk für Wiederherstellungsdatenverkehr verwenden**, und gehen Sie dann wie folgt vor:

    a. Um die Kommunikation zwischen Windows-Proxy-Server und Hypervisor zu aktivieren, wählen Sie das CIDR-Netzwerk aus der Drop-down-Liste aus.

    b. Um die Einschränkung für den SMB-Multichannel zu definieren, sodass die Datenübertragung nur über das ausgewählte Netzwerk übertragen wird, aktivieren Sie das Kontrollkästchen **Dediziertes Ethernet verwenden, wenn der aktuelle Computer SMB Multichannel ermöglicht**.

    Hinweise:

    - Diese Option ist nicht standardmäßig verfügbar. Um diese Option zu aktivieren, erstellen Sie die Zeichenfolgenregistrierung *UseDedicatedEthernet* im folgenden Pfad, und legen Sie dann den Registrierungswert auf 1 fest:

SOFTWARE\Arcserve\Unified Data Protection\Engine

- Wenn Sie einen Wiederherstellungsjob über die Seite "Knoten" ausführen, erstellen Sie einen Registrierungsschlüssel auf dem Sicherungs-Proxy.
- Wenn Sie einen Wiederherstellungsjob vom normalen Agenten mithilfe der RPS-Sicherungssitzung ausführen, erstellen Sie einen Registrierungsschlüssel auf dem normalen Agenten.

4. Legen Sie die Optionen für die Konfliktlösung fest, die von Arcserve UDP ausgeführt werden sollen, wenn während der Wiederherstellung Konflikte auftreten

Bestehenden virtuellen Rechner überschreiben

Mit dieser Option legen Sie fest, ob der vorhandene virtuelle Rechner überschrieben werden soll. Standardmäßig ist diese Option zum Überschreiben deaktiviert.

Hinweis: Für die Option Bestehenden virtuellen Rechner überschreiben wird ein "bestehender virtueller Rechner" als eine VM definiert, die denselben VM-Namen aufweist und sich auf demselben ESXi-Host befindet (VMware-VMs), oder als eine VM, die denselben VM-Namen und dieselbe Instanzen-UUID aufweist und sich auf demselben Hyper-V-Host befindet (Hyper-V-VMs). Für VMware-VM gilt Folgendes: Wenn eine VM den gleichen VM-Namen aufweist, sich jedoch auf einem anderen ESXi-Host (unter dem gleichen vCenter) befindet, funktioniert diese Option zum Überschreiben nicht. In diesem Fall erkennt die VM-Wiederherstellungs-GUI diese VM, zeigt eine Fehlermeldung an und verhindert, dass Sie den Vorgang fortsetzen, damit eine VM nicht versehentlich überschrieben wird. Um dies zu umgehen, müssen Sie entweder die vorhandene VM umbenennen oder die Option "An einem alternativen Speicherort wiederherstellen" verwenden und dann einen anderen VM-Namen festlegen.

- Wenn Sie diese Option aktivieren, wird der Wiederherstellungsvorgang alle vorhandenen Images dieses virtuellen Rechners, die sich am angegebenen Wiederherstellungsziel befinden, überschreiben (ersetzen). Das Image des virtuellen Rechners wird von den Sicherungsdateien wiederhergestellt, unabhängig davon, ob sie derzeit auf Ihrem Wiederherstellungsziel vorhanden sind.
- Wenn Sie diese Option nicht auswählen, zeigt die Benutzeroberfläche für die VM-Wiederherstellung eine Fehlermeldung an und verhindert, dass Sie den Vorgang fortsetzen, wenn die ursprüngliche VM noch am ursprünglichen Speicherort vorhanden ist. Um dies zu umgehen, müssen Sie entweder die vorhandene VM umbenennen oder die Option "An einem alternativen

Speicherort wiederherstellen" verwenden und dann einen anderen VM-Namen festlegen.

Neue Instanzen-UUID für virtuellen Rechner generieren

Mit dieser Option wird festgelegt, ob eine neue Instanzen-UUID für den wiederhergestellten virtuellen Rechner generiert oder die ursprüngliche Instanzen-UUID behalten werden soll.

Hinweis: Wenn Sie diese Option nicht auswählen, wird die ursprüngliche Instanzen-UUID für die wiederhergestellte VM festgelegt. Wenn das vCenter/ESX-Ziel oder der Hyper-V-Host bereits über einen virtuellen Rechner mit derselben Instanzen-UUID verfügt, wird allerdings eine neue UUID verwendet, und eine Warnmeldung wird im Aktivitätsprotokoll des VM-Wiederherstellungsjobs angezeigt.

5. Legen Sie die Option Nach der Wiederherstellung fest.

Virtuellen Rechner starten

Wählen Sie aus, ob die Stromzufuhr für den virtuellen Rechner am Ende des Wiederherstellungsvorgangs angewendet werden soll. Standardmäßig ist diese Option deaktiviert.

Als VM-Vorlage markieren (nur für VMware-VMs verfügbar)

Legen Sie fest, ob die wiederhergestellte VM in eine Vorlage konvertiert werden soll. Wenn der Quellknoten als VM gesichert wird, ist diese Option nicht standardmäßig aktiviert. Wenn der Quellknoten als Vorlage gesichert wird, ist diese Option standardmäßig aktiviert.

Die Wiederherstellungsoptionen sind für die Wiederherstellung eines virtuellen Rechners festgelegt.

Definieren der Wiederherstellungsoptionen des ursprünglichen Speicherorts

Während des Konfigurationsvorgangs zur Wiederherstellung der VM ist es erforderlich, dass Sie die Option auswählen, mit der Sie bestimmen können, wo der virtuelle Rechner wiederhergestellt wird. Die verfügbaren Auswahlmöglichkeiten sind **Wiederherstellung am ursprünglichen Speicherort** und **Wiederherstellung an einem alternativen Speicherort**.

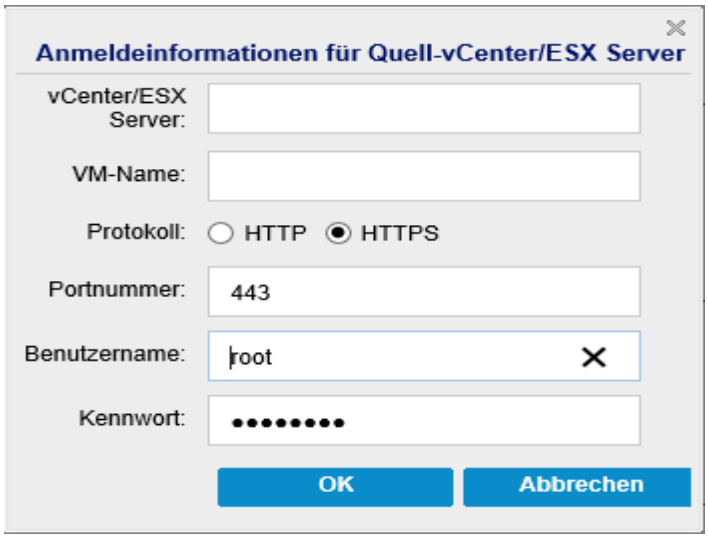
Dieser Vorgang erklärt, wie ein virtueller Rechner am ursprünglichen Speicherort wiederhergestellt wird.

Gehen Sie wie folgt vor:

1. Nachdem Sie die Optionen **Konflikte lösen** und **Nach der Wiederherstellung** angegeben haben, aktivieren Sie im Dialogfeld **Wiederherstellungsoptionen** die Option **Am ursprünglichen Speicherort wiederherstellen**, und klicken Sie auf **Weiter**.

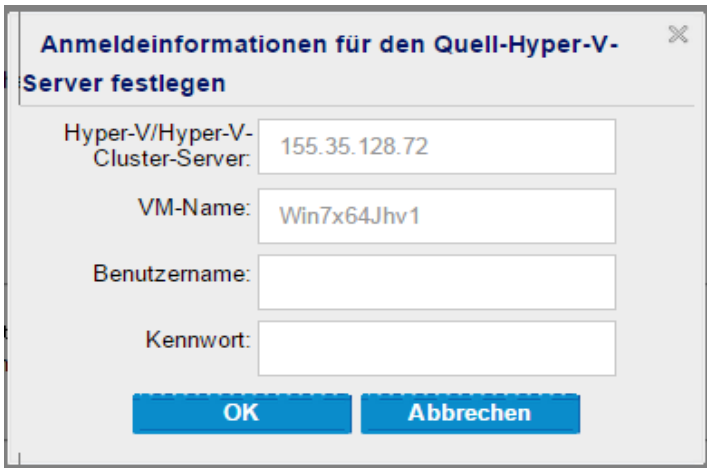
   Das entsprechende Dialogfeld für VMware oder Hyper-V wird angezeigt.

   - Für VMware wird das Dialogfeld **Anmeldeinformationen für Quell-vCenter/ESX Server festlegen** angezeigt.



   - Für Hyper-V wird das Dialogfeld **Anmeldeinformationen für den Quell-**

Hyper-V-Server festlegen angezeigt.



2. Geben Sie die Anmeldeinformationen ein, um auf den virtuellen Rechner zuzugreifen.

   - Füllen Sie für VMware die folgenden Felder aus.

     vCenter/ESX Server

     Gibt den Hostnamen oder die IP-Adresse für das Ziel des vCenter- oder ESX-Serversystems an.

     Hinweis: Dieses Feld kann nicht bearbeitet werden. Sie können nur Details anzeigen.

     VM-Name

     Zeigt den Namen des virtuellen Rechners, den Sie wiederherstellen, an.

     Hinweis: Dieses Feld kann nicht bearbeitet werden. Sie können nur Details anzeigen.

     Protokoll

     Gibt das Protokoll an, das Sie für die Kommunikation mit dem Zielserver verwenden möchten. Die verfügbare Auswahl ist "HTTP" und "HTTPS".

     Portnummer

     Gibt den Port an, den Sie für den Datentransfer zwischen dem Quellserver und dem Zielserver verwenden möchten.

     Standard: 443.

     Benutzername

     Geben Sie den Benutzernamen an, der über Zugriffsrechte verfügt, um sich auf dem vCenter/ESX-Server anzumelden, auf dem Sie den virtuellen Rechner wiederherstellen möchten.

Kennwort

Gibt das entsprechende Kennwort für den Benutzernamen an.

- Füllen Sie für Hyper-V die folgenden Felder aus.

Hyper-V/Hyper-V-Cluster-Server

Gibt den Hostnamen oder die IP-Adresse für das Ziel des Hyper-V-Serversystems oder des Hyper-V-Cluster-Serversystems an.

Hinweis: Dieses Feld kann nicht bearbeitet werden. Sie können nur Details anzeigen.

VM-Name

Zeigt den Namen des virtuellen Rechners, den Sie wiederherstellen, an.

Hinweis: Dieses Feld kann nicht bearbeitet werden. Sie können nur Details anzeigen.

Benutzername

Gibt den Namen des Benutzers an, der über Zugriffsrechte verfügt, um sich beim Hyper-V-Server anzumelden, auf dem Sie den virtuellen Rechner wiederherstellen möchten. Geben Sie für die Hyper-V-Cluster-VM das Domänenkonto an, das über Administratorrechte des Clusters verfügt.

Kennwort

Gibt das entsprechende Kennwort für den Benutzernamen an.

3. Klicken Sie auf **OK**.

Das Dialogfeld **Wiederherstellungs-Übersicht** wird geöffnet.

Die Wiederherstellungsoptionen für den ursprünglichen Speicherort sind festgelegt.

Definieren der Wiederherstellungsoptionen des alternativen Speicherorts

Während des Konfigurationsvorgangs zur Wiederherstellung der VM müssen Sie angeben, wo der wiederhergestellte virtuelle Rechner gespeichert werden soll. Die verfügbaren Auswahlmöglichkeiten sind **Wiederherstellung am ursprünglichen Speicherort** und **Wiederherstellung an einem alternativen Speicherort**.

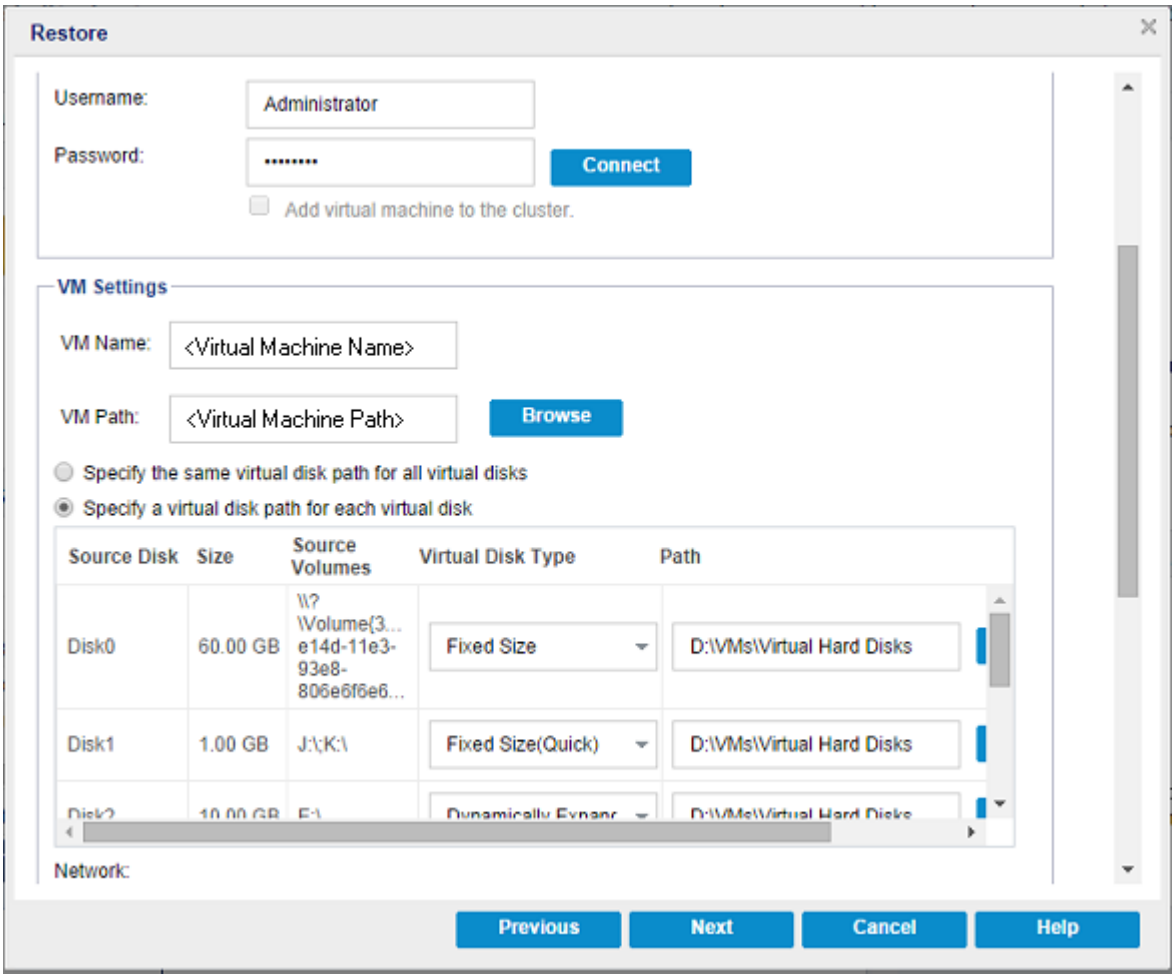
Dieser Vorgang erklärt, wie ein virtueller Rechner an einem alternativen Speicherort oder auf einem anderen Datenspeicher wiederhergestellt wird.

Gehen Sie wie folgt vor:

1. Nachdem Sie die Optionen **Konflikte lösen** und **Nach der Wiederherstellung** angegeben haben, wählen Sie im Dialogfeld **Wiederherstellungsoptionen** die Option **Am ursprünglichen Speicherort wiederherstellen** aus.

   - Für VMware wird das Dialogfeld **Wiederherstellungsoptionen** mit zusätzlichen Optionen für Wiederherstellungen an alternativen Speicherorten erweitert.
   - Für Hyper-V wird das Dialogfeld **Wiederherstellungsoptionen** mit zusätzlichen Optionen für Wiederherstellungen an alternativen Speicherorten erweitert.

   Wenn Sie die Option "**Für jeden virtuellen Datenträger einen Pfad angeben**" auswählen, dann wird folgendes Dialogfeld angezeigt:



2. Geben Sie die entsprechenden Serverinformationen an.

   - Füllen Sie für VMware folgende Felder aus:

     vCenter/ESX Server

     Gibt den Hostnamen oder die IP-Adresse für das Ziel des vCenter- oder ESX-Serversystems an.

     Benutzername

     Geben Sie den Benutzernamen an, der über Zugriffsrechte verfügt, um sich auf dem vCenter/ESX-Server anzumelden, auf dem Sie den virtuellen Rechner wiederherstellen möchten.

     Kennwort

     Gibt das entsprechende Kennwort für den Benutzernamen an.

     Protokoll

     Gibt das Protokoll an, das Sie für die Kommunikation mit dem Zielserver verwenden möchten. Die verfügbare Auswahl ist "HTTP" und "HTTPS".

     Standard: HTTPS.

Hinweis: VMware Virtual Disk Development Kit (VDDK) 6.x.x ist in Arcserve UDP Version 6.5 enthalten, wobei VDDK 6.x.x jedoch HTTP nicht unterstützt. Stellen Sie sicher, dass HTTPS ausgewählt ist, es sei denn, Sie ersetzen das integrierte VDDK 6.x.x manuell durch eine andere VDDK-Version.

Portnummer

Gibt den Port an, den Sie für den Datentransfer zwischen dem Quellserver und dem Zielserver verwenden möchten.

Standard: 443.

- Füllen Sie für Hyper-V folgende Felder aus:

Hyper-V-Server

Gibt den Hostnamen oder die IP-Adresse für das Ziel des Hyper-V-Serversystems an.

Benutzername

Gibt den Namen des Benutzers an, der über Zugriffsrechte verfügt, um sich beim Hyper-V-Server anzumelden, auf dem Sie den virtuellen Rechner wiederherstellen möchten. Geben Sie für die Hyper-V-Cluster-VM das Domänenkonto an, das über Administratorrechte des Clusters verfügt.

Kennwort

Gibt das entsprechende Kennwort für den Benutzernamen an.

Virtuellen Rechner zum Cluster hinzufügen

Wählen Sie die Option aus, wenn Sie den virtuellen Rechner, den Arcserve UDP wiederherstellt, in den Cluster hinzufügen möchten. Beachten Sie folgende Optionen:

- Wenn Sie den Cluster-Knotennamen als Hyper-V-Servernamen angeben, dann ist das Kontrollkästchen standardmäßig deaktiviert und ausgewählt. Dadurch wird der virtuelle Rechner automatisch in den Cluster hinzugefügt.
- Wenn Sie den Hostnamen eines Hyper-V-Servers angeben, der Teil des Clusters ist, dann ist das Kontrollkästchen aktiviert, und Sie können auswählen, dass der virtuelle Rechner in den Cluster hinzugefügt wird.
- Wenn Sie den Hostnamen eines eigenständigen Hyper-V-Servers angeben, der nicht Teil des Clusters ist, dann ist das Kontrollkästchen deaktiviert und nicht ausgewählt.

3. Wenn die Serverinformationen für vCenter/ESX oder Hyper-V festgelegt sind, klicken Sie auf die Schaltfläche **Mit vCenter/ESX Server verbinden** bzw. **Mit diesem Hyper-V-Server verbinden**.

   Wenn die alternativen Anmeldeinformationen für den Serverzugriff korrekt sind, werden die Felder für **VM-Einstellungen** aktiviert.

4. Geben Sie die **VM-Einstellungen** an.

   - Füllen Sie für VMware die folgenden Felder aus.

     VM-Name

     Gibt den Namen des virtuellen Rechners, den Sie wiederherstellen, an.

     ESX Server

     Gibt das Ziel des ESX-Servers an. Das Drop-down-Menü enthält eine Auflistung aller ESX-Server, die mit dem vCenter-Server verbunden sind.

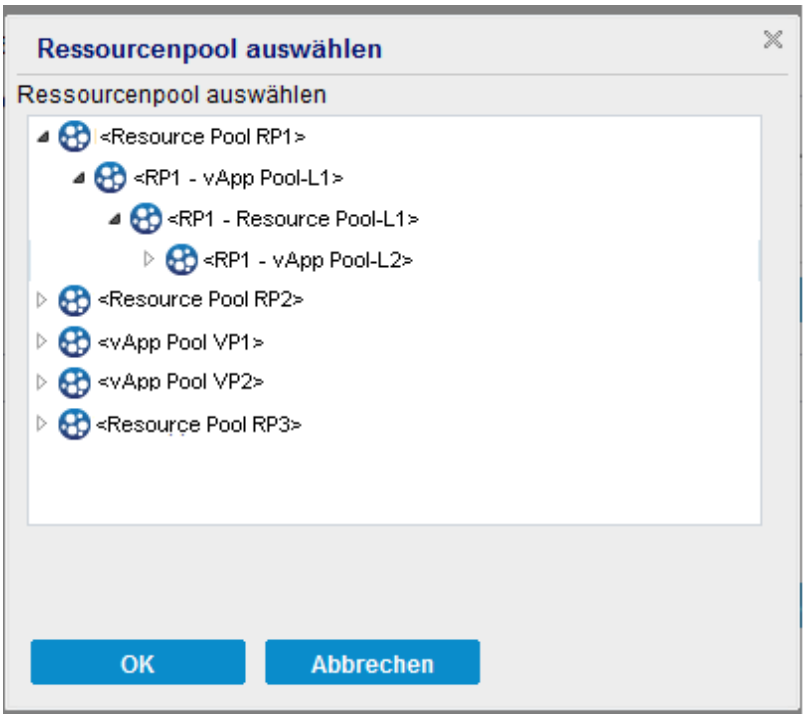
     Ressourcenpool

     Wählt den **Ressourcenpool** oder **vApp-Pool** aus, den Sie für die Wiederherstellung des virtuellen Rechners verwenden möchten.

     Hinweis: Ein Ressourcenpool ist eine konfigurierte Sammlung von CPU- und Speicherressourcen. Ein vApp-Pool ist eine Sammlung von einem oder mehreren virtuellen Rechnern, die als ein einzelnes Objekt verwaltet werden können.

     Standardeinstellung: Leer.

     Klicken Sie auf die Schaltfläche **Ressourcenpool durchsuchen**. Das Dialogfeld **Ressourcenpool auswählen** wird angezeigt. Dieses Dialogfeld enthält eine Auflistung aller verfügbaren Ressourcenpools und vApp-Pools für den Ziel-ESX-Server. Wählen Sie den Pool aus, der für die Wiederherstellung des virtuellen Rechners verwendet werden soll. Sie können dieses Feld leer lassen, wenn Sie dieser Wiederherstellung des Rechners keinen Ressourcenpool oder vApp-Pool zuweisen möchten.



Speicherrichtlinie

Geben Sie die VM-Speicherrichtlinie an, die auf die Ausgangs-VM der wiederhergestellten VM angewendet wird. Wählen Sie den Datenspeicherstandard aus, wenn die VM-Speicherrichtlinie nicht angewendet werden soll.

Hinweis: Wenn nur der Datenspeicherstandard angezeigt wird, tatsächlich aber weitere Speicherrichtlinien in vCenter definiert sind, so verfügt das für die Verbindung mit vCenter verwendete Konto nicht über ausreichende Berechtigungen, um die Speicherrichtlinie von vCenter abzurufen. Überprüfen, ob das Konto über die Berechtigung "Profilgesteuerte Speicheransicht" auf der vCenter-Ebene verfügt.

VM-Datenspeicher

Geben Sie den Zieldatenspeicher für die Ausgangs-VM der wiederhergestellten VM an.

Hinweis: Standardmäßig werden nur die mit der ausgewählten Speicherrichtlinie kompatiblen Datenspeicher aufgeführt. Um alle Datenspeicher anzuzeigen, deaktivieren Sie das Kontrollkästchen **Nur kompatible Datenspeicher für die ausgewählten Speicherrichtlinie anzeigen** unterhalb der Tabelle "Datenträgerdatenspeicher".

Datenträgerdatenspeicher

Geben Sie für jeden virtuellen Datenträger des virtuellen Computers den Typ des virtuellen Datenträgers, die Speicherrichtlinie sowie den Zieldatenspeicher an.

- Virtueller Datenträgertyp: Wählen Sie eine der folgenden Optionen aus: Thin, Thick Lazy Zeroed oder Thick Eager Zeroed.
- Speicherrichtlinie: Wählen Sie die VM-Speicherrichtlinie aus, die auf diesen virtuellen Datenträger angewendet wird. Wählen Sie den Datenspeicherstandard aus, wenn die VM-Speicherrichtlinie nicht angewendet werden soll.
- Zieldatenspeicher: Wählen Sie den Datenspeicher aus, auf dem der virtuellen Datenträger wiederhergestellt wird.

Hinweis: Standardmäßig werden nur die Datenspeicher aufgeführt, die mit der ausgewählten Speicherrichtlinie kompatibel sind. Um alle Datenspeicher anzuzeigen, deaktivieren Sie das Kontrollkästchen **Nur kompatible Datenspeicher für die ausgewählten Speicherrichtlinie anzeigen** unterhalb der Tabelle "Datenträgerdatenspeicher".

Netzwerk

Gibt die Konfigurationsdetails "vSphere Standard Switch/vSphere Distributed Switch" an.

- Füllen Sie für Hyper-V folgende Felder aus.

VM-Name

Gibt den Namen des virtuellen Rechners, den Sie wiederherstellen, an.

VM-Pfad

Gibt den Zielpfad (auf dem Hyper-V-Server) an, unter dem die Konfigurationsdatei der Hyper-V-VM gespeichert werden soll. Standardmäßig wird der Standardordner der VM-Konfigurationsdatei für den Hyper-V-Server angezeigt. Sie können den Pfad direkt im Feld ändern oder auf **Durchsuchen** klicken, um einen Pfad auszuwählen.

Hinweis: Wenn Sie den virtuellen Rechner im Hyper-V-Cluster wiederherstellen, und wenn Sie möchten, dass der virtuelle Rechner unter den Cluster-Knoten migriert wird, dann geben Sie das CSV (Cluster Shared Volume) sowohl für den VM-Pfad als auch für den virtuellen Datenträgerpfad an.

Geben Sie für alle virtuellen Datenträger den gleichen Pfad an

Geben Sie einen einzigen Pfad (auf dem Hyper-V-Server) an, unter dem alle virtuellen Datenträger der VM gemeinsam gespeichert werden soll.

Der Standardordner der VM-Datenträgerdatei für den Hyper-V-Server wird standardmäßig angezeigt. Sie können den Pfad direkt im Feld ändern oder auf **Durchsuchen** klicken, um einen Pfad auszuwählen.

Hinweis: Wenn Sie den virtuellen Rechner im Hyper-V-Cluster wiederherstellen, und wenn Sie möchten, dass der virtuelle Rechner unter den Cluster-Knoten migriert wird, dann geben Sie das CSV (Cluster Shared Volume) sowohl für den VM-Pfad als auch für den virtuellen Datenträgerpfad an.

Für jeden virtuellen Datenträger einen Pfad angeben

Geben Sie die Pfade (auf dem Hyper-V-Server) für einzelnen virtuellen Datenträger der VM an. Der Standardordner der VM-Datenträgerdatei für den Hyper-V-Server wird standardmäßig angezeigt. Sie können den Pfad direkt im Feld ändern oder auf **Durchsuchen** klicken, um einen Pfad auszuwählen. Um den virtuellen Datenträgertyp zuzuweisen, wählen Sie eine der folgenden Optionen: "Feste Größe", "Feste Größe (schnell)", "Wird dynamisch erweitert" und "Als Quelldatenträger beibehalten".

Hinweise:

- Wenn Sie den virtuellen Rechner im Hyper-V-Cluster wiederherstellen, und wenn Sie möchten, dass der virtuelle Rechner unter den Cluster-Knoten migriert wird, dann geben Sie das CSV (Cluster Shared Volume) sowohl für den VM-Pfad als auch für den virtuellen Datenträgerpfad an.
- Verwenden Sie nicht die Option "Feste Größe (schnell)", außer wenn Sie sicher sind, dass Sie zuvor keine vertraulichen Informationen auf dem Speichergerät gespeichert haben, auf dem sich die virtuelle Datenträgerdatei befindet.

Feste Größe (schnell)

Mit dieser Option können Sie Datenträger mit fester Größe auf schnelle Weise wiederherstellen. Sie müssen nicht verwendete Datenträgerblöcke nicht auf null löschen, während Sie den Datenträger wiederherstellen. Allerdings blieben einige Fragmente der ursprünglichen Daten deswegen auf dem zugrundeliegenden Speicher. Dies führt zu Risiken von Informationslecks. Nachdem der Datenträger in den virtuellen Rechner geladen wurde, kann der Benutzer des virtuellen Rechners einige Datenträgertools verwenden, um die Rohdaten im Datenträger zu analysieren und die ursprünglichen Daten auf dem Hyper-V-Server-Speichergerät abzurufen, auf dem sich die Datei des virtuellen Datenträgers befindet.

Netzwerk

Gibt die Netzwerkkonfigurationsdetails für die VM an.

5. Klicken Sie auf **"OK**".

   Das Dialogfeld **Wiederherstellungs-Übersicht** wird geöffnet.

   Die Wiederherstellungsoptionen für den alternativen Speicherort sind festgelegt.

Wiederherstellen eines virtuellen Rechners

Die **Wiederherstellungs-Übersicht** ist hilfreich, um sämtliche Wiederherstellungsoptionen, die Sie festgelegt haben, zu überprüfen und bei Bedarf zu ändern.

Überprüfen Sie die Informationen im Dialogfeld **Wiederherstellungs-Übersicht**, um die Richtigkeit aller Wiederherstellungsoptionen und Einstellungen sicherzustellen.

- Wenn die Übersichtsinformationen Fehler enthalten, klicken Sie auf **Zurück**, und ändern Sie die inkorrekten Einstellungen im entsprechenden Dialogfeld.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsprozess zu starten.

Der virtuelle Rechner wird wiederhergestellt.

Überprüfen, dass der virtuelle Rechner wiederhergestellt wurde

Überprüfen Sie nach dem Abschluss der Wiederherstellung, ob der virtuelle Rechner im angegebenen Ziel wiederhergestellt wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Wiederherstellungsziel, das Sie angegeben haben.

   Wenn Sie beispielsweise auswählen, dass der virtuelle Rechner im Wiederherstellungsziel als ursprünglicher Speicherort wiederhergestellt werden soll, melden Sie sich beim ursprünglichen vCenter/ESX-Server oder Hyper-V-Server an, und überprüfen Sie, ob der virtuelle Rechner vorhanden ist.

   Wenn Sie auswählen, dass der virtuelle Rechner im alternativen Speicherort wiederhergestellt werden soll, melden Sie sich beim alternativen vCenter/ESX-Server oder Hyper-V-Server an, der in den Wiederherstellungsoptionen angegeben ist, und überprüfen Sie, ob der virtuelle Rechner vorhanden ist.

2. Überprüfen Sie, ob der virtuelle Rechner wiederhergestellt wurde.

   Der virtuelle Rechner wurde erfolgreich wiederhergestellt.

So stellen Sie SQL Filestream wieder her

In diesem Abschnitt werden die folgenden Themen behandelt:

So wenden Sie den Patch "T00002266" an

Dieser Abschnitt enthält Informationen zur Anwendung des Patches T00002266.

Bevor Sie den Patch *T00002266* installieren, stellen Sie sicher, dass sich die Datei *SqlRestore.ini* in *C:\Programme\Arcserve\Unified Data Protection\Engine\Configuration* befindet, um Wiederherstellungen durchzuführen.

Gehen Sie wie folgt vor, um den Patch zu installieren:

1. Laden Sie die Datei **T00002266.zip** herunter und extrahieren Sie sie.
2. Klicken Sie zur Installation auf die Datei **T00002266.exe**.

Gehen Sie wie folgt vor, um die Datei "SqlRestore.ini" zu öffnen und zu bearbeiten:

1. Navigieren Sie auf dem Quellrechner zum folgenden Speicherort:

   C:\Programme\Arcserve\Unified Data Protection\Engine\Configuration
2. Öffnen Sie die Datei *SqlRestore.ini* in einem Texteditor, und fügen Sie den folgenden Eintrag ein:

   RestoreInstanceName = {Name der Ziel-SQLServer-Instanz}

   MDF-Wiederherstellungsordner = {Speicherort der MDF-Datei}

   LDF-restore-folder = {LDF-Dateispeicherort}

   NDF-Wiederherstellungsordner = {NDF-Dateispeicherort}

   FILESTREAM-restore-folder = {Speicherort der FileStreams-Datei}
3. Bearbeiten Sie je nach dem, wo Sie die Datenbanken wiederherstellen möchten, die Inhalte in geschweiften Klammern mit den Speicherorten der Ordner.

   Ersetzen Sie zum Beispiel:

   MDF-Wiederherstellungsordner = {Speicherort der MDF-Datei}

   mit

   MDF-Wiederherstellungsordner = C:\Rest\MDF1

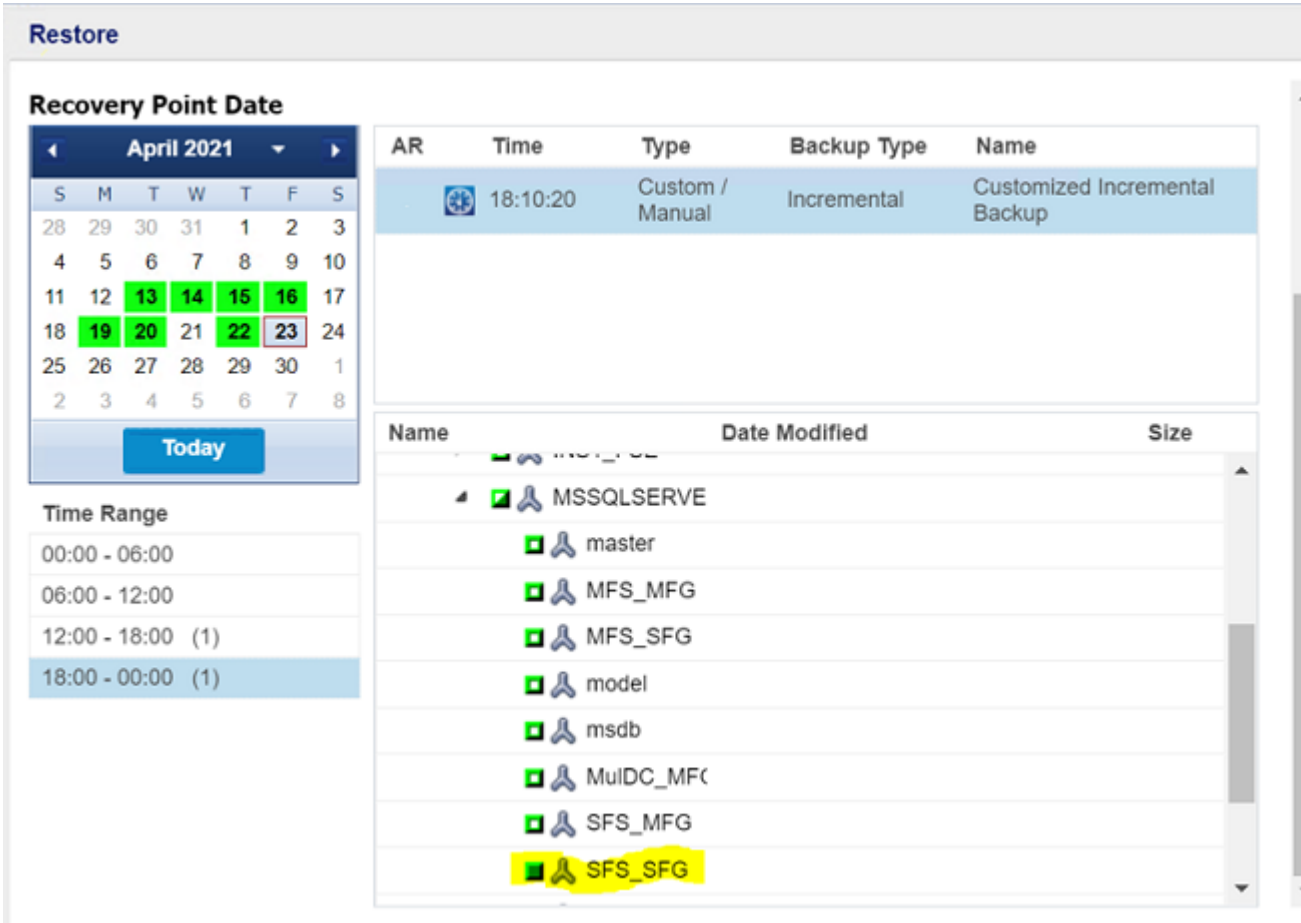
   Hinweis: Der Inhalt in geschweiften Klammern gibt Platzhalter für den Namen und die Speicherorte an, und die geschweiften Klammern sind bei der Verwendung der eigentlichen Daten nicht erforderlich.
4. Führen Sie nach Bedarf eine Wiederherstellung für eine SQL-Datenbank durch.

Wiederherstellen der SQL-Datenbank am ursprünglichen Speicherort

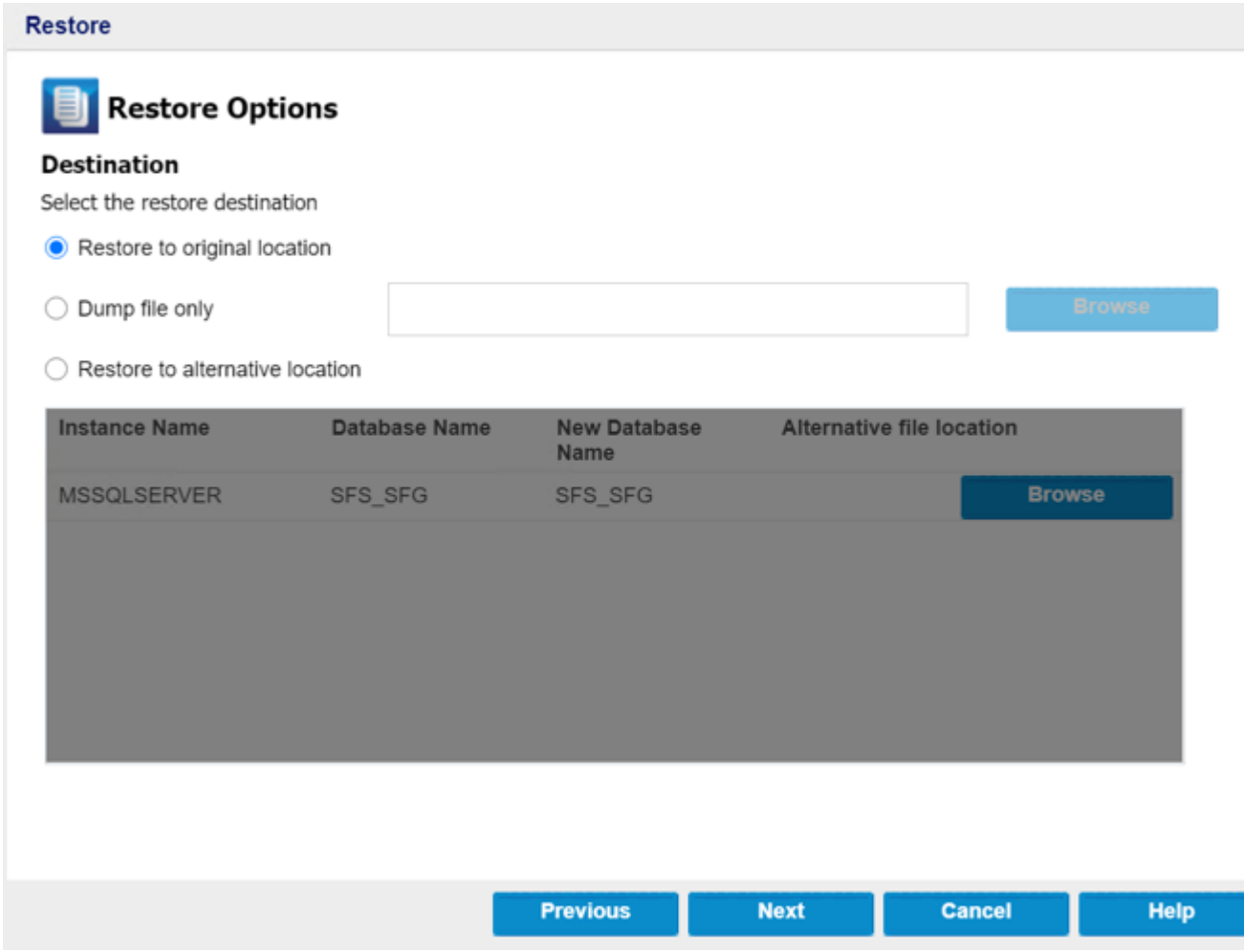
Dieser Abschnitt enthält Informationen zum Wiederherstellen der SQL-Datenbank mit aktiviertem Filestream an einem ursprünglichen Speicherort.

Befolgen Sie diese Schritte:

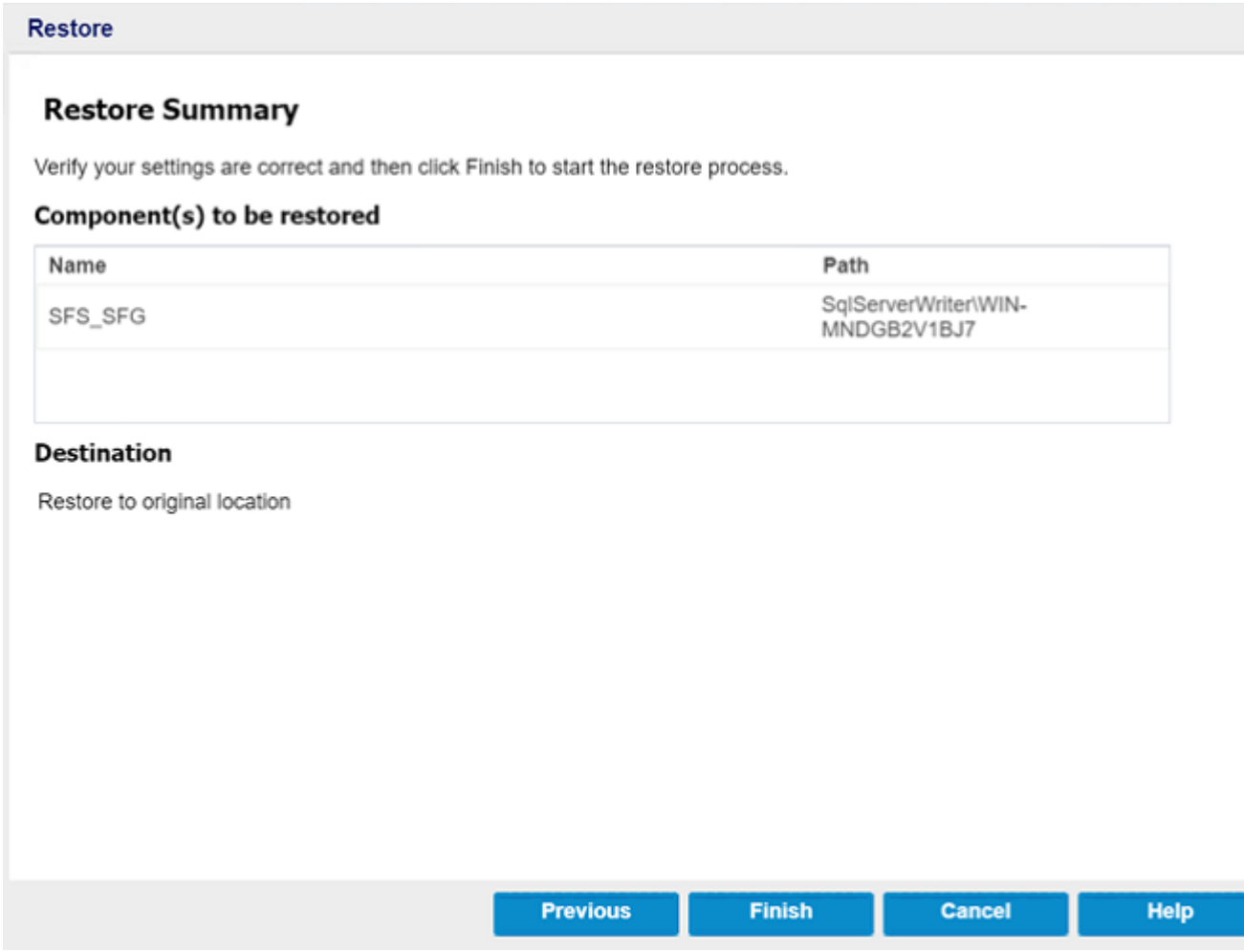
1. Wählen Sie im Fenster "Wiederherstellen" das Datum, den Zeitbereich und die SQL-Datenbank des Wiederherstellungspunkts aus, und klicken Sie auf **Weiter**.



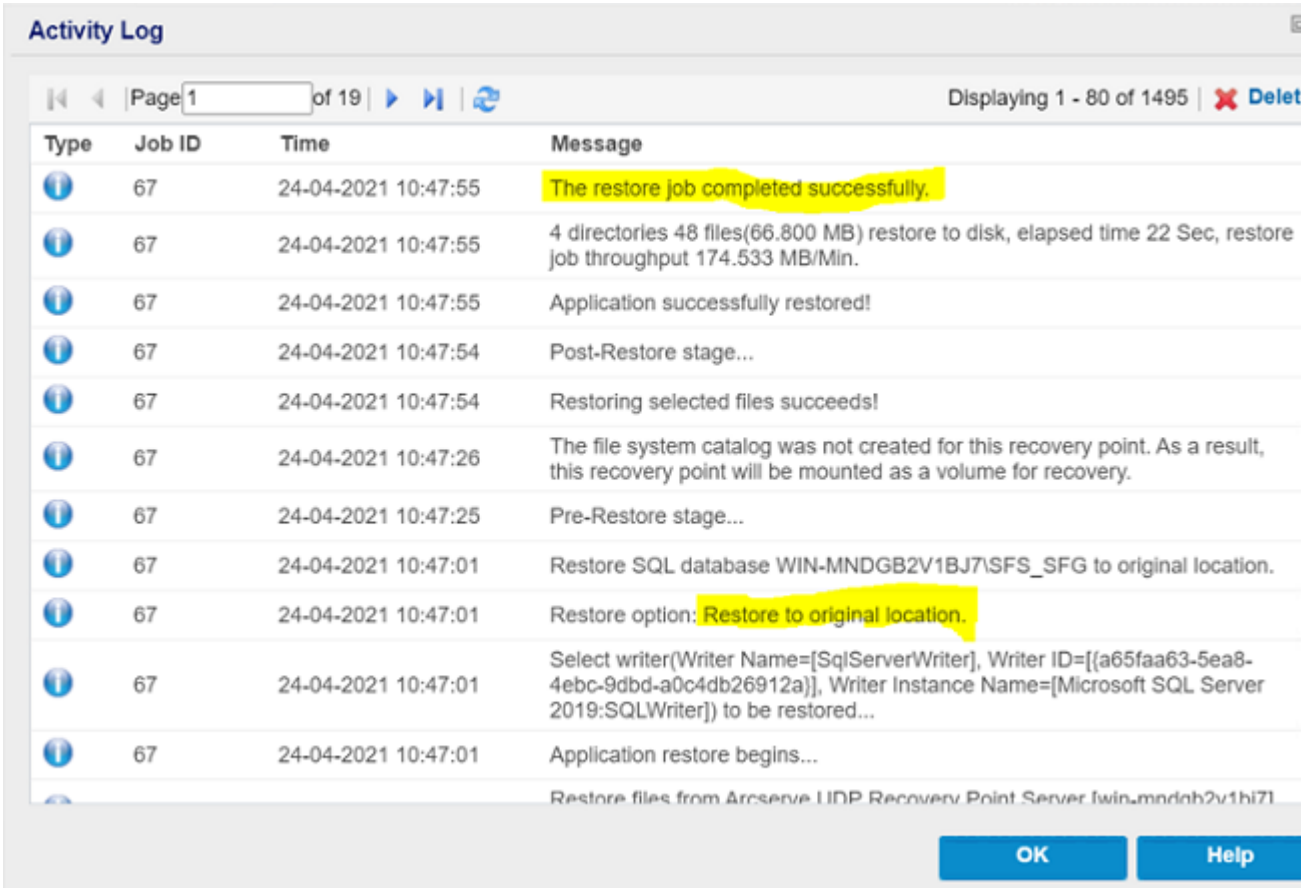
2. Wählen Sie im Bildschirm "Wiederherstellungsoptionen" unter "Ziel" die Option **Am ursprünglichen Speicherort wiederherstellen** aus, und klicken Sie dann auf die Schaltfläche **Durchsuchen**, um die Instanz auszuwählen.



3. Wählen Sie die Instanz aus, und klicken Sie dann auf **Weiter**.
4. Überprüfen Sie, ob die Einstellungen richtig sind, und klicken Sie dann auf **Fertig stellen**, um den Wiederherstellungsprozess am ursprünglichen Speicherort zu starten.



Zeigen Sie die Aktivitätsprotokolle an, um zu überprüfen, ob der Status der Wiederherstellung erfolgreich war.



Wiederherstellen der SQL-Datenbank auf einer alternativen Instanz auf demselben Server

Dieser Abschnitt enthält Informationen zum Wiederherstellen der SQL-Datenbank mit aktiviertem Filestream in einer alternativen Instanz der Filestream-fähigen Datenbank, in der sich beide Instanzen auf demselben SQL-Server befinden.

Befolgen Sie diese Schritte:

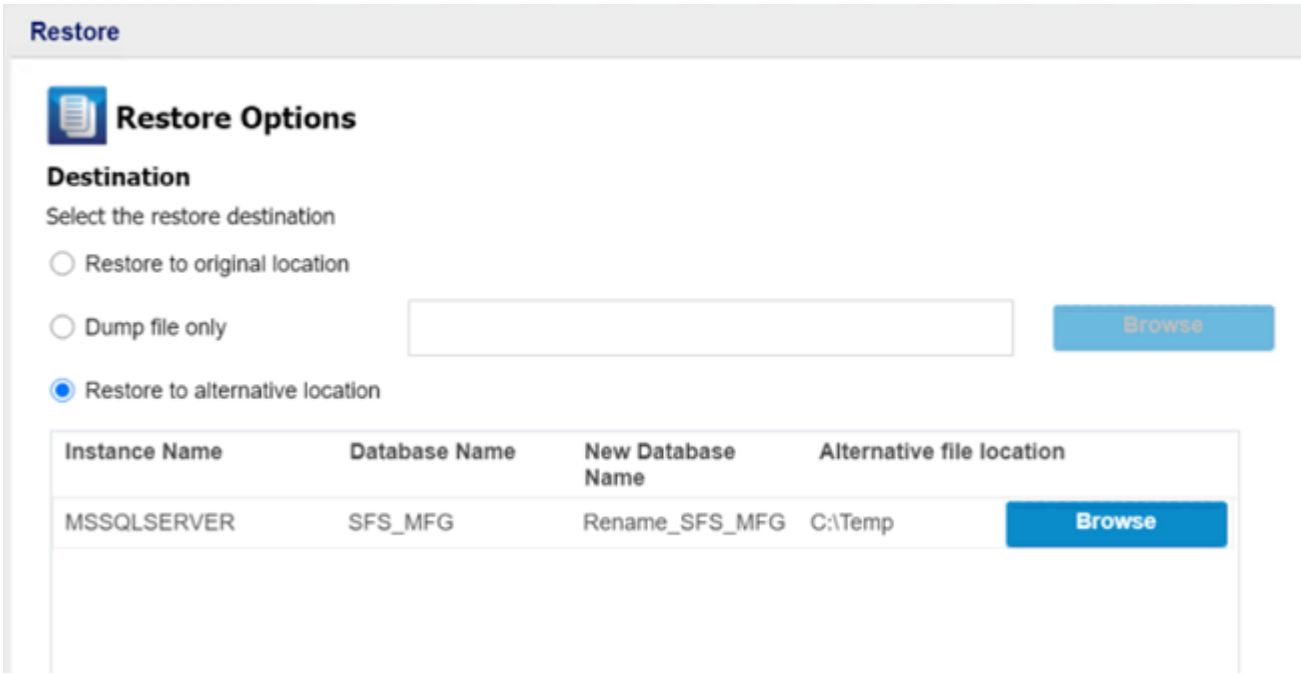
1. Um den Instanznamen zu ändern, öffnen Sie die **SqlRestore.ini**-Datei, und bearbeiten Sie dann den **RestoreInstanceName**.

   Ändern Sie beispielsweise den Instanznamen von *WIN-MNDGB2V1BJ7\MSSQLSERVER* in *WIN-MNDGB2V1BJ7\INS1_FSE*.

   Hinweis: WIN-MNDGB2V1BJ7 gibt den SQL-Server an.

Hinweis: Sie können das Feld *RestoreInstanceName* auch ohne SQL Server angeben. Zum Beispiel: *RestoreInstanceName = INS1_FSE*.

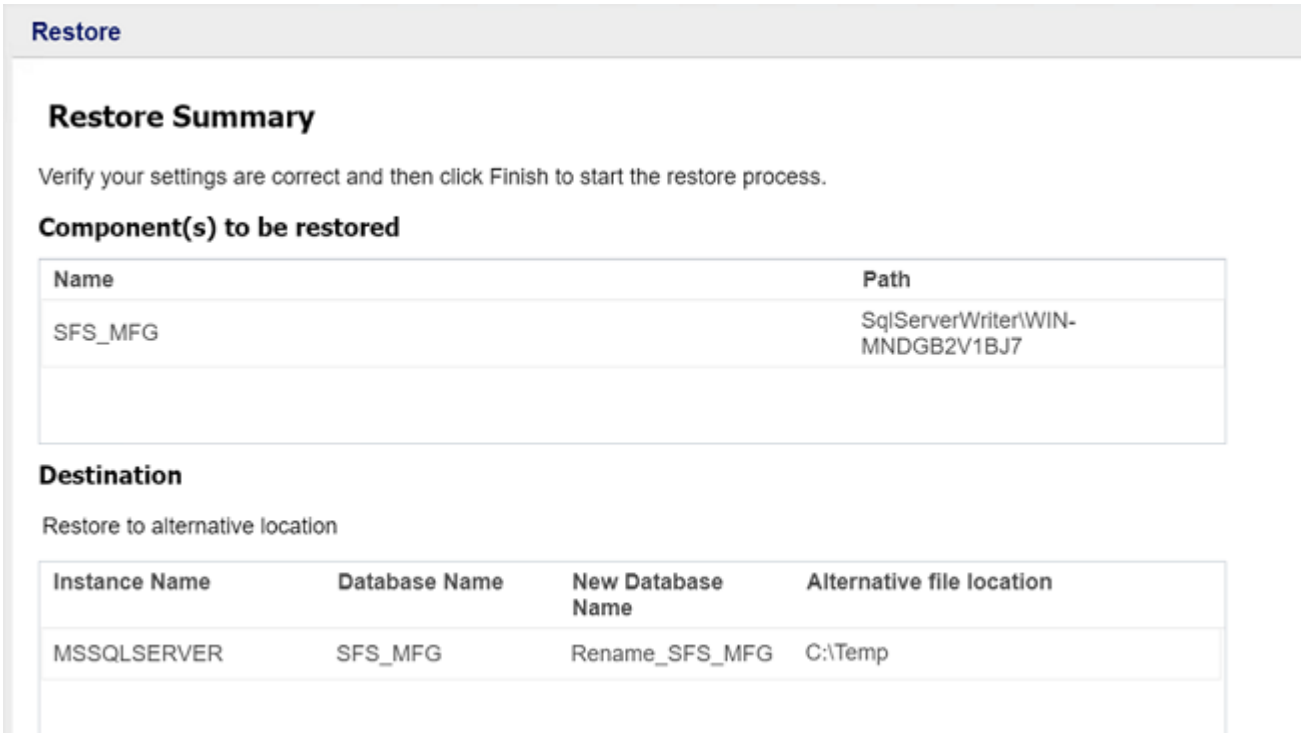
2. Wählen Sie auf dem Agent auf der Seite „Wiederherstellen“ die Datenbank aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **Weiter**.
3. Wählen Sie im Bildschirm "Wiederherstellungsoptionen" die Option **An einem alternativen Speicherort wiederherstellen** aus, und durchsuchen Sie die Instanz.



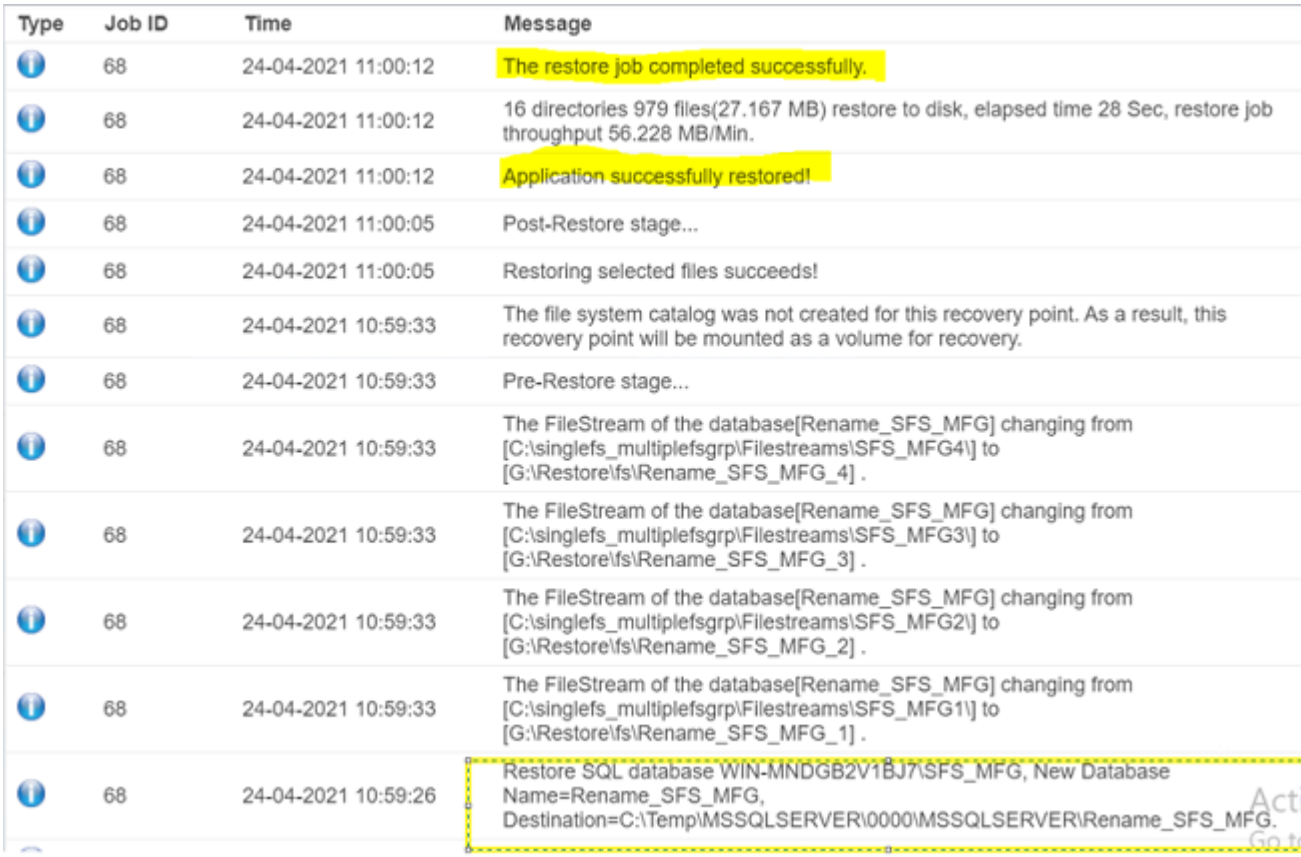
Um den Datenbanknamen umzubenennen, klicken Sie auf den Textbereich **Neuer Datenbankname**, und geben Sie den neuen Namen ein. Zum Beispiel wird *SFS_MFG* in *Rename_SFS_MFG* umbenannt.

Hinweis: Unter „Alternativer Dateispeicherort“ ist ein temporärer Ordner ausgewählt. Dieser Speicherort verarbeitet die Wiederherstellung von Dateien an dem in der Datei "SqlRestore.ini" definierten Speicherort.

4. Überprüfen Sie, ob die Einstellungen richtig sind, und klicken Sie dann auf **Fertig stellen**, um den Wiederherstellungsvorgang zu starten.

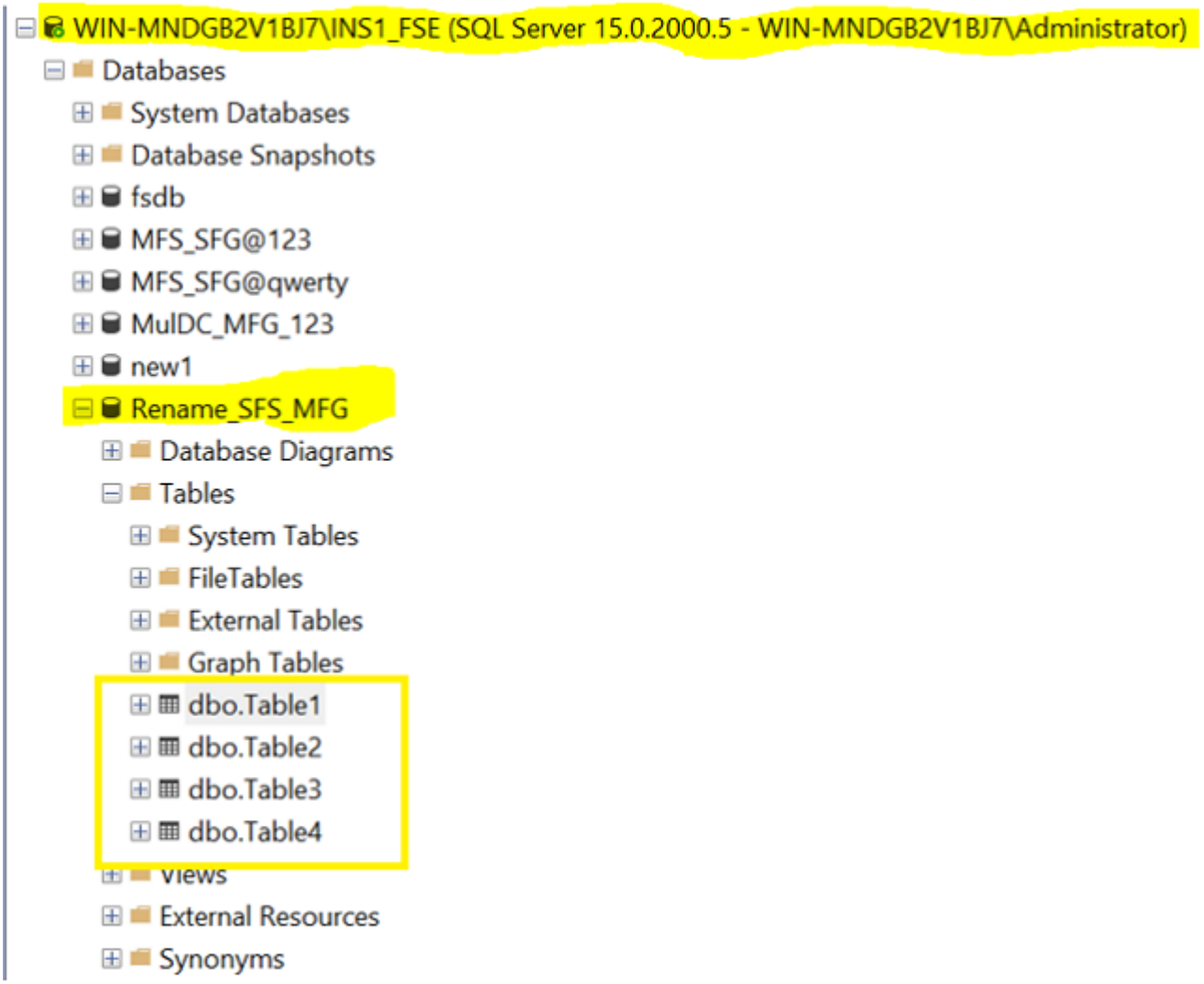


Das Aktivitätsprotokoll zeigt den Status der Wiederherstellung zusammen mit der Umbenennung der Datenbank an.

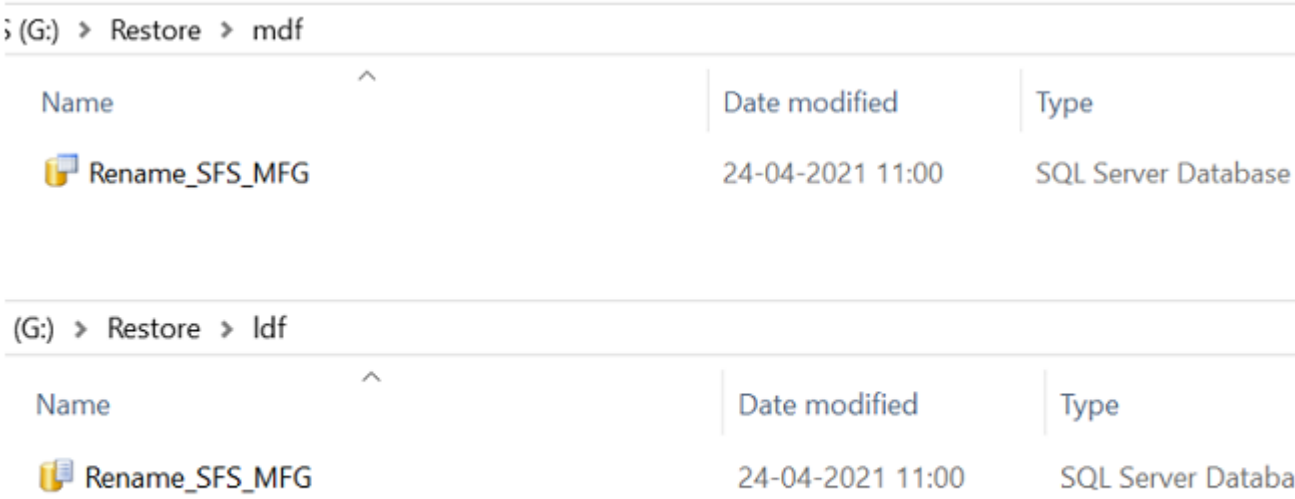


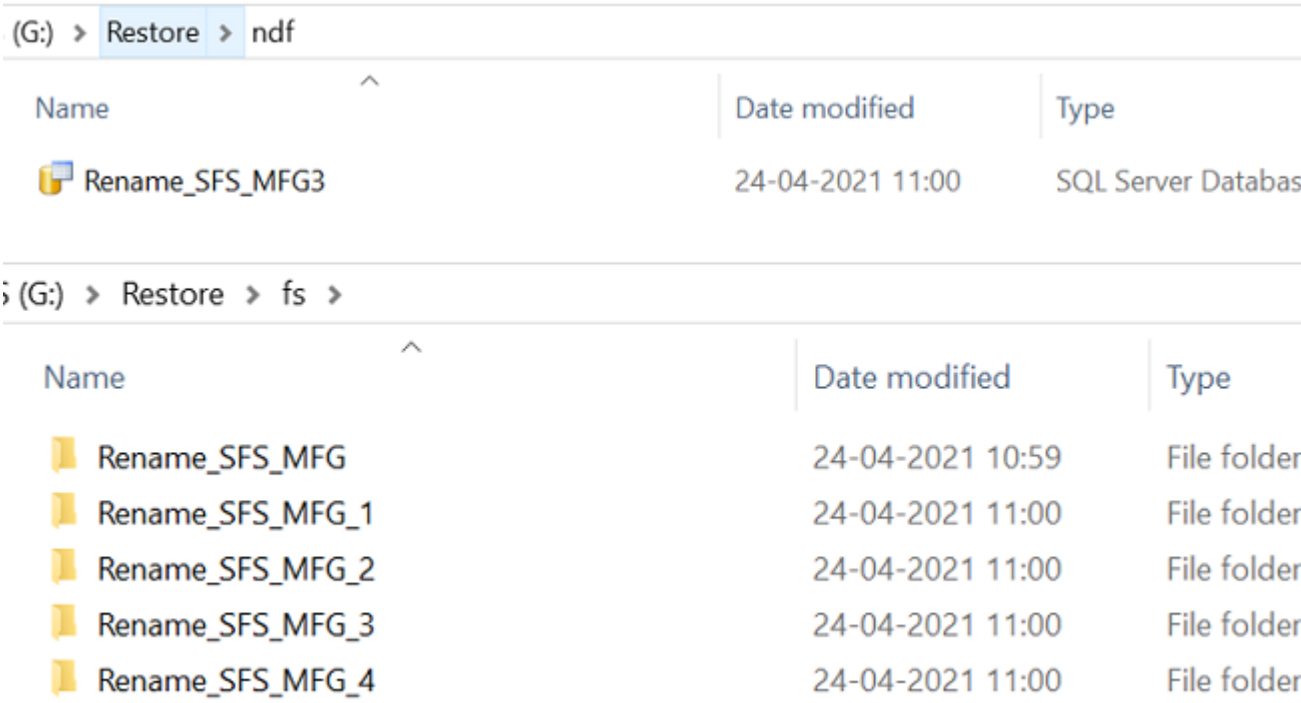
Type	Job ID	Time	Message
	68	24-04-2021 11:00:12	The restore job completed successfully.
	68	24-04-2021 11:00:12	16 directories 979 files(27.167 MB) restore to disk, elapsed time 28 Sec, restore job throughput 56.228 MB/Min.
	68	24-04-2021 11:00:12	Application successfully restored!
	68	24-04-2021 11:00:05	Post-Restore stage...
	68	24-04-2021 11:00:05	Restoring selected files succeeds!
	68	24-04-2021 10:59:33	The file system catalog was not created for this recovery point. As a result, this recovery point will be mounted as a volume for recovery.
	68	24-04-2021 10:59:33	Pre-Restore stage...
	68	24-04-2021 10:59:33	The FileStream of the database[Rename_SFS_MFG] changing from [C:\singlefs_multiplefsgrp\Filestreams\SFS_MFG4\] to [G:\Restore\fs\Rename_SFS_MFG_4] .
	68	24-04-2021 10:59:33	The FileStream of the database[Rename_SFS_MFG] changing from [C:\singlefs_multiplefsgrp\Filestreams\SFS_MFG3\] to [G:\Restore\fs\Rename_SFS_MFG_3] .
	68	24-04-2021 10:59:33	The FileStream of the database[Rename_SFS_MFG] changing from [C:\singlefs_multiplefsgrp\Filestreams\SFS_MFG2\] to [G:\Restore\fs\Rename_SFS_MFG_2] .
	68	24-04-2021 10:59:33	The FileStream of the database[Rename_SFS_MFG] changing from [C:\singlefs_multiplefsgrp\Filestreams\SFS_MFG1\] to [G:\Restore\fs\Rename_SFS_MFG_1] .
	68	24-04-2021 10:59:26	Restore SQL database WIN-MNDGB2V1BJ7\SFS_MFG, New Database Name=Rename_SFS_MFG, Destination=C:\Temp\MSSQLSERVER\0000\MSSQLSERVER\Rename_SFS_MFG.

Die Änderungen der Instanz- und Datenbanknamen werden in SQL Management Studio übernommen.



Wie in der Datei "SqlRestore.ini" definiert, werden die LDF-, MDF- und File-stream-Dateien in ihren jeweiligen Ordnern gespeichert.



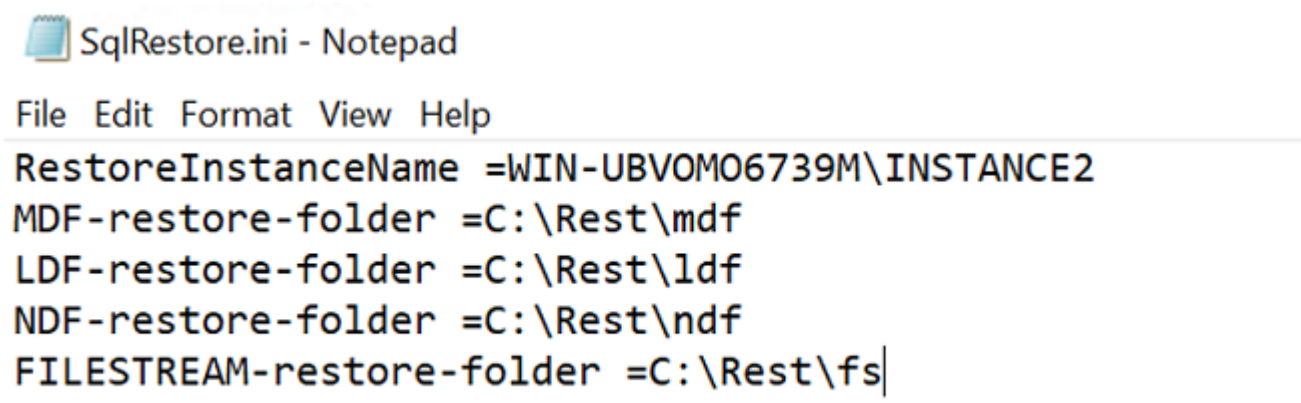


Wiederherstellen der SQL-Datenbank auf einer alternativen Instanz auf einem anderen Server

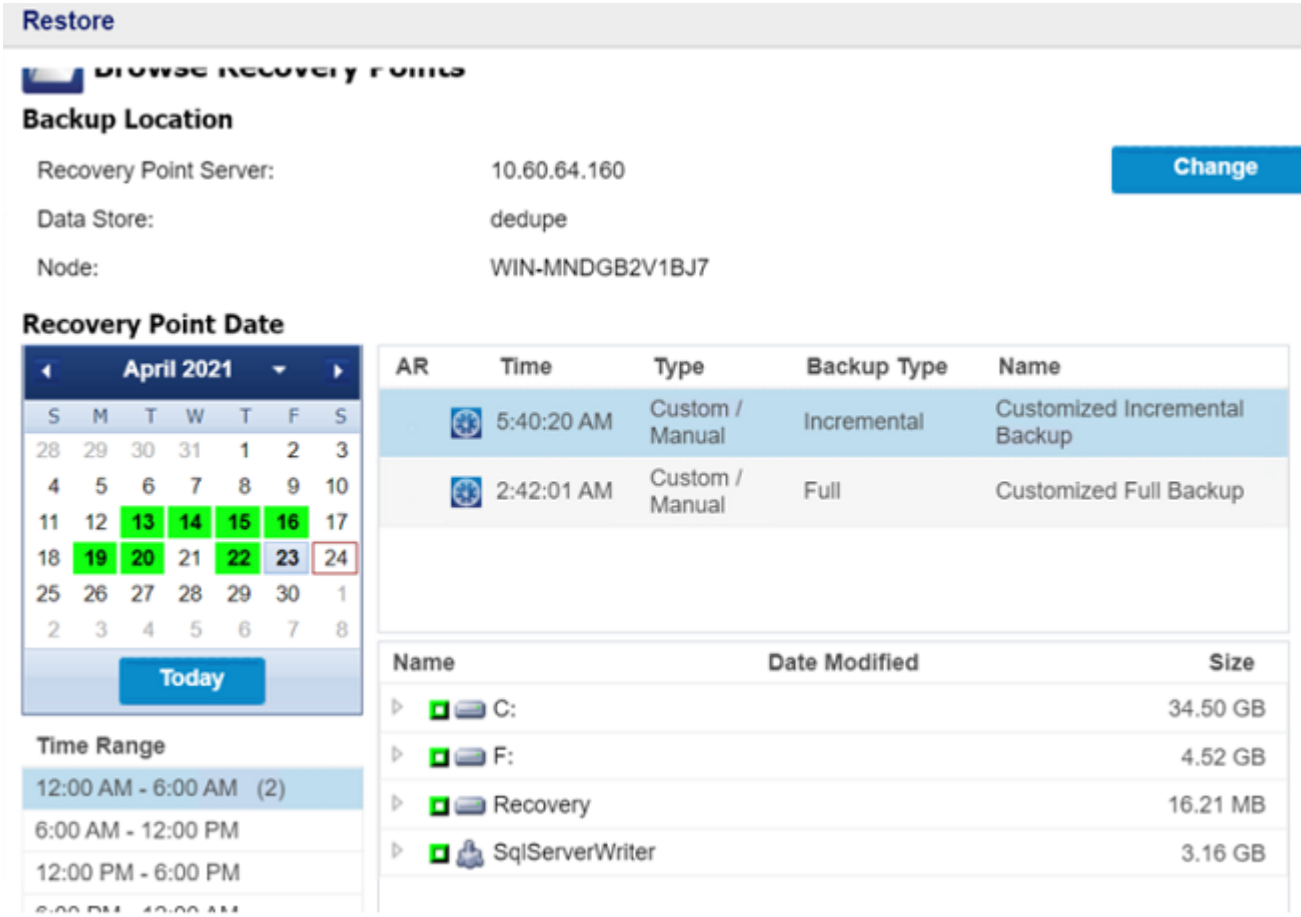
Dieser Abschnitt enthält Informationen zum Wiederherstellen der SQL-Datenbank mit aktiviertem Filestream in einer alternativen Instanz der Filestream-fähigen Datenbank, in der sich beide Instanzen auf einem anderen SQL-Server befinden. Wenn sich die Datenbank beispielsweise im Quellserver WIN-MNDGB2V1BJ7 und in der Quellinstanz MSSQLSERVER befindet, kann sie auf dem Zielserver WIN-UBVOMO6739M und der Zielinstanz INSTANCE2 wiederhergestellt werden.

Befolgen Sie diese Schritte:

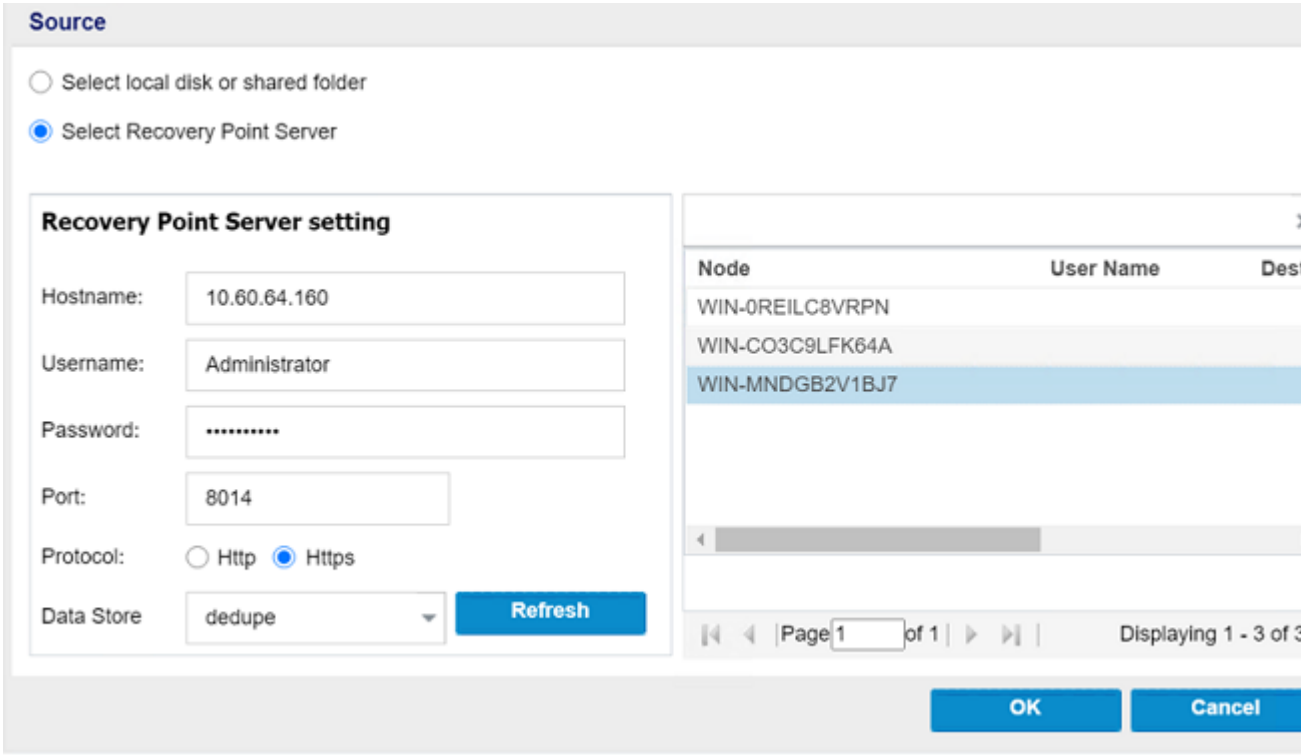
1. Um die Datenbank auf dem alternativen Server (WIN-UBVOMO6739M) und der Instanz (INSTANCE2) wiederherzustellen, ändern Sie die Datei "SqlRestore.ini".



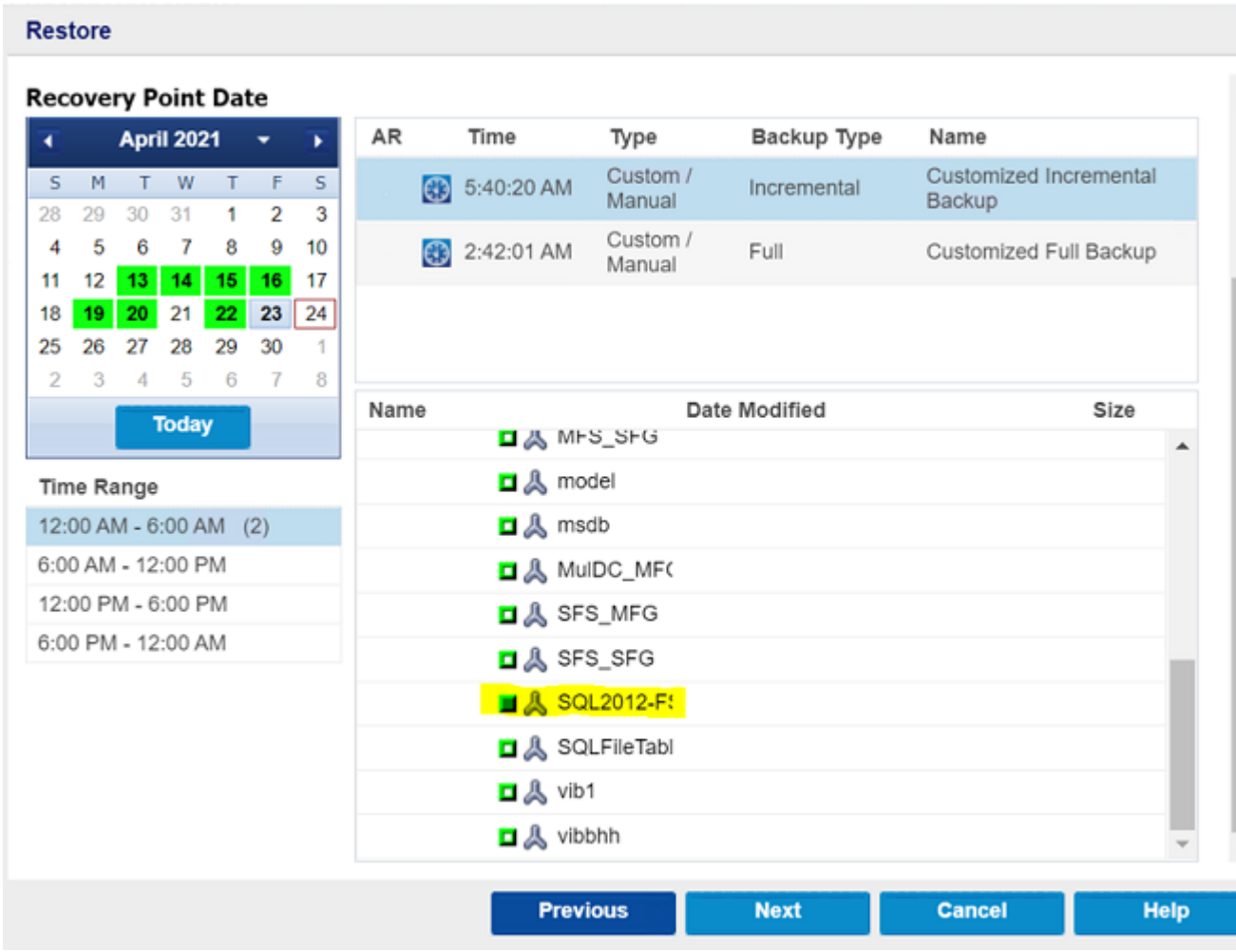
2. Um den Speicherort des Recovery Point Server (RPS) für die Wiederherstellung der Server und Instanzen auf einem alternativen Server zu ändern, klicken Sie auf die Schaltfläche **Ändern**, und geben Sie dann die neuen RPS-Details ein.



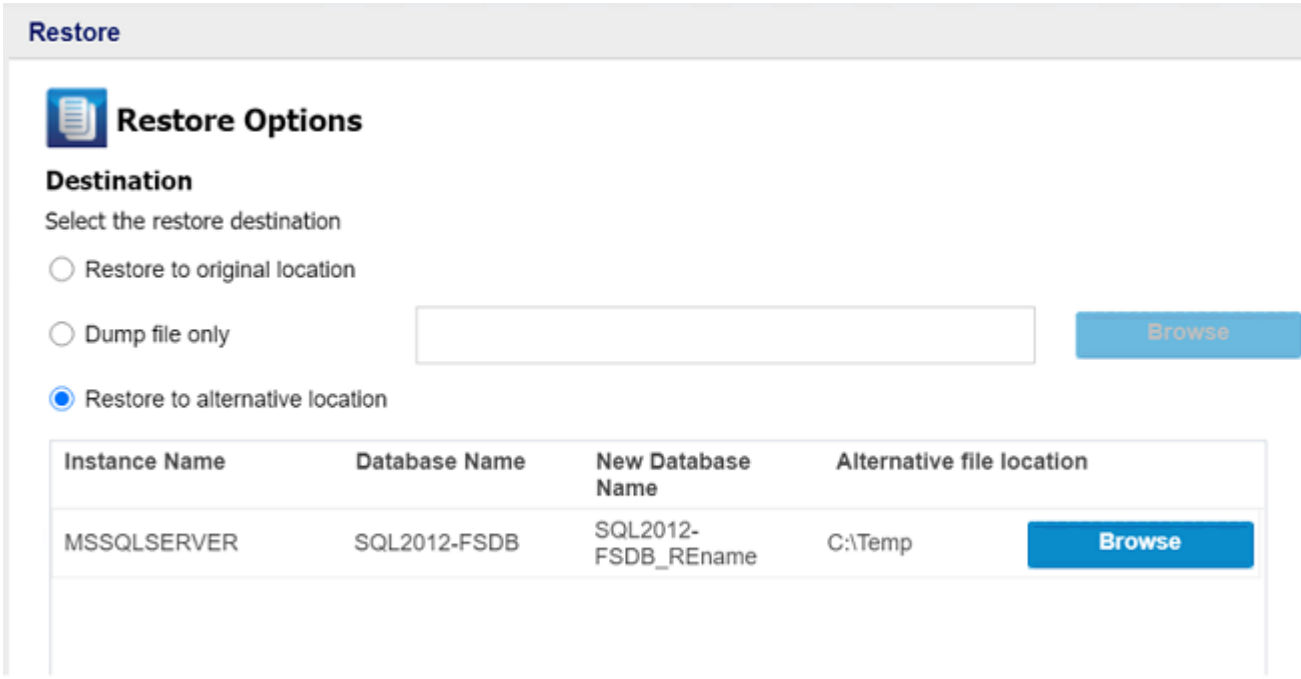
3. Um den Quell-RPS auszuwählen, klicken Sie auf **Recover Point Server auswählen**, wählen Sie den Quellserver (WIN-MNDGB2V1BJ7) aus, und klicken Sie dann auf **OK**.



4. Um auf einem alternativen Server wiederherzustellen, wählen Sie die Datenbank (SQL2012-FSDB) aus, und klicken Sie dann auf **Weiter**.



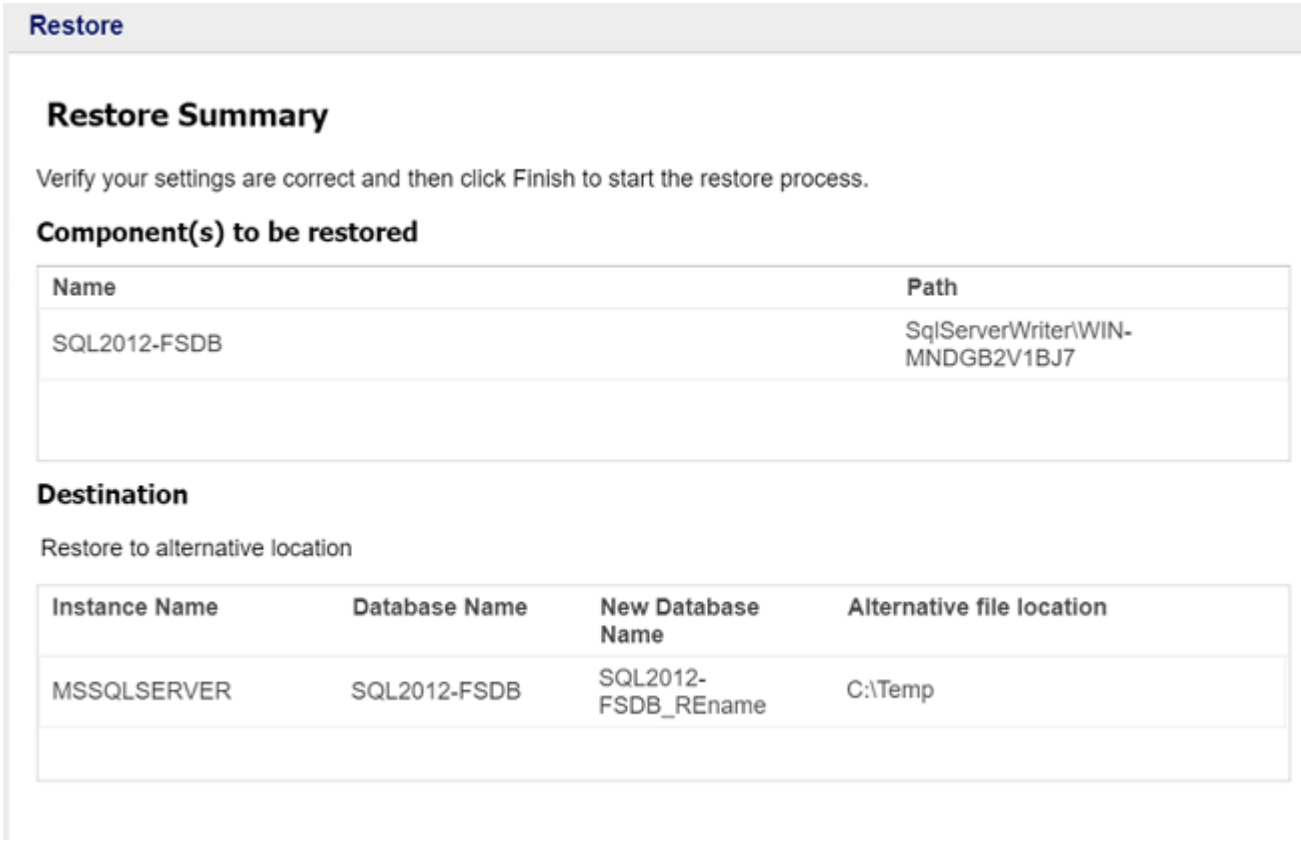
5. Wählen Sie im Bildschirm "Wiederherstellungsoptionen" die Option **An einem alternativen Speicherort wiederherstellen** aus, und durchsuchen Sie die Instanz.



Um den Datenbanknamen umzubenennen, klicken Sie auf den Textbereich **Neuer Datenbankname**, und geben Sie den neuen Namen ein. SQL2012-FSDB wird beispielsweise in "SQL2012-FSDB-REname" umbenannt.

Hinweis: Unter "Alternativer Dateispeicherort" ist ein temporärer Ordner ausgewählt. Dieser Speicherort verarbeitet die Wiederherstellung von Dateien an dem in der Datei "SqlRestore.ini" definierten Speicherort.

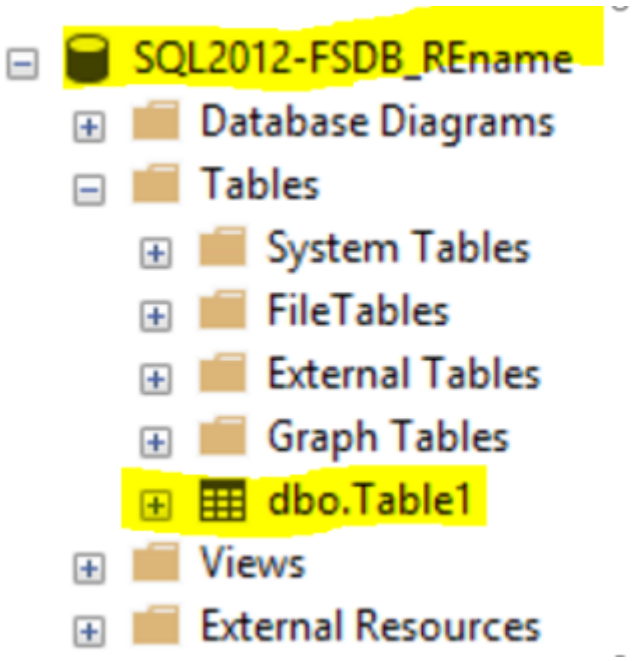
6. Überprüfen Sie, ob die Einstellungen richtig sind, und klicken Sie dann auf **Fertig stellen**, um den Wiederherstellungsvorgang zu starten.



Das Aktivitätsprotokoll zeigt den Status der Wiederherstellung zusammen mit der Umbenennung der Datenbank an.

Type	Job ID	Time	Message
	99	4/24/2021 1:12:48 AM	The restore job completed successfully.
	99	4/24/2021 1:12:48 AM	12 directories 38 files(10.250 MB) restore to disk, elapsed time 3 Sec, restore job throughput 154.348 MB/Min.
	99	4/24/2021 1:12:48 AM	Application successfully restored!
	99	4/24/2021 1:12:47 AM	Post-Restore stage...
	99	4/24/2021 1:12:47 AM	Restoring selected files succeeds!
	99	4/24/2021 1:12:39 AM	The file system catalog was not created for this recovery point. As a result, this reco point will be mounted as a volume for recovery.
	99	4/24/2021 1:12:38 AM	Pre-Restore stage...
	99	4/24/2021 1:12:38 AM	The FileStream of the database[SQL2012-FSDB_REname] changing from [F:\MSSQL15.MSSQLSERVER\MSSQL\DATA\fs3\] to [C:\Rest\fs\SQL2012-FSDB_REname_3] .
	99	4/24/2021 1:12:38 AM	The FileStream of the database[SQL2012-FSDB_REname] changing from [F:\MSSQL15.MSSQLSERVER\MSSQL\DATA\fs2\] to [C:\Rest\fs\SQL2012-FSDB_REname_2] .
	99	4/24/2021 1:12:38 AM	The FileStream of the database[SQL2012-FSDB_REname] changing from [F:\MSSQL15.MSSQLSERVER\MSSQL\DATA\fs1\] to [C:\Rest\fs\SQL2012-FSDB_REname_1] .
	99	4/24/2021 12:16:46 AM	Restore SQL database WIN-MNDGB2V1BJ7\SQL2012-FSDB, New Database Name=SQL2012-FSDB_REname, Destination=C:\Temp\MSSQLSERVER\0000\MSSQLSERVER\SQL2012-FSDB_REname.
	99	4/24/2021 12:16:46 AM	Restore option: Restore to alternate location.

Die Änderung des Datenbanknamens wird in SQL Management Studio übernommen.



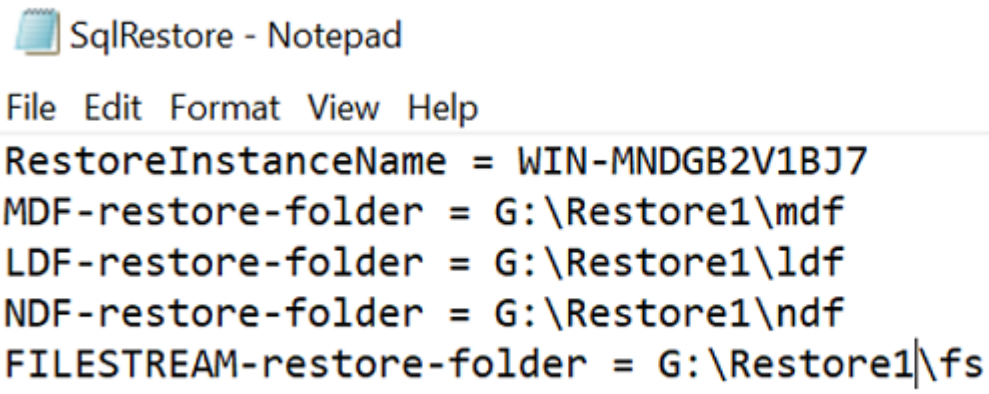
Wiederherstellen der SQL-Datenbank an einem alternativen Speicherort auf derselben Instanz

Dieser Abschnitt enthält Informationen zum Wiederherstellen der SQL-Datenbank mit aktiviertem Datei-Stream an einem alternativen Speicherort, jedoch auf derselben Instanz, während die Datenbank umbenannt wird.

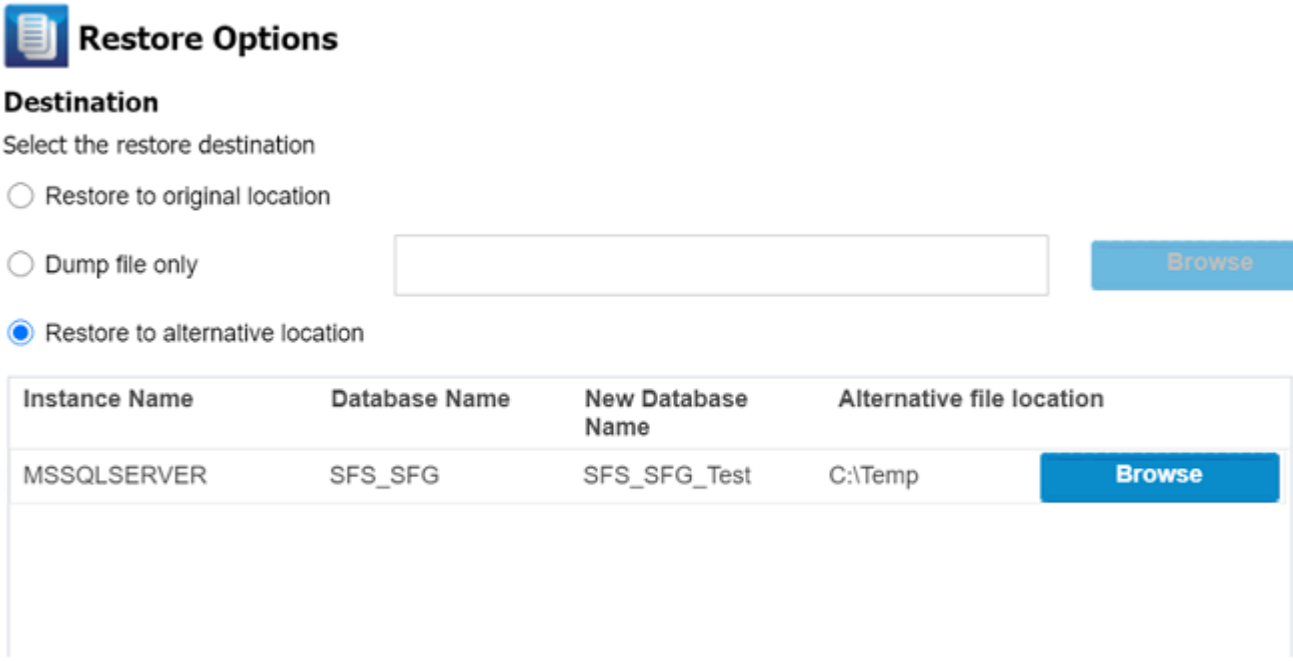
Gehen Sie wie folgt vor:

1. Um die Wiederherstellungsdatenbank an einem alternativen Speicherort zu ändern, öffnen Sie die Datei "SqlRestore.ini", und ändern Sie dann die Speicherorte der Ordner nach Bedarf.

   Ändern Sie zum Beispiel den Ordnerstandort von *C:\Singlefs_singlefsgrp\SFS_SFG1* in *G:\Restore1\fs1*.

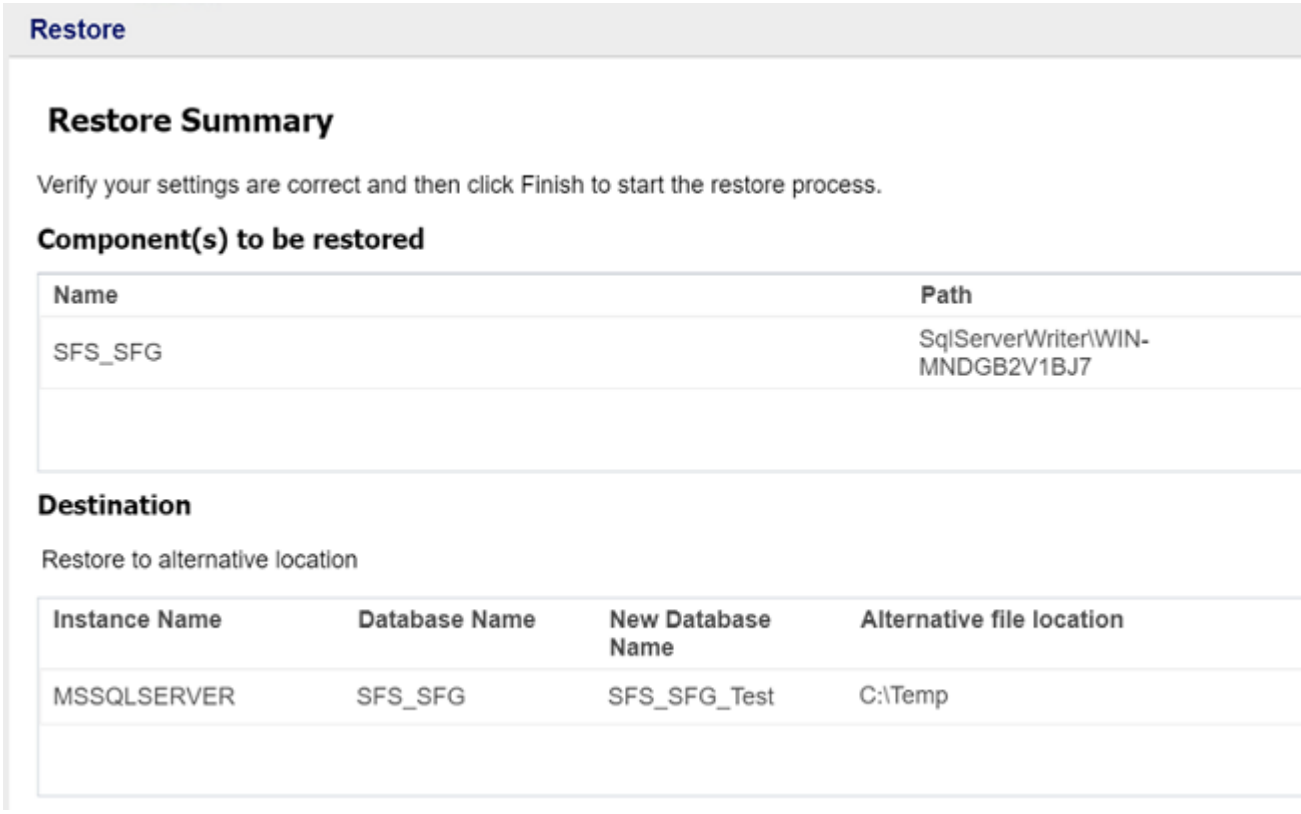
2. Wählen Sie auf dem Agent auf der Seite "Wiederherstellen" die Datenbank aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **Weiter**.
3. Wählen Sie im Bildschirm "Wiederherstellungsoptionen" die Option **An einem alternativen Speicherort wiederherstellen** aus, und durchsuchen Sie die Instanz.



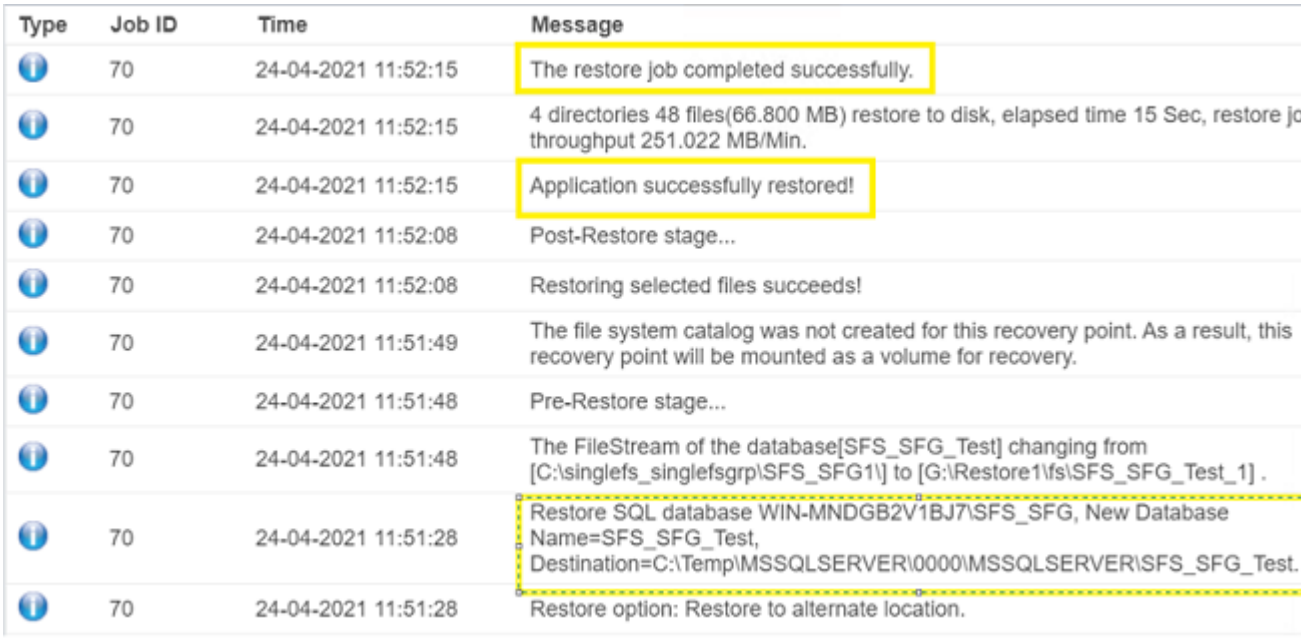
Um den Datenbanknamen umzubenennen, klicken Sie auf den Textbereich **Neuer Datenbankname**, und geben Sie den neuen Namen ein. Zum Beispiel wird *SFS_SFG* in *SFS_SFG_Test* umbenannt.

Hinweis: Unter "Alternativer Dateispeicherort" ist ein temporärer Ordner ausgewählt. Dieser Speicherort verarbeitet die Wiederherstellung von Dateien an dem in der Datei "SqlRestore.ini" definierten Speicherort.

4. Überprüfen Sie, ob die Einstellungen richtig sind, und klicken Sie dann auf **Fertig stellen**, um den Wiederherstellungsvorgang zu starten.

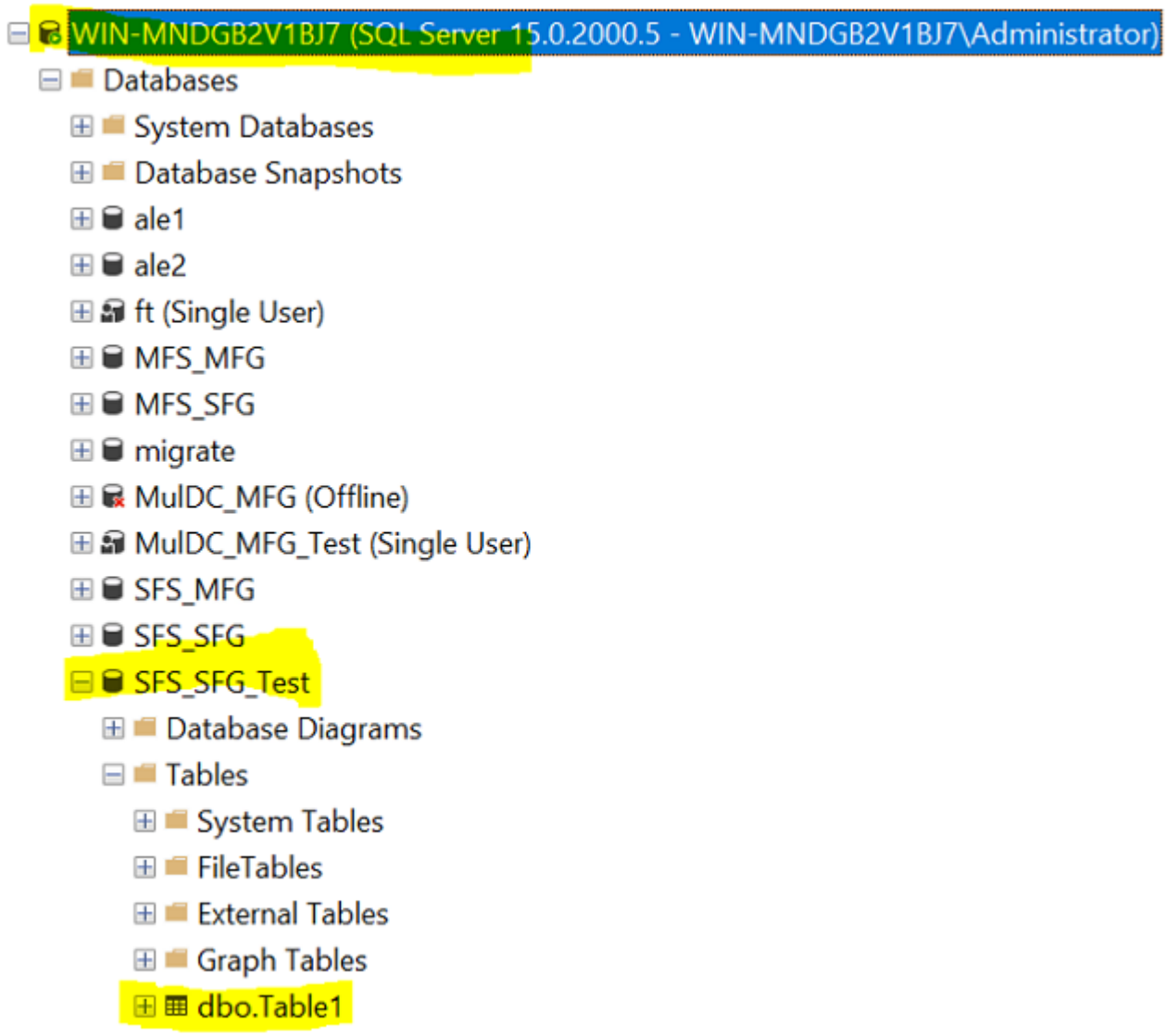


Das Aktivitätsprotokoll zeigt den Status der Wiederherstellung zusammen mit der Umbenennung der Datenbank an.



Type	Job ID	Time	Message
	70	24-04-2021 11:52:15	The restore job completed successfully.
	70	24-04-2021 11:52:15	4 directories 48 files(66.800 MB) restore to disk, elapsed time 15 Sec, restore jo throughput 251.022 MB/Min.
	70	24-04-2021 11:52:15	Application successfully restored!
	70	24-04-2021 11:52:08	Post-Restore stage...
	70	24-04-2021 11:52:08	Restoring selected files succeeds!
	70	24-04-2021 11:51:49	The file system catalog was not created for this recovery point. As a result, this recovery point will be mounted as a volume for recovery.
	70	24-04-2021 11:51:48	Pre-Restore stage...
	70	24-04-2021 11:51:48	The FileStream of the database[SFS_SFG_Test] changing from [C:\singlefs_singlefsgrp\SFS_SFG1\] to [G:\Restore1\fs\SFS_SFG_Test_1] .
	70	24-04-2021 11:51:28	Restore SQL database WIN-MNDGB2V1BJ7\SFS_SFG, New Database Name=SFS_SFG_Test, Destination=C:\Temp\MSSQLSERVER\0000\MSSQLSERVER\SFS_SFG_Test.
	70	24-04-2021 11:51:28	Restore option: Restore to alternate location.

Die Änderung des Datenbanknamens wird in SQL Management Studio übernommen.

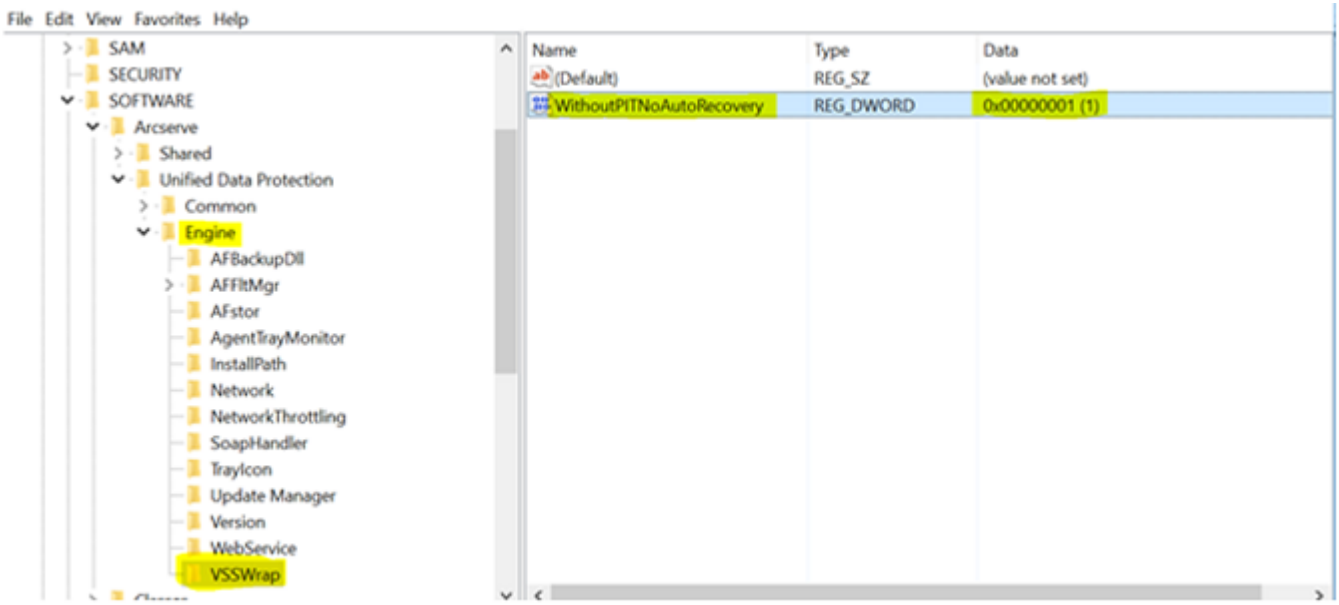


Wiederherstellen des Modus über den Registrierungsschlüssel

Dieser Abschnitt enthält Informationen zur Verwendung des Wiederherstellungsmodus mithilfe des Registrierungsschlüssels. Diese Methode stellt die für Filestream aktivierte Datenbank in der alternativen Instanz (INS1_FSE) wieder her.

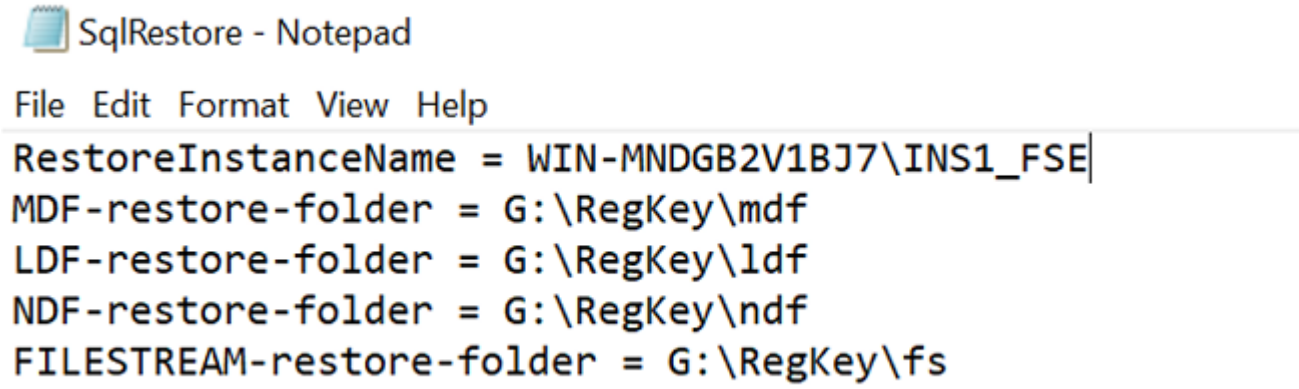
Nachdem die Sicherung erfolgreich war, fügen Sie den Registrierungsschlüssel im Ordner "VSSWrap" mit dem 32-Bit-Wert "DWORD" ohne den Namen *WITHPITNoAutoRecovery* hinzu, und legen Sie den Wert auf 1 fest.

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\VSSWrap\

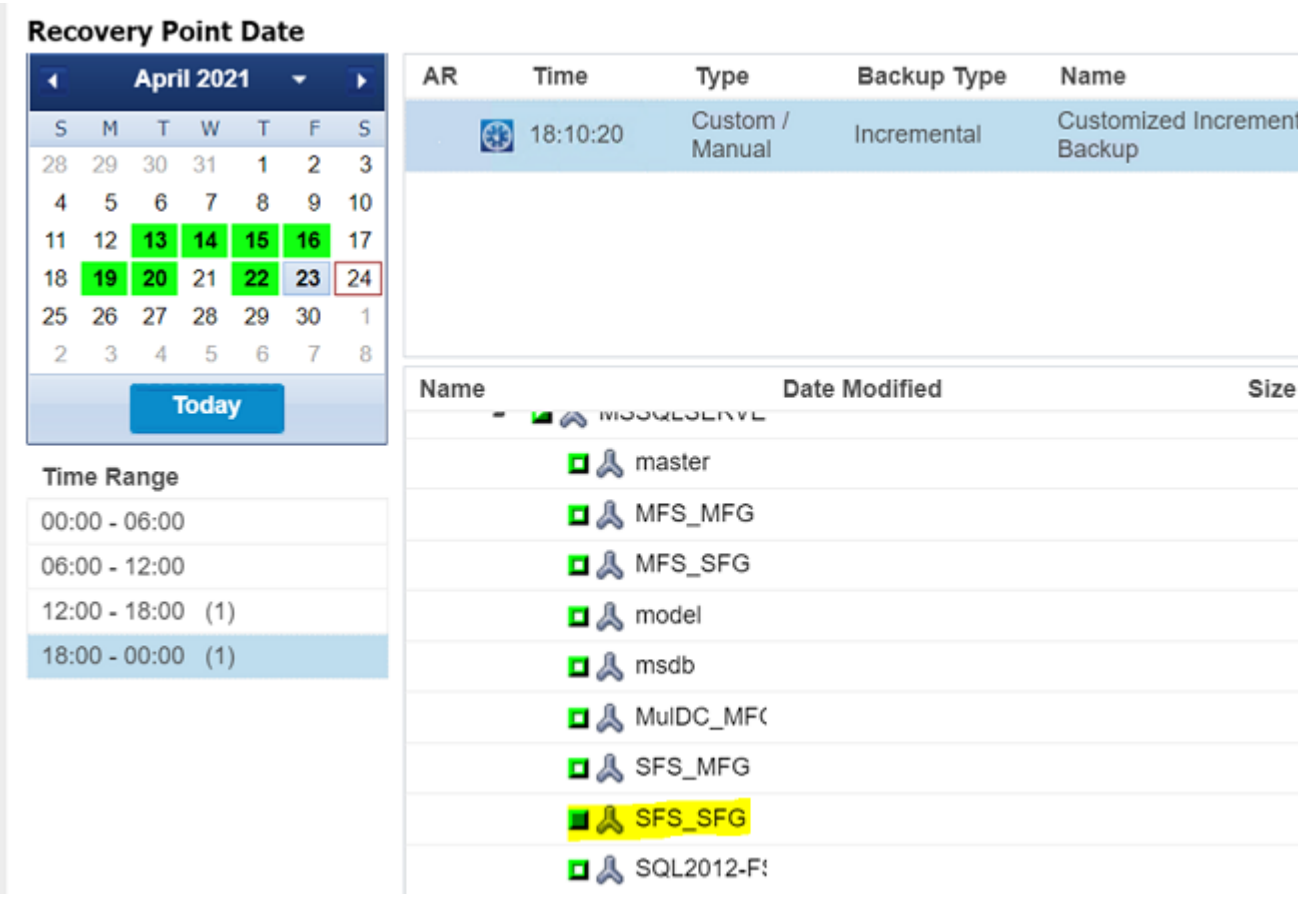


Befolgen Sie diese Schritte:

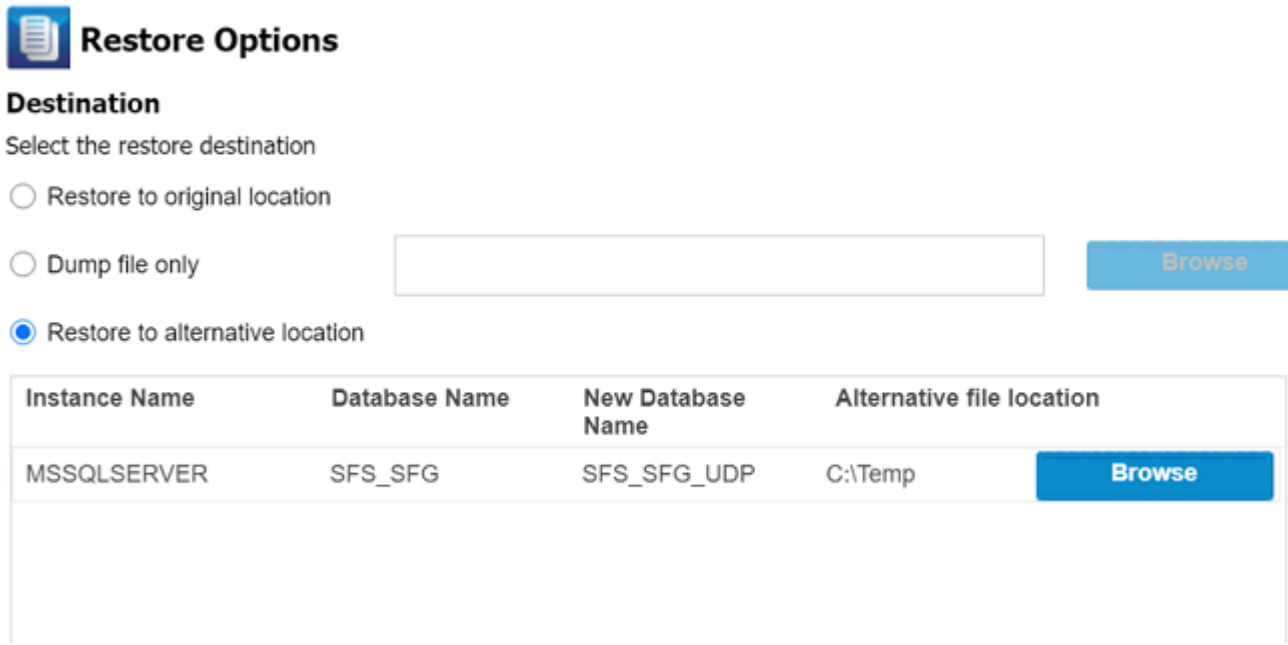
1. Um die Datenbank auf einer alternativen Instanz wiederherzustellen, öffnen Sie die Datei "SqlRestore.ini", und ändern Sie dann die Speicherorte des Ordners nach Bedarf.



2. Wählen Sie auf dem Agent auf der Seite "Wiederherstellen" die Datenbank aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **Weiter**.



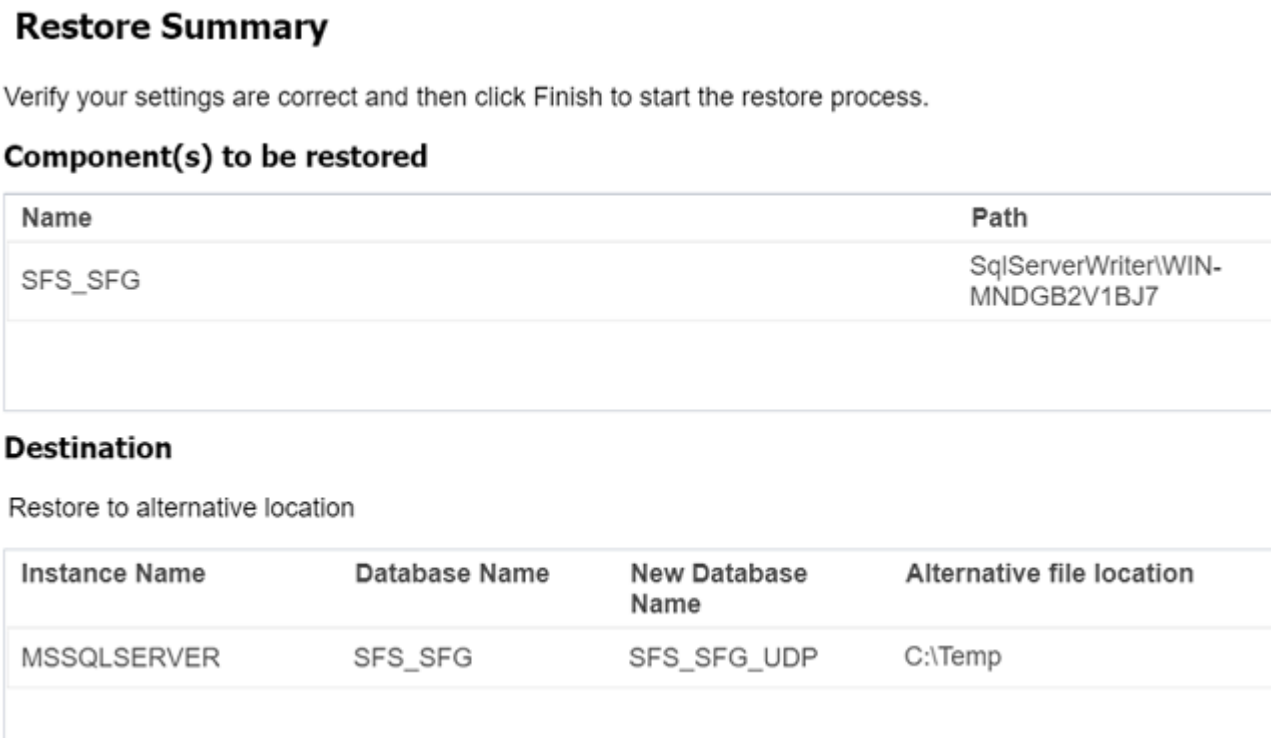
3. Wählen Sie im Bildschirm "Wiederherstellungsoptionen" die Option **An einem alternativen Speicherort wiederherstellen** aus, und durchsuchen Sie die Instanz.



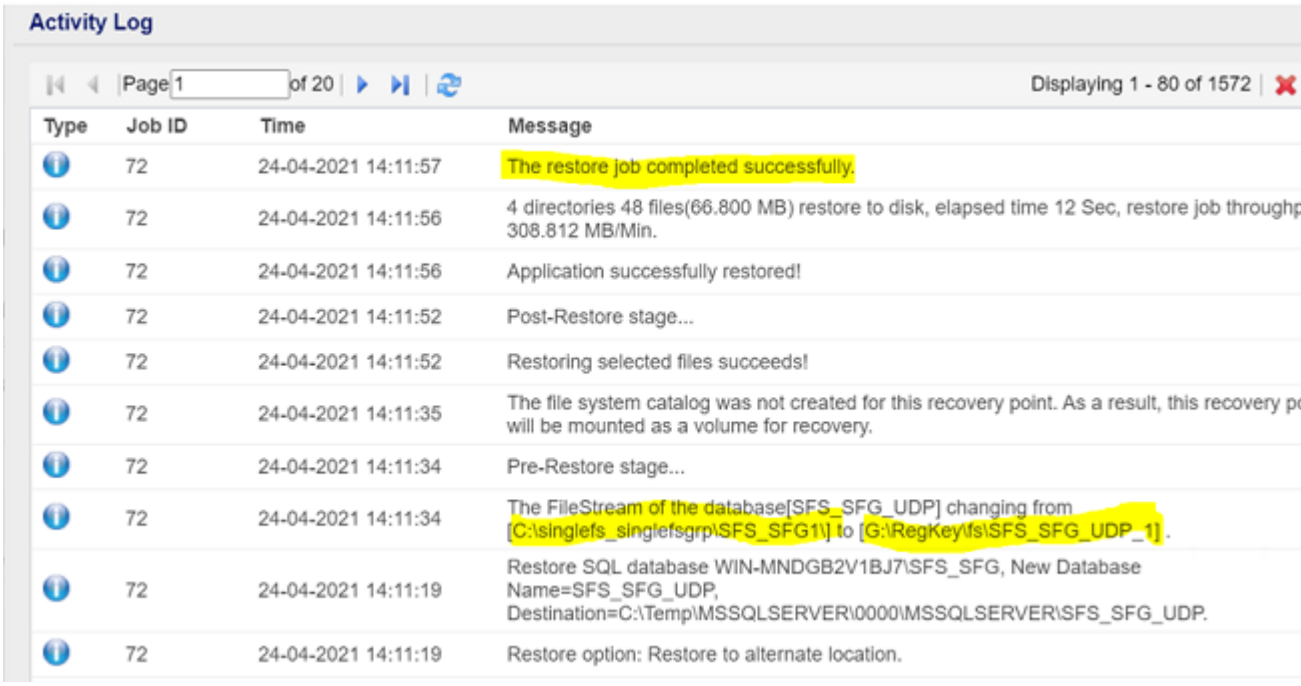
Um den Datenbanknamen umzubenennen, klicken Sie auf den Textbereich **Neuer Datenbankname**, und geben Sie den neuen Namen ein. Zum Beispiel wird *SFS_SFG* in *SFS_SFG_UDP* umbenannt.

Hinweis: Unter "Alternativer Dateispeicherort" ist ein temporärer Ordner ausgewählt. Dieser Speicherort verarbeitet die Wiederherstellung von Dateien an dem in der Datei "SqlRestore.ini" definierten Speicherort.

4. Überprüfen Sie, ob die Einstellungen richtig sind, und klicken Sie dann auf **Fertig stellen**, um den Wiederherstellungsvorgang zu starten.



Das Aktivitätsprotokoll zeigt den Status der Wiederherstellung zusammen mit der Umbenennung der Datenbank an.

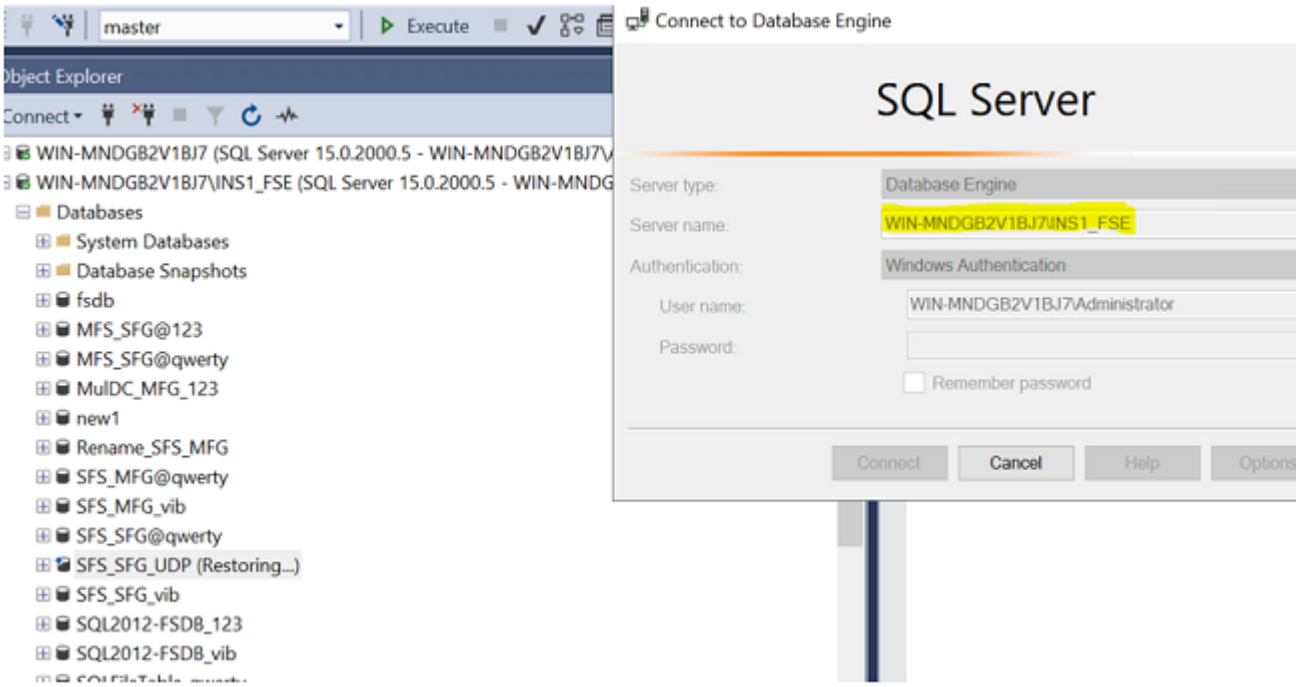


In bestimmten Fällen wird die Datenbank auch nach erfolgreichem Abschluss des Jobs als wiederhergestellt angezeigt.

Gehen Sie folgendermaßen vor, um die Datenbank aus dem Wiederherstellungsmodus zu entfernen:

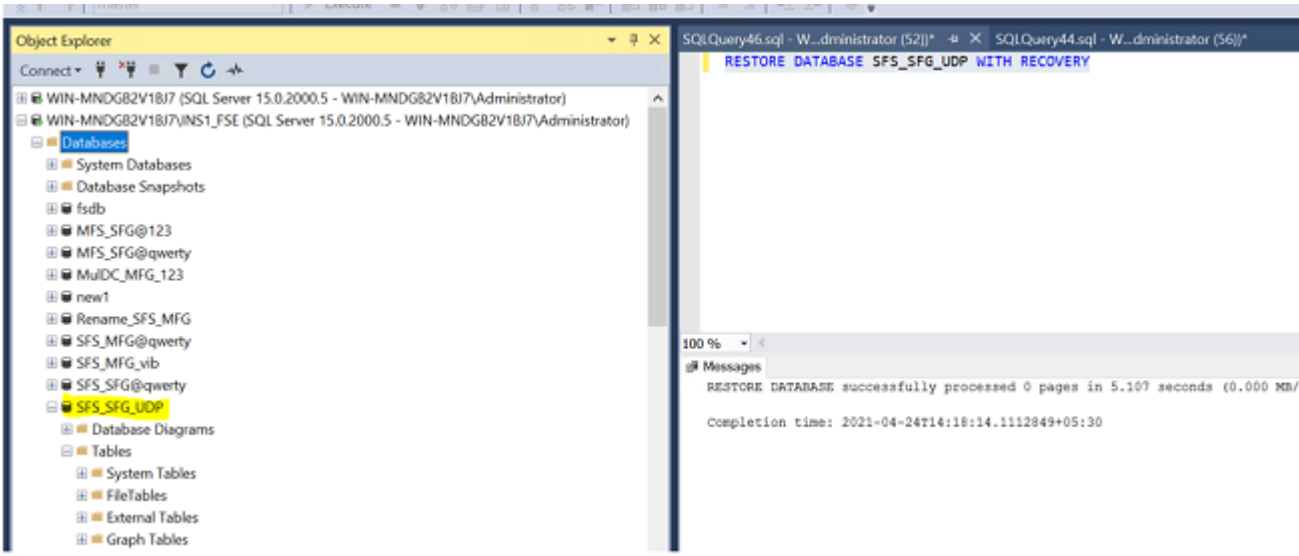
1. Klicken Sie mit der rechten Maustaste auf die Datenbank, und wählen Sie dann **Neue Abfrage** aus.

Das Fenster wird geöffnet und stellt eine Verbindung zur wiederhergestellten Instanz her.



2. Führen Sie im Abfragefenster die folgende Abfrage aus.

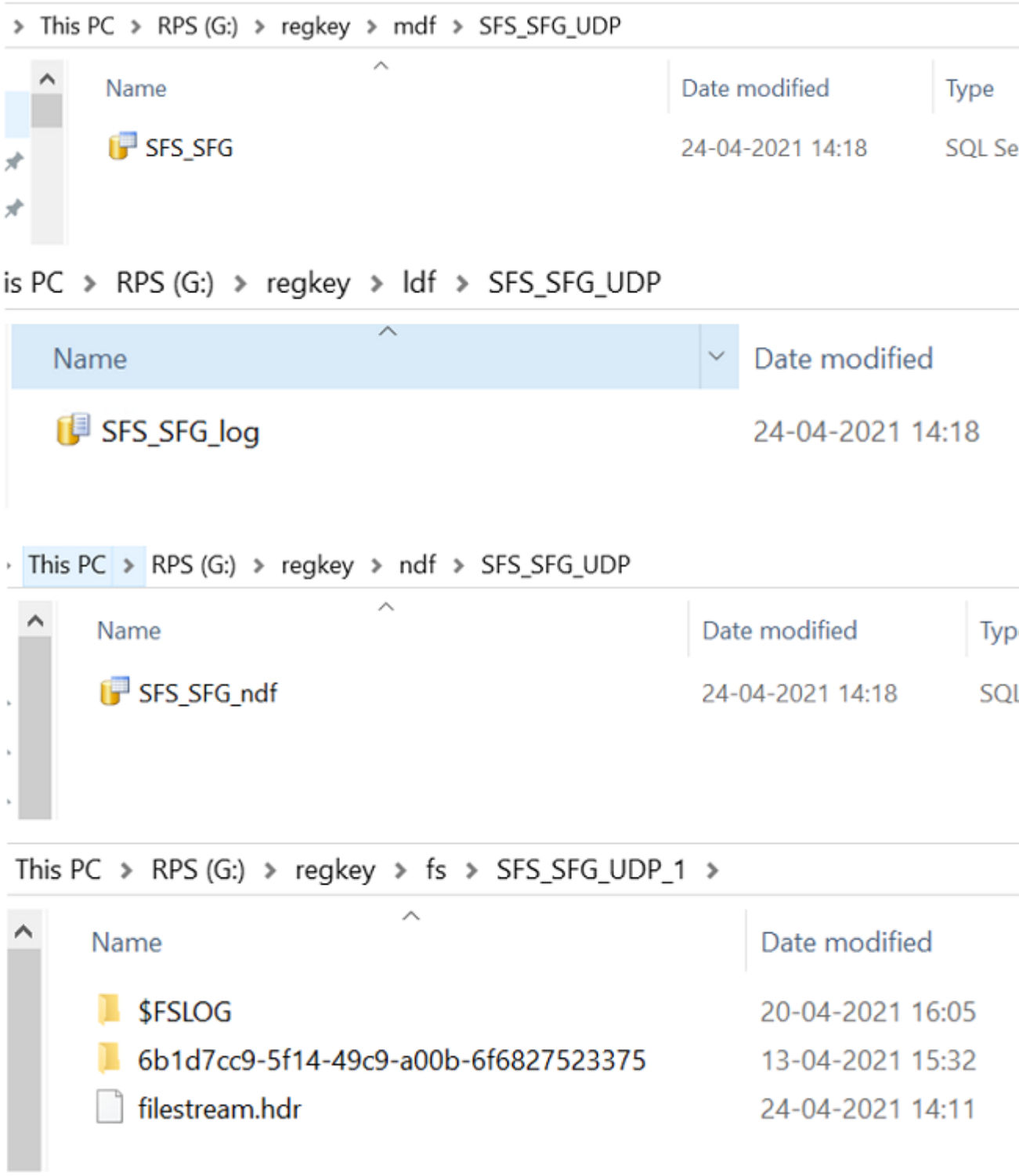
   WIEDERHERSTELLEN DER DATENBANK [DATENBANKNAME] MIT WIEDERHERSTELLUNG



Der Wiederherstellungsmodus wird aus der Datenbank entfernt.

Hinweis: Wenn das Umbenennen einer Datenbankdatei während der Verwendung der Registrierung nicht erfolgreich ist, zeigt der primäre Ordner den

neuen Namen an. Datenbankdateien wie MDF, NDF und LDF zeigen jedoch den ursprünglichen Datenbanknamen an.



Verwenden des Hilfsprogramms zur spezifischen Wiederherstellung von Exchange-Objekten (GRT)

Dieser Abschnitt enthält die folgenden Informationen über das Hilfsprogramm zur spezifischen Wiederherstellung von Exchange-Objekten:

Einführung

Überprüfen der Voraussetzungen und Hinweise

Wiederherstellen von Microsoft Exchange-Daten mit dem Hilfsprogramm zur spezifischen Wiederherstellung von Exchange-Objekten (GRT)

Einführung

Das Hilfsprogramm zur spezifischen Wiederherstellung von Exchange-Objekten wird sowohl für E-Mail-als auch Nicht-E-Mail-Objekte in Microsoft Exchange verwendet. Das Hilfsprogramm beinhaltet die Möglichkeit zum Hinzufügen von Elementen wie E-Mails von Offline-Datenbanken (*EDB) und Protokolldateien bis zu den ursprünglichen Live-Exchange-Datenbanken sowie zur spezifischen Datenextraktion auf PST-Dateien (Personal Storage Files).

Das Hilfsprogramm bietet die folgenden wesentlichen Vorteile:

- Unterstützt Nicht-E-Mail-Objekte (z. B. Kalender, Kontakte, Aufgaben) und öffentliche Ordner.
- Ggf. auch für Datenbankdateien geeignet. Protokolle sind nicht obligatorisch, sorgen aber dafür, dass neuere Daten für die Wiederherstellung zur Verfügung stehen.
- Es muss keinen Katalog zu generieren, und stellt die E-Mails direkt vom geladenen Wiederherstellungspunkt wieder her.
- Elemente auf Postfachebene aus Datenbanken oder Benutzerpostfächern beliebiger Größe sind innerhalb kürzester Zeit wiederhergestellt.
- Unterstützt die Befehlszeilenoptionen zur Verarbeitung mehrerer Datenbanken.

Hinweis: Weitere Informationen zu den unterstützten Spezifikationen, Funktionen und anderen Merkmalen finden Sie im Exchange-Benutzerhandbuch zur spezifischen Wiederherstellung (esr.pdf).

Überprüfen der Voraussetzungen und Hinweise

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Wiederherstellung ausführen:

- Das Hilfsprogramm zur spezifischen Wiederherstellung von Exchange-Objekten ist unter folgendem Pfad verfügbar:

  Das Tool wird mit Arcserve UDP Agent im folgenden Verzeichnis installiert:

  ```
  X:\Programme\Arcserve\Unified Data Protection\Engine\Exchange GRT
  ```

  Hinweis: Das Tool wird zusammen mit Arcserve UDP Agent installiert.

- Der Wiederherstellungsjob wird über den Exchange-Rechner oder den HBBU-Proxy-Rechner ausgeführt.

  Hinweis: Wenn der Wiederherstellungsjob auf einem anderen Rechner ausgeführt werden soll, suchen Sie im Sicherungsziel nach dem gewünschten Wiederherstellungspunkt.

- Der Datenbankname, Servername, Pfad zur Datenbank (.edb) und die Protokolldateien des Benutzers werden zur Durchführung des Wiederherstellungsjobs identifiziert.

  Verwenden Sie zur Identifizierung die Exchange-Verwaltungskonsole (Exchange Management Console, EMC), die Exchange-Systemsteuerung (Exchange Control Panel, ECP) oder die Exchange-Verwaltungsshell (Exchange Management Shell).

  Beispiel:

  ```
  Get-Mailbox -identity "username" | fl Database
  ```

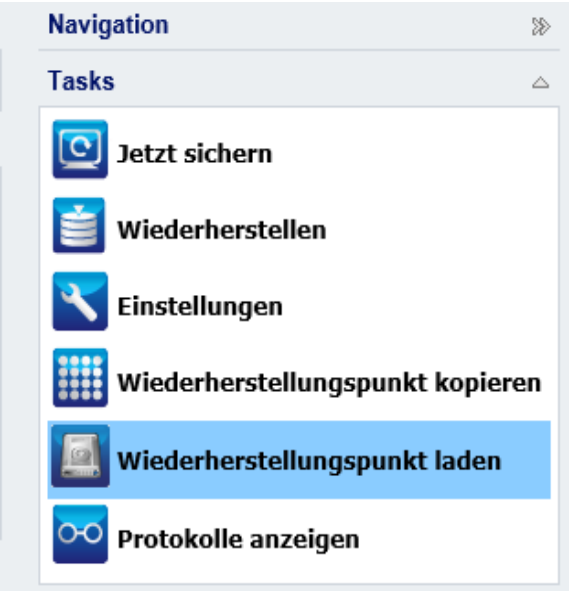
  ```
  Get-MailboxDatabase -identity "Databasename" | fl Name, Server, EdbFilePath,LogFolderPath
  ```

Wiederherstellen von Microsoft Exchange-Daten mit dem Hilfsprogramm zur spezifischen Wiederherstellung von Exchange-Objekten (GRT)

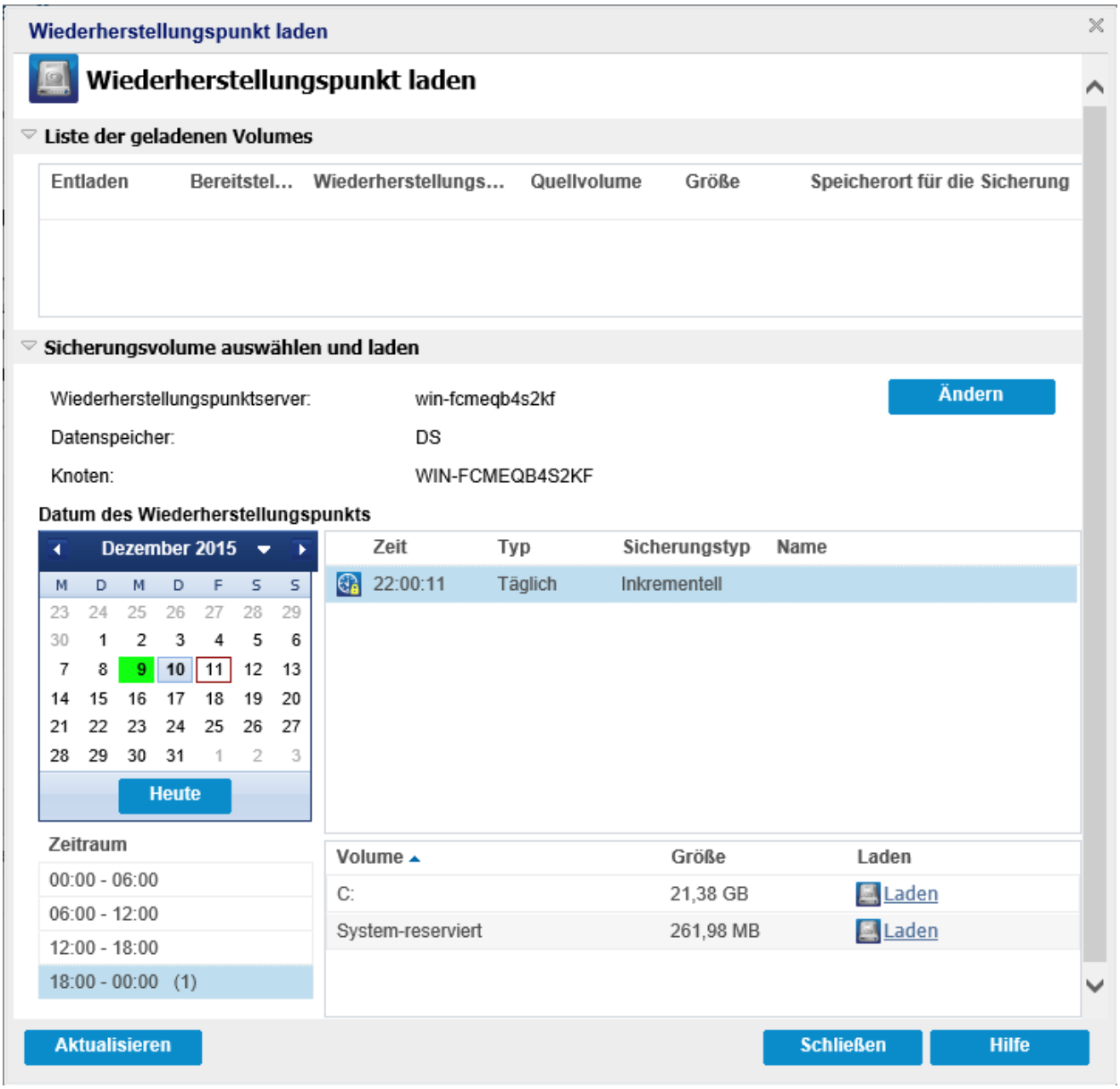
Bevor Sie beginnen, überprüfen Sie die Voraussetzungen und Hinweise.

Führen Sie die folgenden Schritte aus, um Microsoft Exchange-Mailbox-Objekte mit dem Hilfsprogramm für die spezifische Wiederherstellung von Exchange-Objekten wiederherzustellen:

1. Wählen Sie in der Arcserve UDP Agent-Konsole den Task Wiederherstellungspunkt laden (empfohlen) aus, oder stellen Sie die Exchange-Datenbank auf dem lokalen Laufwerk wieder her. Das Dialogfeld Wiederherstellungspunkt laden wird geöffnet.

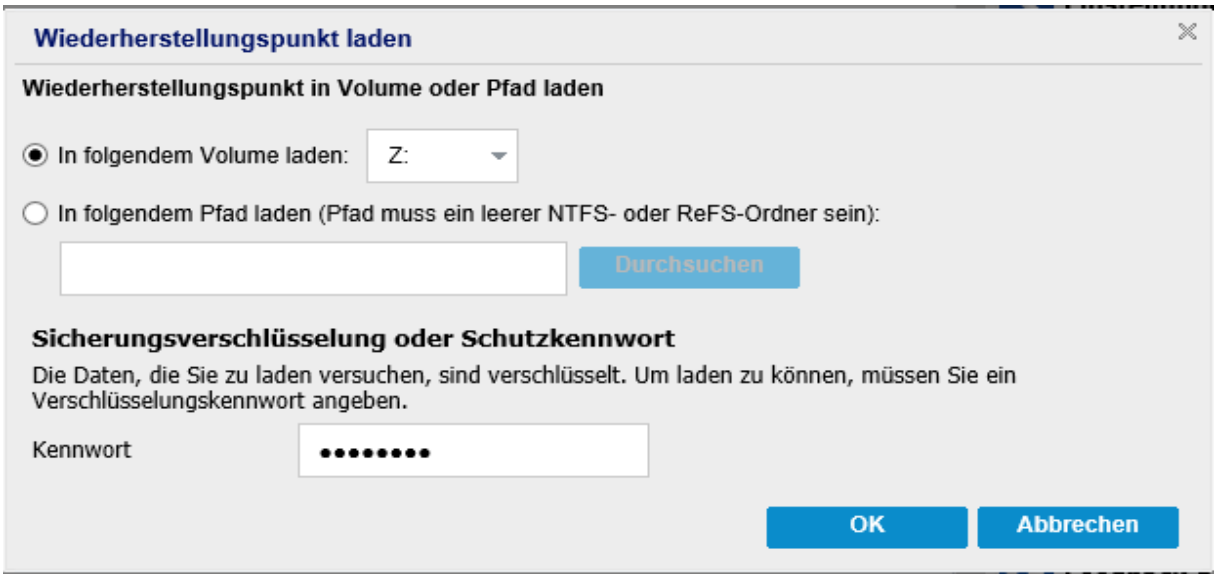


2. Wählen Sie das Datum des Wiederherstellungspunkts aus, und klicken Sie für die Volumes, die Exchange-Datenbanken und Protokolle enthalten auf **Laden**.



Hinweis: Ist der Server, der den Job ausführt, nicht der Exchange-Server oder HBBU-Proxy, klicken Sie auf **Ändern**, um den entsprechenden Recovery Point Server, Datenspeicher und Exchange-Server auszuwählen.

3. Wählen Sie den Laufwerksbuchstaben aus, um das Volume zu laden, und klicken Sie auf **OK**.



4. Starten Sie das Hilfsprogramm zur spezifischen Wiederherstellung von Exchange-Objekten unter einem der folgenden Pfade:

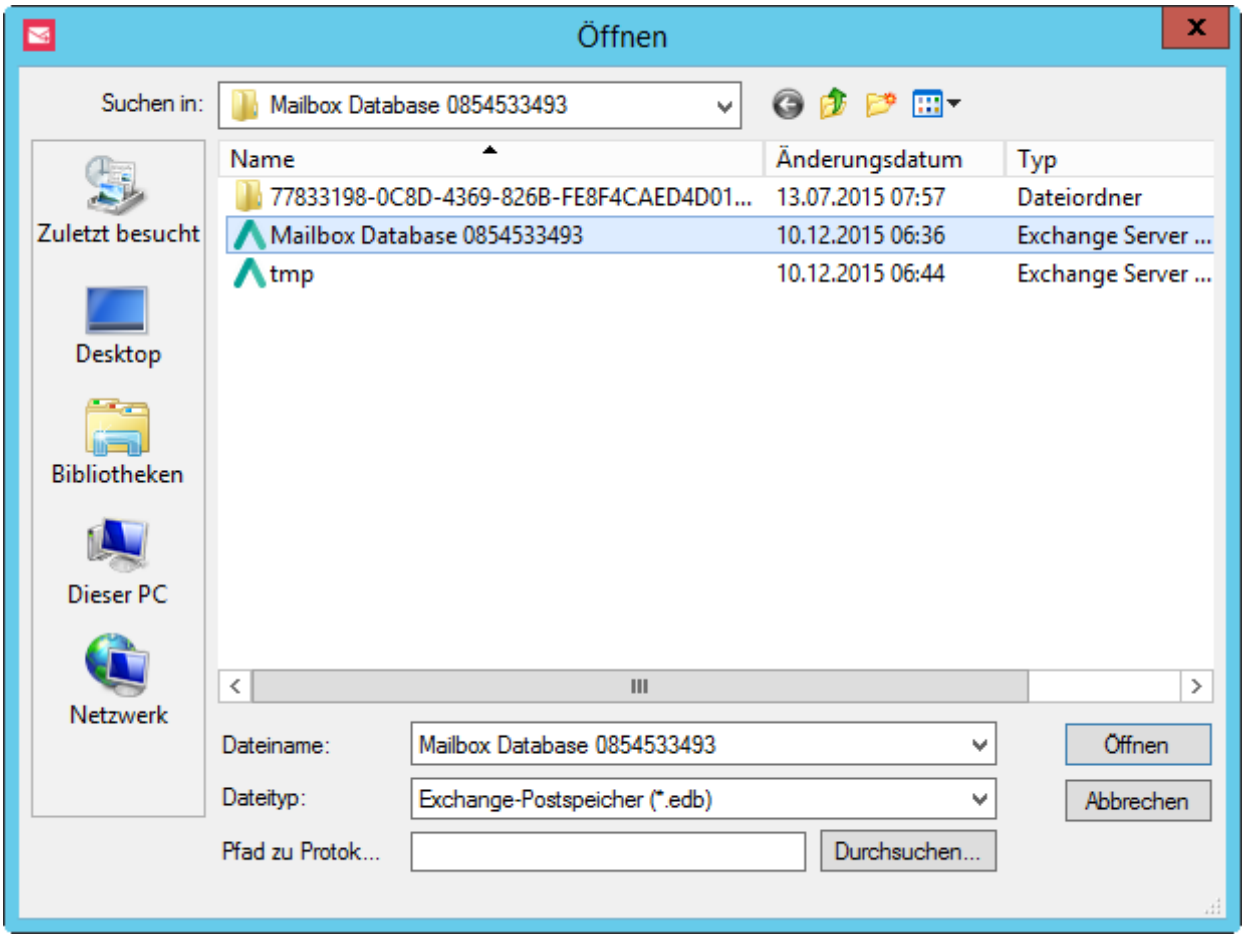
   Start > Programme > Arcserve > Unified Data Protection > Arcserve UDP Exchange Granular Restore

   oder

   X:\Programme\Arcserve\Unified Data Protection\Engine\Exchange GRT\esr.exe

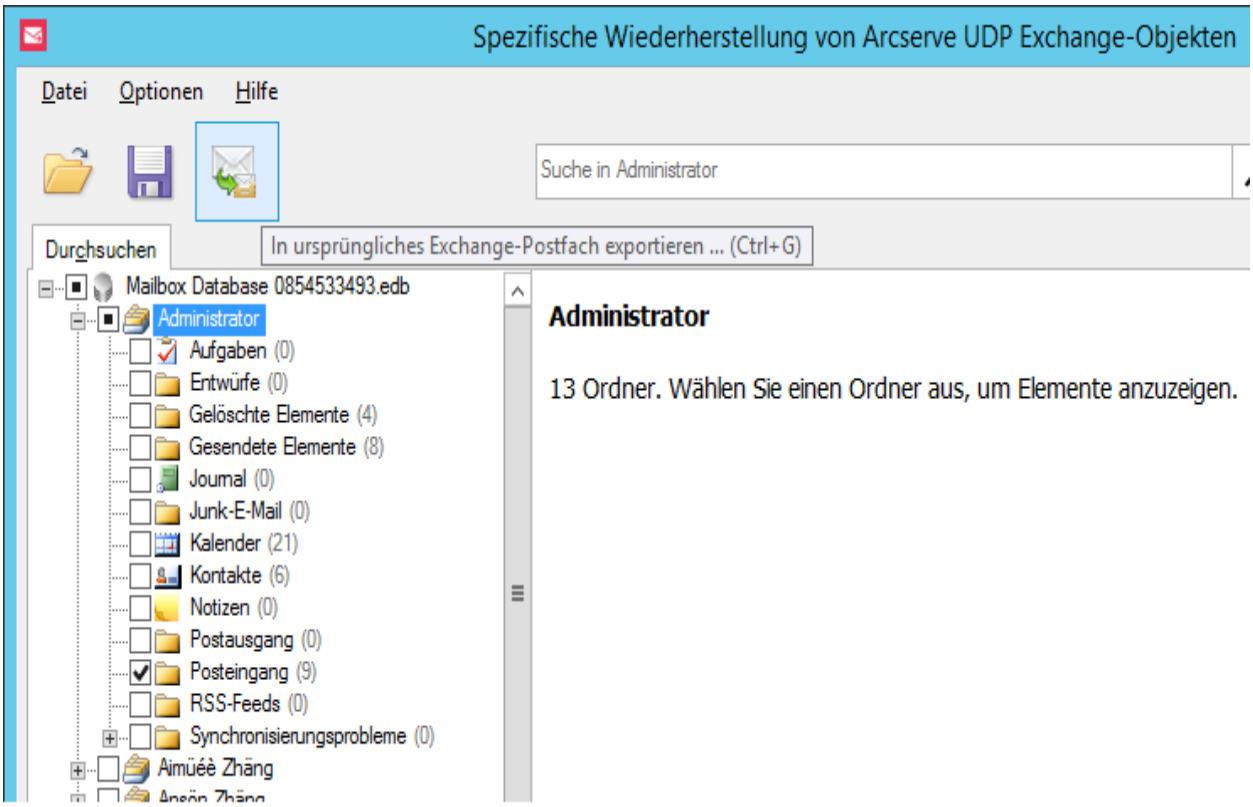
   Es wird ein Dialogfeld angezeigt, in dem Sie den Pfad für die Datenbank und Protokolldateien angeben können.

5. Geben Sie den Pfad für das geladene Volume an, und klicken Sie auf **Öffnen**.



Das Arcserve UDP Exchange Granular Restore-Hilfsprogramm wird geöffnet.

6. Wählen Sie die wiederherzustellenden Benutzerdaten aus, und klicken Sie auf **In ursprüngliche Mailbox exportieren** oder **In PST exportieren**.



Hinweise:

- Weitere Informationen zu den unterstützten Spezifikationen, Funktionen, Benutzeroptionen und Beschränkungen finden Sie im Exchange-Benutzerhandbuch zur spezifischen Wiederherstellung (esr.pdf) unter:

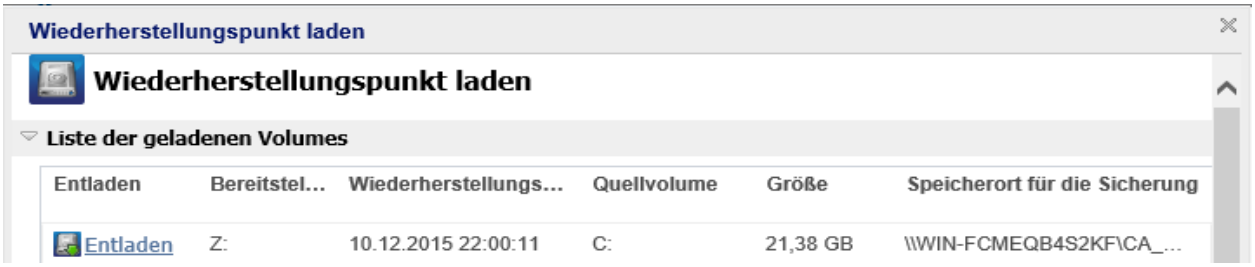
  %ProgramFiles%\Arcserve\Unified Data Protection\Engine\Exchange GRT oder Bookshelf.

- Standardmäßig verwendet das Hilfsprogramm den aktuellen, bei Windows angemeldeten Benutzer zur Herstellung der Verbindung. Wenn der aktuelle Benutzer nicht über die Berechtigungen verfügt, die Identität des ausgewählten Benutzers anzunehmen, wird eine Fehlermeldung im Bereich **Details** angezeigt.

  Wenn ein Fehler gemeldet wird, empfehlen wir, sich auf dem Rechner mit einem Konto anzumelden, das über Rechte zum Identitätswechsel für den ausgewählten Benutzer oder das Konto des ausgewählten Benutzers verfügt.

7. Wenn der Wiederherstellungsjob abgeschlossen ist, entladen Sie das Volume, das für die Wiederherstellung verwendet wurde.

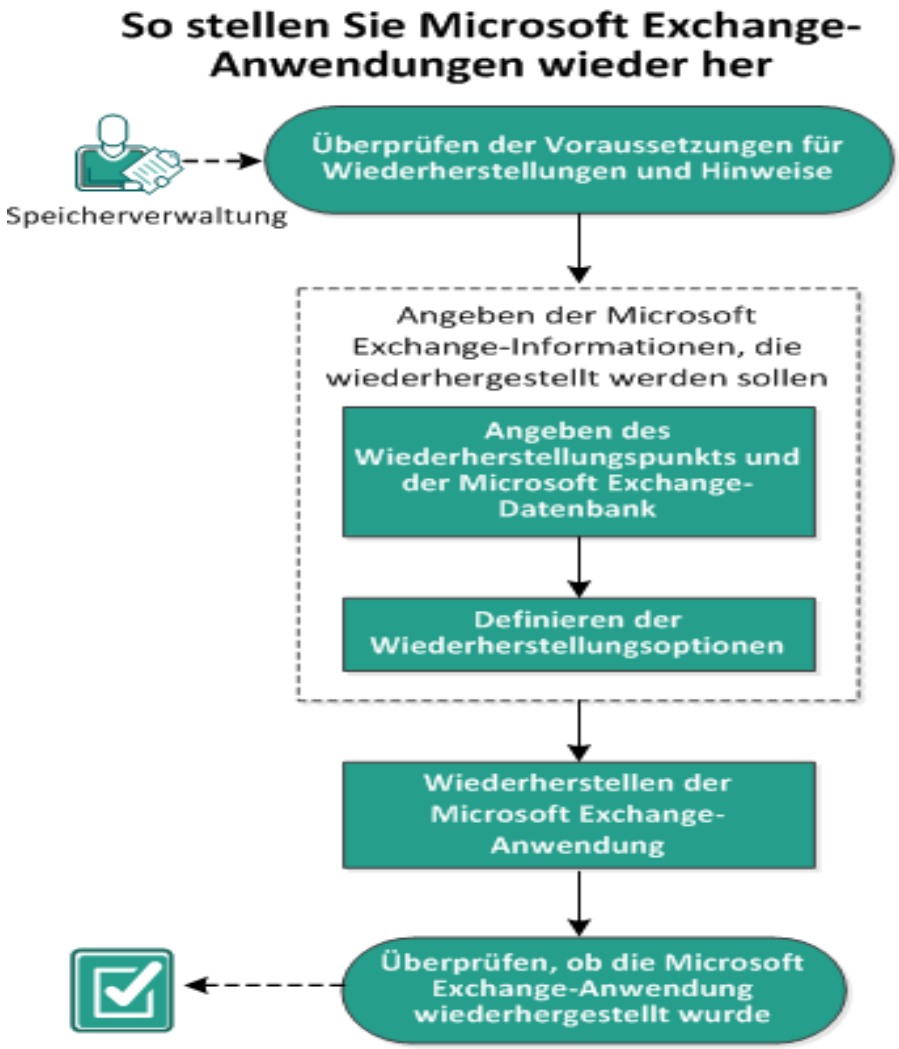
   Zum Entladen des Volumes klicken Sie in der Arcserve UDP Agent-Konsole auf **Wiederherstellungspunkt laden** und dann auf **Entladen**.


Wiederherstellungspunkt laden
Wiederherstellungspunkt laden
Liste der geladenen Volumes
Entladen
Bereitstel...
Wiederherstellungs...
Quellvolume
Größe
Speicherort für die Sicherung
Entladen
Z:
10.12.2015 22:00:11
C:
21,38 GB
\\WIN-FCMEQB4S2KF\CA_...

Wiederherstellen von Microsoft Exchange-Anwendungen

Mit Arcserve UDP Agent (Windows) können Sie nicht nur Ihre Daten schützen und wiederherstellen, sondern auch die Anwendungen, die diese gesicherten Daten verwenden, in Betrieb nehmen. Sämtliche Wiederherstellungen auf Anwendungsebene können ausschließlich mit der Methode "Wiederherstellung nach Wiederherstellungspunkten" wiederhergestellt werden. Während einer Anwendungswiederherstellung verwendet Arcserve UDP Agent (Windows) den Windows Volume Shadows Copy Service (VSS), um die Datenkonsistenz aller VSS-Anwendungen zu gewährleisten. Mit Arcserve UDP Agent (Windows) können Sie die Microsoft Exchange Server-Anwendung wiederherstellen, ohne eine vollständige Disaster Recovery durchzuführen.

Das folgende Diagramm veranschaulicht den Prozess zum Wiederherstellen einer Microsoft Exchange-Anwendung:



Führen Sie die folgenden Aufgaben aus, um eine Microsoft Exchange-Anwendung wiederherzustellen:

1. Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise
2. Angeben der Microsoft Exchange-Informationen, die wiederhergestellt werden sollen
    a. Angeben des Wiederherstellungspunkts und der Microsoft Exchange-Datenbank
    b. Definieren der Wiederherstellungsoptionen
3. Wiederherstellen der Microsoft Exchange-Anwendung
4. Überprüfen, ob die Microsoft Exchange-Anwendung wiederhergestellt wurde

Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise

Arcserve UDP Agent (Windows) unterstützt folgende Versionen von Microsoft Exchange Server:

- Microsoft Exchange 2010 - Einzelserverumgebung und Database Availability Group (DAG).
- Microsoft Exchange 2013 und 2016 – Einzelserverumgebung und Database Availability Group (DAG).

  Für Microsoft Exchange Server 2010-, 2013- und 2016-DAG-Umgebungen muss Arcserve UDP Agent (Windows) auf allen Mitgliedsservern in der DAG-Gruppe installiert sein. Ein Sicherungsjob kann auf allen Mitgliedsservern für aktive und passive Datenbankkopien durchgeführt werden, Wiederherstellungen können jedoch nur auf aktiven Datenbankkopien erfolgreich abgeschlossen werden.
- Zwar können alle DAG-Mitglieder Teil desselben oder eines anderen Backup-Plans sein, jedoch empfehlen wir, dieselben Deduplizierungs-Datenspeicher zu verwenden, um doppelte Daten zu vermeiden.

Sie können Microsoft Exchange Server auf den folgenden Ebenen wiederherstellen:

Microsoft Exchange Writer

Wenn Sie alle Microsoft Exchange Server-Daten wiederherstellen möchten, können Sie eine Wiederherstellung auf der Ebene von Microsoft Exchange Writer durchführen.

Speichergruppe

Wenn Sie eine bestimmte Speichergruppe wiederherstellen möchten, können Sie eine Wiederherstellung auf der Ebene der entsprechenden Gruppe durchführen.

Hinweis: Für Microsoft Exchange Server 2010, 2013 und 2016 ist die Speichergruppenebene nicht anwendbar.

Postfachdatenbank (Microsoft Exchange 2010, 2013 und 2016)

Wenn Sie eine bestimmte Postfachdatenbank wiederherstellen möchten, können Sie eine Wiederherstellung auf der Ebene der entsprechenden Postfachdatenbank durchführen.

Postfachebene (Microsoft Exchange 2010, 2013 und 2016)

Legt fest, ob Sie ein bestimmtes Postfach oder E-Mail-Objekt wiederherstellen möchten.

Stellen Sie sicher, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Microsoft Exchange-Wiederherstellung durchführen:

Wiederherstellung auf Datenbankebene

- Der Zielcomputer hat den gleichen Namen, und die gleiche Microsoft Exchange-Version ist installiert.
- Die Zieldatenbank hat den gleichen Datenbanknamen und den gleichen Namen für die Speichergruppe (Microsoft Exchange 200X) und gehört zur gleichen Microsoft Exchange-Organisation.

Wiederherstellung auf spezifischer Ebene

- Verwenden Sie das Hilfsprogramm zur spezifischen Wiederherstellung von Exchange-Objekten, um Microsoft Exchange-Daten wiederherzustellen.

Angeben der Microsoft Exchange-Informationen, die wiederhergestellt werden sollen

Mit Arcserve UDP Agent (Windows) können Sie nicht nur Ihre Daten schützen und wiederherstellen. Sie können darüber hinaus die Microsoft Exchange Server-Anwendungen abrufen, für deren Ausführung die wiederhergestellten Daten benötigt werden. Die Wiederherstellung des Microsoft Exchange Server kann nur über die Option "Wiederherstellung nach Wiederherstellungspunkten" durchgeführt werden.

Der Prozess für das Wiederherstellen von Microsoft Exchange-Anwendungen verläuft folgendermaßen:

1. Angeben des Wiederherstellungspunkts und der Microsoft Exchange-Datenbank
2. Definieren der Wiederherstellungsoptionen

Angeben des Wiederherstellungspunkts und der Microsoft Exchange-Datenbank

Verwenden Sie die Option **Nach Wiederherstellungspunkten suchen**, um von einem Wiederherstellungspunkt aus wiederherzustellen. Wenn Sie ein Datum für die Wiederherstellung auswählen, werden alle dazugehörigen Wiederherstellungspunkte angezeigt. Sie können die Microsoft Exchange-Datenbank für die Wiederherstellung suchen und auswählen.

Gehen Sie wie folgt vor:

1. Verwenden Sie eine der folgenden Vorgangsweisen, um auf das Dialogfeld zur Auswahl der Wiederherstellungsmethoden zuzugreifen:

   In Arcserve UDP:

   a. Melden Sie sich bei Arcserve UDP an.

   b. Klicken Sie auf die Registerkarte **Ressourcen**.

   c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

   e. Klicken Sie bei den Drop-down-Optionen unter **Aktionen** auf **Wiederherstellen**.

      Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

      Hinweis: Sie werden automatisch im Agentenknoten angemeldet, und das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird im Agentenknoten geöffnet.

   In Arcserve UDP Agent (Windows):

   a. Melden Sie sich bei Arcserve UDP Agent (Windows) an.

   b. Wählen auf der Startseite **Wiederherstellen** aus.

   Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

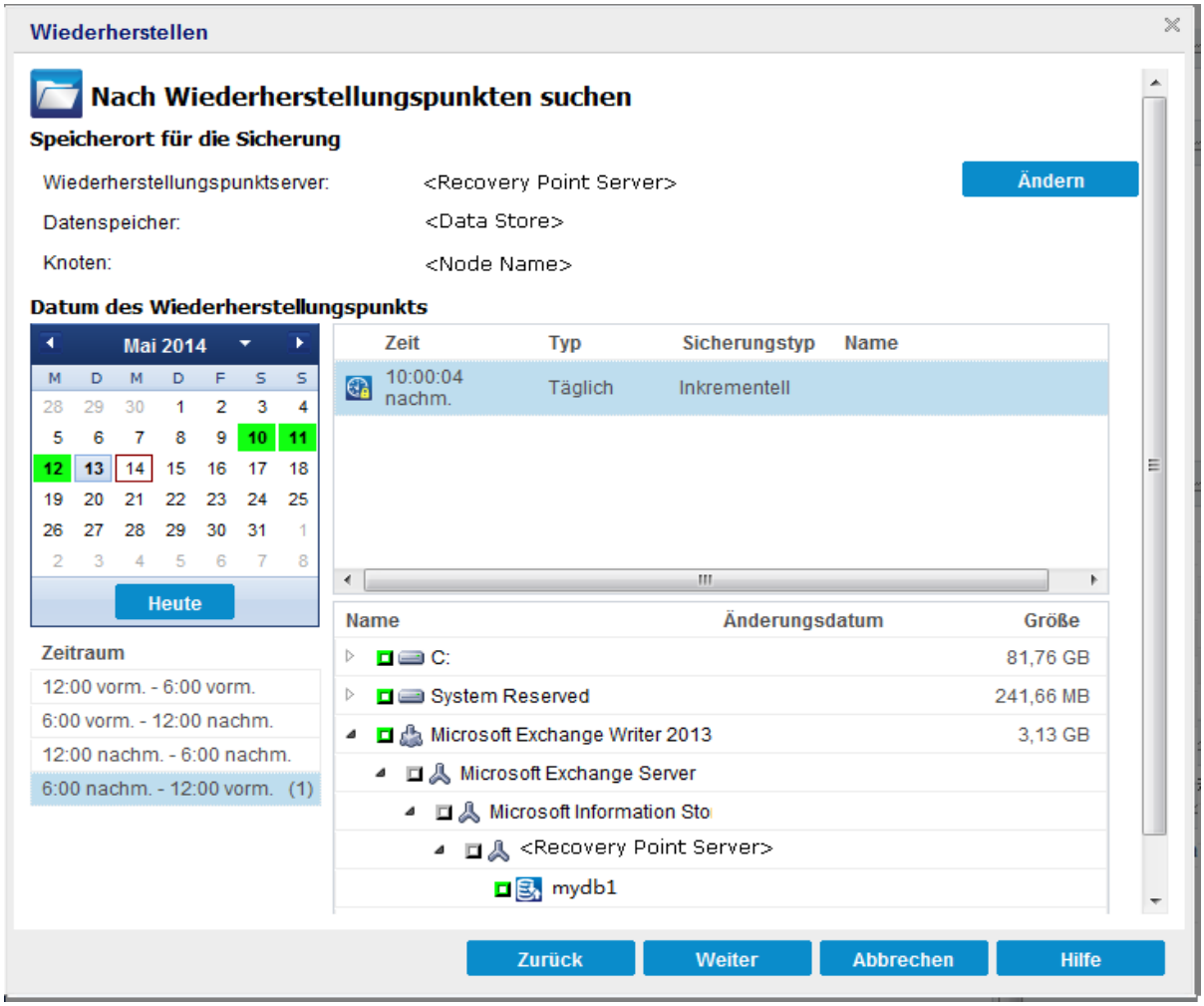
2. Klicken Sie auf die Option **Nach Wiederherstellungspunkten suchen**.

   Das Dialogfeld **Nach Wiederherstellungspunkten suchen** wird angezeigt.

3. Wählen Sie zunächst den Wiederherstellungspunkt (Datum und Uhrzeit), und anschließend die wiederherzustellende Microsoft Exchange-Datenbank.

Um anzuzeigen, dass die Datenbank zur Wiederherstellung ausgewählt wurde, wird das entsprechende Markierungskästchen grün aufgefüllt.

Hinweis: Wenn Sie nicht möchten, dass die Transaktionsprotokolldateien nach der Wiederherstellung angewendet werden, müssen Sie die Dateien vor der Wiederherstellung manuell löschen. Weitere Informationen zum manuellen Löschen von Transaktionsprotokolldateien finden Sie in der Dokumentation zu Microsoft Exchange Server.



4. Klicken Sie auf **Weiter**.

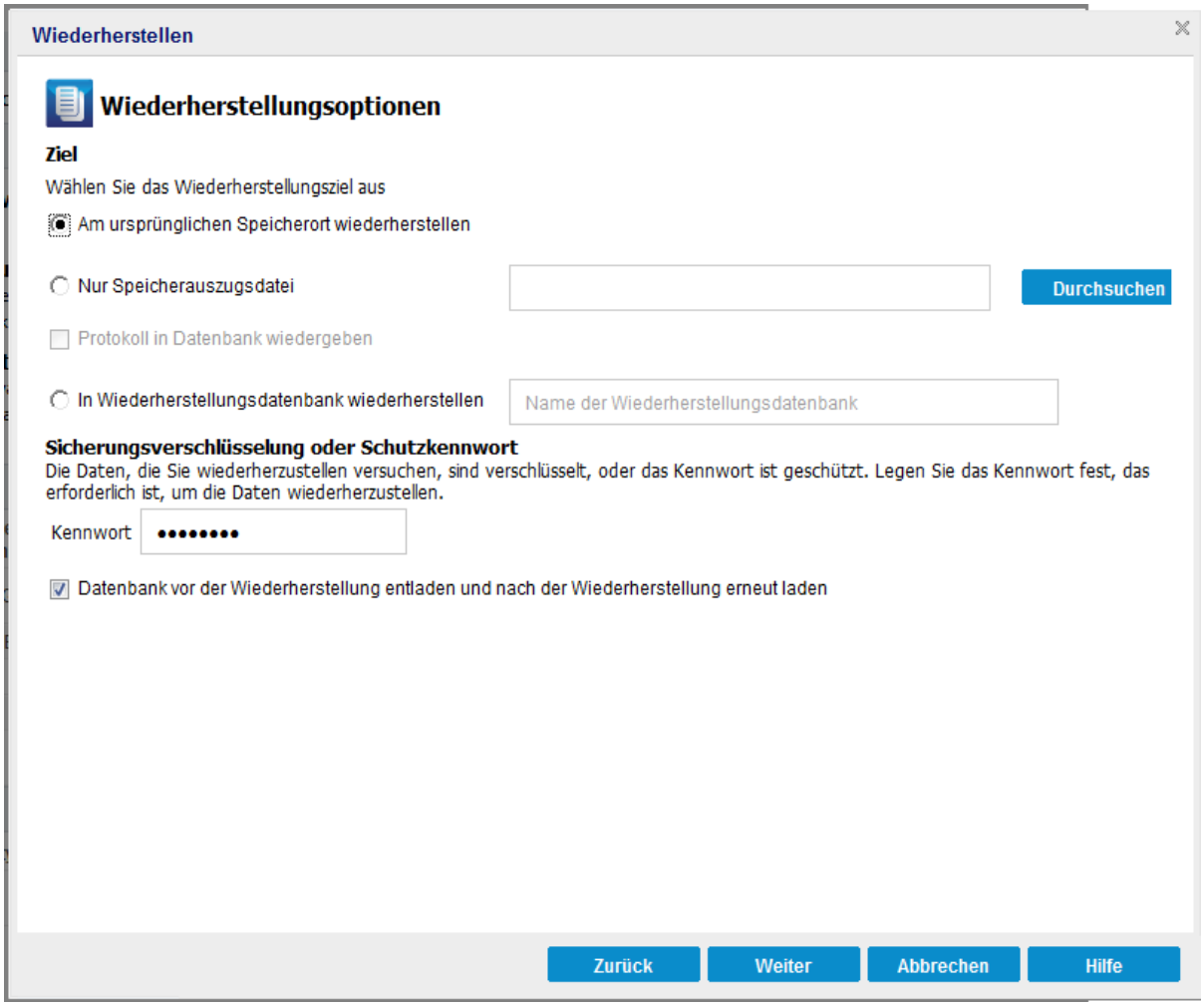
Das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet.

Definieren der Wiederherstellungsoptionen

Nachdem Sie Wiederherstellungspunkt und wiederherzustellenden Inhalt festgelegt haben, definieren Sie die Kopieroptionen für den ausgewählten Wiederherstellungspunkt.

Gehen Sie wie folgt vor:

1. Geben Sie das Wiederherstellungsziel im Dialogfeld **Wiederherstellungsoptionen** an.



2. Wählen Sie das Ziel für die Wiederherstellung aus.

Es stehen Optionen zur Wiederherstellung am ursprünglichen Speicherort der Sicherheitskopie, zur ausschließlichen Wiederherstellung der Speicherauszugsdatei oder zur Wiederherstellung in einer Wiederherstellungsspeichergruppe/Wiederherstellungspostfachdatenbank zur Verfügung.

Am ursprünglichen Speicherort wiederherstellen

Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

Nur Speicherauszugsdatei

Stellt nur die Speicherauszugsdatei wieder her.

Mit dieser Option stellt Arcserve UDP Agent (Windows) die Microsoft Exchange-Datenbankdatei in einem festgelegten Ordner wieder her und stellt sie nach der Wiederherstellung nicht online. Sie können sie manuell auf Microsoft Exchange Server laden.

Hinweis: Wenn eine Wiederherstellungspostfachdatenbank vorhanden ist, schlägt die Wiederherstellung mit der Option **Nur Speicherauszugsdatei** fehl.

Protokoll in Datenbank wiedergeben

Legt fest, dass Sie alle Microsoft Exchange-Transaktionsprotokolldateien wiedergeben und in die Datenbank übergeben können, wenn die Datenbankdateien im Zielordner abgelegt sind.

Datenbank vor der Wiederherstellung entladen und sie nach der Wiederherstellung erneut laden

Normalerweise führt Microsoft Exchange vor einer Wiederherstellung einige Überprüfungen durch, um Folgendes sicherzustellen:

- Die wiederherzustellende Datenbank befindet sich im Status *Abgesetzt*
- Die Datenbank wird nicht unerwartet wiederhergestellt.

Damit eine Microsoft Exchange-Produktionsdatenbank nicht unerwartet wiederhergestellt wird, wird ein Schalter hinzugefügt, sodass die Datenbank während der Wiederherstellung überschrieben werden kann. Microsoft Exchange wird keine Datenbanken wiederherstellen, wenn dieser Schalter nicht festgelegt ist.

Bei Arcserve UDP Agent (Windows) werden diese zwei Optionen über die Option "Datenbank vor der Wiederherstellung entladen und nach der Wiederherstellung erneut laden" gesteuert. Mit dieser Option können Sie die Wiederherstellung in Arcserve UDP Agent (Windows) automatisch, ohne manuelle

Vorgänge, starten. (Sie können auch angeben, Datenbanken manuell zu entladen/laden)

- Wenn diese Option aktiviert ist, wird die Microsoft Exchange-Datenbank vor dem Wiederherstellungsprozess automatisch entladen, und nach Abschluss der Wiederherstellung erneut geladen. Außerdem können Exchange-Datenbanken während der Wiederherstellung überschrieben werden, wenn diese Option aktiviert ist.
- Wenn diese Option nicht aktiviert ist, wird die Microsoft Exchange-Datenbank vor der Wiederherstellung nicht automatisch entladen und nach der Wiederherstellung nicht erneut geladen.

Der Exchange-Administrator muss in diesem Fall einige manuelle Vorgänge ausführen, wie z. B. die Exchange-Datenbank entladen, "Überschreibung zulassen" für die Datenbank einrichten und die Microsoft Exchange-Datenbank laden. (Exchange führt den Wiederherstellungsvorgang während dem Laden der Datenbank aus)

Wenn diese Option nicht aktiviert ist, können Microsoft Exchange-Datenbanken während der Wiederherstellung außerdem nicht überschrieben werden.

In Wiederherstellungsdatenbank wiederherstellen (Microsoft Exchange 2010 und 2013)

Stellt die Datenbank in einer Wiederherstellungsdatenbank wieder her. Eine Wiederherstellungsdatenbank ist eine Datenbank, die für Wiederherstellungen verwendet werden kann. Sie können eine gesicherte Microsoft Exchange-Postfachdatenbank in einer Wiederherstellungsdatenbank wiederherstellen und aus ihr Daten wiederherstellen und extrahieren, ohne, dass sich dies auf die Datenbank auswirkt, auf die von den Endbenutzern zugegriffen wird.

Bevor Sie eine Wiederherstellung einer Microsoft Exchange 2010- oder Exchange 2013-Datenbank in einer Wiederherstellungsdatenbank durchführen, müssen Sie eine Wiederherstellungsdatenbank erstellen.

3. Klicken Sie auf **Weiter**.

Das Dialogfeld **Wiederherstellungsübersicht** wird geöffnet.

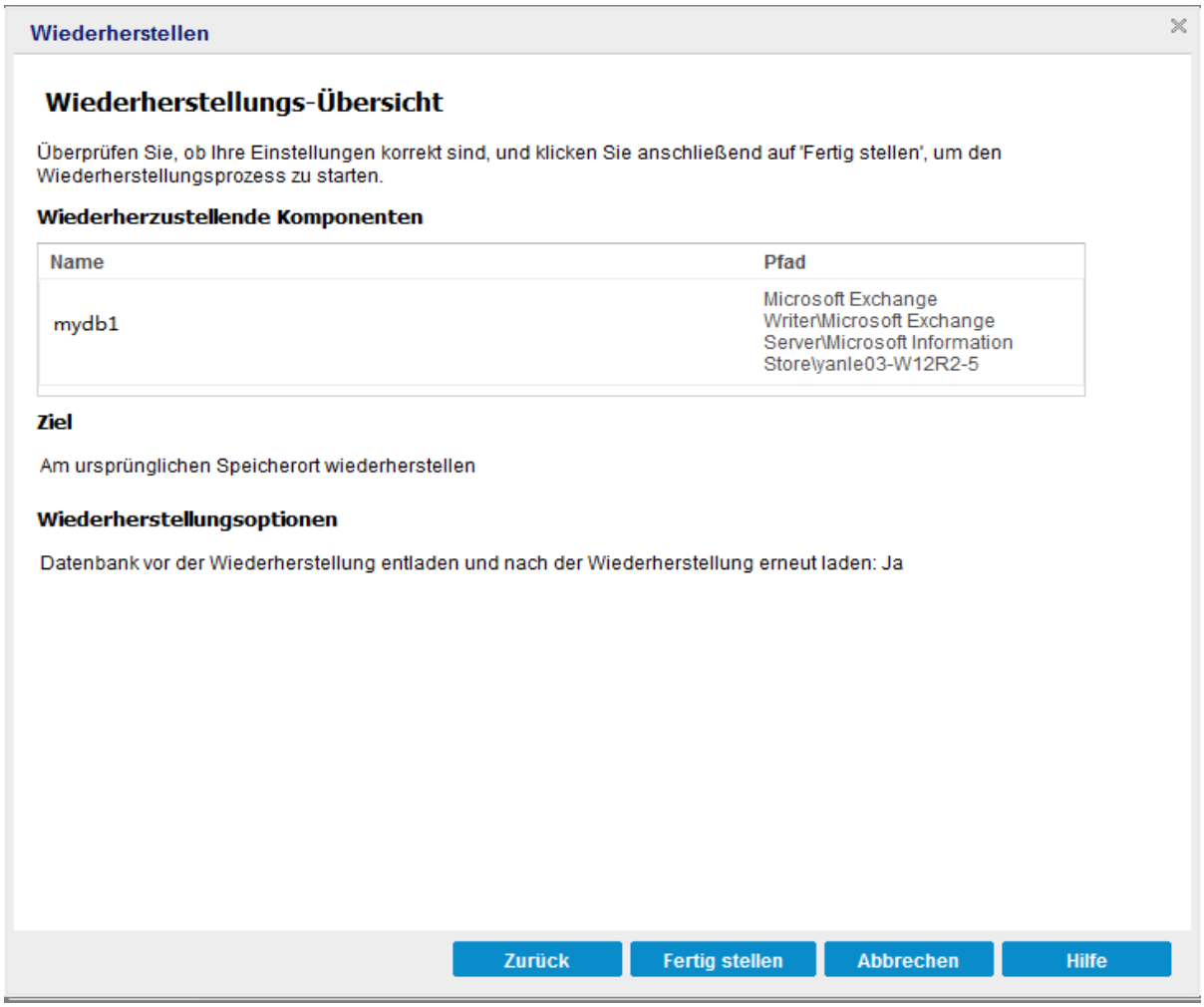
Wiederherstellen der Microsoft Exchange-Anwendung

Nachdem Sie die Wiederherstellungsoptionen definiert haben, überprüfen Sie, dass Ihre Einstellungen korrekt sind, und bestätigen Sie den Wiederherstellungsprozess. Die **Wiederherstellungsübersicht** ist hilfreich, um sämtliche Wiederherstellungsoptionen, die Sie festgelegt haben, zu überprüfen und bei Bedarf zu ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die angezeigten Informationen im Dialogfeld **Wiederherstellungsübersicht**, um die Richtigkeit aller Wiederherstellungsoptionen und

Einstellungen sicherzustellen.



- Wenn die Übersichtsinformationen nicht korrekt sind, klicken Sie auf **Zurück**, und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**, um den Wiederherstellungsprozess zu starten.

Die Microsoft Exchange-Anwendung wird wiederhergestellt.

Überprüfen, ob die Microsoft Exchange-Anwendung wiederhergestellt wurde

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Arcserve UDP Agent (Windows)-Wiederherstellungsziel, das Sie angegeben haben.

   Wenn Sie beispielsweise ausgewählt haben, dass die Microsoft Exchange-Datenbank am ursprünglichen Speicherort wiederhergestellt werden soll, überprüfen Sie nach Abschluss der Wiederherstellung am physischen Speicherort, ob die Microsoft Exchange-Datenbank und die Protokolle wiederhergestellt wurden.

   Wenn Sie auswählen, dass die Microsoft Exchange-Datenbank nur am Speicherort der Speicherauszugsdatei wiederhergestellt werden soll, stellt Arcserve UDP Agent (Windows) die Microsoft Exchange-Datenbank und die Protokolle an einem angegebenen Speicherort wieder her.

2. Überprüfen Sie, ob die Microsoft Exchange-Anwendung wiederhergestellt wurde und ob die Datenbank geladen und zugreifbar ist.

   Die Microsoft Exchange-Anwendung ist erfolgreich wiederhergestellt.

Wiederherstellen von Exchange-Daten auf einem virtuellen VMware-Rechner

Wichtig! Um Microsoft Exchange-Daten auf einem virtuellen VMware-Rechner wiederherzustellen, wird empfohlen, das Hilfsprogramm zur spezifischen Wiederherstellung von Exchange-Objekten zu verwenden.

So laden Sie Dateien/Ordner ohne Wiederherstellung herunter

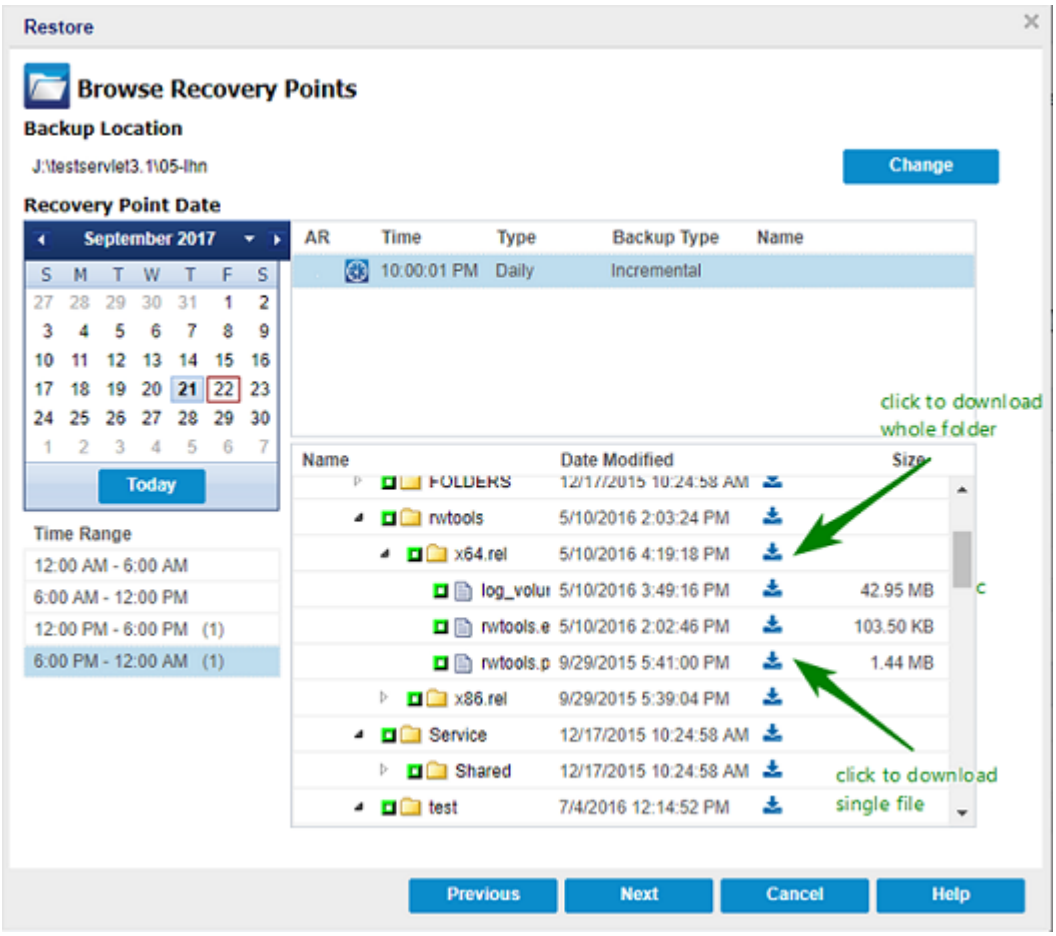
Mit Arcserve UDP können Sie eine Datei oder einen kompletten Ordner ohne Wiederherstellung herunterladen. Vom Wiederherstellungsassistenten aus können Sie über den Bildschirm "Nach Wiederherstellungspunkten suchen" eine Datei oder einen kompletten Ordner mit allen Dateien direkt herunterladen. Durch das Herunterladen vor der Wiederherstellung können Sie eine schnelle Überprüfung der Dateien vornehmen, um zu verhindern, dass unerwünschte Dateien wiederhergestellt werden.

Hinweis: Beim Herunterladen der Dateien werden keine Berechtigungen für Dateien oder Ordner beibehalten.

Eine einzelne Datei wird direkt im selben Format heruntergeladen, ein Ordner dagegen als Zip-Datei. Der Name der Zip-Datei hat das folgende Format:

[nodename]_[sessionid]_[timestamp].zip

Zum Herunterladen müssen Sie einfach den Bildschirm "Nach Wiederherstellungspunkten suchen" im Wiederherstellungsassistenten aufrufen. Im unten stehenden Screenshot wird erklärt, wie Sie eine Datei oder einen Ordner herunterladen:



Hinweise zum Download:

- Das Herunterladen oder Verpacken als Zip-Datei ist nicht für alle Systemdateien möglich. Der Agent-Tomcat-Service verfügt nicht über ausreichende Zugriffsrechte, um auf die Systemdatei oder Benutzerdateien anderer geschützter Knoten zuzugreifen.
- Um einen zu hohen Verbrauch des Tomcat-Speichers und eine zu starke CPU-Auslastung zu vermeiden, empfehlen wir, beim Herunterladen einer großen Datei oder eines Ordners einen Wiederherstellungsauftrag an einen alternativen Pfad zu übergeben.
- Möglicherweise können Sie die heruntergeladenen Zip-Dateien nicht mit Windows-Tools für komprimierte Ordner durchsuchen, da einige Zip-Eintragsnamen für die Tools zum Durchsuchen zu lang sind. Wir empfehlen die Verwendung anderer Zip-Tools zum Öffnen der Datei, zum Beispiel WinZip oder WinRAR, 7-Zip.
- Ein IE9-Benutzer, der https in IE9 und einen Agent-Webdienst zum Bereitstellen des Dienstes verwendet, kann die Dateien möglicherweise nicht herunterladen. Ein bekanntes Problem, das bei IE9 beim Herunterladen von

Ressourcen von einer dynamischen Seite über https auftritt, führt dazu, dass der Download fehlschlägt. Weitere Informationen und die Lösung des Problems finden Sie in dem Microsoft-Artikel unter diesem Link.

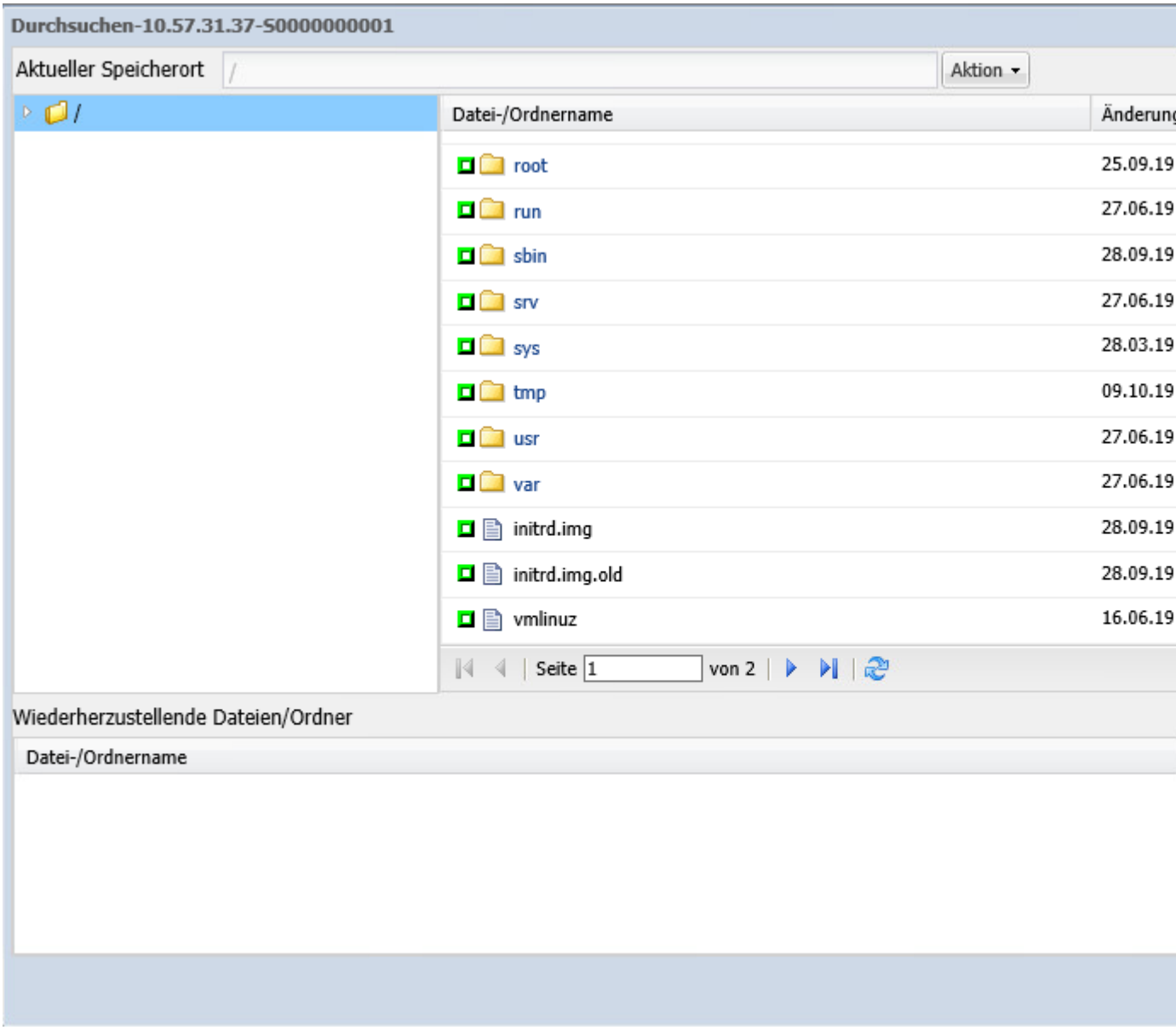
So laden Sie Dateien/Ordner ohne Wiederherstellung herunter/Ordner ohne Wiederherstellung für Linux-Knoten herunter

Mit Arcserve UDP können Sie eine Datei oder einen kompletten Ordner ohne Wiederherstellung herunterladen. Vom Wiederherstellungsassistenten aus können Sie über den Bildschirm "Nach Wiederherstellungspunkten suchen" eine Datei oder einen kompletten Ordner mit allen Dateien direkt herunterladen. Durch das Herunterladen vor der Wiederherstellung können Sie eine schnelle Überprüfung der Dateien vornehmen, um zu verhindern, dass unerwünschte Dateien wiederhergestellt werden.

Eine einzelne Datei wird direkt im selben Format heruntergeladen, ein Ordner dagegen als Zip-Datei. Der Name der Zip-Datei hat das folgende Format:

[nodename]_[sessionid]_[timestamp].zip

Zum Herunterladen müssen Sie einfach den Bildschirm "Nach Wiederherstellungspunkten suchen" im Wiederherstellungsassistenten aufrufen. Im unten stehenden Screenshot wird erklärt, wie Sie eine Datei oder einen Ordner für Linux-Knoten herunterladen:



Um die heruntergeladenen Dateien zu öffnen, verwenden Sie ZIP-Tools wie WinZip, WinRAR, 7-Zip usw.

So stellen Sie Microsoft SQL Server-Anwendungen wieder her

Mit Arcserve UDP Agent (Windows) können Sie nicht nur Ihre Daten schützen und wiederherstellen, sondern auch die Anwendungen, die diese gesicherten Daten verwenden, in Betrieb nehmen. Sämtliche Wiederherstellungen auf Anwendungsebene können ausschließlich mit der Methode "Wiederherstellung nach Wiederherstellungspunkten" wiederhergestellt werden. Während einer Anwendungswiederherstellung verwendet Arcserve UDP Agent (Windows) den Windows Volume Shadows Copy Service (VSS), um die Datenkonsistenz aller VSS-Anwendungen zu gewährleisten. Mit Arcserve UDP Agent (Windows) können Sie die Microsoft SQL Server-Anwendung wiederherstellen, ohne eine vollständige Disaster Recovery durchzuführen.

Das folgende Diagramm veranschaulicht den Prozess zum Wiederherstellen einer Microsoft SQL Server-Anwendung:

Führen Sie die folgenden Aufgaben aus, um eine Microsoft SQL Server-Anwendung wiederherzustellen:

1. Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise
2. Angeben von Microsoft SQL Server-Informationen, die wiederhergestellt werden sollen
    a. Angeben des Wiederherstellungspunkts und der Microsoft SQL Server-Datenbank
    b. Definieren der Wiederherstellungsoptionen
3. Wiederherstellen der Microsoft SQL Server-Anwendung
4. Überprüfen, ob die Microsoft SQL Server-Anwendung wiederhergestellt wurde

Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Wiederherstellung ausführen:

- Sie benötigen die Microsoft SQL Server-Instanz, bevor Sie eine Wiederherstellung der SQL-Anwendung ausführen.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Überprüfen Sie die folgenden Wiederherstellungshinweise:

- Die Datenbank kann nicht instanzübergreifend wiederhergestellt werden. Wiederherstellung an einem alternativem Speicherort bedeutet in Arcserve UDP Agent (Windows), dass die Datenbank wiederhergestellt und ihr Name und Speicherort geändert werden kann. Weitere Informationen finden Sie in den Hinweisen zur Wiederherstellung von Microsoft SQL Server an einem alternativen Speicherort.
- Wenn die Jobs nicht für dieselbe VM sind, können Sie mit Arcserve UDP mehrere Wiederherstellungsjobs zur gleichen Zeit ausführen. Wenn Sie versuchen, einen Wiederherstellungsjob zu starten, während ein anderer Wiederherstellungsjob für dieselbe VM ausgeführt wird, öffnet sich eine Hinweismeldung, die Sie darüber informiert, dass ein anderer Job ausgeführt wird, und Sie auffordert, es später erneut zu versuchen.
- Arcserve UDP kann nur einen Wiederherstellungsjob zur gleichen Zeit ausführen. Wenn Sie versuchen, einen Wiederherstellungsjob manuell zu starten, während ein anderer Wiederherstellungsjob ausgeführt wird, öffnet sich eine Hinweismeldung, die Sie darüber informiert, dass ein anderer Job ausgeführt wird, und Sie auffordert, es später erneut zu versuchen.

Hinweise zur Wiederherstellung von Microsoft SQL Server an einem alternativen Speicherort

Wenn Sie festlegen, dass eine Microsoft SQL Server-Anwendung an einem alternativen Speicherort wiederhergestellt werden soll, können Sie sie entweder an einem alternativen Speicherort auf dem gleichen Rechner oder auf einem anderen Rechner wiederherstellen.

Bevor Sie eine Arcserve UDP Agent (Windows)-Wiederherstellung einer Microsoft SQL Server-Anwendung an einem alternativen Speicherort ausführen, sollten Sie Folgendes berücksichtigen:

Wenn sich der alternative Speicherort auf dem gleichen Rechner befindet

Bei dieser Option können Sie eine Datenbank entweder an einem neuen Speicherort (mit dem gleichen Namen) oder mit einem neuen Namen (am gleichen Speicherort) wiederherstellen:

- **Gleicher Name - Neuer Speicherort**

  Wenn beispielsweise Datenbank A im aktuellen SQL Server unter "C:\DB_A" installiert ist und gesichert wurde. Sie können diese Option verwenden und "Alternativer Dateispeicherort" angeben, um Datenbank A an einem alternativen Speicherort wie z. B. "D:\Alternate_A" wiederherzustellen.

  Nachdem die Datenbank wiederhergestellt wurde, wird die Datenbankdatei verwendet, die sich am neuen Speicherort "D:\Alternate_A" befindet.

  Wichtig! Wenn Sie während der Wiederherstellung den Datenbankspeicherort ändern, aber den Namen der Datenbank beibehalten, wird die frühere Datenbank gelöscht, nachdem die Wiederherstellung abgeschlossen ist. Die wiederhergestellte Datenbankdatei verweist auf den neuen Speicherort.

  Wenn Sie an einem alternativen Speicherort wiederherstellen, ist der Abschnitt für den Instanzennamen nicht verfügbar, da der Instanzenname immer der gleiche sein muss und nicht geändert werden kann. Daher ist es nicht möglich, eine Datenbank an einer alternativen, derzeit auf demselben MS SQL Server vorhandenen Instanz wiederherzustellen.

- **Gleicher Speicherort - Neuer Name**

  Wenn beispielsweise zwei Datenbanken (Datenbank A und Datenbank B) im aktuellen SQL Server installiert sind und beide gesichert wurden. Sie können diese Option verwenden und "Neuer Datenbankname" angeben, um Datenbank A am gleichen Speicherort als "Datenbank A_New" wiederherzustellen.

  Nachdem die Datenbanken wiederhergestellt wurden, verfügt dieser Speicherort über drei Datenbanken (Datenbank A, Datenbank B und Datenbank A_New).

Wenn sich der alternative Speicherort auf dem anderen Rechner befindet

- Der SQL Server-Installationspfad muss identisch mit dem Pfad sein, der bei der Ausführung der Sicherung vorhanden war.

  Wenn die Sicherung von SQL Server beispielsweise unter "C:\SQLServer" installiert ist, muss SQL Server auf dem neuen Arcserve UDP Agent (Windows)-Server dann auch unter "C:\SQLServer" installiert werden.

- Der gleiche Instanzenname für die Datenbank, die bei der Ausführung der Sicherung vorhanden war, muss auf dem Arcserve UDP Agent (Windows)-Server installiert sein, da ansonsten die Datenbank, die mit dieser Instanz verbunden

ist, von der Wiederherstellung übersprungen wird.

Dies ist beispielsweise der Fall, wenn die SQL Server-Sicherung "Instance_1" mit Datenbank A und Datenbank B und "Instance_2" mit Datenbank C enthält, der Arcserve UDP Agent (Windows)-Server aber nur über "Instance_1" verfügt. Nachdem die Wiederherstellung abgeschlossen ist, werden Datenbank A und Datenbank B wiederhergestellt, und Datenbank C wird nicht wiederhergestellt.

- Die SQL Server-Version auf dem Arcserve UDP Agent (Windows)-Server muss abwärtskompatibel mit der SQL Server-Version sein, die während der Sicherungssitzung verwendet wurde.

  Sie können beispielsweise einen SQL Server 2008-Rechner auf einen SQL Server 2010-Rechner wiederherstellen. Allerdings können Sie einen SQL Server 2010-Rechner nicht auf einen SQL Server 2008-Rechner wiederherstellen.

- Wiederherstellungen einer Datenbank von einer 64-Bit-Instanz auf eine 32-Bit-Instanz wird nicht unterstützt.

Hinweise zur Wiederherstellung von Microsoft SQL Server 2012/2014 AAG

Wenn Sie eine Microsoft SQL Server 2012/2014-Datenbank wiederherstellen, die Teil einer AlwaysOn-Verfügbarkeitsgruppe (AlwaysOn Availability Group (AAG)) ist, sollten Sie folgende Hinweise berücksichtigen.

Wenn die MS SQL-Datenbank Teil der MS SQL 2012/2014 AlwaysOn Availability Group (AAG) ist, und die Wiederherstellung auf den ursprünglichen Speicherort fehlschlägt, sollten Sie folgende Aufgaben ausführen:

1. Entfernen Sie die wiederherzustellende Datenbank aus der AlwaysOn-Verfügbarkeitsgruppe. Über den Link können Sie sich eingehender informieren.
2. Geben Sie die Sicherungssitzung auf jedem Knoten der Availability Group für Arcserve UDP Agent (Windows) frei und stellen Sie die Sitzung durch Arcserve UDP Agent (Windows) auf jedem Knoten der Availability Group wieder her.
3. Fügen Sie die Datenbank wieder einer Availability Group hinzu. Über den Link können Sie sich eingehender informieren.

Angeben von Microsoft SQL Server-Informationen, die wiederhergestellt werden sollen

Mit Arcserve UDP Agent (Windows) können Sie nicht nur Ihre Daten schützen und wiederherstellen. Sie können darüber hinaus die Microsoft SQL Server-Anwendungen abrufen, für deren Ausführung die wiederhergestellten Daten benötigt werden. Die Wiederherstellung des Microsoft SQL Server kann nur über die Option "Wiederherstellung nach Wiederherstellungspunkten" durchgeführt werden.

Der Prozess für das Wiederherstellen von Microsoft SQL Server-Anwendungen verläuft folgendermaßen:

1. Angeben des Wiederherstellungspunkts und der Microsoft SQL Server-Datenbank
2. Definieren der Wiederherstellungsoptionen

Angeben des Wiederherstellungspunkts und der Microsoft SQL Server-Datenbank

Verwenden Sie die Option **Nach Wiederherstellungspunkten suchen**, um von einem Wiederherstellungspunkt aus wiederherzustellen. Wenn Sie ein Datum für die Wiederherstellung auswählen, werden alle dazugehörigen Wiederherstellungspunkte angezeigt. Sie können die Microsoft SQL Server-Datenbank für die Wiederherstellung suchen und auswählen.

Gehen Sie wie folgt vor:

1. Verwenden Sie eine der folgenden Vorgangsweisen, um auf das Dialogfeld zur Auswahl der Wiederherstellungsmethoden zuzugreifen:

   - In Arcserve UDP:

     a. Melden Sie sich bei Arcserve UDP an.

     b. Klicken Sie auf die Registerkarte **Ressourcen**.

     c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

     Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

     d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

     e. Klicken Sie im Drop-down-Menü "Servername" auf **Wiederherstellen**.

     Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

     Hinweis: Sie werden automatisch im Agentenknoten angemeldet, und das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird im Agentenknoten geöffnet.

   - In Arcserve UDP Agent (Windows):

     a. Melden Sie sich bei Arcserve UDP Agent (Windows) an.

     b. Wählen Sie auf der Startseite **Wiederherstellen** aus.

     Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

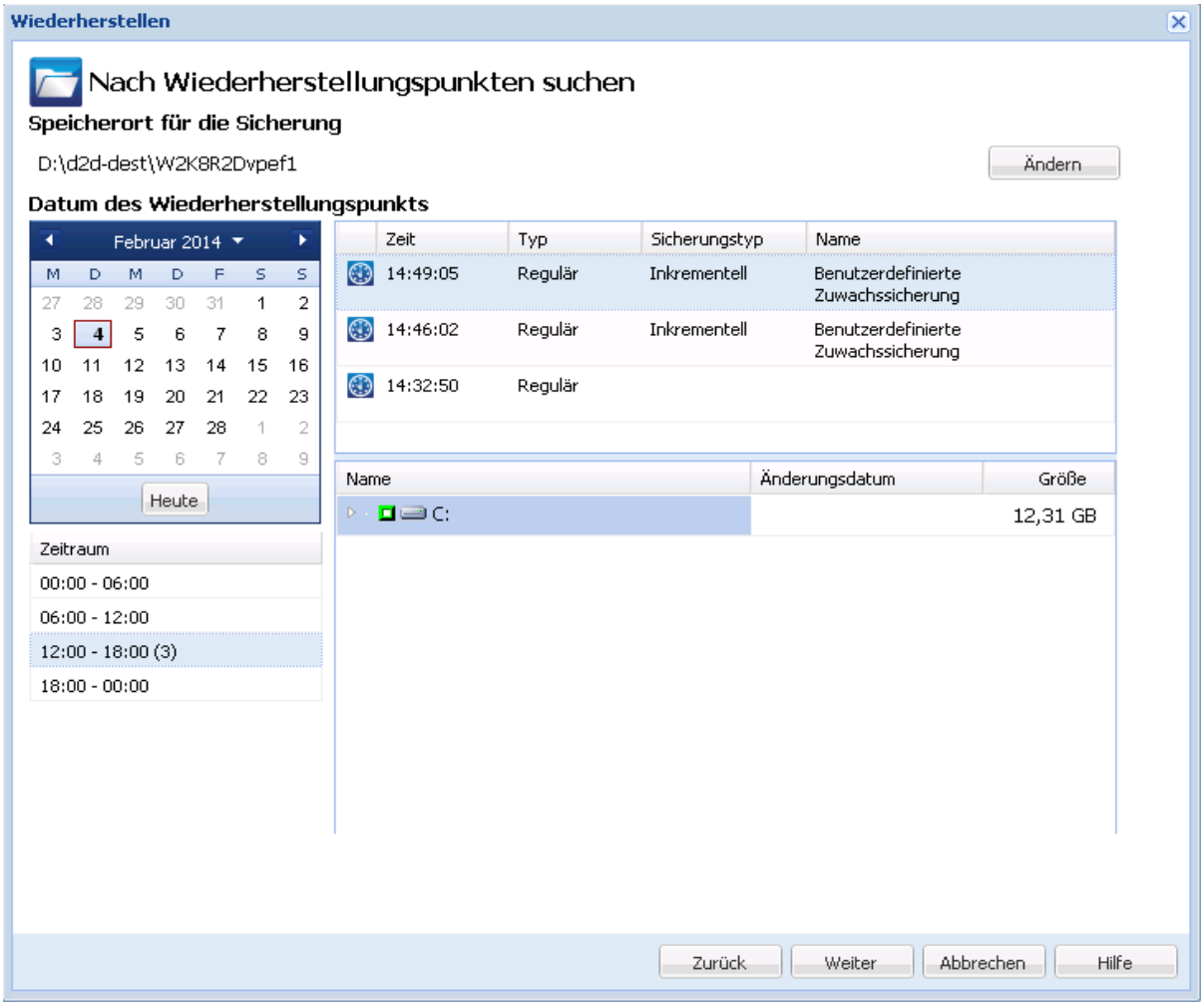
6. Klicken Sie auf die Option **Nach Wiederherstellungspunkten suchen**.

   Das Dialogfeld **Nach Wiederherstellungspunkten suchen** wird angezeigt.

7. Wählen Sie zunächst den Wiederherstellungspunkt (Datum und Uhrzeit), und anschließend die wiederherzustellende Microsoft SQL Server-Datenbank.

8. Um anzuzeigen, dass die Datenbank zur Wiederherstellung ausgewählt wurde, wird das entsprechende Markierungskästchen grün aufgefüllt.

Hinweis: Wenn Sie nicht möchten, dass die Transaktionsprotokolldateien nach der Wiederherstellung angewendet werden, müssen Sie die Dateien vor der Wiederherstellung manuell löschen. Weitere Informationen zum manuellen Löschen von Transaktionsprotokolldateien finden Sie in der Dokumentation zu Microsoft SQL Server.



9. Klicken Sie auf **Weiter**.

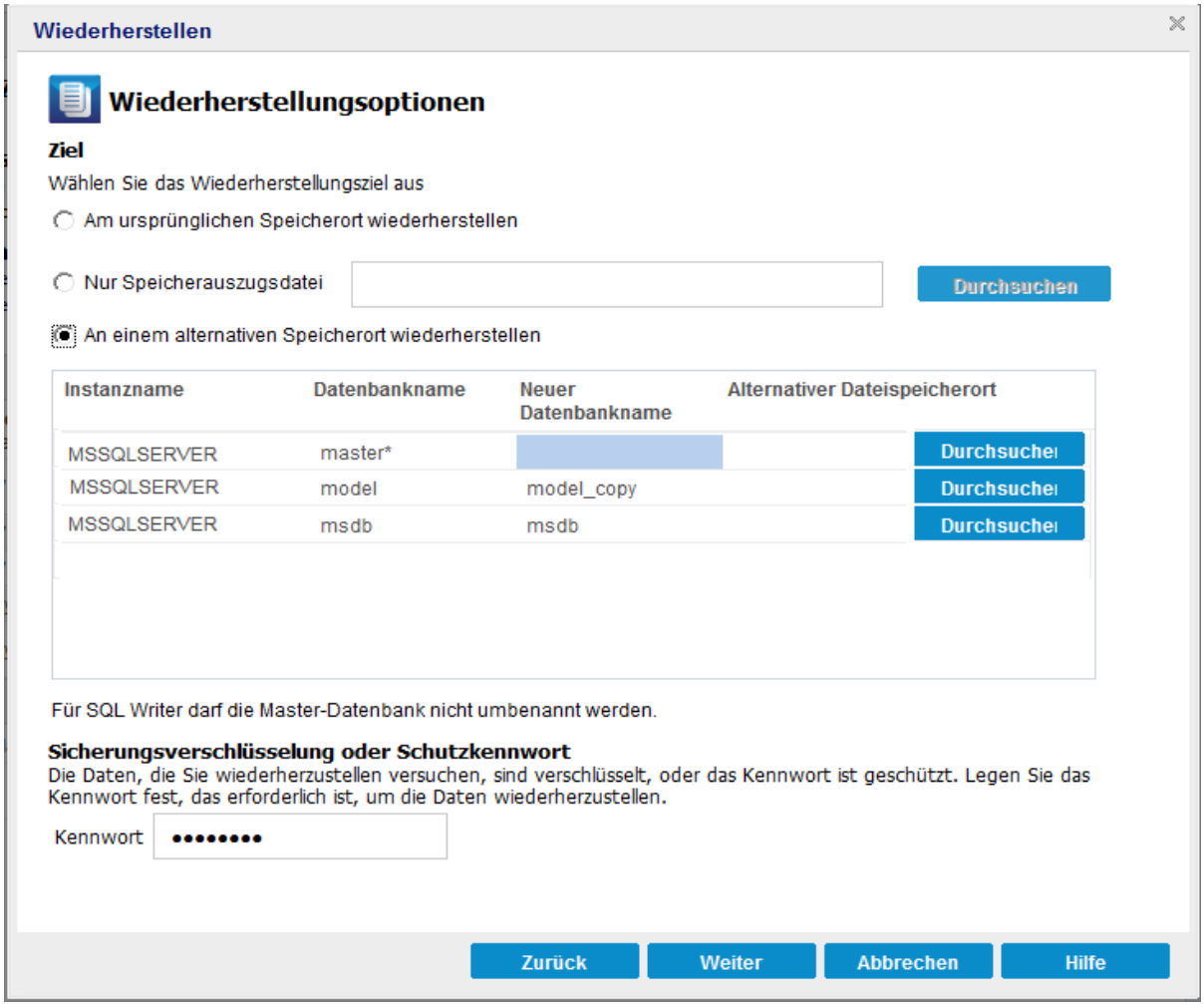
   Das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet.

Definieren der Wiederherstellungsoptionen

Nachdem Sie Wiederherstellungspunkt und wiederherzustellenden Inhalt festgelegt haben, definieren Sie die Kopieroptionen für den ausgewählten Wiederherstellungspunkt.

Gehen Sie wie folgt vor:

1. Geben Sie das Wiederherstellungsziel im Dialogfeld **Wiederherstellungsoptionen** an.



2. Wählen Sie das Ziel für die Wiederherstellung aus.

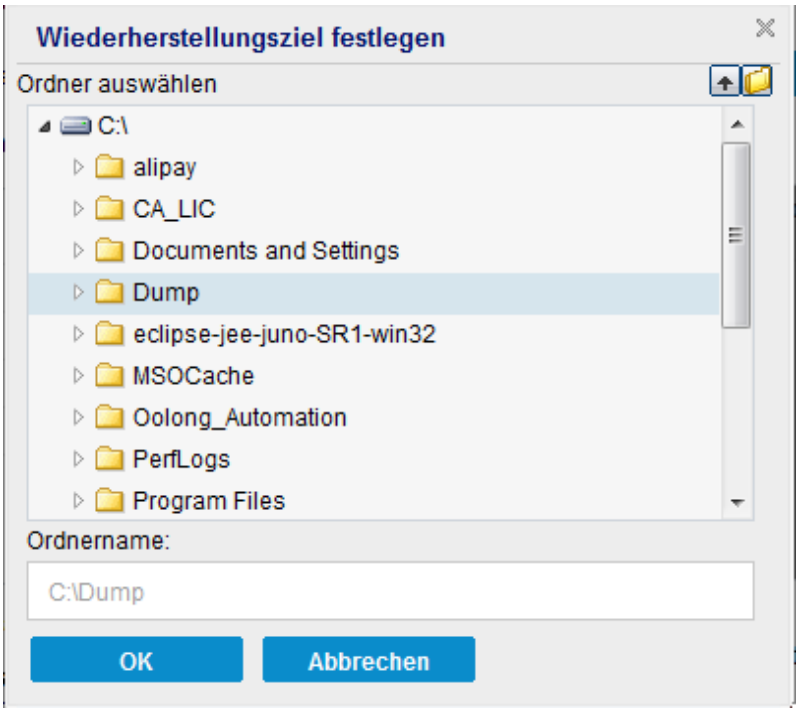
   Es stehen Optionen zur Wiederherstellung am ursprünglichen Speicherort, zur ausschließlichen Wiederherstellung der Sicherungsdatei oder zur Wiederherstellung an einem alternativen Speicherort zur Verfügung.

   Am ursprünglichen Speicherort wiederherstellen

   Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

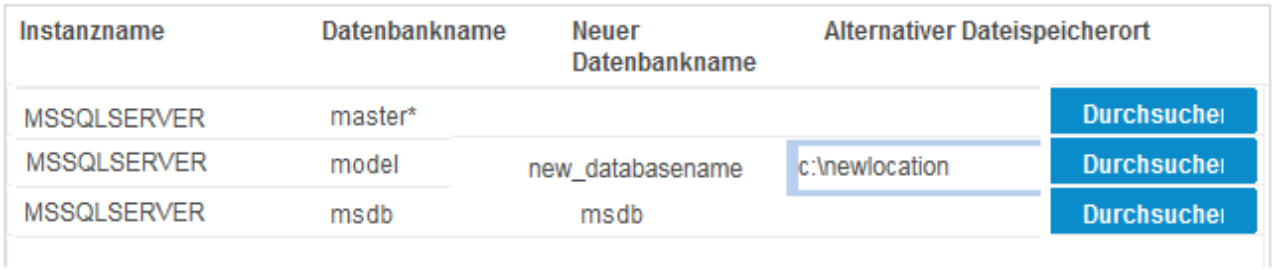
   Nur Speicherauszugsdatei

   Für diese Option erstellt Arcserve UDP Agent (Windows) im angegebenen Ordner einen Speicherauszug der ausgewählten Microsoft SQL-Datenbankdateien. Wenn diese Option ausgewählt ist, können Sie den Ordner, in dem die Speicherauszugsdatei wiederhergestellt wird, festlegen oder das System danach durchsuchen.



   An einem alternativen Speicherort wiederherstellen

   Stellt an einem alternativen Speicherort wieder her (nicht am ursprünglichen Speicherort).



Sicherungen können zum Netzwerkspeicherort kopiert und von mehreren SQL Server-Instanzen verwendet werden. Sie können mehrere Datenbanken gleichzeitig auf Instanzebene wiederherstellen. Sie können aus dieser Liste die Datenbankinstanz auswählen und einen neuen Datenbanknamen sowie einen alternativen Speicherort für ihre Wiederherstellung angeben. Zusätzlich können Sie das System nach dem alternativen Speicherort für die Wiederherstellung durchsuchen.

Das Wiederherstellen von Microsoft SQL Server-Anwendungen an einem alternativen Speicherort unterliegt bestimmten Beschränkungen, die Sie berücksichtigen sollten. Weitere Informationen finden Sie im Abschnitt **Wiederherstellen von Microsoft SQL Server-Anwendungen an einem alternativen Speicherort** unter dem Thema Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise.

3. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsübersicht** wird geöffnet.

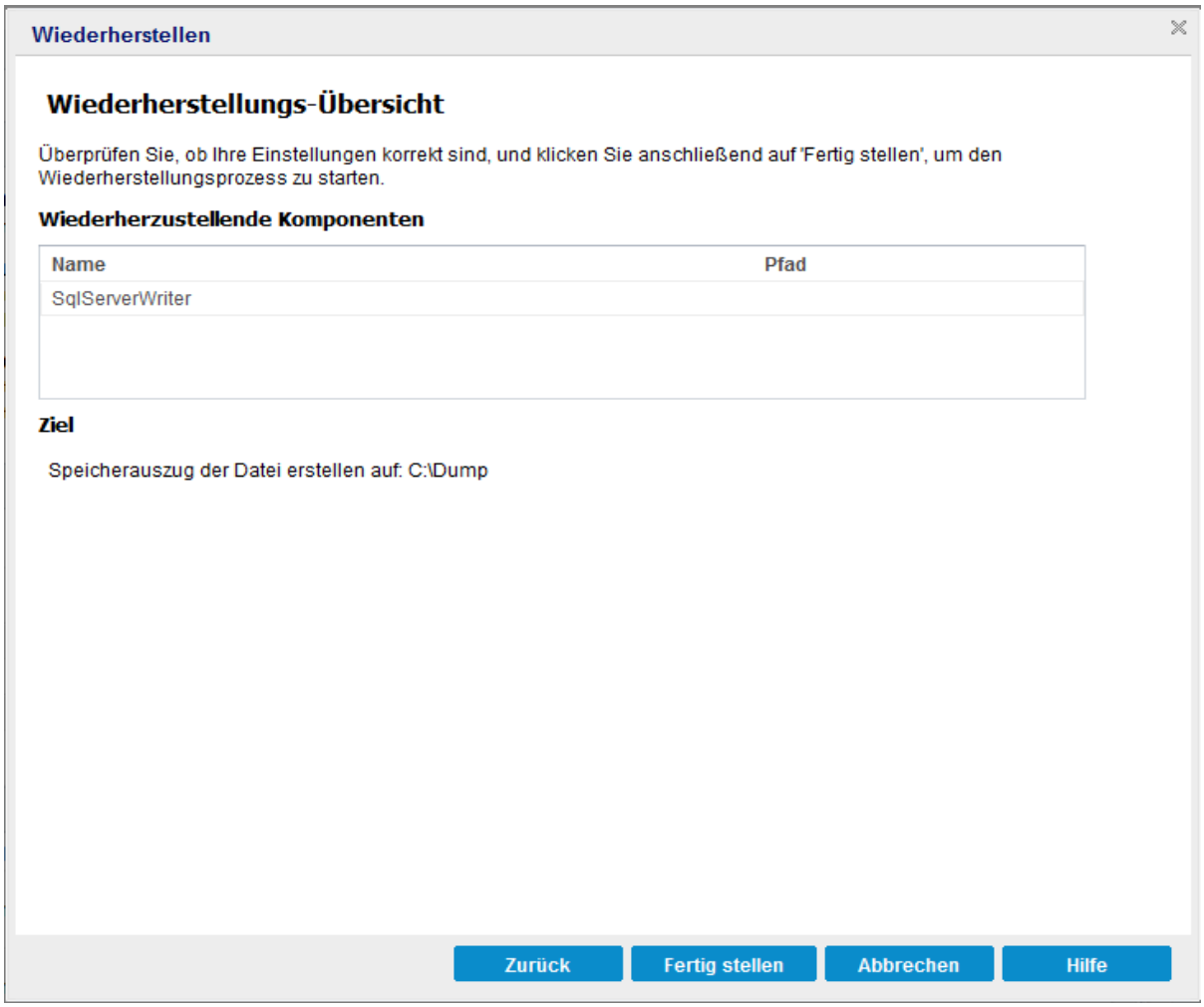
Wiederherstellen der Microsoft SQL Server-Anwendung

Nachdem Sie die Wiederherstellungsoptionen definiert haben, überprüfen Sie, dass Ihre Einstellungen korrekt sind, und bestätigen Sie den Wiederherstellungsprozess. Die **Wiederherstellungsübersicht** ist hilfreich, um sämtliche Wiederherstellungsoptionen, die Sie festgelegt haben, zu überprüfen und bei Bedarf zu ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die angezeigten Informationen im Dialogfeld **Wiederherstellungsübersicht**, um die Richtigkeit aller Wiederherstellungsoptionen und

Einstellungen sicherzustellen.



- Wenn die Übersichtsinformationen nicht korrekt sind, klicken Sie auf **Zurück**, und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsprozess zu starten.

Die Microsoft SQL Server-Anwendung ist wiederhergestellt.

Überprüfen, ob die Microsoft SQL Server-Anwendung wiederhergestellt wurde

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Arcserve UDP Agent (Windows)-Wiederherstellungsziel, das Sie angegeben haben.

   Wenn Sie beispielsweise ausgewählt haben, dass die Microsoft SQL Server-Datenbank am ursprünglichen Speicherort wiederhergestellt werden soll, überprüfen Sie nach Abschluss der Wiederherstellung am physischen Speicherort, ob die Microsoft SQL Server-Datenbank und die Protokolle wiederhergestellt wurden.

   Wenn Sie auswählen, dass die Microsoft SQL-Datenbank nur am Speicherort der Speicherauszugsdatei wiederhergestellt werden soll, stellt Arcserve UDP Agent (Windows) die Microsoft SQL-Datenbank und die Protokolle an einem angegebenen Speicherort wieder her.

2. Überprüfen Sie, ob die Microsoft SQL Server-Anwendung wiederhergestellt wurde und ob die Datenbank geladen und zugreifbar ist.

   Die Microsoft SQL Server-Anwendung ist erfolgreich wiederhergestellt.

Wiederherstellen von einem UNC/NFS-Pfad aus

Jedes Mal, wenn Arcserve UDP eine erfolgreiche UNC/NFS-Pfadsicherung ausführt, werden alle Dateien/Ordner gesichert, die nach dem letzten erfolgreichen Job geändert wurden. Diese Wiederherstellungsmethode ermöglicht es Ihnen, sich die archivierten Dateien/Ordner anzuschauen und genau anzugeben, welche Datei Sie wiederherstellen möchten.

Führen Sie die folgenden Aufgaben aus, um von einem Wiederherstellungspunkt aus wiederherzustellen:

1. Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise
2. Angeben der wiederherzustellenden Dateien/Verzeichnisse in einem UNC/NFS-Pfad
    a. Angeben der wiederherzustellenden Dateien und Inhalte
    b. Definieren der Wiederherstellungsoptionen
3. Wiederherstellen des Dateien und Inhalte
4. Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Wiederherstellung ausführen:

- Sie haben mindestens einen Wiederherstellungspunkt zur Wiederherstellung zur Verfügung.
- Sie haben ein gültiges und zugreifbares Wiederherstellungspunktziel, von dem aus Sie den Inhalt des Wiederherstellungspunkts wiederherstellen können.
- Sie haben einen gültigen und zugreifbaren Zielspeicherort, auf dem Sie den Inhalt des Wiederherstellungspunkts wiederherstellen können.

Angeben der UNC/NFS-Pfad-Informationen, die wiederhergestellt werden sollen

Arcserve UDP bietet eine Option, Daten von einem UNC/NFS-Pfad aus wiederherzustellen. Das Ziel eines Wiederherstellungsjobs besteht darin, schnell zu erkennen, welche Daten benötigt werden, und sie vom entsprechenden Sicherungsdatenträger abzurufen. Für jeden Wiederherstellungsjob ist eine Quelle und ein Ziel erforderlich.

Der Prozess für das Wiederherstellen von einem UNC/NFS-Pfad aus verläuft folgendermaßen:

1. Angeben der wiederherzustellenden Dateien/Ordner und Inhalte
2. Definieren der Wiederherstellungsoptionen

Angeben der wiederherzustellenden UNC/NFS-Dateien/-Ordner und -Inhalte

Dieser Abschnitt enthält Informationen über die Vorgehensweise zum Angeben der UNC/NFS-Dateien/Ordner und des wiederherzustellenden Inhalts.

Gehen Sie wie folgt vor:

1. Verwenden Sie eines der folgenden Verfahren, um auf das Dialogfeld zur Auswahl der Wiederherstellungsmethoden zuzugreifen:

   Über die Arcserve UDP-Konsole:

   a. Melden Sie sich bei der Arcserve UDP-Konsole an.

   b. Navigieren Sie zu **Ressourcen** > **Knoten** > **Alle Knoten**.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   c. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie dann **Wiederherstellen** aus.

      Sie werden automatisch bei der Konsole des Agentenknotens angemeldet, und das Dialogfeld "Wiederherstellen" wird geöffnet.

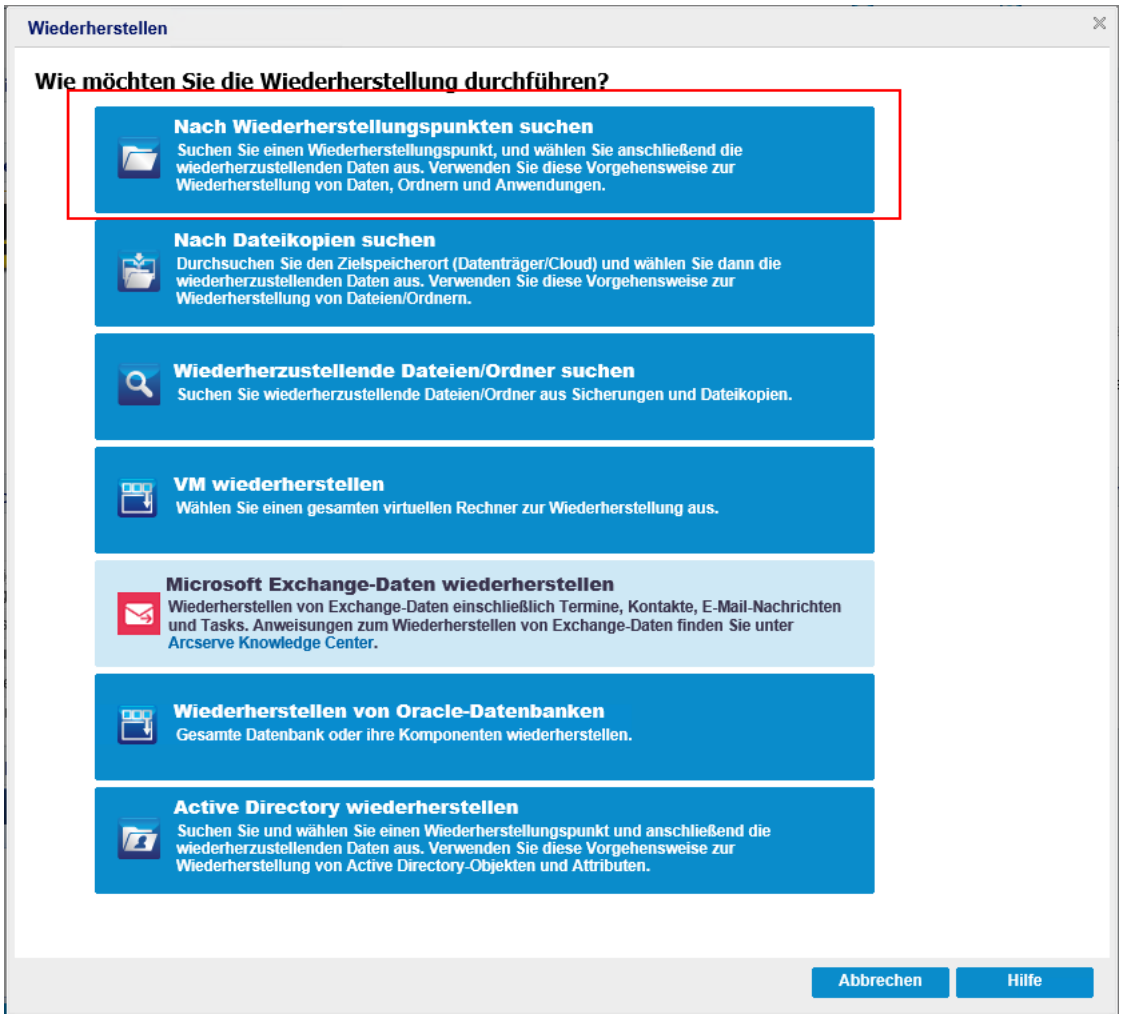
   In Arcserve UDP Agent (Windows):

   a. Melden Sie sich bei Arcserve UDP Agent (Windows) an.

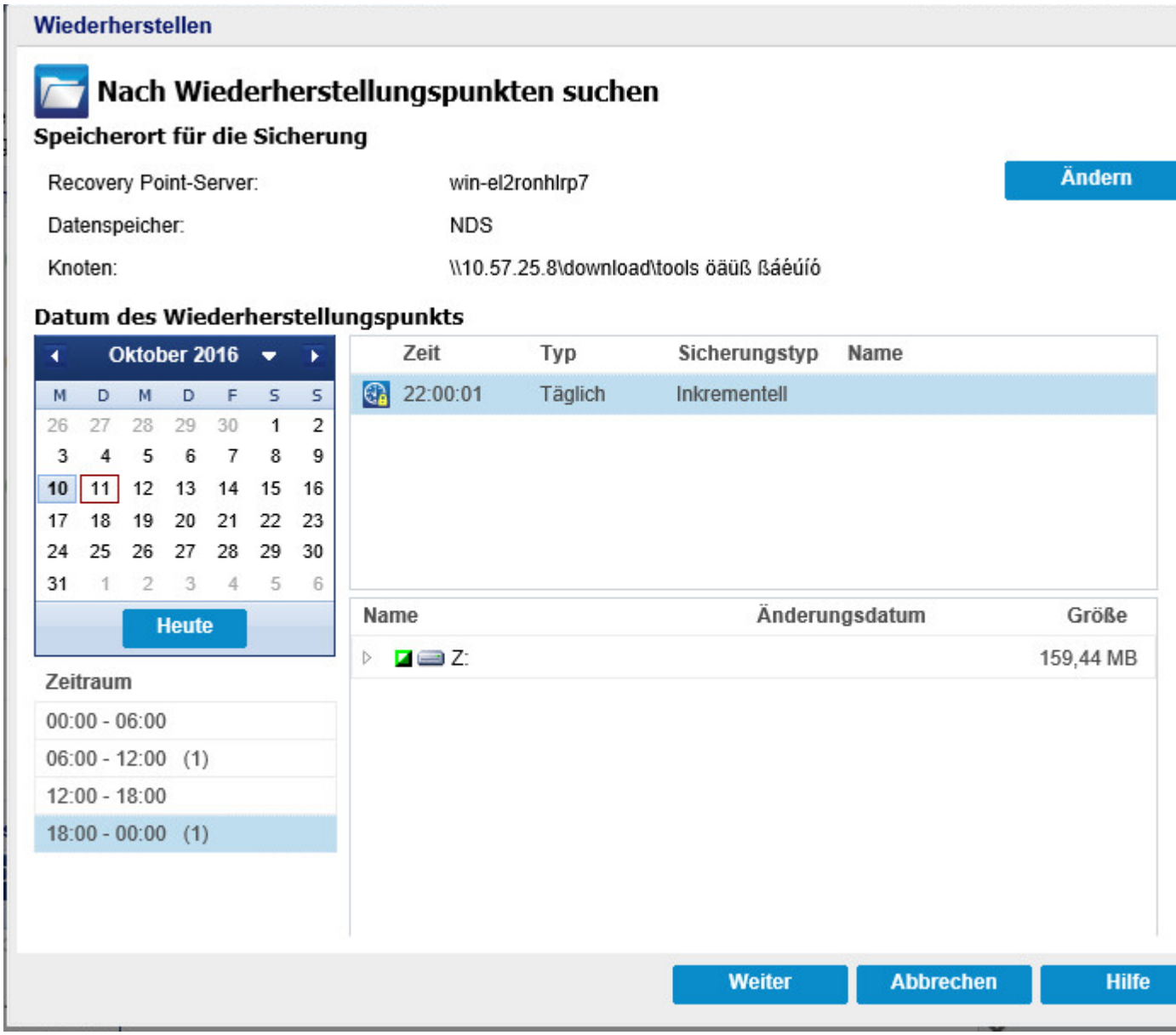
   b. Wählen Sie auf der Startseite **Wiederherstellen** aus.

      Das Dialogfeld Wiederherstellen wird geöffnet.

2. Klicken Sie im Dialogfeld "Wiederherstellen" auf **Nach Wiederherstellungspunkten suchen**.



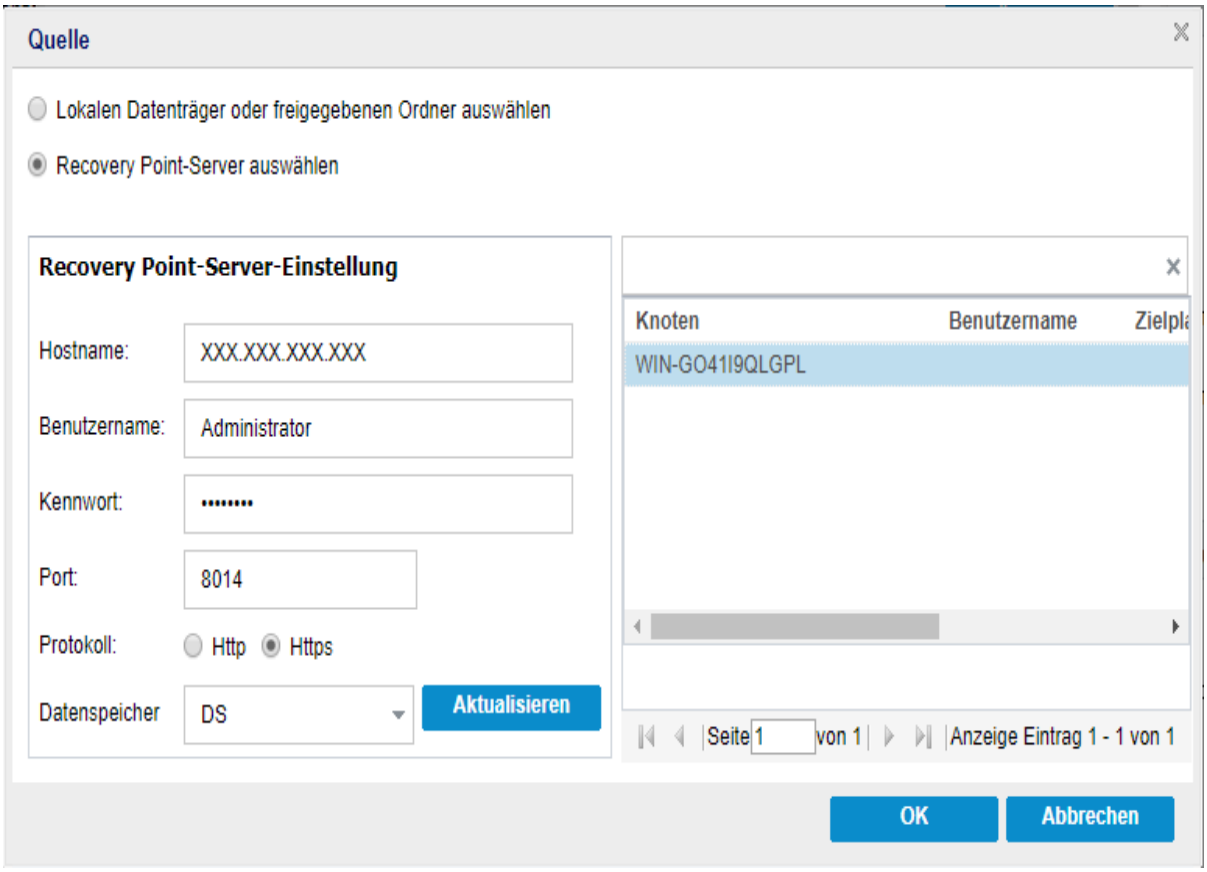
3. Gehen Sie auf der Seite "Nach Wiederherstellungspunkten suchen" folgendermaßen vor:



a. Klicken Sie auf **Ändern**, um den Speicherort für die Sicherung zu aktualisieren.

   Das Dialogfeld Quelle wird geöffnet.

b. Wählen Sie im Dialogfeld "Quelle" einen der folgenden Speicherorte für die Sicherung aus, und klicken Sie dann auf **OK**:



Lokalen Datenträger oder freigegebenen Ordner auswählen

1. Legen Sie den Speicherort fest, unter dem Ihre Sicherungs-Images gespeichert werden, und wählen Sie die entsprechende Sicherungsquelle aus.
2. Um die Verbindung zum angegebenen Speicherort zu überprüfen, klicken Sie auf die Schaltfläche mit dem grünen Pfeil. Falls erforderlich, geben Sie den Benutzernamen und das Kennwort für den Zugriff auf diesen Quellspeicherort ein.

   Das Dialogfeld "Speicherort für die Sicherung auswählen" wird geöffnet.
3. Wählen Sie den Ordner aus, in dem die Wiederherstellungspunkte gespeichert sind, und klicken Sie dann auf **OK**.

   Das Dialogfeld "Speicherort für die Sicherung auswählen" wird geschlossen, und der Sicherungsspeicherort wird im Dialogfeld "Quelle" angezeigt.

   Die Wiederherstellungspunkte werden im Dialogfeld Nach Wiederherstellungspunkten suchen aufgelistet.

Auswählen des Recovery Point-Servers

1. Geben Sie die Details für die Einstellungen des Recovery Point Servers an, und klicken Sie dann auf **Aktualisieren**.

   Alle Agenten werden in der Spalte "Data Protection Agent" im Dialogfeld Quelle aufgelistet.

2. Wählen Sie den Agenten in der angezeigten Liste aus.

   Die Wiederherstellungspunkte werden im Dialogfeld "Nach Wiederherstellungspunkten suchen" aufgelistet.

c. Geben Sie das Datum des Sicherungs-Images an, das Sie wiederherstellen möchten.

   Alle Daten, die Wiederherstellungspunkte für die angegebene Sicherungsquelle enthalten, werden grün hervorgehoben.

   Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp (vollständige Sicherung, Zuwachssicherung oder Überprüfungssicherung) und der Name der Sicherung angezeigt.

d. Wählen Sie einen wiederherzustellenden Wiederherstellungspunkt aus.

   Der Sicherungsinhalt (einschließlich aller Anwendungen) für die ausgewählten Wiederherstellungspunkte wird angezeigt.

   Hinweis: Wenn eine Uhr mit einem Schlosssymbol angezeigt wird, bedeutet dies, dass der Wiederherstellungspunkt verschlüsselte Informationen enthält und möglicherweise ein Kennwort zur Wiederherstellung benötigt wird.

e. Wählen Sie den wiederherzustellenden Inhalt aus.

   - Bei einer Wiederherstellung auf Volume-Ebene können Sie angeben, ob das gesamte Volume oder ausgewählte Dateien/Ordner wiederhergestellt werden sollen.
   - Bei einer Wiederherstellung auf Anwendungsebene können Sie festlegen, ob die gesamte Anwendung, oder ausgewählte Komponenten, Datenbanken, Instanzen etc. wiederhergestellt werden sollen.

4. Klicken Sie auf **Weiter**.

   Das Dialogfeld Wiederherstellungsoptionen wird geöffnet.

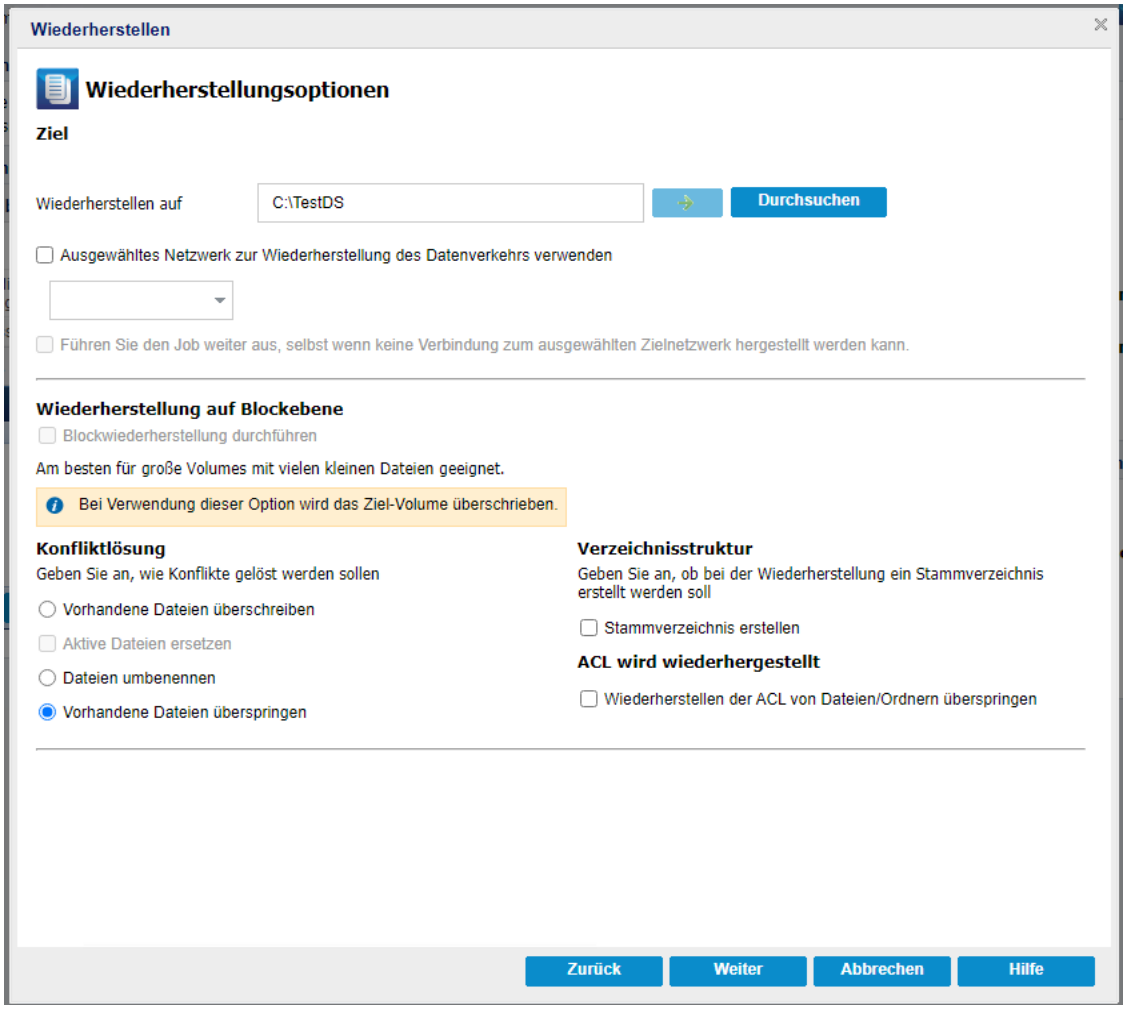
   Wiederherstellungspunkt und wiederherzustellender Inhalt werden festgelegt.

Definieren der Wiederherstellungsoptionen

Nachdem Sie Wiederherstellungspunkt und wiederherzustellenden Inhalt festgelegt haben, definieren Sie die Kopieroptionen für den ausgewählten Wiederherstellungspunkt.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld Wiederherstellungsoptionen das Wiederherstellungsziel aus.



Verfügbare Zieloption:

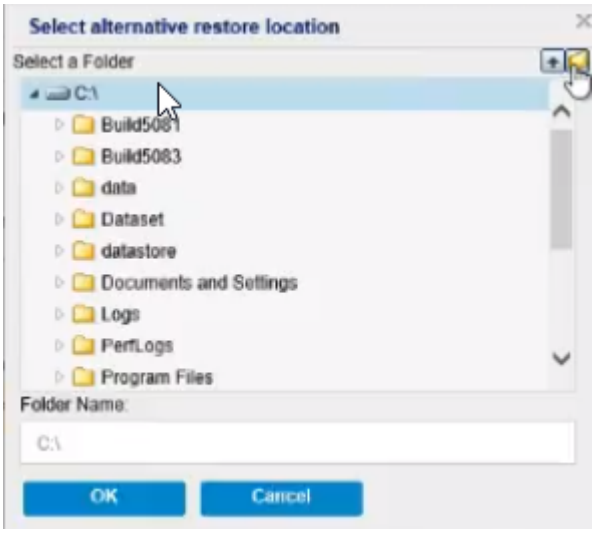
Wiederherstellen auf

Stellt am angegebenen Speicherort wieder her. Gehen Sie folgendermaßen vor, um die Daten am angegebenen Speicherort wiederherzustellen:

a. Klicken Sie auf **Durchsuchen**, um das Ziel anzugeben.

   Das Dialogfeld "Alternativen Wiederherstellungsort auswählen" wird angezeigt.

b. Wählen Sie den vorhandenen Ordner aus, oder erstellen Sie einen neuen Ordner nach Bedarf, und klicken Sie dann auf **OK**.



c. Um die Verbindung zum angegebenen Speicherort zu überprüfen, klicken Sie auf die Schaltfläche mit dem grünen Pfeil. Falls erforderlich, geben Sie den Benutzernamen und das Kennwort ein, um Zugriff auf diesen Speicherort zu erhalten.

Hinweis: Wiederherstellung auf NFS-Freigabe aus einem NFS-Schutzplan ist nicht zulässig.

2. Um die Kommunikation zwischen dem ausgewählten Netzwerk und dem Recovery Point Server zu ermöglichen, aktivieren Sie das Kontrollkästchen **Ausgewähltes Netzwerk zur Wiederherstellung des Datenverkehrs verwenden**, und wählen Sie dann das Netzwerk in der Drop-down-Liste aus.

   Hinweis: Um den Sicherungsjob mit dem verfügbaren Netzwerk oder dem Standardnetzwerk fortzusetzen, falls das ausgewählte Sicherungsnetzwerk nicht zugänglich ist, aktivieren Sie das Kontrollkästchen **Führen Sie den Job weiter aus, selbst wenn keine Verbindung zum ausgewählten Sicherungsnetzwerk hergestellt werden kann**.

3. Legen Sie die Option für die **Konfliktlösung** fest, die von Arcserve UDP ausgeführt werden soll, wenn während der Wiederherstellung Konflikte auftreten.

   Es sind folgende Optionen verfügbar:

   Vorhandene Dateien überschreiben

Überschreibt (ersetzt) alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind. Alle Objekte werden aus den Sicherungsdateien wiederhergestellt, unabhängig davon, ob sie auf Ihrem Rechner vorhanden sind.

Aktive Dateien ersetzen

Ersetzt alle aktiven Dateien nach einem Neustart. Wenn Arcserve UDP Agent (Windows) während eines Wiederherstellungsversuchs entdeckt, dass die vorhandene Datei gerade verwendet wird oder gerade auf sie zugegriffen wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

Diese Option ist nur verfügbar, wenn Sie die Option **Vorhandene Dateien überschreiben** auswählen.

Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien im Wiederherstellungsprozess übersprungen.

Dateien umbenennen

Erstellt eine neue Datei, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit demselben Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten sind dann in einer neuen Datei wiederhergestellt.

Vorhandene Dateien überspringen

Überspringt alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, und überschreibt (ersetzt) sie nicht. Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

Standard: Vorhandene Dateien überspringen

4. Um während der Wiederherstellung ein Stammverzeichnis zu erstellen, geben Sie die **Verzeichnisstruktur** an.

Stammverzeichnis erstellen

Legt fest, dass Arcserve UDP eine ggf. vorhandene Stammverzeichnisstruktur des erfassten Sicherungs-Images im Zielpfad der Wiederherstellung neu erstellt.

Wenn diese Option nicht ausgewählt wird, wird die Datei oder der Ordner direkt im Zielordner wiederhergestellt.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt" und "C:\Ordner1\Unterordner2\B.txt" erfasst und als Wiederherstellungsziel "D:\Wiederherstellen" ausgewählt.

- Wenn Sie die Wiederherstellung der Dateien "A.txt" und "B.txt" einzeln festgelegt haben, werden die Dateien in "D:\Wiederherstellen\A.txt" und "D:\Wiederherstellen\B.txt" wiederhergestellt (das Stammverzeichnis über der ausgewählten Dateiebene wird nicht wiederhergestellt).
- Wenn Sie eine Wiederherstellung auf "Unterordner2"-Ebene auswählen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Unterordner2\A.txt" und "D:\Wiederherstellen\Unterordner2\B.txt" (das Stammverzeichnis über der ausgewählten Ordnerebene wird nicht wiederhergestellt).

Wenn diese Option ausgewählt ist, wird der gesamte Stammverzeichnispfad für die Dateien/Ordner (einschließlich des Volume-Namens) im Zielordner neu erstellt. Wenn Dateien/Ordner vom selben Volume-Name wiederhergestellt werden sollen, ist dieser Volume-Name nicht im Wiederherstellungsziel-Stammverzeichnispfad enthalten. Wenn Dateien/Ordner von einem anderen Volume-Name wiederhergestellt werden sollen, enthält der Wiederherstellungsziel-Stammverzeichnispfad diesen Volume-Namen.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt", "C:\Ordner1\Unterordner2\B.txt" und E:\Ordner3\Unterordner4\C.txt erfasst, und bei der Wiederherstellung "D:\Wiederherstellen" als Wiederherstellungsziel ausgewählt.

- Wenn Sie nur die Datei "A.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Ordner1\Unterordner2\A.txt" (das gesamte Stammverzeichnis wird ohne den Volume-Namen erneut erstellt).
- Wenn Sie die Dateien "A.txt" und "C.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\C\Ordner1\Unterordner2\A.txt" und "D:\Wiederherstellen\ E\Ordner3\Unterordner4\C.txt" (das gesamte Stammverzeichnis wird mit dem Volume-Namen erneut erstellt).

5. Geben Sie an, ob Sie möchten, dass die wiederherstellende Zugriffssteuerungsliste das Wiederherstellen von Zugriffssteuerungslisten von Dateien/Ordnern überspringen soll.

   Wenn die Option aktiviert ist, dass die Wiederherstellung von Zugriffssteuerungslisten von Dateien/Ordnern übersprungen wird , werden nur Quelldateien/-ordner wiederhergestellt. Die Attribute von Dateien/Ordnern werden nicht wiederhergestellt, sodass jeder Zugriff hat.

   Standard: Quelldateien/-ordner werden mit dem Attribut wiederhergestellt – Zugriffssteuerungsliste.

6. Wenn die Daten, die Sie wiederherstellen möchten, verschlüsselt sind, geben Sie bei Bedarf das **Verschlüsselungskennwort der Sicherung** an.

   Es ist kein Kennwort erforderlich, wenn Sie versuchen, die Wiederherstellung über denselben Arcserve UDP Agent (Windows)-Rechner durchzuführen, auf dem die verschlüsselte Sicherung ausgeführt wurde. Wenn Sie jedoch versuchen, die Wiederherstellung über einen anderen Arcserve UDP Agent (Windows)-Rechner durchzuführen, ist ein Kennwort erforderlich.

   Hinweis: Wenn eine Uhr mit einem Schlosssymbol angezeigt wird, bedeutet dies, dass der Wiederherstellungspunkt verschlüsselte Informationen enthält und möglicherweise ein Kennwort zur Wiederherstellung benötigt wird.

7. Klicken Sie auf **Weiter**.

   Das Dialogfeld Wiederherstellungsübersicht wird geöffnet.

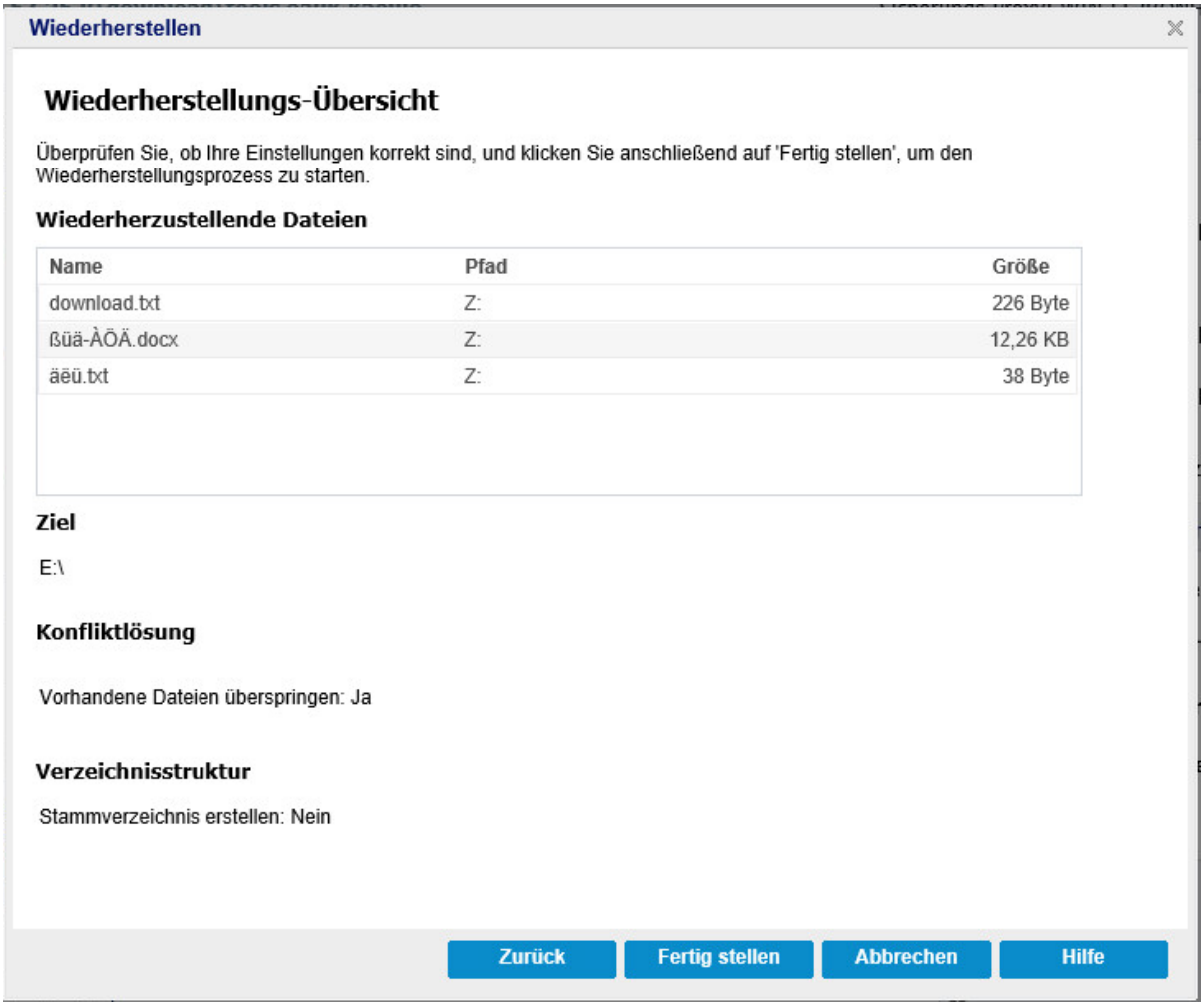
   Die Wiederherstellungsoptionen sind für die Wiederherstellung von einem Wiederherstellungspunkt aus festgelegt.

Wiederherstellen der unter dem UNC/NFS-Pfad gespeicherten Dateien/Ordner und Inhalte

Nachdem Sie die Wiederherstellungsoptionen definiert haben, überprüfen Sie, dass Ihre Einstellungen korrekt sind, und bestätigen Sie den Wiederherstellungsprozess. Die Seite "Wiederherstellungs-Übersicht" ist hilfreich, um sämtliche Wiederherstellungsoptionen, die Sie festgelegt haben, zu überprüfen und bei Bedarf zu ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Informationen im Dialogfeld Wiederherstellungsübersicht, um die Richtigkeit aller Wiederherstellungsoptionen und Einstellungen sicherzustellen.



2. Wählen Sie eine der folgenden Vorgehensweisen:
   - Wenn die Übersichtsinformationen Fehler enthalten, klicken Sie auf **Zurück**, und ändern Sie die inkorrekten Einstellungen im entsprechenden Dialogfeld.

- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsprozess zu starten.

Der Wiederherstellungspunktinhalt wurde wiederhergestellt.

Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen Sie nach Abschluss des Wiederherstellungsjobs, dass alle Dateien im Zielknoten wiederhergestellt wurden. Überprüfen Sie die Registerkarten "**Jobübersicht**" und "**Aktivitätsprotokoll**" im Fenster "Status", um den Fortschritt des Wiederherstellungsprozesses zu überwachen.

Gehen Sie wie folgt vor:

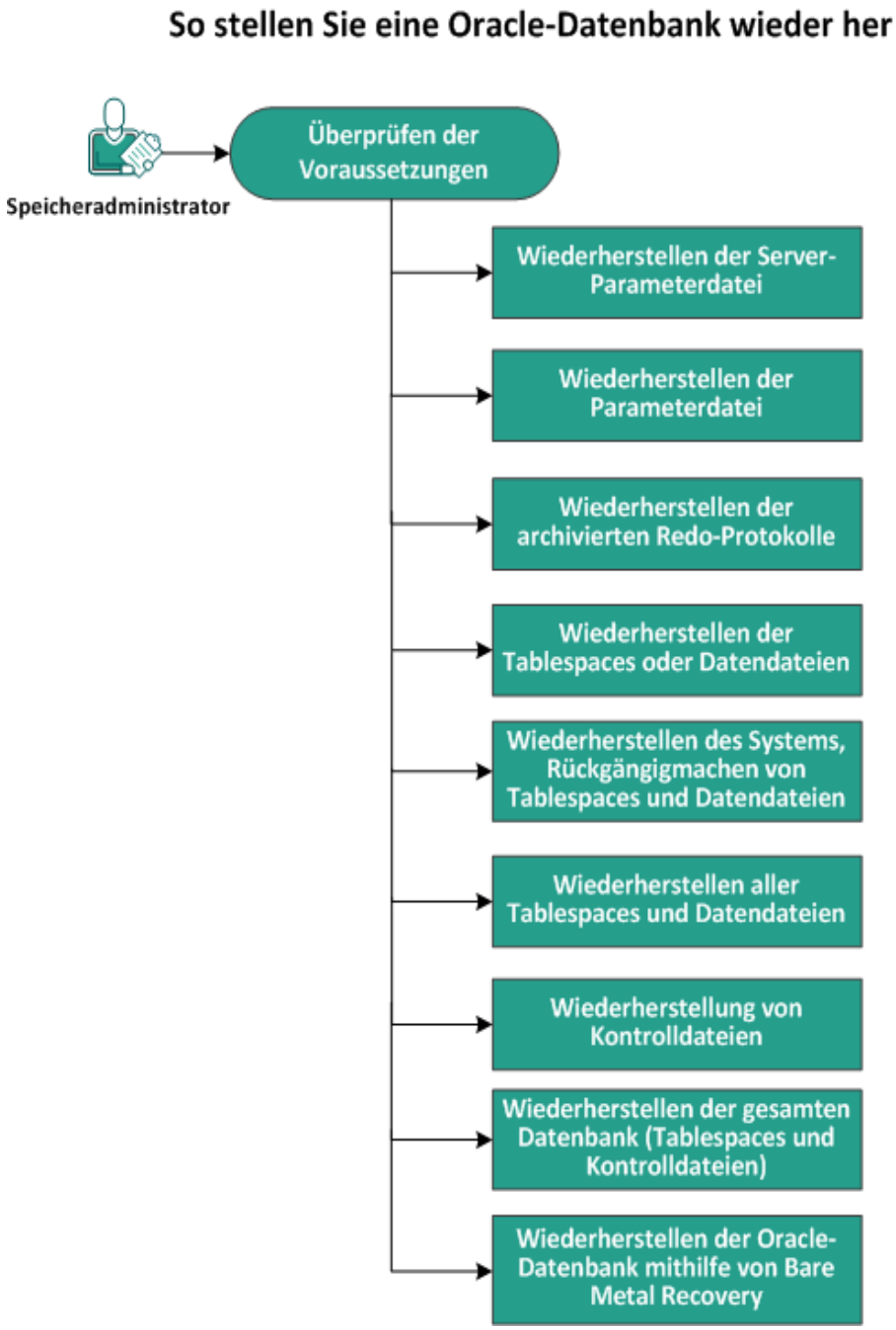
1. Navigieren Sie zu dem Zielcomputer, auf dem Sie die Daten wiederhergestellt haben.
2. Überprüfen Sie, dass die erforderlichen Daten vom Wiederherstellungspunkt wiederhergestellt wurden.

   Der wiederhergestellte Inhalt wurde erfolgreich überprüft.

Wiederherstellen von Oracle-Datenbanken

Sie können bestimmte Dateien und Tablespaces oder die gesamte Oracle-Datenbank mithilfe des Wiederherstellungs-Assistenten wiederherstellen. Um eine Oracle-Datenbank wiederherzustellen, suchen Sie die Dateien oder Tablespaces auf dem Zielknoten. Dann stellen Sie die Dateien oder das Tablespace mithilfe des Wiederherstellungs-Assistenten wieder her.

Das folgende Diagramm veranschaulicht den Prozess zum Wiederherstellen einer Oracle-Datenbank:



Führen Sie folgende Aufgaben aus, um eine Oracle-Datenbank wiederherzustellen:

- Überprüfen der Voraussetzungen
- Wiederherstellen der Server-Parameterdatei
- Wiederherstellen der Parameterdatei
- Wiederherstellen der archivierten Redo-Protokolle
- Wiederherstellen der Tablespaces oder Datendateien
- Wiederherstellen des Systems, Rückgängigmachen von Tablespaces und Datendateien
- Wiederherstellen aller Tablespaces und Datendateien
- Wiederherstellung von Kontrolldateien
- Wiederherstellen der gesamten Datenbank (Tablespaces und Kontrolldateien)
- Wiederherstellen der Oracle-Datenbank mithilfe von Bare Metal Recovery

Überprüfen der Voraussetzungen und Hinweise

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie die Oracle-Datenbank wiederherstellen:

- Der Oracle VSS-Writer auf dem Sicherungsknoten funktioniert ordnungsgemäß. Wenn der Oracle VSS-Writer nicht ordnungsgemäß funktioniert, dann erhalten Sie einen Warnhinweis im Aktivitätsprotokoll, der mit dem Sicherungsjob verknüpft ist.
- Sie haben einen gültigen Wiederherstellungspunkt.
- Um Wiederherstellungsfehler zu vermeiden, haben Sie ein Duplikat Ihrer Systemdateien gespeichert, bevor Sie die ursprünglichen Dateien überschreiben.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Wiederherstellen der Server-Parameterdatei

Die Server-Parameterdatei ist ein Repository für Initialisierungsparameter. Bevor Sie eine Wiederherstellung durchführen, müssen Sie die Datei suchen. Wenn Sie die Dateien finden, stellen Sie sicher, dass die Datenbank im Status "Öffnen" ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, auf dem Sie die Dateien wiederherstellen möchten.
2. Suchen Sie die Server-Parameterdatei mithilfe des folgenden Befehls:

   SQL> SHOW PARAMETER SPFILE;
3. Fahren Sie die Datenbank oder die Oracle-Instanz herunter, bevor Sie mit dem Wiederherstellungsvorgang beginnen:

   SQL> SHUTDOWN IMMEDIATE;
4. Melden Sie sich bei der Arcserve UDP-Konsole an.
5. Stellen Sie die Server-Parameterdatei mithilfe des Wiederherstellungsassistenten wieder her. Weitere Informationen zum Wiederherstellungsvorgang finden Sie unter "So führen Sie eine Wiederherstellung von einem Wiederherstellungspunkt aus".
6. Melden Sie sich beim Sicherungscomputer an.
7. Navigieren Sie zu den bestimmten Ordnern, und überprüfen Sie, ob die Dateien wiederhergestellt wurden.
8. Stellen Sie eine Verbindung mit SQL*Plus her, um die Oracle-Instanz mit der wiederhergestellten Server-Parameterdatei neu zu starten.

   Die Server-Parameterdatei ist wiederhergestellt.

Wiederherstellen der Parameterdatei

Die Parameterdatei enthält eine Liste der Initialisierungsparameter und Werte für alle Parameter. Bevor Sie eine Wiederherstellung durchführen, müssen Sie die Datei suchen. Wenn Sie die Dateien finden, stellen Sie sicher, dass die Datenbank im Status "Öffnen" ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, auf dem Sie die Dateien wiederherstellen möchten.
2. Suchen Sie die Parameterdatei (pfile).

   Normalerweise befindet sich die Datei "pfile" (INIT<SID>.ORA) im "%ORACLE_HOME/database"-Verzeichnis. Sie können "INIT<SID>.ORA" eingeben, um die pfile-Datei zu finden.
3. Fahren Sie die Datenbank oder die Oracle-Instanz herunter, bevor Sie mit dem Wiederherstellungsvorgang beginnen:

   SQL> SHUTDOWN IMMEDIATE;
4. Melden Sie sich bei der Arcserve UDP-Konsole an.
5. Stellen Sie die Parameterdatei mithilfe des Wiederherstellungsassistenten wieder her. Weitere Informationen zum Wiederherstellungsvorgang finden Sie unter "So führen Sie eine Wiederherstellung von einem Wiederherstellungspunkt aus".
6. Melden Sie sich beim Sicherungscomputer an.
7. Navigieren Sie zu den bestimmten Ordnern, und überprüfen Sie, ob die Dateien wiederhergestellt wurden.
8. Stellen Sie eine Verbindung mit SQL*Plus her, um die Oracle-Instanz mit der wiederhergestellten Parameterdatei neu zu starten.

   Die Parameterdatei ist wiederhergestellt.

Wiederherstellen der archivierten Redo-Protokolle

Archivierte Redo-Protokolle werden verwendet, um eine Datenbank wiederherzustellen oder um eine Standby-Datenbank zu aktualisieren. Bevor Sie eine Wiederherstellung durchführen, müssen Sie die Datei suchen. Wenn Sie die Dateien finden, stellen Sie sicher, dass die Datenbank im Status "Öffnen" ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, auf dem Sie die Dateien wiederherstellen möchten.
2. Suchen Sie die archivierten Redo-Protokolle mithilfe des folgenden Befehls.

   SQL> ARCHIVE LOG LIST;

   SQL> SHOW PARAMETER DB_RECOVERY_FILE_DEST;
3. Melden Sie sich bei der Arcserve UDP-Konsole an.
4. Stellen Sie die archivierten Redo-Protokolle mithilfe des Wiederherstellungsassistenten wieder her. Weitere Informationen zum Wiederherstellungsvorgang finden Sie unter "So führen Sie eine Wiederherstellung von einem Wiederherstellungspunkt aus".
5. Melden Sie sich beim Sicherungscomputer an.
6. Navigieren Sie zu den bestimmten Ordnern, und überprüfen Sie, ob die archivierten Redo-Protokolle wiederhergestellt wurden.

   Die archivierten Redo-Protokolle sind wiederhergestellt.

Wiederherstellen der Tablespaces oder Datendateien

Sie können den Tablespace oder die Datendateien wiederherstellen. Bevor Sie eine Wiederherstellung durchführen, müssen Sie die Datei suchen. Wenn Sie die Dateien finden, stellen Sie sicher, dass die Datenbank im Status "Öffnen" ist. Wenn die Datenbank offen ist, verwenden Sie "ALTER TABLESPACE". OFFLINE-Anweisung, um die Tablespaces oder Datendateien offline zu schalten, bevor Sie mit der Wiederherstellung beginnen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, auf dem Sie die Tablespaces oder Datendateien wiederherstellen möchten.
2. Suchen Sie die Benutzer-Tablespaces oder Datendateien mithilfe des folgenden Befehls:

   SQL> SELECT FILE_NAME, TABLESPACE_NAME FROM DBA_DATA_FILES;
3. Ändern Sie den Status der Datenbank auf "mount", "nomount" oder "shutdown", bevor Sie die Tablespaces oder Datendateien wiederherstellen.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Melden Sie sich bei der Arcserve UDP-Konsole an.
5. Stellen Sie die Tablespaces oder Datendateien mithilfe des Wiederherstellungsassistenten wieder her. Weitere Informationen zum Wiederherstellungsvorgang finden Sie unter "So führen Sie eine Wiederherstellung von einem Wiederherstellungspunkt aus".
6. Melden Sie sich beim Sicherungscomputer an.
7. Navigieren Sie zu den bestimmten Ordnern, und überprüfen Sie, ob die Tablespaces oder Datendateien wiederhergestellt wurden.
8. Stellen Sie den Tablespace oder die Datendateien wieder her.
   - Um einen Tablespace wiederherzustellen, geben Sie den folgenden Befehl in der SQL*Plus-Eingabeaufforderung ein:

     SQL> RECOVER TABLESPACE "tablespace_name";
   - Um eine Datendatei wiederherzustellen, geben Sie den folgenden Befehl in der SQL*Plus-Eingabeaufforderung ein:

     SQL> RECOVER DATAFILE 'path';

Oracle sucht nach den Archiv-Redo-Protokolldateien, die angewendet werden müssen, und die Namen der Dateien werden in einer Sequenz angezeigt.

9. Geben Sie AUTO in der SQL*Plus-Eingabeaufforderung ein, um die Dateien anzuwenden.

   Oracle verwendet die Protokolldateien, um Datendateien wiederherzustellen. Nachdem Oracle die Redo-Protokolldatei angewendet hat, werden folgende Meldungen angezeigt:

   Applying suggested logfile

   Log applied

   Oracle wendet die Redo-Protokolldateien nacheinander an, bis das Recovery vollständig ist.

10. Geben Sie folgenden Befehl ein, um den Tablespace online zu stellen:

    SQL> ALTER TABLESPACE "Name_des_Tablespace" ONLINE;

    Das Tablespace-Recovery wird nun bis zur letzten verfügbaren Protokolldatei durchgeführt.

Wiederherstellen des Systems oder Rückgängigmachen der Tablespaces oder Datendateien

Sie können ein System wiederherstellen, oder Sie können Tablespaces oder Datendateien rückgängig machen. Bevor Sie eine Wiederherstellung durchführen, müssen Sie die Datei suchen. Wenn Sie die Dateien finden, stellen Sie sicher, dass die Datenbank im Status "Öffnen" ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Computer an, wo Sie das System wiederherstellen oder die Tablespaces oder Datendateien rückgängig machen möchten.
2. Suchen Sie die Benutzer-Tablespaces oder Datendateien mithilfe des folgenden Befehls:

   SQL> SELECT TABLESPACE_NAME, FILE_NAME FROM DBA_DATA_FILES;
3. Ändern Sie den Status der Datenbank auf "mount", "nomount" oder "shutdown", bevor Sie die Tablespaces oder Datendateien wiederherstellen.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Melden Sie sich bei der Arcserve UDP-Konsole an.
5. Stellen Sie die Tablespaces oder Datendateien mithilfe des Wiederherstellungsassistenten wieder her. Weitere Informationen zum Wiederherstellungsvorgang finden Sie unter "So führen Sie eine Wiederherstellung von einem Wiederherstellungspunkt aus".
6. Melden Sie sich beim Zielcomputer an.
7. Navigieren Sie zu den bestimmten Ordnern, und überprüfen Sie, ob das System oder die Tablespaces oder Datendateien wiederhergestellt wurden.
8. Stellen Sie den Tablespace oder die Datendateien wieder her.
   - Um einen Tablespace wiederherzustellen, geben Sie den folgenden Befehl in der SQL*Plus-Eingabeaufforderung ein:

     SQL> RECOVER TABLESPACE "tablespace_name";
   - Um eine Datendatei wiederherzustellen, geben Sie den folgenden Befehl in der SQL*Plus-Eingabeaufforderung ein:

     SQL> RECOVER DATAFILE 'path';

Oracle sucht nach den Archiv-Redo-Protokolldateien, die angewendet werden müssen, und die Namen der Dateien werden in einer Sequenz angezeigt.

9. Geben Sie AUTO in der SQL*Plus-Eingabeaufforderung ein, um die Dateien anzuwenden.

   Oracle verwendet die Protokolldateien, um Datendateien wiederherzustellen. Nachdem Oracle die Redo-Protokolldatei angewendet hat, werden folgende Meldungen angezeigt:

   Applying suggested logfile

   Log applied

   Oracle wendet die Redo-Protokolldateien nacheinander an, bis das Recovery vollständig ist.

10. Geben Sie folgenden Befehl ein, um den Tablespace online zu stellen:

    SQL> ALTER TABLESPACE "Name_des_Tablespace" ONLINE;

    Das Tablespace-Recovery wird nun bis zur letzten verfügbaren Protokolldatei durchgeführt.

Wiederherstellen aller Tablespaces und Datendateien

Sie können alle Tablespaces und Datendateien wiederherstellen. Bevor Sie eine Wiederherstellung durchführen, müssen Sie die Datei suchen. Wenn Sie die Dateien finden, stellen Sie sicher, dass die Datenbank im Status "Öffnen" ist. Wenn die Datenbank offen ist, verwenden Sie "ALTER TABLESPACE". OFFLINE -Anweisung, um die Tablespaces oder Datendateien offline zu stellen, bevor Sie mit der Wiederherstellung beginnen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, auf dem Sie die Tablespaces oder Datendateien wiederherstellen möchten.
2. Suchen Sie die Benutzer-Tablespaces oder Datendateien mithilfe des folgenden Befehls:

   SQL> SELECT FILE_NAME, TABLESPACE_NAME FROM DBA_DATA_FILES;
3. Ändern Sie den Status der Datenbank auf "mount", "nomount" oder "shutdown", bevor Sie die Tablespaces oder Datendateien wiederherstellen.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Melden Sie sich bei der Arcserve UDP-Konsole an.
5. Stellen Sie die Tablespaces oder Datendateien mithilfe des Wiederherstellungsassistenten wieder her. Weitere Informationen zum Wiederherstellungsvorgang finden Sie unter So führen Sie eine Wiederherstellung von einem Wiederherstellungspunkt aus.
6. Melden Sie sich beim Sicherungscomputer an.
7. Navigieren Sie zu den bestimmten Ordnern, und überprüfen Sie, ob die Tablespaces oder Datendateien wiederhergestellt wurden.
8. Wiederherstellen der Datenbank.

   SQL> RECOVER DATABASE;

   Oracle sucht nach den Archiv-Redo-Protokolldateien, die angewendet werden müssen, und die Namen der Dateien werden in einer Sequenz angezeigt.
9. Geben Sie AUTO in der SQL*Plus-Eingabeaufforderung ein, um die Dateien anzuwenden.

Oracle verwendet die Protokolldateien, um Datendateien wiederherzustellen. Nachdem Oracle die Redo-Protokolldatei angewendet hat, werden folgende Meldungen angezeigt:

Applying suggested logfile

Log applied

Oracle wendet die Redo-Protokolldateien nacheinander an, bis das Recovery vollständig ist.

Hinweis: Wenn Oracle in einer Fehlermeldung angibt, dass die Protokolldatei nicht geöffnet werden kann, ist die Protokolldatei möglicherweise nicht verfügbar. Führen Sie in solchen Fällen die unvollständige Datenträgerwiederherstellung aus, um die Datenbank erneut wiederherzustellen. Sobald alle Protokolldateien angewendet wurden, ist das Datenbank-Recovery abgeschlossen. Weitere Informationen zur unvollständiger Datenträger-Recovery finden Sie in der Oracle-Dokumentation.

10. Geben Sie folgenden Befehl ein, um die Datenbank online zu stellen:

    SQL> ALTER DATABASE OPEN;

    Die Datenbank wird nun bis zur letzten verfügbaren Protokolldatei durchgeführt.

    Hinweis: Wenn Sie eine unvollständige Datenträgerwiederherstellung ausführen, geben Sie den folgenden Befehl ein, um die Datenbank in einen offenen Status zu ändern:

    SQL> ALTER DATABASE OPEN RESETLOGS;

Wiederherstellung von Kontrolldateien

Sie können die Kontrolldateien wiederherstellen, die die physische Struktur der Datenbank speichern. Bevor Sie eine Wiederherstellung durchführen, müssen Sie die Datei suchen. Wenn Sie die Dateien finden, stellen Sie sicher, dass die Datenbank im Status "Öffnen" ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, auf dem Sie die Kontrolldateien wiederherstellen möchten.
2. Suchen Sie die Kontrolldateien mithilfe des folgenden Befehls:

   SQL> SHOW PARAMETER CONTROL FILES;
3. Ändern Sie den Status der Datenbank auf "nomount" oder "shutdown", bevor Sie die Kontrolldateien wiederherstellen.

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Melden Sie sich bei der Arcserve UDP-Konsole an.
5. Stellen Sie die Kontrolldatei mithilfe des Wiederherstellungsassistenten wieder her. Weitere Informationen zum Wiederherstellungsvorgang finden Sie unter "So führen Sie eine Wiederherstellung von einem Wiederherstellungspunkt aus".
6. Melden Sie sich beim Sicherungscomputer an.
7. Navigieren Sie zu den bestimmten Ordnern, und überprüfen Sie, ob die Kontrolldateien wiederhergestellt wurden.
8. Laden Sie die Datenbank, um mit der Datenbankwiederherstellung zu beginnen:

   SQL> STARTUP MOUNT
9. Geben Sie den RECOVER-Befehl mit der USING BACKUP CONTROLFILE-Klausel ein.

   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE

   Der Recovery-Vorgang für die Datenbank beginnt.
10. (Optional) Geben Sie die UNTIL CANCEL-Klausel an, um eine unvollständige Wiederherstellung auszuführen.

    SQL> RECOVER DATABASE USING BACKUP CONTROLFILE UNTIL CANCEL
11. Wenden Sie die aufgeforderten archivierten Protokolle an.

    Hinweis: Wenn das erforderliche archivierte Protokoll fehlt, dann bedeutet dies, dass sich ein notwendiger Redo-Datensatz in den Online-Redo-Protokollen befindet. Dies tritt auf, weil sich unarchivierte Änderungen in den Online-Protokollen

befinden, als die Instanz fehlgeschlagen ist. Sie können den vollständigen Pfad einer Online-Redo-Protokolldatei angeben, und drücken Sie die Eingabetaste (möglicherweise müssen Sie dies ein paar Mal probieren, bis Sie das richtige Protokoll finden).

12. Geben Sie den folgenden Befehl ein, um die Informationen der Kontrolldatei zum Redo-Protokoll einer Datenbank zurückzugeben:

    SQL>SELECT * FROM V$LOG;

13. (Optional) Geben Sie den folgenden Befehl ein, um die Namen aller Mitglieder einer Gruppe anzuzeigen:

    SQL>SELECT * FROM V$LOGFILE;

    Beispiel: Nachdem Sie die aufgeforderten archivierten Protokolle angewendet haben, werden möglicherweise folgende Nachrichten angezeigt:

    ORA-00279: change 55636 generated at 24/06/2014 16:59:47 needed for thread 1

    ORA-00289: suggestion e:\app\Administrator\flash_recovery_ area\orcl\ARCHIVELOG\2014_06_24\ O1_MF_1_2_9TKXGGG2_.ARC

    ORA-00280: change 55636 for thread 1 is in sequence #24

    Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

14. Geben Sie den vollständigen Pfad der Online-Redo-Protokolldatei an, und drücken Sie die Eingabetaste.

    Beispiel: E:\app\Administrator\oradata\orcl\redo01.log

    Hinweis: Sie müssen den vollständigen Pfad mehrmals angeben, bis Sie das richtige Protokoll erhalten.

    Die folgenden Nachrichten werden angezeigt:

    Log applied

    Media recovery complete

15. Öffnen Sie die Datenbank mit der RESETLOGS-Klausel, nachdem Sie den Wiederherstellungsprozess abgeschlossen haben.

    SQL> ALTER DATABASE OPEN RESETLOGS;

    Die verlorenen Kontrolldateien werden wiederhergestellt.

Wiederherstellen der gesamten Datenbank (Tablespaces und Kontrolldateien)

Sie können die gesamte Datenbank (alle Tablespaces und Kontrolldateien) wiederherstellen. Bevor Sie eine Wiederherstellung durchführen, müssen Sie die Datei suchen. Wenn Sie die Dateien finden, stellen Sie sicher, dass die Datenbank im Status "Öffnen" ist. Wenn die Datenbank offen ist, verwenden Sie "ALTER TABLESPACE". OFFLINE -Anweisung, um die Tablespaces oder Datendateien offline zu stellen, bevor Sie mit der Wiederherstellung beginnen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, auf dem Sie die Tablespaces oder Datendateien wiederherstellen möchten.
2. Suchen Sie die Benutzer-Tablespaces oder Datendateien mithilfe des folgenden Befehls:

   SQL> SELECT TABLESPACE_NAME, FILE_NAME from DBA_DATA_FILES;

   SQL> SHOW PARAMETER CONTROL FILES;
3. Ändern Sie den Status der Datenbank auf "nomount" oder "shutdown", bevor Sie die Tablespaces oder Datendateien wiederherstellen.

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Melden Sie sich bei der Arcserve UDP-Konsole an.
5. Stellen Sie die Tablespaces oder Datendateien mithilfe des Wiederherstellungsassistenten wieder her. Weitere Informationen zum Wiederherstellungsvorgang finden Sie unter So führen Sie eine Wiederherstellung von einem Wiederherstellungspunkt aus.
6. Melden Sie sich beim Sicherungscomputer an.
7. Navigieren Sie zu den bestimmten Ordnern, und überprüfen Sie, ob die Tablespaces oder Datendateien wiederhergestellt wurden.
8. Wiederherstellen der Datenbank.

   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE UNTIL CANCEL;
9. Wenden Sie die aufgeforderten archivierten Protokolle an.

   Hinweis: Wenn das erforderliche archivierte Protokoll fehlt, dann bedeutet dies, dass sich ein notwendiger Redo-Datensatz in den Online-Redo-Protokollen befindet. Dies tritt auf, weil sich unarchivierte Änderungen in den Online-Protokollen befinden, als die Instanz fehlgeschlagen ist. Sie können den vollständigen Pfad einer

Online-Redo-Protokolldatei angeben, und drücken Sie die Eingabetaste (möglicherweise müssen Sie dies ein paar Mal probieren, bis Sie das richtige Protokoll finden).

10. Geben Sie den folgenden Befehl ein, um die Informationen der Kontrolldatei zum Redo-Protokoll einer Datenbank zurückzugeben:

    SQL>SELECT * FROM V$LOG;

11. (Optional) Geben Sie den folgenden Befehl ein, um die Namen aller Mitglieder einer Gruppe anzuzeigen:

    SQL>SELECT * FROM V$LOGFILE;

    Beispiel: Nachdem Sie die aufgeforderten archivierten Protokolle angewendet haben, werden möglicherweise folgende Nachrichten angezeigt:

    ORA-00279: change 55636 generated at 24/06/2014 16:59:47 needed for thread 1

    ORA-00289: suggestion e:\app\Administrator\flash_recovery_ area\orcl\ARCHIVELOG\2014_06_24\ O1_MF_1_2_9TKXGGG2_.ARC

    ORA-00280: change 55636 for thread 1 is in sequence #24

    Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

12. Geben Sie den vollständigen Pfad der Online-Redo-Protokolldatei an, und drücken Sie die Eingabetaste.

    Beispiel: E:\app\Administrator\oradata\orcl\redo01.log

    Hinweis: Sie müssen den vollständigen Pfad mehrmals angeben, bis Sie das richtige Protokoll erhalten.

    Die folgenden Nachrichten werden angezeigt:

    Log applied

    Media recovery complete

13. Öffnen Sie die Datenbank mit der RESETLOGS-Klausel, nachdem Sie den Wiederherstellungsprozess abgeschlossen haben.

    SQL> ALTER DATABASE OPEN RESETLOGS;

    Hinweis: Für mehrinstanzenfähige Datenbanken (CDB/PDB) müssen Sie auch alle Pluggable-Datenbanken öffnen.

    SQL > PLUGGABLE-DATENBANK ÄNDERN <PDB_NAME>OPEN;</PDB_NAME>

    Die gesamte Datenbank ist wiederhergestellt.

14. Starten Sie den Oracle-Server neu, nachdem Sie die Schritte 1 bis 13 für mehrinstanzenfähige Datenbanken durchgeführt haben.

    Hinweis: Dieser Schritt ist nicht erforderlich, wenn der Server nur mit eigenständigen Datenbanken arbeitet.

Wiederherstellen der Oracle-Datenbank mithilfe von Bare Metal Recovery

Mit einer Bare-Metal-Recovery können Sie das gesamte Computersystem während eines Systemausfalls wiederherstellen und neu erbauen. Sie können den ursprünglichen Computer wiederherstellen, oder Sie können einen anderen Computer wiederherstellen.

Gehen Sie wie folgt vor:

1. Stellen Sie den Computer wieder her, indem Sie eine der folgenden Methoden verwenden:
   - Wenn die Wiederherstellungspunkte von einer Agent-basierten Sicherung sind, führen Sie eine BMR aus, um den Computer wiederherzustellen.
   - Wenn die Wiederherstellungspunkte von einer hostbasierten Sicherung ohne Agent sind, dann verwenden Sie "VM wiederherstellen", um den Computer wiederherzustellen.
2. Melden Sie sich beim wiederhergestellten Computer an.
3. Öffnen Sie die Eingabeaufforderung, und stellen Sie eine Verbindung mit der Oracle-Instanz (zum Beispiel ORCL) als "sysdba" auf.
4. Überprüfen Sie den Status der Oracle-Instanz.

   SQL> SELECT STATUS FROM V$INSTANCE;
5. Führen Sie abhängig von dem Status der Oracle-Instanz einen der folgenden Schritte aus:
   - Wenn der Status "Shutdown" ist, dann starten und öffnen Sie die Instanz.

     SQL> STARTUP;

     SQL> ALTER DATABASE OPEN;
   - Wenn der Status "Nomount" ist, dann laden und öffnen Sie die Instanz.

     SQL> ALTER DATABASE MOUNT;

     SQL> ALTER DATABASE OPEN;
   - Wenn der Status "Mount" ist, dann öffnen Sie die Oracle-Instanz.

     SQL> ALTER DATABASE OPEN;
6. Wiederherstellung durch die Ausführung des RECOVER-Befehls, wenn die Datenbank eine Datenträger-Recovery benötigt

   SQL> RECOVER DATABASE;

7. Öffnen Sie die Oracle-Instanz, nachdem die Datenträger-Recovery abgeschlossen ist.

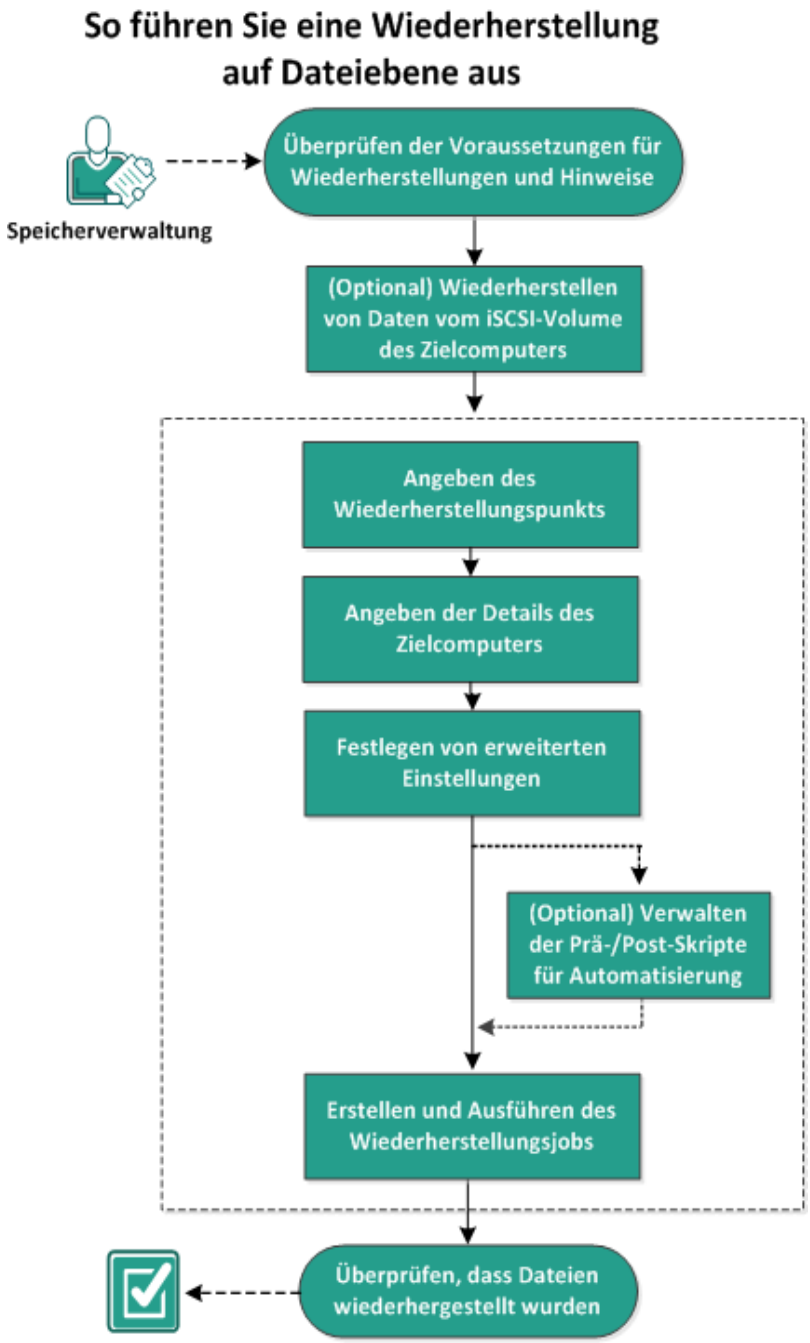
   SQL> ALTER DATABASE OPEN;

   Die Oracle-Datenbank wird mithilfe der Bare-Metal-Recovery wiederhergestellt.

So führen Sie eine Wiederherstellung der Dateiebene unter Linux-Knoten aus

Bei einer Wiederherstellung auf Dateiebene werden einzelne Dateien und Verzeichnisse von einem Wiederherstellungspunkt aus wiederhergestellt. Sie können auch nur eine Datei von dem Wiederherstellungspunkt aus wiederherstellen. Diese Option ist hilfreich, wenn Sie nur ausgewählte Dateien und nicht den gesamten Wiederherstellungspunkt wiederherstellen möchten.

Folgendes Diagramm zeigt den Prozess an, um eine Wiederherstellung der Dateiebene auszuführen:



Gehen Sie zum Ausführen einer Wiederherstellung auf Dateiebene wie folgt vor:

- Überprüfen der Voraussetzungen für die Wiederherstellung
- (Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers
- Angeben des Wiederherstellungspunkts
- Angeben der Details des Zielcomputers
- Festlegen von erweiterten Einstellungen
- (Optional) Verwalten der Prä-/Post-Skripte für Automatisierung

- Erstellen und Ausführen des Wiederherstellungsjobs
- Überprüfen, dass Dateien wiederhergestellt wurden

Überprüfen der Voraussetzungen

Beachten Sie Folgendes, bevor Sie eine Wiederherstellung auf Dateiebene ausführen:

- Sie verfügen über einen gültigen Wiederherstellungspunkt und, falls erforderlich, über das Verschlüsselungskennwort.
- Sie verfügen über einen gültigen Zielknoten zum Wiederherstellen der Daten.
- Sie haben sichergestellt, dass der Linux-Sicherungsserver das Dateisystem unterstützt, das Sie wiederherstellen möchten.

  RedHat 7.x unterstützt zum Beispiel nicht das Dateisystem *reiserfs*. Wenn das Betriebssystem des Sicherungsservers RedHat 7.x ist und Sie das Dateisystem "reiserfs" wiederherstellen möchten, müssen Sie den Dateisystemtreiber installieren, um "reiserfs" zu unterstützen. Sie können die Wiederherstellung auf Dateiebene auch mit Arcserve Unified Data Protection Agent for Linux-Live-CD ausführen, da Live-CD alle Dateisystemtypen unterstützt.
- Sie haben die folgenden Pakete auf dem Linux-Sicherungsserver installiert:
  - mdadm
  - kpartx
  - lvm2
  - Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

(Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers

Wenn Sie Ihre Daten auf einem iSCSI-Zieldatenträger gespeichert haben, können Sie eine Verbindung mit dem iSCSI-Volume herstellen und Daten wiederherstellen. Das iSCSI-Volume ermöglicht das Verwalten und Übertragen von Daten über ein Netzwerk.

Stellen Sie sicher, dass Sie die neueste Version der iSCSI-Initiator-Software auf Ihrem Sicherungsserver installiert haben. In RHEL-Systemen ist die Initiator-Software als "iscsi-initiator-utils" gepackt. In SLES-Systemen ist die Initiator-Software als "open-iscsi" gepackt.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Shell-Umgebung des Sicherungsservers an.
2. Führen Sie einen der folgenden Befehle aus, um den iSCSI-Initiator-Daemon zu starten.
   - Für RHEL-Systeme:

     /etc/init.d/iscsid start

     In RHEL-Systemen heißt der Dienst "iscsid".
   - Für SLES-Systeme:

     /etc/init.d/open-iscsi start

     In SLES-Systemen heißt der Dienst "open-iscsi".
3. Führen Sie ein Discovery-Skript aus, um den iSCSI-Zielhost zu erkennen.

   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>

   Der Standardportwert des iSCSI-Zielhost ist 3260.
4. Notieren Sie den iSCSI Qualified Name (IQN) des iSCSI-Zielhost, der durch das Discovery-Skript gefunden wird, bevor Sie sich manuell beim erkannten Zielcomputer anmelden.
5. Listen Sie das verfügbare Blockgerät des Sicherungsservers auf.

   #fdisk -l
6. Melden Sie sich beim erkannten Ziel an.

   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l

   Im Verzeichnis /dev des Sicherungsservers wird ein Blockgerät angezeigt.

7. Führen Sie den folgenden Befehl aus, um den Namen des neuen Geräts abzurufen:

   #fdisk -l

   Im Sicherungsserver können Sie ein zusätzliches Gerät, /dev/sd<x>, sehen.

   In diesem Beispiel ist der Name des Geräts "/dev/sdc". In den folgenden Schritten wird dieser Gerätename verwendet, um eine Partition und ein Dateisystem zu erstellen.

8. Laden Sie das iSCSI-Volume mithilfe der folgenden Befehle:

   # mkdir /iscsi

   # mount /dev/sdc1 /iscsi

   Hinweis: Wenn Sie den Sitzungsspeicherort im Wiederherstellungsassistenten angeben, müssen Sie "Lokal" auswählen und den Pfad /iscsi eingeben.

   Beispiel: <path>/iscsi

9. (Optional) Fügen Sie folgenden Datensatz zur Datei "/etc/fstab" hinzu, damit das iSCSI-Volume automatisch eine Verbindung zum Sicherungsserver herstellt, nachdem Sie den Server neu gestartet haben.

   /dev/sdc1 /iscsi ext3 _netdev 0 0

   Der Sicherungsserver kann jetzt eine Verbindung mit dem iSCSI-Volume herstellen und Daten vom iSCSI-Volume wiederherstellen.

Angeben des Wiederherstellungspunkts für agentenbasierte Sicherung

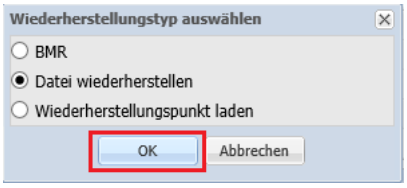
Bei jedem Ausführen einer Sicherung wird ein Wiederherstellungspunkt erstellt. Geben Sie die Informationen zu den Wiederherstellungspunkten im Wiederherstellungsassistenten an, damit genau die gewünschten Daten wiederhergestellt werden. Sie können je nach Bedarf bestimmte Dateien oder alle Dateien wiederherstellen.

Gehen Sie wie folgt vor:

1. Führen Sie einen der folgenden Vorgänge durch, um auf den Wiederherstellungsassistenten zuzugreifen:
   - **Von Arcserve UDP :**
     a. Melden Sie sich bei Arcserve UDP an.
     b. Navigieren Sie zu **Ressourcen** > **Knoten** > **Alle Knoten**.

        Alle hinzugefügten Knoten werden im mittleren Fensterbereich angezeigt.
     c. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie dann **Wiederherstellen** aus.

        Die Webbenutzeroberfläche von Arcserve UDP Agent (Linux) wird geöffnet, und das Dialogfeld "Wiederherstellungstyp auswählen" wird angezeigt.
     d. Klicken Sie im Dialogfeld "Wiederherstellungstyp auswählen" auf die Option **Datei wiederherstellen** und anschließend auf **OK**.

        Hinweis: Sie werden automatisch beim Agentenknoten angemeldet, und der Wiederherstellungsassistent wird vom Agentenknoten aus geöffnet.
   - **Von Arcserve Unified Data Protection Agent for Linux :**
     a. Öffnen Sie die Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche.

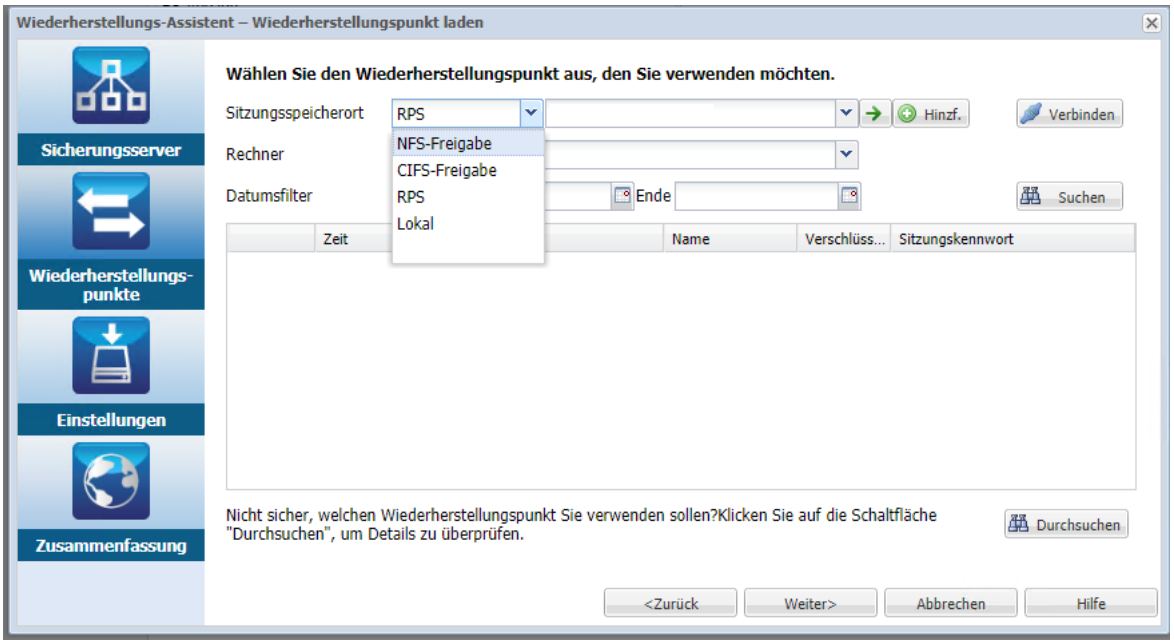
Hinweis: Während der Installation von Arcserve Unified Data Protection Agent for Linux haben Sie die URL erhalten, um auf den Server zugreifen und ihn verwalten zu können. Melden Sie sich bei Arcserve Unified Data Protection Agent for Linux an.

b. Klicken Sie im Menü "Assistent" auf **Wiederherstellen**, und wählen Sie dann **Datei wiederherstellen** aus.

   Das Dialogfeld "Wiederherstellungsassistent - Dateiwiederherstellung" wird geöffnet.

2. Auf der Seite "Sicherungsserver" des Wiederherstellungsassistenten wird der Sicherungsserver angezeigt. Sie können in der Drop-down-Liste Sicherungsserver keine Optionen auswählen. Klicken Sie auf **Weiter**.

3. Gehen Sie auf der Seite "Wiederherstellungspunkte" des Wiederherstellungsassistenten wie folgt vor:



Wichtig! Wenn Sie den Assistenten über die Konsole geöffnet haben, werden der Sitzungsspeicherort und die Rechnerdetails automatisch angezeigt. Sie können zu Schritt 4 springen.

a. Wählen Sie **CIFS-Freigabe/NFS-Freigabe/RPS-Server/Lokal** in der Drop-down-Liste "Sitzungsspeicherort" aus.

b. Führen Sie je nach Sitzungsspeicherort einen der folgenden Schritte aus:

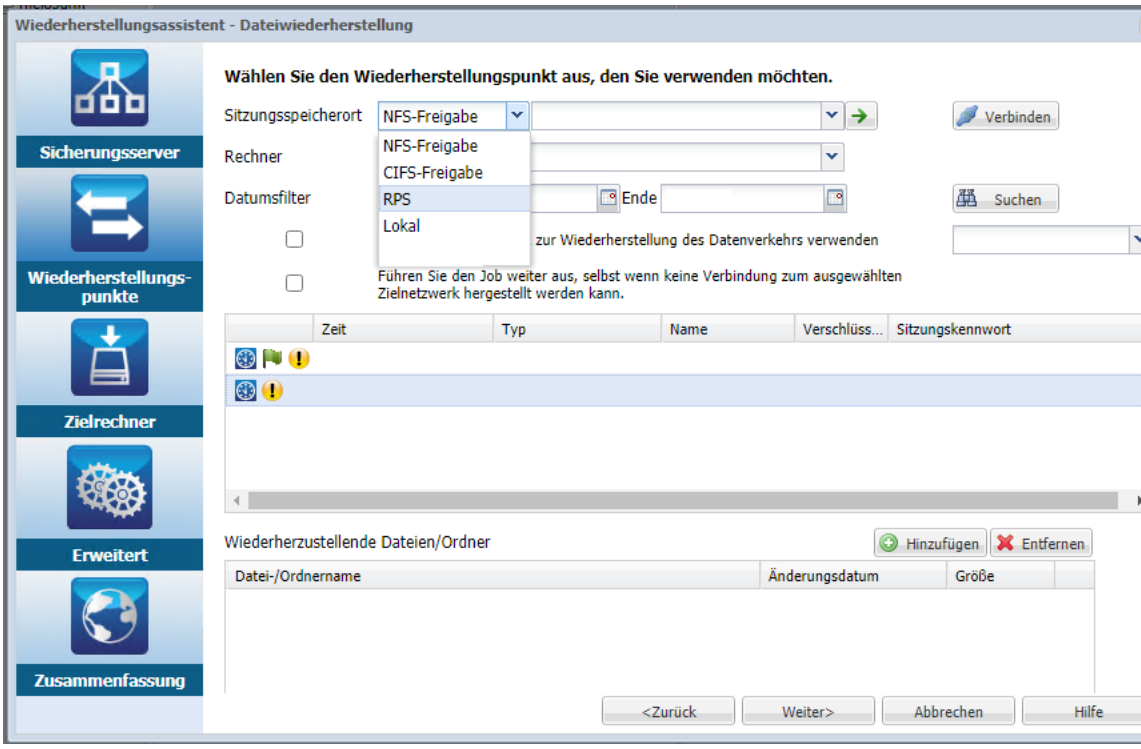
Für CIFS-Freigabe/NFS-Freigabe/lokal

Geben Sie den vollständigen Pfad der CIFS-Freigabe/NFS-Freigabe/lokalen Freigabe an, und klicken Sie dann auf **Verbinden**.

Alle Rechner werden in der Drop-down-Liste "Rechner" aufgelistet.

Hinweis: Wenn Sie die Option **CIFS-Freigabe** auswählen, geben

Sie den Benutzernamen und das Kennwort ein.



Für RPS-Server:

a. Wählen Sie den RPS-Server aus, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld "Recovery Point-Server-Informationen" wird geöffnet.

b. Geben Sie die RPS-Details ein, und klicken Sie dann auf **Ja**.

c. Wählen Sie den Datenspeicher in der Drop-down-Liste aus.

   Das Dialogfeld "Recovery Point-Server-Informationen" wird geschlossen, und der Assistent wird angezeigt.

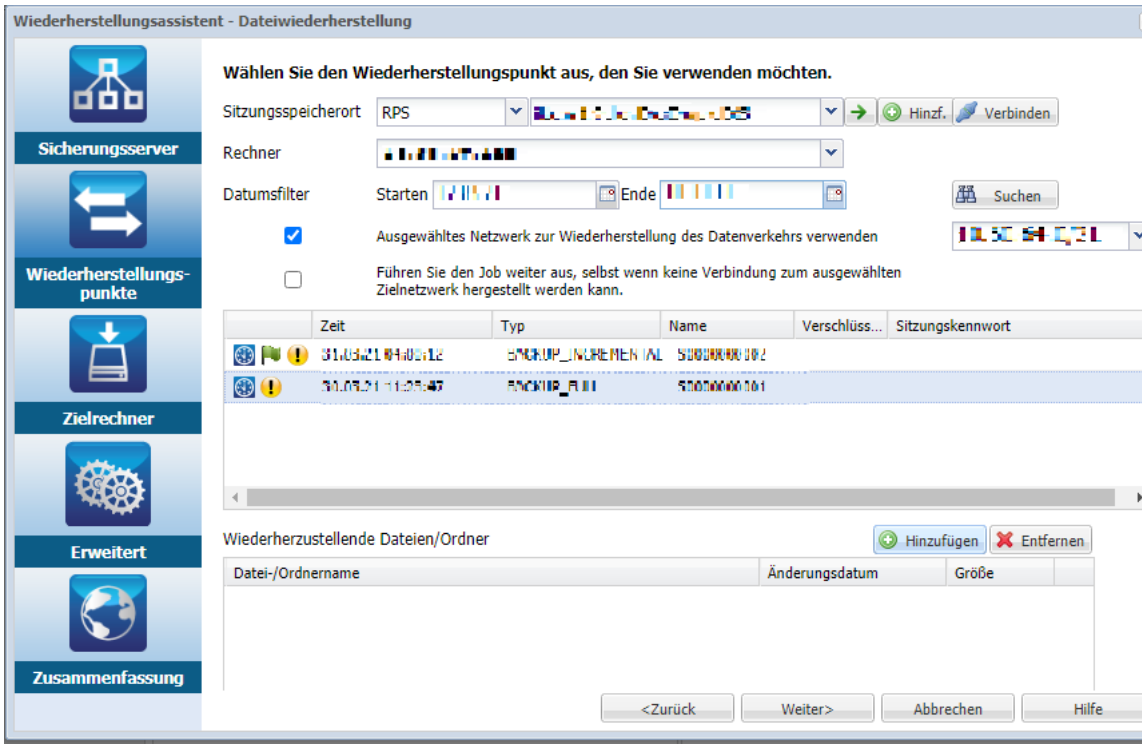
d. Klicken Sie auf **Verbinden**.

   Alle Knoten, die an diesem Speicherort gesichert wurden, werden in der Drop-down-Liste Rechner aufgelistet.

e. Wählen Sie in der Drop-down-Liste "Rechner" den Knoten aus, den Sie wiederherstellen möchten.

   Es werden alle Wiederherstellungspunkte des ausgewählten Kno-

tens aufgelistet.



4. Wenden Sie den Datumsfilter an, um die Wiederherstellungspunkte anzuzeigen, die zwischen den angegebenen Daten generiert wurden, und klicken Sie dann auf **Suchen**.

   Standard: Die letzten zwei Wochen.

   Alle verfügbaren Wiederherstellungspunkte zwischen den angegebenen Datumswerten werden angezeigt.

5. Um die Kommunikation zwischen Linux-Agent und Recovery Point Server zu ermöglichen, aktivieren Sie das Kontrollkästchen **Ausgewähltes Netzwerk zur Wiederherstellung des Datenverkehrs verwenden**, und wählen Sie dann das Netzwerk in der Drop-down-Liste aus.

   Hinweis: Um den Sicherungsjob mit dem verfügbaren Netzwerk oder dem Standardnetzwerk fortzusetzen, falls das ausgewählte Sicherungsnetzwerk nicht zugänglich ist, aktivieren Sie das Kontrollkästchen **Führen Sie den Job weiter aus, selbst wenn keine Verbindung zum ausgewählten Sicherungsnetzwerk hergestellt werden kann**.

6. Wählen Sie den Wiederherstellungspunkt aus, den Sie wiederherstellen möchten. Wenn der Wiederherstellungspunkt verschlüsselt ist, geben Sie das Verschlüsselungskennwort ein, um die Daten wiederherzustellen.

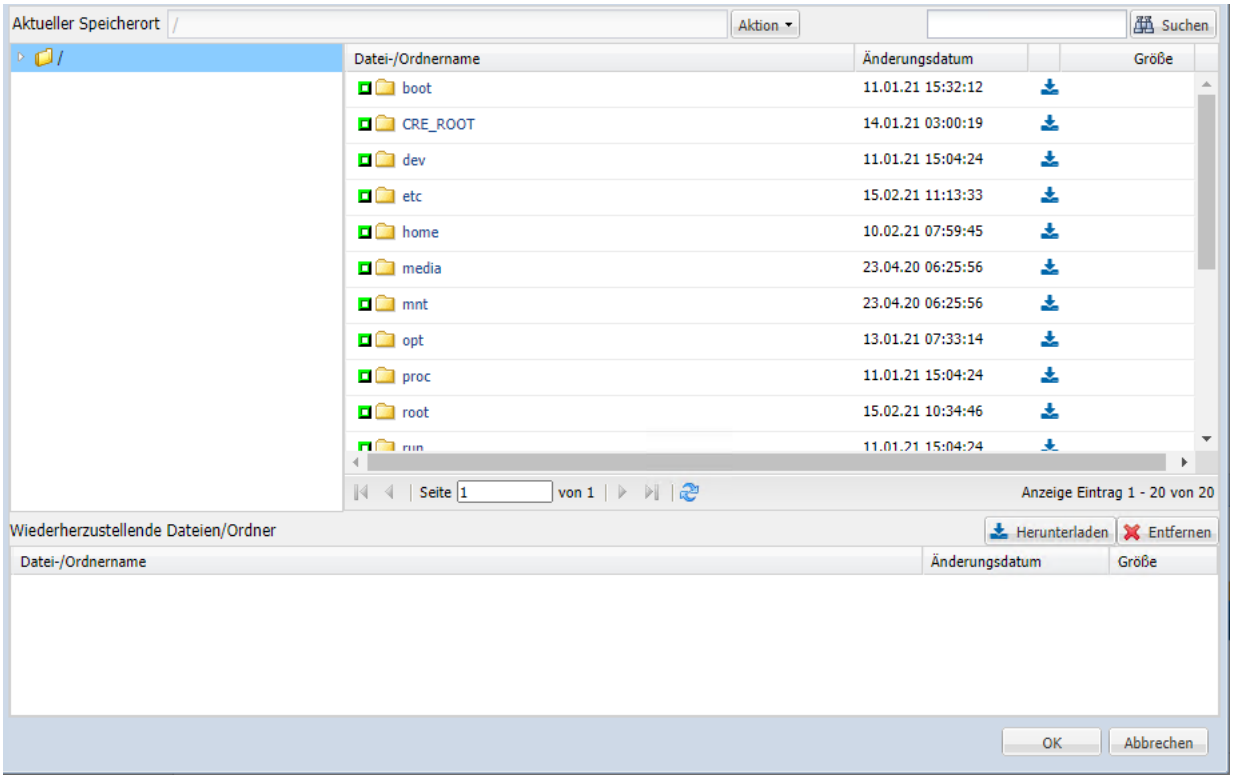
7. Klicken Sie für "Wiederherzustellende Dateien/Ordner" auf **Hinzufügen**.

Das Dialogfeld <Knotenname> durchsuchen wird geöffnet.

Wichtig! Wenn die Warnmeldung "Die Dateien/Ordner werden unter der Gerätedatei angezeigt. Klicken Sie hier für weitere Informationen." in der Konsole angezeigt wird, finden Sie im folgenden Hinweis eine Lösung.

Hinweis: Für einige komplexe Datenträgerlayouts wird das Dateisystem von der Gerätedatei angezeigt. Die Änderung im Anzeigeverhalten des Dateisystems wirkt sich nicht auf die Funktion der hostbasierten Linux VM-Wiederherstellung auf Dateiebene aus. Sie können das Dateisystem unter der Gerätedatei durchsuchen. Sie können auch die Suchfunktion verwenden, um nach einer bestimmten Datei oder einem Verzeichnis zu suchen.

8. Wählen Sie im Dialogfeld "<Knotenname> durchsuchen" die Datei oder den Ordner aus, die bzw. den Sie wiederherstellen möchten, und klicken Sie dann auf **OK**.



Hinweis: Wenn Sie versuchen, eine Datei oder einen Ordner mithilfe des **Suchfeldes** zu finden, stellen Sie sicher, dass Sie den höchsten Ordner in der Hierarchie auswählen. Die Suche wird in allen untergeordneten Ordnern des ausgewählten Ordners durchgeführt.

Das Dialogfeld <Knotenname> durchsuchen wird geschlossen, und Sie gelangen erneut zur Seite Wiederherstellungspunkte. Die ausgewählten Dateien und Ordner sind unter Wiederherzustellende Dateien/Ordner aufgeführt.

9. Klicken Sie auf **Weiter**.

   Die Seite Zielcomputer wird geöffnet.

Der Wiederherstellungspunkt wird angegeben.

Angeben der Details des Zielcomputers

Geben Sie die Details des Zielknotens an, damit Daten auf diesem Knoten wiederhergestellt werden. Sie können die ausgewählten Dateien oder Ordner auf dem Quellknoten oder einem neuen Knoten wiederherstellen.

Gehen Sie wie folgt vor, um die Daten auf dem Knoten wiederherzustellen, von dem sie gesichert wurden:

1. Wählen Sie auf der Seite "Zielrechner" die Option **Am ursprünglichen Speicherort wiederherstellen** aus.

2. Geben Sie den Benutzernamen und das Kennwort des Knotens ein.
3. Wählen Sie eine der folgenden Optionen, um Dateikonflikte zu lösen:

   Vorhandene Dateien überschreiben

Gibt an, dass die Sicherungsdatei vom Wiederherstellungspunkt die vorhandene Datei ersetzt, wenn die Datei auf dem Zielcomputer vorhanden ist.

Dateien umbenennen

Gibt an, dass, wenn die Datei im Zielcomputer vorhanden ist, eine neue Datei mit dem selben Dateinamen und der Dateierweiterung *.d2d-duplicate<x>* erstellt wird. <x> gibt an, wie oft die Datei wiederhergestellt wird. Alle Daten werden dann in eine neue Datei wiederhergestellt.

Vorhandene Dateien überspringen

Gibt an, dass die Dateien, wenn dieselbe Datei auf dem Zielcomputer vorhanden ist, nicht vom Wiederherstellungspunkt wiederhergestellt werden.

4. (Optional) Wählen Sie **Stammverzeichnis erstellen**.
5. Klicken Sie auf **Weiter**.

   Die Seite Erweitert wird geöffnet.

Gehen Sie wie folgt vor, um die Wiederherstellung auf einen neuen Knoten durchzuführen:

1. Wählen Sie auf der Seite "Zielrechner" die Option **An einem alternativen Speicherort wiederherstellen** aus.

2. Geben Sie den Hostnamen oder die IP-Adresse des Zielknotens ein.
3. Geben Sie den Benutzernamen und das Kennwort des Knotens ein.
4. Geben Sie den Pfad ein, in dem die Daten wiederhergestellt werden sollen, oder klicken Sie auf **Durchsuchen**, um den Ordner auszuwählen, in dem die Daten wiederhergestellt werden sollen. Klicken Sie dann auf **OK**.
5. Wählen Sie eine der folgenden Optionen, um Dateikonflikte zu lösen:

   Vorhandene Dateien überschreiben

   Gibt an, dass die Sicherungsdatei vom Wiederherstellungspunkt die vorhandene Datei ersetzt, wenn die Datei auf dem Zielcomputer vorhanden ist.

   Dateien umbenennen

   Gibt an, dass, wenn die Datei im Zielcomputer vorhanden ist, eine neue Datei mit dem selben Dateinamen und der Dateierweiterung *.d2d-duplicate<x>* erstellt wird. <x> gibt an, wie oft die Datei wiederhergestellt wird. Alle Daten werden dann in eine neue Datei wiederhergestellt.

Vorhandene Dateien überspringen

Gibt an, dass die Dateien, wenn dieselbe Datei auf dem Zielcomputer vorhanden ist, nicht vom Wiederherstellungspunkt wiederhergestellt werden.

6. (Optional) Wählen Sie **Stammverzeichnis erstellen**.
7. Klicken Sie auf **Weiter**.

   Die Seite Erweitert wird geöffnet.

Die Details des Zielcomputers sind angegeben.

Festlegen von erweiterten Einstellungen

Geben Sie die erweiterten Einstellungen an, um eine geplante Wiederherstellung der Daten auszuführen. Mit einer geplanten Wiederherstellung wird sichergestellt, dass die Daten auch bei Ihrer Abwesenheit zur angegebenen Zeit wiederhergestellt werden.

Gehen Sie wie folgt vor:

1. Legen Sie Datum und Uhrzeit für den Beginn fest, indem Sie eine der folgenden Optionen auswählen:

   Jetzt ausführen

   Startet den Wiederherstellungsjob auf Dateiebene sofort, nachdem Sie den Job übergeben haben.

   Startdatum und -zeitpunkt festlegen

   Startet den Wiederherstellungsjob auf Dateiebene zum angegebenen Datum und Zeitpunkt, nachdem Sie den Job übergeben haben.

2. (Optional) Wählen Sie "**Geschätzte Dateigröße**".

3. (Optional) Wählen Sie ein Skript aus der Option **Einstellungen für Prä-/Post-Skripts** aus.

   Diese Skripte führen Skriptbefehle für Aktionen aus, die vor dem Start des Jobs und/oder nach Abschluss des Jobs durchgeführt werden sollen.

   Hinweis: Die Felder für **Einstellungen vor/nach dem Skript** werden nur aufgefüllt, wenn Sie bereits eine Skriptdatei erstellt und an folgendem Speicherort platziert haben:

   /opt/Arcserve/d2dserver/usr/prepost

   Hinweis: Weitere Informationen zur Erstellung der Prä-/Post-Skripte finden Sie unter *Verwalten der Prä-/Post-Skripte für Automatisierung*.

4. Klicken Sie auf **Weiter**.

   Die Seite **"Zusammenfassung"** wird geöffnet.

   Die erweiterten Einstellungen sind angegeben.

(Optional) Verwalten der Prä-/Post-Skripte für Automatisierung

Mit Prä-/Post-Skripts können Sie Ihre eigene Geschäftslogik in bestimmten Phasen eines laufenden Jobs ausführen. Sie können in **Einstellungen vor/nach dem Skript** des **Sicherungsassistenten** und des **Wiederherstellungsassistenten** auf der Benutzeroberfläche angeben, wann Ihre Skripte ausgeführt werden sollen. Die Skripts können je nach Einstellung auf dem Sicherungsserver ausgeführt werden.

Das Verwalten von Prä-/Post-Skripts ist ein zweiteiliger Vorgang, der das Erstellen des Prä-/Post-Skripts und das Einfügen des Skripts in den "prepost"-Ordners umfasst.

Erstellen von Prä-/Post-Skripts

Gehen Sie wie folgt vor:

1. Melden Sie sich als Root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie eine Skriptdatei, indem Sie die Umgebungsvariablen in Ihrer bevorzugten Skripterstellungssprache verwenden.

   Umgebungsvariablen des Prä-/Post-Skripts

   Verwenden Sie die folgenden Umgebungsvariablen, um Ihr Skript zu erstellen:

   D2D_JOBNAME

   Gibt den Namen des Jobs an.

   D2D_JOBID

   Gibt die Job-ID an. Die Job-ID ist eine Nummer, die für den Job vergeben wird, wenn Sie den Job ausführen. Wenn Sie den gleichen Job erneut ausführen, erhalten Sie eine neue Jobnummer.

   D2D_TARGETNODE

   Identifiziert den Knoten, der gesichert oder wiederhergestellt wird.

   D2D_JOBTYPE

   Identifiziert den Typ des ausgeführten Jobs. Die folgenden Werte identifizieren die D2D_JOBTYPE-Variable:

   backup.full

   Identifiziert den Job als eine vollständige Sicherung.

   backup.incremental

   Identifiziert den Job als eine Zuwachssicherung.

backup.verify

Identifiziert den Job als eine Überprüfungssicherung.

restore.bmr

Identifiziert den Job als eine Bare-Metal-Recovery (BMR). Dies ist ein Wiederherstellungsjob.

restore.file

Identifiziert den Job als eine Wiederherstellung auf Dateiebene. Dies ist ein Wiederherstellungsjob.

D2D_SESSIONLOCATION

Identifiziert den Speicherort, an dem die Wiederherstellungspunkte gespeichert sind.

D2D_PREPOST_OUTPUT

Identifiziert eine Temp-Datei. Der Inhalt der Anfangszeile der Temp-Datei wird im Aktivitätsprotokoll angezeigt.

D2D_JOBSTAGE

Gibt die Phase des Jobs an. Die folgenden Werte identifizieren die D2D_ JOBSTAGE-Variable:

pre-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, bevor der Job startet.

post-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Job startet.

post-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Snapshot erfasst wird.

post-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Snapshot erfasst wird.

D2D_TARGETVOLUME

Identifiziert das Volume, das während eines Sicherungsjobs gesichert wird. Diese Variable ist anwendbar für Prä-/Post-Snapshot-Skripts für einen Sicherungsjob.

D2D_JOBRESULT

Identifiziert das Ergebnis für ein Post-Job-Skript. Die folgenden Werte identifizieren die D2D_JOBRESULT-Variable:

success

Identifiziert das Ergebnis als erfolgreich.

fail

Identifiziert das Ergebnis als nicht erfolgreich.

D2DSVR_HOME

Identifiziert den Ordner, in dem der Sicherungsserver installiert ist. Diese Variable ist anwendbar für die Skripts, die auf dem Sicherungsserver ausgeführt werden.

Das Skript ist erstellt.

Hinweis: Bei allen Skripten zeigt der Rückgabewert von Null eine erfolgreiche Erstellung an, und ein Rückgabewert, der ungleich Null ist, weist auf einen Fehler hin.

Einfügen des Skripts in den Ordner "Prepost" und Überprüfung des Skripts

Alle Prä-/Post-Skripts für einen Sicherungsserver werden zentral vom Ordner "prepost" am folgenden Speicherort verwaltet:

/opt/Arcserve/d2dserver/usr/prepost

Gehen Sie wie folgt vor:

1. Fügen Sie die Datei in folgenden Speicherort des Sicherungsservers ein:

   /opt/Arcserve/d2dserver/usr/prepost

2. Geben Sie der Skriptdatei Ausführungsberechtigungen.
3. Melden Sie sich bei der Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche an.
4. Öffnen Sie den **Sicherungsassistenten** oder **Wiederherstellungsassistenten**, und navigieren Sie zur Registerkarte **Erweitert**.
5. Wählen Sie die Skriptdatei in der Drop-down-Liste **Einstellungen vor/nach dem Skript** aus, und übergeben Sie den Job.

6. Klicken Sie auf "**Aktivitätsprotokoll**", und stellen Sie sicher, dass das Skript für den angegebenen Sicherungsjob ausgeführt wird.

   Das Skript wird ausgeführt.

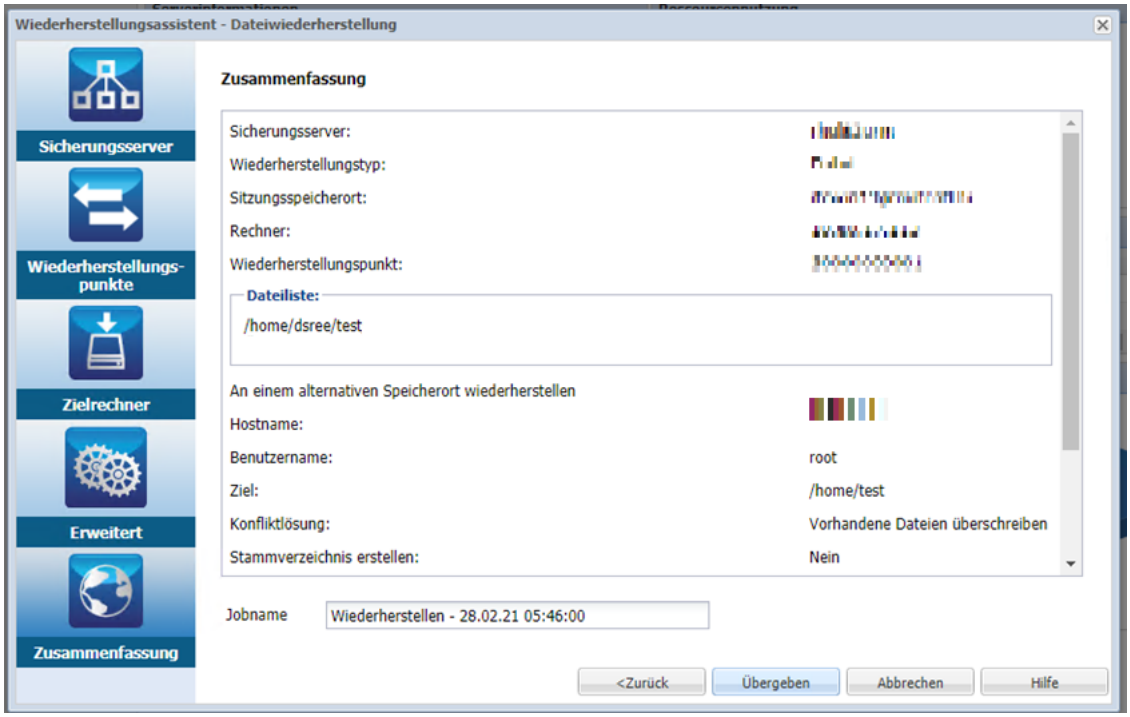
   Die Prä-/Post-Skripte wurden erfolgreich erstellt und befinden sich im Ordner "pre-post".

Erstellen und Ausführen des Wiederherstellungsjobs

Erstellen Sie den Wiederherstellungsjob, und führen Sie ihn aus, sodass Sie die Wiederherstellung auf Dateiebene initiieren können. Überprüfen Sie die Wiederherstellungspunktinformationen, bevor Sie die Dateien wiederherstellen. Gehen Sie bei Bedarf zurück, und ändern Sie die Wiederherstellungseinstellungen im Assistenten.

Gehen Sie wie folgt vor:

1. Überprüfen Sie auf der Seite "Zusammenfassung" des Wiederherstellungsassistenten die Wiederherstellungsdetails.



2. Wählen Sie eine der folgenden Vorgehensweisen:
   - Wenn die Übersichtsinformationen Fehler enthalten, klicken Sie auf **Zurück**, und ändern Sie die inkorrekten Einstellungen im entsprechenden Dialogfeld.
   - Wenn die Übersichtsinformationen korrekt sind, geben Sie einen Jobnamen ein, und klicken Sie dann auf **Übergeben**, um den Wiederherstellungsprozess zu starten.

Hinweis: Im Feld "Jobname" ist zunächst ein Standardname angegeben. Sie können einen neuen Jobnamen Ihrer Wahl eingeben, dürfen das Feld jedoch nicht leer lassen.

Der Wiederherstellungsassistent wird geschlossen. Der Status des Jobs wird auf der Seite "Jobstatus" angezeigt.

Der Wiederherstellungsjob wurde erfolgreich erstellt und ausgeführt.

Überprüfen, dass Dateien wiederhergestellt wurden

Überprüfen Sie nach Abschluss des Wiederherstellungsjobs, dass alle Dateien im Zielknoten wiederhergestellt wurden. Überprüfen Sie die Registerkarten **Jobübersicht** und **Aktivitätsprotokoll** im Fenster **Status**, um den Fortschritt des Wiederherstellungsprozesses zu überwachen.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Zielcomputer, auf dem Sie die Daten wiederhergestellt haben.
2. Überprüfen Sie, dass die erforderlichen Daten vom Wiederherstellungspunkt wiederhergestellt wurden.

   Die Dateien wurden erfolgreich überprüft.

   Die Wiederherstellung auf Dateiebene wurde erfolgreich ausgeführt.

Ausführen von Wiederherstellungen auf Dateiebene über eine hostbasierte, agentenlose Sicherung für Linux-Knoten

Bei einer Wiederherstellung auf Dateiebene werden einzelne Dateien und Verzeichnisse von einem Wiederherstellungspunkt aus wiederhergestellt. Sie können auch nur eine Datei von dem Wiederherstellungspunkt aus wiederherstellen. Diese Option ist hilfreich, wenn Sie nur ausgewählte Dateien und nicht den gesamten Wiederherstellungspunkt wiederherstellen möchten.

Gehen Sie zum Ausführen einer Wiederherstellung auf Dateiebene wie folgt vor:

- Überprüfen der Voraussetzungen für die Wiederherstellung
- Angeben des Wiederherstellungspunkts
- Angeben der Details des Zielcomputers
- Festlegen von erweiterten Einstellungen
- (Optional) Verwalten der Prä-/Post-Skripte für Automatisierung
- Erstellen und Ausführen des Wiederherstellungsjobs
- Überprüfen, dass Dateien wiederhergestellt wurden

Überprüfen der Voraussetzungen

Beachten Sie Folgendes, bevor Sie eine Wiederherstellung auf Dateiebene ausführen:

- Sie verfügen über einen gültigen Wiederherstellungspunkt und, falls erforderlich, über das Verschlüsselungskennwort.
- Sie verfügen über einen gültigen Zielknoten zum Wiederherstellen der Daten.
- Sie haben sichergestellt, dass der Linux-Sicherungsserver das Dateisystem unterstützt, das Sie wiederherstellen möchten.

  RedHat 7.x unterstützt zum Beispiel nicht das Dateisystem *reiserfs*. Wenn das Betriebssystem des Sicherungsservers RedHat 7.x ist und Sie das Dateisystem "reiserfs" wiederherstellen möchten, müssen Sie den Dateisystemtreiber installieren, um "reiserfs" zu unterstützen. Sie können Arcserve Unified Data Protection Agent for Linux-Live-CD auch verwenden, um die Wiederherstellung auf Dateiebene auszuführen, da Live-CD alle Dateisystemtypen unterstützt.
- Sie haben die folgenden Pakete auf dem Linux-Sicherungsserver installiert:
  - mdadm
  - kpartx
  - lvm2
  - Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Angeben des Wiederherstellungspunkts

Bei jedem Ausführen einer Sicherung wird ein Wiederherstellungspunkt erstellt. Geben Sie die Informationen zu den Wiederherstellungspunkten im **Wiederherstellungsassistenten** an, damit genau die gewünschten Daten wiederhergestellt werden. Sie können je nach Bedarf bestimmte Dateien oder alle Dateien wiederherstellen.

Gehen Sie wie folgt vor:

1. Führen Sie einen der folgenden Vorgänge durch, um auf den Wiederherstellungsassistenten zuzugreifen:

   Von Arcserve UDP :

   a. Melden Sie sich bei Arcserve UDP an.

   b. Klicken Sie auf die Registerkarte **Ressourcen**.

   c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

   e. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

      Die Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche wird geöffnet. Das Auswahldialogfeld für den Wiederherstellungstyp wird in der Benutzeroberfläche des Agenten angezeigt.

   f. Wählen Sie den Wiederherstellungstyp aus, und klicken Sie auf **OK**.

      Hinweis: Sie werden automatisch beim Agentenknoten angemeldet, und der **Wiederherstellungsassistent** wird im Agentenknoten geöffnet.

   Von Arcserve Unified Data Protection Agent for Linux :

   a. Öffnen Sie die Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche.

      Hinweis: Während der Installation von Arcserve Unified Data Protection Agent for Linux haben Sie die URL erhalten, um auf den Server zugreifen und ihn verwalten zu können. Melden Sie sich bei Arcserve Unified Data Protection Agent for Linux an.

   b. Klicken Sie im Menü **Assistent** auf **Wiederherstellen**, und wählen Sie **Datei wiederherstellen** aus.

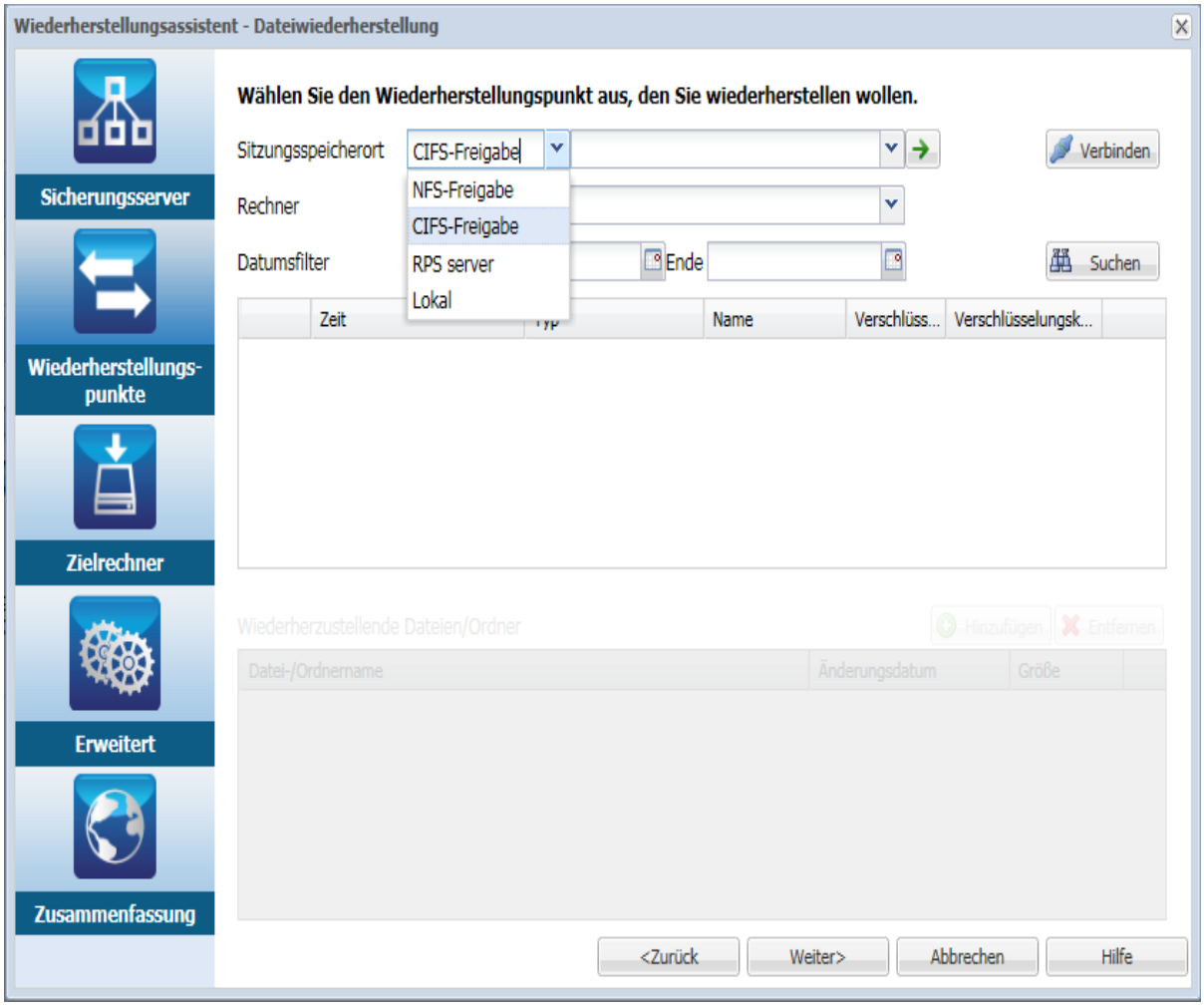
      Wiederherstellungsassistent – Datei-Wiederherstellung wird geöffnet.

Der Sicherungsserver wird auf der Seite **Sicherungsserver** des **Wiederherstellungsassistenten** angezeigt. Sie können in der Drop-down-Liste **Sicherungsserver** keine Optionen auswählen.

2. Klicken Sie auf **Weiter**.

   Die Seite **Wiederherstellungspunkte** des **Wiederherstellungsassistenten** wird geöffnet.

   Wichtig! Wenn Sie den Assistenten über die Konsole geöffnet haben, werden der Sitzungsspeicherort und die Rechnerdetails automatisch angezeigt. Sie können zu Schritt 5 springen.



3. Wählen Sie entweder **CIFS-Freigabe** oder **RPS-Server** aus der Drop-down-Liste zum **Sitzungsspeicherort** aus.

   Hinweis: Sie können für die Wiederherstellung von per hostbasierter agentenloser Sicherung gesicherten Sitzungen nicht "NFS-Freigabe" oder "Lokal" auswählen.

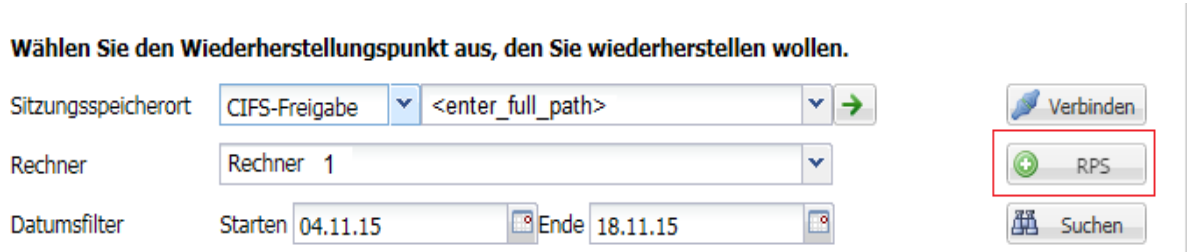
4. Führen Sie je nach Sitzungsspeicherort einen der folgenden Schritte aus:

Für CIFS-Freigaben

a. Geben Sie den vollständigen Pfad der CIFS-Freigabe ein, und klicken Sie auf **Verbinden**.

b. Geben Sie den Benutzernamen und das Kennwort ein, um eine Verbindung mit der CIFS-Freigabe herzustellen, und klicken Sie auf **OK**.

   Alle Rechner werden in der Drop-down-Liste "Rechner" aufgelistet, und neben "Rechner" wird eine RPS-Schaltfläche angezeigt.



c. Wählen Sie den Rechner aus der Drop-down-Liste aus, und klicken Sie auf "RPS".

   Das Dialogfeld **Recovery Point Server-Informationen** wird geöffnet.

d. Geben Sie die RPS-Details ein, und klicken Sie auf "Ja".

   Das Dialogfeld **Recovery Point Server-Informationen** wird geschlossen. Alle Wiederherstellungspunkte des ausgewählten Rechners werden unter der Option **Datumsfilter** angezeigt.

Für RPS-Server:

a. Wählen Sie den RPS-Server aus, und klicken Sie auf "Hinzufügen".

   Das Dialogfeld **Recovery Point Server-Informationen** wird geöffnet.

b. Geben Sie die RPS-Details ein, und klicken Sie auf "Laden".

c. Wählen Sie den Datenspeicher aus der Drop-down-Liste aus, und klicken Sie auf **Ja**.

   Das Dialogfeld **Recovery Point Server-Informationen** wird geschlossen, und der Assistent wird angezeigt.

d. Klicken Sie auf **Verbinden**.

   Alle Rechner werden in der Drop-down-Liste "Rechner" aufgelistet.

e. Wählen Sie in der Drop-down-Liste den Rechner aus.

   Alle Wiederherstellungspunkte des ausgewählten Rechners werden unter der Option **Datumsfilter** angezeigt.

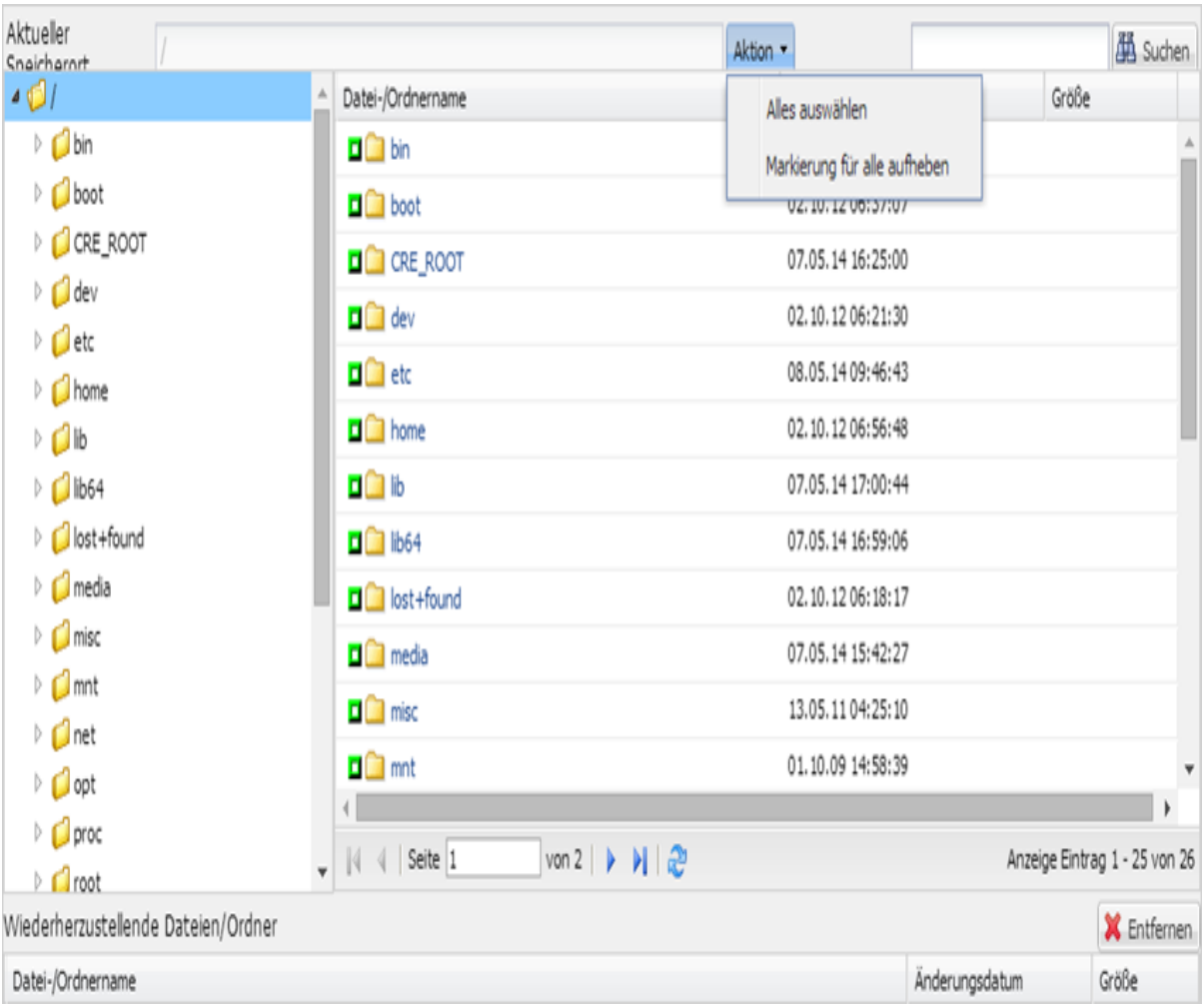
5. Wenden Sie den Datumsfilter an, um die Wiederherstellungspunkte anzuzeigen, die zwischen dem angegebenen Datum generiert werden, und klicken Sie auf **Suchen**.

   Standard: Die letzten zwei Wochen.

   Alle verfügbaren Wiederherstellungspunkte zwischen den angegebenen Datumswerten werden angezeigt.

6. Wählen Sie den gewünschten Wiederherstellungspunkt aus, und klicken Sie auf **Hinzufügen**. Wenn der Wiederherstellungspunkt verschlüsselt ist, geben Sie das Verschlüsselungskennwort ein, um die Daten wiederherzustellen.

   Das Dialogfeld **<Knotenname> durchsuchen** wird geöffnet.



Wichtig! Wenn die Warnmeldung "Die Dateien/Ordner werden unter der Gerätedatei angezeigt. Klicken Sie hier für weitere Informationen." auf der Konsole finden Sie im folgenden Hinweis eine Lösung.

Hinweis: Für einige komplexe Datenträgerlayouts wird das Dateisystem von der Gerätedatei angezeigt. Die Änderung im Anzeigeverhalten des Dateisystems wirkt

sich nicht auf die Funktion der hostbasierten Linux VM-Wiederherstellung auf Dateiebene aus. Sie können das Dateisystem unter der Gerätedatei durchsuchen. Sie können auch die Suchfunktion verwenden, um nach einer bestimmten Datei oder einem Verzeichnis zu suchen.

7. Wählen Sie die Dateien und Ordner aus, die Sie wiederherstellen möchten, und klicken Sie auf **OK**.

   Hinweis: Wenn Sie versuchen, eine Datei oder einen Ordner mithilfe des **Suchfeldes** zu finden, stellen Sie sicher, dass Sie den höchsten Ordner in der Hierarchie auswählen. Die Suche wird in allen untergeordneten Ordnern des ausgewählten Ordners durchgeführt.

   Das Dialogfeld **<Knotenname> durchsuchen** wird geschlossen, und Sie gelangen erneut zur Seite **Wiederherstellungspunkte**. Die ausgewählten Dateien und Ordner sind unter **Wiederherzustellende Dateien/Ordner** aufgeführt.

8. Klicken Sie auf **Weiter**.

   Die Seite **Zielcomputer** wird geöffnet.

   Der Wiederherstellungspunkt wird angegeben.

Angeben der Details des Zielcomputers

Geben Sie die Details des Zielknotens an, damit Daten auf diesem Knoten wiederhergestellt werden. Sie können die ausgewählten Dateien oder Ordner auf dem Quellknoten oder einem neuen Knoten wiederherstellen.

Gehen Sie wie folgt vor, um die Daten auf dem Knoten wiederherzustellen, von dem sie gesichert wurden:

1. Wählen Sie auf der Seite **Zielcomputer** die Option **Am ursprünglichen Speicherort wiederherstellen** aus.

   Das Feld **Hostname** unter **Einstellungen des Zielcomputers** wird mit dem Namen des Quellknotens gefüllt.

2. Geben Sie den Benutzernamen und das Kennwort des Knotens ein.
3. Wählen Sie eine der folgenden Optionen, um Dateikonflikte zu lösen:

   Vorhandene Dateien überschreiben

Gibt an, dass die Sicherungsdatei vom Wiederherstellungspunkt die vorhandene Datei ersetzt, wenn die Datei auf dem Zielcomputer vorhanden ist.

Dateien umbenennen

Gibt an, dass, wenn die Datei im Zielcomputer vorhanden ist, eine neue Datei mit demselben Dateinamen und der Dateierweiterung *.d2d-duplicate<x>* erstellt wird. <x> gibt an, wie oft die Datei wiederhergestellt wird. Alle Daten werden dann in eine neue Datei wiederhergestellt.

Vorhandene Dateien überspringen

Gibt an, dass die Dateien, wenn dieselbe Datei auf dem Zielcomputer vorhanden ist, nicht vom Wiederherstellungspunkt wiederhergestellt werden.

4. Klicken Sie auf **Weiter**.

   Die Seite **Erweitert** wird geöffnet.

Gehen Sie wie folgt vor, um die Wiederherstellung auf einen neuen Knoten durchzuführen:

1. Wählen Sie auf der Seite **Zielcomputer** die Option **An einem alternativen Speicherort wiederherstellen** aus.

2. Geben Sie den Hostnamen oder die IP-Adresse des Zielknotens ein.
3. Geben Sie den Benutzernamen und das Kennwort des Knotens ein.
4. Geben Sie den Pfad ein, in dem die Daten wiederhergestellt werden sollen, oder klicken Sie auf **Durchsuchen**, um den Ordner auszuwählen, in dem die Daten wiederhergestellt werden sollen, und klicken Sie dann auf **OK**.
5. Wählen Sie eine der folgenden Optionen, um Dateikonflikte zu lösen:

   Vorhandene Dateien überschreiben

   Gibt an, dass die Sicherungsdatei vom Wiederherstellungspunkt die vorhandene Datei ersetzt, wenn die Datei auf dem Zielcomputer vorhanden ist.

   Dateien umbenennen

   Gibt an, dass, wenn die Datei im Zielcomputer vorhanden ist, eine neue Datei mit demselben Dateinamen und der Dateierweiterung *.d2d-duplicate<x>* erstellt wird. <x> gibt an, wie oft die Datei wiederhergestellt wird. Alle Daten werden dann in eine neue Datei wiederhergestellt.

Vorhandene Dateien überspringen

Gibt an, dass die Dateien, wenn dieselbe Datei auf dem Zielcomputer vorhanden ist, nicht vom Wiederherstellungspunkt wiederhergestellt werden.

6. (Optional) Wählen Sie **Stammverzeichnis erstellen**.
7. Klicken Sie auf **Weiter**.

   Die Seite **Erweitert** wird geöffnet.

Die Details des Zielcomputers sind angegeben.

Festlegen von erweiterten Einstellungen

Geben Sie die erweiterten Einstellungen an, um eine geplante Wiederherstellung der Daten auszuführen. Mit einer geplanten Wiederherstellung wird sichergestellt, dass die Daten auch bei Ihrer Abwesenheit zur angegebenen Zeit wiederhergestellt werden.

Gehen Sie wie folgt vor:

1. Legen Sie Datum und Uhrzeit für den Beginn fest, indem Sie eine der folgenden Optionen auswählen:

   Jetzt ausführen

   Startet den Wiederherstellungsjob auf Dateiebene sofort, nachdem Sie den Job übergeben haben.

   Startdatum und -zeitpunkt festlegen

   Startet den Wiederherstellungsjob auf Dateiebene zum angegebenen Datum und Zeitpunkt, nachdem Sie den Job übergeben haben.

2. (Optional) Wählen Sie "**Geschätzte Dateigröße**".

3. (Optional) Wählen Sie ein Skript aus der Option **Einstellungen für Prä-/Post-Skripts** aus.

   Diese Skripte führen Skriptbefehle für Aktionen aus, die vor dem Start des Jobs und/oder nach Abschluss des Jobs durchgeführt werden sollen.

   Hinweis: Die Felder für **Einstellungen vor/nach dem Skript** werden nur aufgefüllt, wenn Sie bereits eine Skriptdatei erstellt und an folgendem Speicherort platziert haben:

   /opt/Arcserve/d2dserver/usr/prepost

   Hinweis: Weitere Informationen zur Erstellung der Prä-/Post-Skripte finden Sie unter *Verwalten der Prä-/Post-Skripte für Automatisierung*.

4. Klicken Sie auf **Weiter**.

   Die Seite **"Zusammenfassung"** wird geöffnet.

   Die erweiterten Einstellungen sind angegeben.

(Optional) Verwalten der Prä-/Post-Skripte für Automatisierung

Mit Prä-/Post-Skripts können Sie Ihre eigene Geschäftslogik in bestimmten Phasen eines laufenden Jobs ausführen. Sie können in **Einstellungen vor/nach dem Skript** des **Sicherungsassistenten** und des **Wiederherstellungsassistenten** auf der Benutzeroberfläche angeben, wann Ihre Skripte ausgeführt werden sollen. Die Skripts können je nach Einstellung auf dem Sicherungsserver ausgeführt werden.

Das Verwalten von Prä-/Post-Skripts ist ein zweiteiliger Vorgang, der das Erstellen des Prä-/Post-Skripts und das Einfügen des Skripts in den "prepost"-Ordners umfasst.

Erstellen von Prä-/Post-Skripts

Gehen Sie wie folgt vor:

1. Melden Sie sich als Root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie eine Skriptdatei, indem Sie die Umgebungsvariablen in Ihrer bevorzugten Skripterstellungssprache verwenden.

   Umgebungsvariablen des Prä-/Post-Skripts

   Verwenden Sie die folgenden Umgebungsvariablen, um Ihr Skript zu erstellen:

   D2D_JOBNAME

   Gibt den Namen des Jobs an.

   D2D_JOBID

   Gibt die Job-ID an. Die Job-ID ist eine Nummer, die für den Job vergeben wird, wenn Sie den Job ausführen. Wenn Sie den gleichen Job erneut ausführen, erhalten Sie eine neue Jobnummer.

   D2D_TARGETNODE

   Identifiziert den Knoten, der gesichert oder wiederhergestellt wird.

   D2D_JOBTYPE

   Identifiziert den Typ des ausgeführten Jobs. Die folgenden Werte identifizieren die D2D_JOBTYPE-Variable:

   backup.full

   Identifiziert den Job als eine vollständige Sicherung.

   backup.incremental

   Identifiziert den Job als eine Zuwachssicherung.

backup.verify

Identifiziert den Job als eine Überprüfungssicherung.

restore.bmr

Identifiziert den Job als eine Bare-Metal-Recovery (BMR). Dies ist ein Wiederherstellungsjob.

restore.file

Identifiziert den Job als eine Wiederherstellung auf Dateiebene. Dies ist ein Wiederherstellungsjob.

D2D_SESSIONLOCATION

Identifiziert den Speicherort, an dem die Wiederherstellungspunkte gespeichert sind.

D2D_PREPOST_OUTPUT

Identifiziert eine Temp-Datei. Der Inhalt der Anfangszeile der Temp-Datei wird im Aktivitätsprotokoll angezeigt.

D2D_JOBSTAGE

Gibt die Phase des Jobs an. Die folgenden Werte identifizieren die D2D_ JOBSTAGE-Variable:

pre-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, bevor der Job startet.

post-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Job startet.

post-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Snapshot erfasst wird.

post-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Snapshot erfasst wird.

D2D_TARGETVOLUME

Identifiziert das Volume, das während eines Sicherungsjobs gesichert wird. Diese Variable ist anwendbar für Prä-/Post-Snapshot-Skripts für einen Sicherungsjob.

D2D_JOBRESULT

Identifiziert das Ergebnis für ein Post-Job-Skript. Die folgenden Werte identifizieren die D2D_JOBRESULT-Variable:

success

Identifiziert das Ergebnis als erfolgreich.

fail

Identifiziert das Ergebnis als nicht erfolgreich.

D2DSVR_HOME

Identifiziert den Ordner, in dem der Sicherungsserver installiert ist. Diese Variable ist anwendbar für die Skripts, die auf dem Sicherungsserver ausgeführt werden.

Das Skript ist erstellt.

Hinweis: Bei allen Skripten zeigt der Rückgabewert von Null eine erfolgreiche Erstellung an, und ein Rückgabewert, der ungleich Null ist, weist auf einen Fehler hin.

Einfügen des Skripts in den Ordner "Prepost" und Überprüfung des Skripts

Alle Prä-/Post-Skripts für einen Sicherungsserver werden zentral vom Ordner "prepost" am folgenden Speicherort verwaltet:

/opt/Arcserve/d2dserver/usr/prepost

Gehen Sie wie folgt vor:

1. Fügen Sie die Datei in folgenden Speicherort des Sicherungsservers ein:

   /opt/Arcserve/d2dserver/usr/prepost

2. Geben Sie der Skriptdatei Ausführungsberechtigungen.
3. Melden Sie sich bei der Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche an.
4. Öffnen Sie den **Sicherungsassistenten** oder **Wiederherstellungsassistenten**, und navigieren Sie zur Registerkarte **Erweitert**.
5. Wählen Sie die Skriptdatei in der Drop-down-Liste **Einstellungen vor/nach dem Skript** aus, und übergeben Sie den Job.

6. Klicken Sie auf "**Aktivitätsprotokoll**", und stellen Sie sicher, dass das Skript für den angegebenen Sicherungsjob ausgeführt wird.

   Das Skript wird ausgeführt.

   Die Prä-/Post-Skripte wurden erfolgreich erstellt und befinden sich im Ordner "pre-post".

Erstellen und Ausführen des Wiederherstellungsjobs

Erstellen Sie den Wiederherstellungsjob, und führen Sie ihn aus, sodass Sie die Wiederherstellung auf Dateiebene initiieren können. Überprüfen Sie die Wiederherstellungspunktinformationen, bevor Sie die Dateien wiederherstellen. Bei Bedarf können Sie zurückgehen und die Wiederherstellungseinstellungen im Assistenten ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Wiederherstellungsdetails auf der Seite **Zusammenfassung** des **Wiederherstellungsassistenten**.
2. Klicken Sie auf **Zurück**, um Informationen zu ändern, die Sie auf den Seiten des **Wiederherstellungsassistenten** eingegeben haben (optional).
3. Geben Sie einen Jobnamen ein, und klicken Sie auf **Übergeben**.

   Im Feld **Jobname** ist zunächst ein Standardname angegeben. Sie können einen neuen Jobnamen Ihrer Wahl eingeben, wobei das Feld jedoch nicht leer gelassen werden darf.

   Der **Wiederherstellungsassistent** wird geschlossen. Der Status des Jobs wird auf der Registerkarte **Jobstatus** angezeigt.

   Der Wiederherstellungsjob wurde erfolgreich erstellt und ausgeführt.

Überprüfen, dass Dateien wiederhergestellt wurden

Überprüfen Sie nach Abschluss des Wiederherstellungsjobs, dass alle Dateien im Zielknoten wiederhergestellt wurden. Überprüfen Sie die Registerkarten **Jobübersicht** und **Aktivitätsprotokoll** im Fenster **Status**, um den Fortschritt des Wiederherstellungsprozesses zu überwachen.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Zielcomputer, auf dem Sie die Daten wiederhergestellt haben.
2. Überprüfen Sie, dass die erforderlichen Daten vom Wiederherstellungspunkt wiederhergestellt wurden.

   Die Dateien wurden erfolgreich überprüft.

   Die Wiederherstellung auf Dateiebene wurde erfolgreich ausgeführt.

So führen Sie eine IVM-Migration (vom Linux-Wiederherstellungspunkt) aus der Cloud auf einen lokalen Rechner durch

Wenn Sie über einen Linux-Wiederherstellungspunkt auf Amazon S3 verfügen, können Sie einen IVM-Job in AWS ausführen und dann die IVM aus AWS auf einen lokalen Rechner migrieren.

Führen Sie zum Durchführen einer IVM-Migration die folgenden Tasks aus:

- Überprüfen der Voraussetzungen für die IVM-Migration
- Durchführen der IVM-Migration aus der Cloud auf einen lokalen Rechner

Überprüfen der Voraussetzungen und besonderen Aspekte für die IVM-Migration

Voraussetzungen:

- Sie verfügen über einen gültigen Wiederherstellungspunkt und, falls erforderlich, über das Verschlüsselungskennwort für die Wiederherstellung.
- Sie haben ein Amazon EC2- und Amazon S3-Konto.
- Samba-Server ist auf dem Linux-Sicherungsserver installiert.

Besondere Aspekte:

Diese Funktion wird nur auf einem Linux-Sicherungsserver unter RHEL/CentOS/Oracle Linux 7.x oder SLES 12.x unterstützt.

Durchführen der IVM-Migration aus der Cloud auf einen lokalen Rechner

Sie können eine IVM mit drei detaillierten Verfahren aus der Cloud auf einen lokalen Rechner migrieren. Klicken Sie auf die Links der einzelnen Verfahren, und führen Sie die angegebenen Schritte aus, um die Migration durchzuführen.

- Um eine Instant VM in Amazon EC2 zu erstellen, führen Sie eine Instant VM von einem Linux VM-Wiederherstellungspunkt in Amazon EC2 aus.
- Installieren Sie den Linux-Sicherungsserver in dieser soeben erstellten Instant VM. Führen Sie die Sicherung in der IVM aus, und wählen Sie Amazon S3 als Sicherungsziel.
- Sichern Sie den Linux-Rechner auf Amazon S3.
- Führen Sie einen BMR-Job von dem Wiederherstellungspunkt in Amazon S3 aus, den Sie gesichert haben.

So führen Sie eine Bare-Metal-Recovery (BMR) für Linux-Rechner aus

Eine BMR stellt das Betriebssystem und die Software-Anwendungen sowie alle gesicherten Daten wieder her. Eine BMR ist der Prozess, bei dem ein *Bare-Metal*-Computersystem wiederhergestellt wird. "Bare Metal" bezeichnet einen Computer ohne Betriebssystem, Treiber und Software-Anwendungen. Nachdem die Wiederherstellung abgeschlossen wurde, startet der Zielcomputer automatisch in der gleichen Betriebsumgebung wie der Sicherungsquellknoten neu, und alle Daten werden wiederhergestellt.

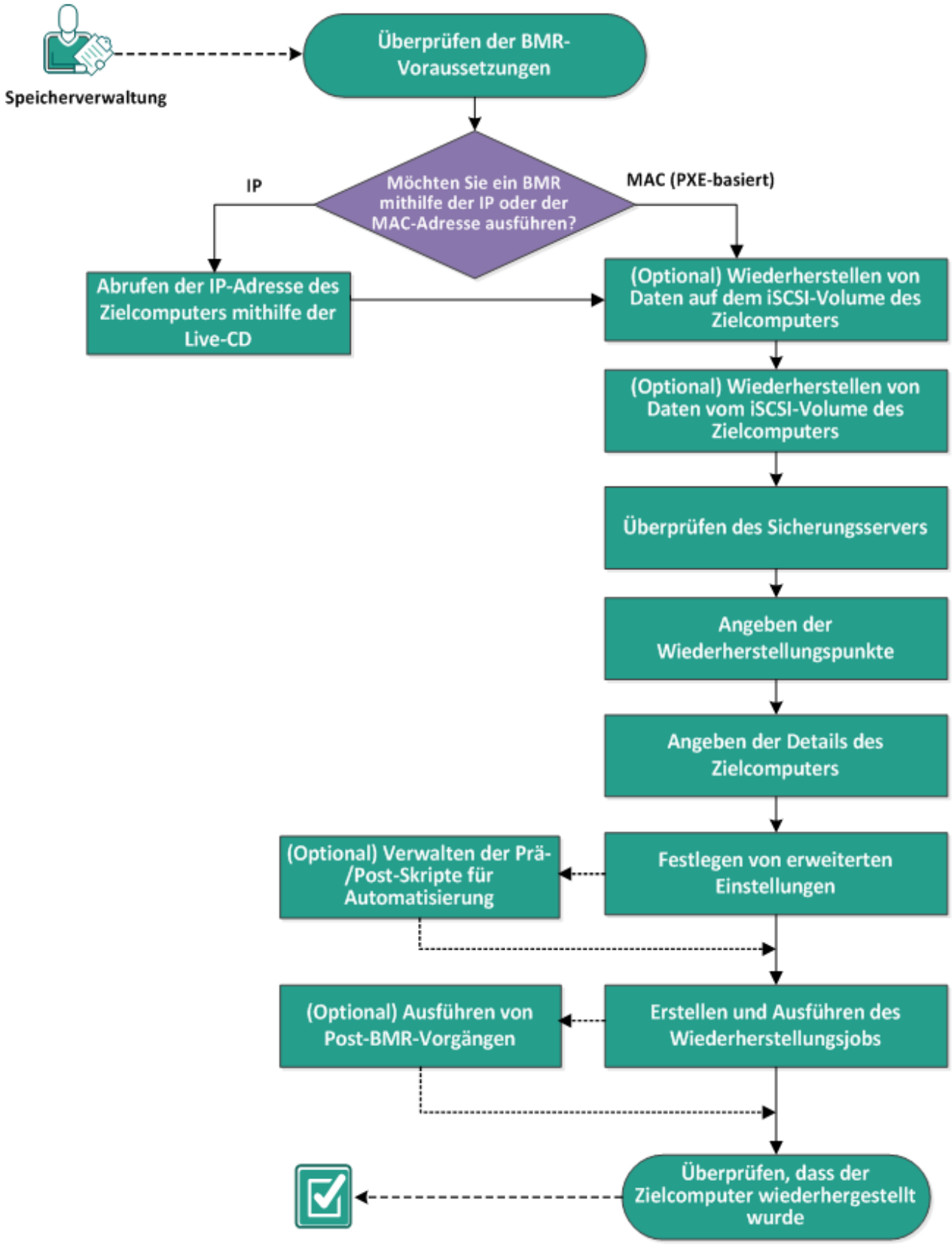
Eine vollständige BMR ist möglich, da beim Ausführen einer Sicherung der Daten auch Informationen aufzeichnet werden, die sich auf das Betriebssystem, die installierten Anwendungen, Treiber usw. beziehen.

Sie können eine BMR unter Verwendung der IP-Adresse oder der MAC-Adresse (Media Access Control) des Zielcomputers ausführen. Wenn Sie den Zielcomputer mithilfe der Arcserve Unified Data Protection Agent for Linux-Live-CD booten, können Sie die IP-Adresse des Zielcomputers abrufen.

Hinweis: Der Rechner kann starten. Nur eine NIC ist konfiguriert.

Folgendes Diagramm zeigt den Prozess an, um eine BMR auszuführen:

So führen Sie eine Bare-Metal-Recovery (BMR) für Linux-Rechner aus



Gehen Sie folgt vor, um eine BMR auszuführen:

- Überprüfen der Voraussetzungen
- Abrufen der IP-Adresse des Zielcomputers mithilfe der Live-CD
- (Optional) Wiederherstellen von Daten auf dem iSCSI-Volume des Zielcomputers
- (Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers
- Überprüfen des Sicherungsservers
- Angeben der Wiederherstellungspunkte
- Angeben der Details des Zielcomputers
- Festlegen von erweiterten Einstellungen
- (Optional) Verwalten der Prä-/Post-Skripte für Automatisierung
- Erstellen und Ausführen des Wiederherstellungsjobs
- (Optional) Ausführen von Post-BMR-Vorgängen
- Überprüfen, dass der Zielcomputer wiederhergestellt wurde

Überprüfen der Voraussetzungen

Beachten Sie Folgendes, bevor Sie eine BMR durchführen:

- Sie verfügen über einen gültigen Wiederherstellungspunkt und, falls erforderlich, über das Verschlüsselungskennwort für die Wiederherstellung.
- Sie verfügen über einen gültigen Zielcomputer für die BMR.
- Sie haben die Arcserve Unified Data Protection Agent for Linux-Live-CD erstellt.
- Wenn Sie eine BMR mithilfe der IP-Adresse ausführen möchten, müssen Sie die IP-Adresse des Zielcomputers mithilfe der Live-CD abrufen.
- Wenn Sie eine PXE-basierte BMR mithilfe der MAC-Adresse ausführen möchten, müssen Sie die MAC-Adresse des Zielcomputers haben.
- Der Wiederherstellungspunkt muss aus einer agentenbasierten Linux-Sicherung stammen.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Abrufen der IP-Adresse des Zielcomputers mithilfe der Live-CD

Bevor Sie eine BMR mithilfe der IP-Adresse ausführen können, müssen Sie die IP-Adresse des Zielcomputers ermitteln. Ein Bare-Metal-Computer verfügt anfänglich nicht über eine IP-Adresse. Sie müssen den Bare-Metal-Computer daher mit der Standard-Live-CD (<Arcserve Unified Data Protection Agent for Linux-Live-CD) oder der CentOS-basierten Live-CD booten, um die IP-Adresse abzurufen. Nachdem Sie die IP-Adresse des Zielcomputers abgerufen haben, können Sie die statische IP des Zielcomputers konfigurieren.

Gehen Sie wie folgt vor:

1. Legen Sie die Live-CD ein oder laden Sie die ISO-Datei der Live-CD im CD-ROM-Laufwerk des Zielknotens.
2. Starten Sie den Zielcomputer von CD-ROM.

   Der Zielcomputer startet in der Umgebung der Arcserve Unified Data Protection Agent for Linux-Live-CD. Auf dem Bildschirm wird die IP-Adresse des Zielcomputers angezeigt.
3. Um die statische IP des Zielcomputers mithilfe der Live-CD zu konfigurieren, führen Sie die folgenden Schritte aus:
   a. Drücken Sie im Fenster des Zielcomputers auf die Eingabetaste, um in die Shell-Umgebung zu gelangen.
   b. Führen Sie folgenden Befehl aus, um die statische IP zu konfigurieren:

      ifconfig <NIC-Name> <statische IP-Adresse> netmask <Netzmaske>

      route add default gw <Gateway-IP-Adresse> <NIC-Name>

   Hinweis: Der Name Ihrer Netzwerkkarte (NIC) hängt von Ihrer Hardware ab. Typische NIC-Namen sind z. B. "eth0" oder "em0".
4. Um die statische IP des Zielcomputers mithilfe der CentOS-basierten Live-CD zu konfigurieren, führen Sie die folgenden Schritte aus:
   a. Öffnen Sie ein Terminal-Fenster auf dem Zielrechner, indem Sie auf "Anwendungen", "System-Tools", "Terminal" klicken.
   b. Führen Sie die folgenden Befehle aus:

      sudo ifconfig <NIC-Name> <statische IP-Adresse> netmask <Netzmaske>

      sudo route add default gw <Gateway-IP-Adresse> <NIC-Name>

   Die statische IP ist konfiguriert.

   Die IP-Adresse des Zielcomputers wird erfasst.

Wichtig! Notieren Sie diese IP-Adresse. Sie wird benötigt, wenn Sie die Details des Zielcomputers im **Wiederherstellungsassistenten** angeben müssen.

(Optional) Wiederherstellen von Daten auf dem iSCSI-Volume des Zielcomputers

Sie können das iSCSI-Volume mit dem Zielcomputer integrieren und es zu einem Teil des Zielcomputers machen. Danach können Sie Daten auf dem iSCSI-Volume des Zielcomputers wiederherstellen. Auf diese Weise können Sie Daten über ein Netzwerk verwalten und übertragen.

Wichtig! Wenn Sie das iSCSI-Volume mit dem Zielcomputer integrieren, verlieren Sie sämtliche vorhandenen Daten auf dem iSCSI-Volume.

Gehen Sie wie folgt vor:

1. Legen Sie die Arcserve Unified Data Protection Agent for Linux-Live-CD ein oder laden Sie die ISO-Datei der Arcserve Unified Data Protection Agent for Linux-Live-CD im CD-ROM-Laufwerk des Zielcomputers.
2. Starten Sie den Zielcomputer über die CD-ROM.

   Der Zielcomputer startet in der Umgebung der Arcserve Unified Data Protection Agent for Linux-Live-CD. Auf dem Bildschirm wird die IP-Adresse des Zielcomputers angezeigt.
3. Geben Sie die Shell-Umgebung des Zielcomputers ein.
4. Führen Sie den folgenden Befehl aus, den iSCSI-Initiator-Daemon zu starten:

   ```
   /etc/init.d/iscsid start
   ```
5. Führen Sie zwecks Erkennung des iSCSI-Zielhosts ein Discovery-Skript aus.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   Der Standardportwert des iSCSI-Zielhost ist 3260.
6. Notieren Sie den iSCSI Qualified Name (IQN) des iSCSI-Zielhost, der durch das Discovery-Skript gefunden wird, bevor Sie sich manuell beim erkannten Zielcomputer anmelden.
7. Listen Sie das verfügbare Blockgerät des Zielknotens auf.

   ```
   #fdisk -l
   ```
8. Melden Sie sich beim erkannten Ziel an.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l
   ```

   Im Verzeichnis /dev des Zielknotens wird ein Blockgerät angezeigt.
9. Führen Sie den folgenden Befehl aus, um den Namen des neuen Geräts abzurufen:

#fdisk -l

Im Zielknoten können Sie ein zusätzliches Gerät, /dev/sd<x>, sehen.

Das iSCSI-Volume wurde mit dem Ziel-Volume integriert.

(Optional) Wiederherstellen von Daten des iSCSI-Volume des Zielcomputers

Wenn Sie Ihre Daten auf einem iSCSI-Zieldatenträger gespeichert haben, können Sie eine Verbindung mit dem iSCSI-Volume herstellen und Daten wiederherstellen. Das iSCSI-Volume ermöglicht das Verwalten und Übertragen von Daten über ein Netzwerk.

Gehen Sie wie folgt vor:

1. Legen Sie die Arcserve Unified Data Protection Agent for Linux-Live-CD ein oder laden Sie die ISO-Datei der Arcserve Unified Data Protection Agent for Linux-Live-CD im CD-ROM-Laufwerk des Zielcomputers.
2. Starten Sie den Zielcomputer über die CD-ROM.

   Der Zielcomputer startet in der Umgebung der Arcserve Unified Data Protection Agent for Linux-Live-CD. Auf dem Bildschirm wird die IP-Adresse des Zielcomputers angezeigt.
3. Geben Sie die Shell-Umgebung des Zielcomputers ein.
4. Führen Sie den folgenden Befehl aus, den iSCSI-Initiator-Daemon zu starten:

   /etc/init.d/iscsid start
5. Führen Sie zwecks Erkennung des iSCSI-Zielhosts ein Discovery-Skript aus.

   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADRESSE>:<Port-nummer>

   Der Standardportwert des iSCSI-Zielhost ist 3260.
6. Notieren Sie den iSCSI Qualified Name (IQN) des iSCSI-Zielhost, der durch das Discovery-Skript gefunden wird, bevor Sie sich manuell beim erkannten Zielcomputer anmelden.
7. Listen Sie das verfügbare Blockgerät des Zielknotens auf.

   #fdisk -l
8. Melden Sie sich beim erkannten Ziel an.

   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADRESSE>:<Portnummer> -l

   Im Verzeichnis /dev des Zielknotens wird ein Blockgerät angezeigt.
9. Führen Sie den folgenden Befehl aus, um den Namen des neuen Geräts abzurufen:

   #fdisk -l

   Im Zielknoten können Sie ein zusätzliches Gerät, /dev/sd<x>, sehen.

In diesem Beispiel ist der Name des Geräts "/dev/sdc". In den folgenden Schritten wird dieser Gerätename verwendet, um eine Partition und ein Dateisystem zu erstellen.

10. Laden Sie das iSCSI-Volume mithilfe der folgenden Befehle:

    # mkdir /iscsi

    # mount /dev/sdc1 /iscsi

    Hinweis: Wenn Sie den Sitzungsspeicherort im Wiederherstellungsassistenten angeben, müssen Sie "Lokal" auswählen und den Pfad /iscsi eingeben.

    Beispiel: <path>/iscsi

    Der Zielcomputer kann jetzt eine Verbindung mit dem iSCSI-Volume herstellen und Daten vom iSCSI-Volume wiederherstellen.

Überprüfen des Backup-Servers

Wenn Sie den **Wiederherstellungsassistenten** öffnen, überprüfen Sie den Sicherungsserver, auf dem die Wiederherstellung ausgeführt werden soll.

Gehen Sie wie folgt vor:

1. Führen Sie einen der folgenden Vorgänge durch, um auf den Wiederherstellungsassistenten zuzugreifen:

   Von Arcserve UDP :

   a. Melden Sie sich bei Arcserve UDP an.

   b. Klicken Sie auf die Registerkarte **Ressourcen**.

   c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

   e. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

      Die Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche wird geöffnet. Das Auswahldialogfeld für den Wiederherstellungstyp wird in der Benutzeroberfläche des Agenten angezeigt.

   f. Wählen Sie den Wiederherstellungstyp aus, und klicken Sie auf **OK**.

      Hinweis: Sie werden automatisch beim Agentenknoten angemeldet, und der **Wiederherstellungsassistent** wird im Agentenknoten geöffnet.

   Von Arcserve Unified Data Protection Agent for Linux :

   a. Öffnen Sie die Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche.

      Hinweis: Während der Installation von Arcserve Unified Data Protection Agent for Linux haben Sie die URL erhalten, um auf den Server zugreifen und ihn verwalten zu können. Melden Sie sich bei Arcserve Unified Data Protection Agent for Linux an.

   b. Klicken Sie auf **Wiederherstellen** im Menü **Assistent**, und wählen Sie **Bare-Metal-Recovery (BMR)** aus.

      Die Seite **Sicherungsserver** in **Wiederherstellungsassistent – BMR** wird geöffnet.

2. Überprüfen Sie den Server in der Drop-down-Liste **Sicherungsserver** auf der Seite **Sicherungsserver**.

Sie können in der Drop-down-Liste **Sicherungsserver** keine Optionen auswählen.

3. Klicken Sie auf **Weiter**.

   Die Seite **Wiederherstellungspunkte** des **Wiederherstellungsassistenten – BMR** wird geöffnet.

   Der Sicherungsserver wird angegeben.

Angeben der Wiederherstellungspunkte

Bei jedem Ausführen einer Sicherung wird ein Wiederherstellungspunkt erstellt. Geben Sie die Informationen zu den Wiederherstellungspunkten im **Wiederherstellungsassistenten** an, damit genau die gewünschten Daten wiederhergestellt werden. Sie können je nach Bedarf bestimmte Dateien oder alle Dateien wiederherstellen.

Wichtig! Um eine BMR von einem Wiederherstellungspunkt ausführen zu können, müssen das root-Volume und das Start-Volume im Wiederherstellungspunkt vorhanden sein.

Gehen Sie wie folgt vor:

1. Führen Sie je nach Sicherungsspeicher einen der folgenden Schritte aus.
   - Führen Sie folgende Schritte aus, um auf Wiederherstellungspunkte zuzugreifen, wenn die Wiederherstellungspunkte auf einem mobilen Gerät gespeichert sind:
     a. Starten Sie den Zielcomputer mithilfe der Live-CD.
     b. Melden Sie sich über die Live-CD bei der Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche an.
     c. Öffnen Sie den **BMR-Assistenten**.
     d. Navigieren Sie zur Seite **Wiederherstellungspunkte**.
     e. Wählen Sie auf der Seite **Wiederherstellungspunkte** des **BMR-Assistenten** als **Sitzungsspeicherort Lokal** aus.
   - Führen Sie folgende Schritte aus, wenn der Sitzungsspeicherort "NFS-Freigabe" oder "CIFS-Freigabe" ist:
     a. Wählen Sie in der Drop-down-Liste **Sitzungsspeicherort** eine Sitzung aus, und geben Sie den vollständigen Pfad der Freigabe ein.

        Nehmen Sie zum Beispiel an, dass der Sitzungsspeicherort eine NFS-Freigabe, xxx.xxx.xxx.xxx die IP-Adresse der NFS-Freigabe und der Ordnername *Daten ist.* Sie geben dann "xxx.xxx.xxx.xxx:/Daten" als Speicherort der NFS-Freigabe an.

        Hinweis: Wenn die gesicherten Daten unter "Quelle – lokal" gespeichert werden, müssen Sie den Quellknoten zuerst in einen NFS-Server

konvertieren und dann den Sitzungsspeicherort freigeben.

2. Klicken Sie auf **Verbinden**.

   Alle Knoten, die an diesem Speicherort gesichert wurden, werden in der Drop-down-Liste **Rechner** aufgelistet.

3. Wählen Sie den Knoten, von dem Sie eine Wiederherstellung vornehmen möchten, in der Drop-down-Liste **Rechner** aus.

   Es werden alle Wiederherstellungspunkte des ausgewählten Knotens aufgelistet.

4. Wenden Sie den Datumsfilter an, um die Wiederherstellungspunkte anzuzeigen, die zwischen dem angegebenen Datum generiert werden, und klicken Sie auf **Suchen**.

   Standard: Die letzten zwei Wochen.

   Alle verfügbaren Wiederherstellungspunkte zwischen den angegebenen Datumswerten werden angezeigt.

5. Wählen Sie den gewünschten Wiederherstellungspunkt aus, und klicken Sie auf **Weiter**.

Die Seite **Zielcomputer** wird geöffnet.

Der Wiederherstellungspunkt wird angegeben.

Angeben der Details des Zielcomputers

Geben Sie die Details des Zielcomputers an, damit Daten auf diesem Rechner wiederhergestellt werden. Ein Zielcomputer ist ein Bare-Metal-Rechner, auf dem Sie eine BMR ausführen. Wenn Sie mithilfe der IP-Adresse wiederherstellen, benötigen Sie die IP-Adresse des Zielcomputers, die Sie zu Beginn dieses Prozesses notiert haben. Wenn Sie mithilfe der MAC-Adresse (Media Access Control) wiederherstellen, benötigen Sie die MAC-Adresse des Zielcomputers.

Gehen Sie wie folgt vor:

1. Geben Sie die MAC-Adresse oder die IP-Adresse des Zielcomputers im Feld **MAC-/IP-Adresse** ein.
2. Geben Sie einen Namen in das Feld **Hostname** ein.

   Der Zielcomputer verwendet diesen Namen als Hostnamen, wenn die Wiederherstellung abgeschlossen ist.
3. Wählen Sie eine der folgenden Optionen als Netzwerk aus:

   DHCP

   Konfiguriert die IP-Adresse automatisch. Dies ist die Standardoption. Verwenden Sie diese Option, wenn Sie über einen DHCP-Server (Dynamic Host Configuration Protocol) verfügen, um über die Wiederherstellung über das DHCP-Netzwerk auszuführen.

   Statische IP

   Konfiguriert die IP-Adresse manuell. Wenn Sie diese Option auswählen, geben Sie **IP-Adresse**, **Subnetzmaske** und **Standard-Gateway** des Zielrechners ein.

   Wichtig! Stellen Sie sicher, dass die statische IP von keinen anderen Rechnern im Netzwerk verwendet wird, während die Wiederherstellung durchgeführt wird.
4. (Optional) Wählen Sie die Option **Sofortige BMR** aus, damit Sie den Zielrechner sofort verwenden können.

   Wenn Sie diese Option aktivieren, stellt Arcserve Unified Data Protection Agent for Linux zunächst die notwendigen Daten her, die erforderlich sind, um den Rechner zu starten. Die verbleibenden Daten werden wiederhergestellt, nachdem der Zielrechner gestartet wurde. Die Netzwerkverbindung muss während der Instant-BMR ständig verfügbar sein.

   Beispiel: Wenn Sie 100 GB Daten haben und Sie eine BMR ausführen möchten und diese Option *nicht* auswählen, werden erst alle 100 GB Daten wiederhergestellt, und Sie können dann den Zielrechner verwenden. Allerdings sind nur 1 GB an Daten erforderlich, den Rechner zu starten. Wenn Sie diese Option aktivieren, werden

zunächst die erforderlichen 1 GB Daten wiederhergestellt, sodass Sie den Rechner starten und nutzen können. Nachdem der Rechner gestartet wurde, werden die verbleibenden 99 GB Daten automatisch wiederhergestellt.

Hinweis: Welche Daten für den Start des Rechners erforderlich sind, hängt von der Konfiguration des Betriebssystems ab. Außerdem können Sie die automatische Wiederherstellung von Daten anhalten oder unterbrechen, wenn die Option **Daten nach Start des Rechners nicht automatisch wiederherstellen** nicht aktiviert ist.

5. (Optional) Wählen Sie die Option **Daten nach Start des Rechners nicht automatisch wiederherstellen** aus, um die automatische Wiederherstellung der Daten zu stoppen, wenn der Zielcomputer gestartet wird.

   Wenn Sie die Option **Sofortige BMR aktivieren** auswählen, sollten standardmäßig erst die erforderlichen Daten wiederhergestellt und anschließend der Rechner neu gestartet werden. Nachdem der Rechner gestartet wird, werden die verbleibenden Daten automatisch wiederhergestellt. Wenn Sie Quelldaten während der Wiederherstellung aktualisieren, werden durch Auswahl dieser Option die Daten bis zu dem Punkt wiederhergestellt, an dem sie aktualisiert werden.

6. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Erweitert** wird geöffnet.

   Die Details des Zielcomputers sind angegeben.

Festlegen von erweiterten Einstellungen

Geben Sie die erweiterten Einstellungen an, um eine geplante BMR der Daten auszuführen. Mit einer geplanten BMR wird sichergestellt, dass die Daten auch bei Ihrer Abwesenheit zur angegebenen Zeit wiederhergestellt werden.

Gehen Sie wie folgt vor:

1. Legen Sie Datum und Uhrzeit für den Beginn fest, indem Sie eine der folgenden Optionen auswählen:

   Jetzt ausführen

   Startet den Wiederherstellungsjob sofort, nachdem Sie den Job übergeben haben.

   Spezielle Zeit festlegen

   Startet den Wiederherstellungsjob zur angegebenen Zeit, nachdem Sie den Job übergeben haben.

2. (Optional) Wählen Sie ein Skript aus der Option "**Einstellungen für Prä-/Post-Skripts**" für den Sicherungsserver und den Zielcomputer aus.

   Diese Skripte führen Skriptbefehle für Aktionen aus, die vor dem Start des Jobs und/oder nach Abschluss des Jobs durchgeführt werden sollen.

   Hinweis: Die Felder für **Einstellungen vor/nach dem Skript** werden nur aufgefüllt, wenn Sie bereits eine Skriptdatei erstellt und an folgendem Speicherort platziert haben:

   /opt/Arcserve/d2dserver/usr/prepost

   Hinweis: Weitere Informationen zur Erstellung der Prä-/Post-Skripte finden Sie unter *Verwalten der Prä-/Post-Skripte für Automatisierung*.

3. (Optional) Klicken Sie auf "**Weitere Einstellungen anzeigen**", um weitere Einstellungen für die BMR anzuzeigen.

4. (Optional) Setzen Sie das Kennwort für den angegebenen Benutzernamen des wiederhergestellten Zielcomputers zurück.

5. (Optional) Geben Sie den vollständigen Pfad des Sicherungsspeicherorts der Wiederherstellungspunkte unter "**Wiederherstellungspunkt - Lokaler Zugriff**" an.

6. (Optional) Geben Sie den vollständigen Namen des Datenträgers im Feld "**Datenträger**" ein, um diese Datenträger auf dem Zielcomputer von der Wiederherstellung auszuschließen.

7. (Optional) Wählen Sie "**Wake-on-LAN aktivieren**", wenn Sie eine PXE-BMR (Preboot Execution Environment) ausführen.

Hinweis: Die Option **Wake-on-LAN aktivieren** kann nur auf physische Rechner angewendet werden. Stellen Sie sicher, ob Sie die Wake-on-LAN-Einstellungen in den BIOS-Einstellungen Ihres physischen Rechners aktiviert haben.

8. (Optional) Wählen Sie die Option **Neu starten** aus, um den Zielknoten nach Abschluss der BMR neu zu starten.
9. Klicken Sie auf **Weiter**.

   Die Seite **"Zusammenfassung"** wird geöffnet.

   Die erweiterten Einstellungen sind angegeben.

(Optional) Verwalten der Prä-/Post-Skripte für Automatisierung

Mit Prä-/Post-Skripts können Sie Ihre eigene Geschäftslogik in bestimmten Phasen eines laufenden Jobs ausführen. Sie können in **Einstellungen vor/nach dem Skript** des **Sicherungsassistenten** und des **Wiederherstellungsassistenten** auf der Benutzeroberfläche angeben, wann Ihre Skripte ausgeführt werden sollen. Die Skripts können je nach Einstellung auf dem Sicherungsserver ausgeführt werden.

Das Verwalten von Prä-/Post-Skripts ist ein zweiteiliger Vorgang, der das Erstellen des Prä-/Post-Skripts und das Einfügen des Skripts in den "prepost"-Ordners umfasst.

Erstellen von Prä-/Post-Skripts

Gehen Sie wie folgt vor:

1. Melden Sie sich als Root-Benutzer beim Sicherungsserver an.
2. Erstellen Sie eine Skriptdatei, indem Sie die Umgebungsvariablen in Ihrer bevorzugten Skripterstellungssprache verwenden.

   Umgebungsvariablen des Prä-/Post-Skripts

   Verwenden Sie die folgenden Umgebungsvariablen, um Ihr Skript zu erstellen:

   D2D_JOBNAME

   Gibt den Namen des Jobs an.

   D2D_JOBID

   Gibt die Job-ID an. Die Job-ID ist eine Nummer, die für den Job vergeben wird, wenn Sie den Job ausführen. Wenn Sie den gleichen Job erneut ausführen, erhalten Sie eine neue Jobnummer.

   D2D_TARGETNODE

   Identifiziert den Knoten, der gesichert oder wiederhergestellt wird.

   D2D_JOBTYPE

   Identifiziert den Typ des ausgeführten Jobs. Die folgenden Werte identifizieren die D2D_JOBTYPE-Variable:

   backup.full

   Identifiziert den Job als eine vollständige Sicherung.

   backup.incremental

   Identifiziert den Job als eine Zuwachssicherung.

backup.verify

Identifiziert den Job als eine Überprüfungssicherung.

restore.bmr

Identifiziert den Job als eine Bare-Metal-Recovery (BMR). Dies ist ein Wiederherstellungsjob.

restore.file

Identifiziert den Job als eine Wiederherstellung auf Dateiebene. Dies ist ein Wiederherstellungsjob.

D2D_SESSIONLOCATION

Identifiziert den Speicherort, an dem die Wiederherstellungspunkte gespeichert sind.

D2D_PREPOST_OUTPUT

Identifiziert eine Temp-Datei. Der Inhalt der Anfangszeile der Temp-Datei wird im Aktivitätsprotokoll angezeigt.

D2D_JOBSTAGE

Gibt die Phase des Jobs an. Die folgenden Werte identifizieren die D2D_ JOBSTAGE-Variable:

pre-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, bevor der Job startet.

post-job-server

Identifiziert das Skript, das auf dem Sicherungsserver ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Job startet.

post-job-target

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Job abgeschlossen ist.

pre-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, bevor der Snapshot erfasst wird.

post-snapshot

Identifiziert das Skript, das auf dem Zielcomputer ausgeführt wird, nachdem der Snapshot erfasst wird.

D2D_TARGETVOLUME

Identifiziert das Volume, das während eines Sicherungsjobs gesichert wird. Diese Variable ist anwendbar für Prä-/Post-Snapshot-Skripts für einen Sicherungsjob.

D2D_JOBRESULT

Identifiziert das Ergebnis für ein Post-Job-Skript. Die folgenden Werte identifizieren die D2D_JOBRESULT-Variable:

success

Identifiziert das Ergebnis als erfolgreich.

fail

Identifiziert das Ergebnis als nicht erfolgreich.

D2DSVR_HOME

Identifiziert den Ordner, in dem der Sicherungsserver installiert ist. Diese Variable ist anwendbar für die Skripts, die auf dem Sicherungsserver ausgeführt werden.

Das Skript ist erstellt.

Hinweis: Bei allen Skripten zeigt der Rückgabewert von Null eine erfolgreiche Erstellung an, und ein Rückgabewert, der ungleich Null ist, weist auf einen Fehler hin.

Einfügen des Skripts in den Ordner "Prepost" und Überprüfung des Skripts

Alle Prä-/Post-Skripts für einen Sicherungsserver werden zentral vom Ordner "prepost" am folgenden Speicherort verwaltet:

/opt/Arcserve/d2dserver/usr/prepost

Gehen Sie wie folgt vor:

1. Fügen Sie die Datei in folgenden Speicherort des Sicherungsservers ein:

   /opt/Arcserve/d2dserver/usr/prepost

2. Geben Sie der Skriptdatei Ausführungsberechtigungen.
3. Melden Sie sich bei der Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche an.
4. Öffnen Sie den **Sicherungsassistenten** oder **Wiederherstellungsassistenten**, und navigieren Sie zur Registerkarte **Erweitert**.
5. Wählen Sie die Skriptdatei in der Drop-down-Liste **Einstellungen vor/nach dem Skript** aus, und übergeben Sie den Job.

6. Klicken Sie auf "**Aktivitätsprotokoll**", und stellen Sie sicher, dass das Skript für den angegebenen Sicherungsjob ausgeführt wird.

   Das Skript wird ausgeführt.

   Die Prä-/Post-Skripte wurden erfolgreich erstellt und befinden sich im Ordner "pre-post".

Erstellen und Ausführen des Wiederherstellungsjobs

Erstellen Sie den Wiederherstellungsjob, und führen Sie ihn aus, sodass Sie den BMR-Prozess initiieren können. Überprüfen Sie die Wiederherstellungspunktinformationen, bevor Sie eine BMR ausführen. Bei Bedarf können Sie zurückgehen und die Wiederherstellungseinstellungen ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Wiederherstellungsdetails auf der Seite **Zusammenfassung** des **Wiederherstellungsassistenten**.
2. (Optional) Klicken Sie auf **Zurück**, um die Wiederherstellungseinstellungen auf den Seiten des **Wiederherstellungsassistenten** zu ändern.
3. Geben Sie einen Jobnamen ein, und klicken Sie auf **Übergeben**.

   Im Feld **Jobname** ist zunächst ein Standardname angegeben. Sie können einen neuen Jobnamen Ihrer Wahl eingeben, wobei das Feld jedoch nicht leer gelassen werden darf.

   Der **Wiederherstellungsassistent** wird geschlossen. Der Job wird auf der Registerkarte **Jobstatus** angezeigt. Wenn Sie die IP-Adresse für die BMR verwenden, startet der Zielcomputer nach dem BMR-Prozess automatisch auf dem gleichen Betriebssystem wie die Sicherungsquelle neu.

   Wenn Sie die MAC-Adresse für die BMR verwenden, ändert sich der Status auf der Registerkarte **Jobstatus** in *Es wird auf das Starten des Zielknotens gewartet*.
4. (Optional) Wenn Sie eine BMR mithilfe der MAC-Adresse ausführen, gehen Sie wie folgt vor: Starten Sie den Zielcomputer, wenn die Meldung *Es wird auf das Starten des Zielknotens gewartet* auf der Registerkarte **Jobstatus** angezeigt wird.

   Hinweis: Wenn der Zielcomputer bereits gestartet wurde, bevor Sie den Wiederherstellungsjob übergeben, müssen Sie den Zielcomputer neu starten. Stellen Sie sicher, dass BIOS so konfiguriert ist, dass vom Netzwerk gestartet wird.

   Der Status in der Spalte **Jobstatus** wird in **Volume wird wiederhergestellt** umgeändert. Dies gibt an, dass die Wiederherstellung in Bearbeitung ist. Nachdem der Wiederherstellungsjob abgeschlossen wurde, startet der Zielcomputer automatisch mit dem gleichen Betriebssystem wie die Sicherungsquelle neu.

   Der Wiederherstellungsjob wurde erfolgreich erstellt und ausgeführt.

(Optional) Ausführen von Post-BMR-Vorgängen

Folgende Themen sind optionale Konfigurationseinstellungen, die Sie möglicherweise nach einer BMR ausführen müssen:

Konfigurieren von X Windows

Wenn Sie eine BMR über verschiedene Hardware ausführen, funktioniert X Windows des wiederhergestellten BS nicht richtig, und der Zielknoten zeigt ein Fehlerdialogfeld an. Das Fehlerdialogfeld wird angezeigt, weil die Anzeigekonfiguration geändert wurde. Um diesen Fehler zu beheben, folgen Sie den Anweisungen im Fehlerdialogfeld, um die Grafikkarte zu konfigurieren. Danach werden X Windows und die Desktop-Benutzeroberfläche angezeigt.

Konfigurieren Sie den FQDN (Fully Qualified Domain Name) des Systems

Wenn Sie einen FQDN benötigen, dann müssen Sie den FQDN konfigurieren. Der BMR-Prozess konfiguriert den FQDN nicht automatisch.

Maximale Zeichenanzahl für FQDN: 63

Führen Sie diese Schritte aus, um den FQDN zu konfigurieren:

1. Bearbeiten Sie die Datei */etc/hosts*, und geben Sie die IP-Adresse, den FQDN-Namen und den Servernamen an.

   #vi /etc/hosts

   ip_of_system servername.domainname.com servername

2. Starten Sie den Netzwerkdienst neu.

   #/etc/init.d/network restart

3. Überprüfen Sie den Hostnamen und den FQDN-Namen.

   #hostname

   servername

   #hostname -f

   servername.domainname.com

   Der FQDN ist konfiguriert.

Erweitern des Daten-Volume nach einer BMR auf verschiedenen Datenträgern

Wenn Sie eine BMR auf einem Datenträger ausführen, der größer ist als der Datenträger auf dem ursprünglichen Knoten, dann wird etwas Festplattenspeicher frei gelassen. Der BMR-Vorgang verarbeitet den freien Festplattenspeicher nicht automatisch. Sie können den Festplattenspeicher in eine separate Partition formatieren, oder Sie können die Größe der vorhandenen

Partition mit dem freien Festplattenspeicher anpassen. Das Volume, dessen Größe Sie anpassen möchten, muss ungenutzt sein, sodass Sie die Größenänderung eines Systemvolumes vermeiden müssen. In diesem Abschnitt wird erläutert, wie ein Datenvolume mit dem freien Festplattenspeicher erweitert wird.

Hinweis: Um Datenverlust zu vermeiden, passen Sie die Größe Ihrer Volumes sofort nach dem BMR-Prozess an. Sie können auch den Knoten sichern, bevor Sie mit der Größenänderung des Volumes starten.

Wenn der Zielcomputer nach der BMR erfolgreich neu startet, dann können Sie das Datenvolume erweitern.

Rohes Partitionsvolume

Zum Beispiel wird ein 2 GB-Datenträger in der Sitzung in einen 16 GB-Datenträger mit dem Namen */dev/sdb* mit nur einer Partition wiederhergestellt. Die rohe Partition */dev/sdb1* wird direkt in das Verzeichnis */data* geladen.

Dieses Beispiel wird verwendet, um den Vorgang zur Erweiterung des rohen Partitionsvolume zu erläutern.

Folgen Sie diesen Schritten:

1. Überprüfen Sie den Status des Volumes "/dev/sdb1".

   # df –h /dev/sdb1

   /dev/sdb1 2.0G 40M 1.9G 3% /data

2. Entladen Sie das Volume "dev/sdb1".

   # umount /data

3. Ändern Sie die Größe von "dev/sdb1", um den gesamten Festplattenspeicher mithilfe des Befehls "fdisk" zu belegen.

   Um diesen Vorgang auszuführen, löschen Sie zuerst Ihre vorhandene Partition, und stellen Sie sie anschließend mit der gleichen Startsektorzahl wieder her. Die gleiche Startsektorzahl ist für die Verhinderung des Datenverlustes verantwortlich.

   # fdisk -u /dev/sdb

   Command (m for help): p

   Disk /dev/sdb: 17,1 GB 17179869184 Byte

   255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

   *Units = sectors of 1 * 512 = 512 bytes*

   Device Boot Start End Blocks Id System

/dev/sdb1 63 4192964 2096451 83 Linux

Command (m for help): d

Selected partition 1

Command (m for help): n

Command action

e extended

p primary partition (1-4)

p

Partition number (1-4): 1

First sector (63-33554431, default 63):

Using default value 63

Last sector or +size or +sizeM or +sizeK (63-33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdb: 17,1 GB 17179869184 Byte

255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

*Units = sectors of 1 * 512 = 512 bytes*

Device Boot Start End Blocks Id System

/dev/sdb1 63 33554431 16777184+ 83 Linux

Command (m for help): w

Die Partition wird in die gleiche Startsektorzahl wie die ursprüngliche Partition geändert, und die Endsektorzahl ist 33554431.

4. Ändern Sie die Größe des Volumes mithilfe des Befehls "resize2fs". Führen Sie im Bedarfsfall zuerst den Befehl "e2fsck" aus.

   # e2fsck -f /dev/sdb1

   # resize2fs /dev/sdb1

5. Laden Sie das Volume auf den Bereitstellungspunkt, und überprüfen Sie den Status des Volumes erneut.

   # mount /dev/sdb1 /data

   # df –h /dev/sdb1

   /dev/sdb1 16G 43M 16G 1% /data

Das Volume wird auf 16 GB erweitert und kann verwendet werden.

LVM-Volume:

Zum Beispiel wird ein 8 GB-Datenträger in der Sitzung in einen 16 GB-Datenträger mit dem Namen */dev/sdc* mit nur einer Partition wiederhergestellt. Die rohe Partition */dev/sdc1* wird als einziges physisches Volume des LVM-logischen Volumes */dev/mapper/VGTest-LVTest* verwendet, dessen Bereitstellungspunkt */lvm* ist.

Dieses Beispiel wird verwendet, um den Vorgang zur Erweiterung des LVM-Volumes zu erläutern.

Folgen Sie diesen Schritten:

1. Überprüfen Sie den Status des Volumes "/dev/mapper/VGTest-LVTest".

   # lvdisplay –m /dev/mapper/VGTest-LVTest

   --- Logical volume ---

   LV Name /dev/VGTest/LVTest

   VG Name VGTest

   LV UUID udoBIx-XKBS-1Wky-3FVQ-mxMf-FayO-tpfPl8

   LV Write Access read/write

   LV Status available

   # open 1

   LV Size 7.88 GB

   Current LE 2018

   Segments 1

   Allocation inherit

   Read ahead sectors 0

   Block device 253:2

   ---Segments---

   Logical extent 0 to 2017:

   Type linear

   Physical volume /dev/sdc1

   Physical extents 0 to 2017

Das physische Volume ist */dev/sdc1*, die Volume-Gruppe ist *VGTest*, und das logische Volume ist */dev/VGTest/LVTest oder /dev/mapper/VGTest-LVTest*.

2. Entladen Sie das Volume "/dev/mapper/VGTest-LVTest".

   # umount /lvm

3. Deaktivieren Sie die Volume-Gruppe, in der sich das physische Volume "/dev/sdc1" befindet.

   # vgchange -a n VGTest

4. Erstellen Sie eine Partition, um den freien Festplattenspeicher mithilfe des Befehls "fdisk" zu belegen.

   # fdisk -u /dev/sdc

   Command (m for help): p

   Disk /dev/sdc: 17,1 GB 17179869184 Byte

   255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

   *Units = sectors of 1 * 512 = 512 bytes*

   Device Boot Start End Blocks Id System

   /dev/sdc1 63 16777215 8388576+ 83 Linux

   Command (m for help): n

   Command action

   e extended

   p primary partition (1-4)

   p

   Partition number (1-4): 2

   First sector (16777216-33554431, default 16777216):

   Using default value 16777216

   Last sector or +size or +sizeM or +sizeK (16777216-33554431, default 33554431):

   Using default value 33554431

   Command (m for help): p

   Disk /dev/sdc: 17,1 GB 17179869184 Byte

   255 heads, 63 sectors/track, 2088 cylinders, total 33554432 sectors

   *Units = sectors of 1 * 512 = 512 bytes*

Device Boot Start End Blocks Id System

/dev/sdc1 63 16777215 8388576+ 83 Linux

/dev/sdc2 16777216 33554431 8388608 83 Linux

Command (m for help): w

Die Partition "/dev/sdc2" ist erstellt.

5. Erstellen Sie ein neues physisches Volume.

   # pvcreate /dev/sdc2

6. Erweitern Sie die Größe der Volumegruppe.

   # vgextend VGTest /dev/sdc2

7. Geben Sie die Volumegruppe frei, die Sie bereits deaktiviert haben.

   # vgchange -a y VGTest

8. Erweitern Sie die logische Volumengröße mithilfe des Befehls "lvextend".

   # lvextend -L +8G /dev/VGTest/LVTest

9. Ändern Sie die Größe des Volumes mithilfe des Befehls "resize2fs". Führen Sie im Bedarfsfall zuerst den Befehl "e2fsck" aus.

   # e2fsck -f /dev/mapper/VGTest-LVTest

   # resize2fs /dev/mapper/VGTest-LVTest

10. Laden Sie das Volume auf den Bereitstellungspunkt, und überprüfen Sie den Status des Volumes erneut.

    # mount /dev/mapper/VGTest-LVTest /lvm

    # lvdisplay -m /dev/mapper/VGTest-LVTest

    ---Logical volume---

    LV Name /dev/VGTest/LVTest

    VG Name VGTest

    LV UUID GTP0a1-kUL7-WUL8-bpbM-9eTR-SVzl-WgA11h

    LV Write Access read/write

    LV Status available

    # open 0

    LV Size 15.88 GB

    Current LE 4066

    Segments 2

Allocation inherit

Read ahead sectors 0

Block device 253:2

--- Segments ---

Logical extent 0 to 2046:

Type linear

Physical volume /dev/sdc1

Physical extents 0 to 2046

Logical extent 2047 to 4065:

Type linear

Physical volume /dev/sdc2

Physical extents 0 to 2018

Das LVM-Volume ist auf 16 GB erweitert und kann verwendet werden.

Überprüfen, dass der Zielknoten wiederhergestellt wurde

Überprüfen Sie nach Abschluss des Wiederherstellungsjobs, dass der Zielknoten mit den relevanten Daten wiederhergestellt wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Zielcomputer, den Sie wiederhergestellt haben.
2. Überprüfen Sie, dass der Zielcomputer über alle Daten verfügt, die Sie gesichert haben.

   Der Zielcomputer wurde erfolgreich überprüft.

   Die BMR wurde erfolgreich für Linux-Rechner ausgeführt.

Durchführen einer Migrations-BMR für Linux-Rechner

Eine Migrations-BMR ist ein zweistufiger Vorgang, bei dem die Daten zunächst auf einem temporären Rechner und dann auf dem eigentlichen Rechner wiederhergestellt werden. Wenn für eine BMR die Option "Instant BMR" aktiviert ist, können Sie Daten auf einem temporären Rechner wiederherstellen. Sie können den temporären Rechner verwenden, bis der eigentliche Rechner bereit ist. Wenn Sie der eigentliche Rechner verfügbar ist, können Sie mit einer Migrations-BMR die Daten vom temporären Rechner auf den eigentlichen Rechner migrieren. Beim Durchführen einer Migrations-BMR werden alle Daten, die Sie auf dem temporäre Rechner erstellt haben, auf den eigentlichen Rechner migriert.

Hinweis: Sie können eine Migrations-BMR nur mit einer agentenbasierten Sicherung durchführen. Die Migrations-BMR wird von agentenlosen Sicherungen nicht unterstützt.

Sie können eine BMR unter Verwendung der IP-Adresse oder der MAC-Adresse (Media Access Control) des Zielcomputers ausführen. Wenn Sie den Zielcomputer mithilfe der Arcserve Unified Data Protection Agent for Linux-Live-CD booten, können Sie die IP-Adresse des Zielcomputers abrufen.

Hinweis: Der Rechner kann starten. Nur eine NIC ist konfiguriert.

Gehen Sie wie folgt vor, um eine Migrations-BMR auszuführen:

- Überprüfen der Voraussetzungen für die Migrations-BMR
- Ausführen einer BMR auf dem temporären Rechner
- Ausführen der Migrations-BMR
- Überprüfen, dass der Zielcomputer wiederhergestellt wurde

Überprüfen der Voraussetzungen für die Migrations-BMR

Beachten Sie Folgendes, bevor Sie eine Migrations-BMR durchführen:

- Sie verfügen über einen gültigen Wiederherstellungspunkt und, falls erforderlich, über das Verschlüsselungskennwort für die Wiederherstellung.
- Sie verfügen über einen gültigen Zielcomputer für die BMR.
- Sie haben die Arcserve Unified Data Protection Agent for Linux-Live-CD erstellt.
- Wenn Sie eine BMR mithilfe der IP-Adresse ausführen möchten, müssen Sie die IP-Adresse des Zielcomputers mithilfe der Live-CD abrufen.
- Wenn Sie eine PXE-basierte BMR mithilfe der MAC-Adresse ausführen möchten, müssen Sie die MAC-Adresse des Zielcomputers haben.
- Der Wiederherstellungspunkt muss aus einer agentenbasierten Linux-Sicherung stammen.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Ausführen einer BMR auf dem temporären Rechner

Bevor Sie eine Migrations-BMR durchführen, müssen Sie Daten aus der Quelle auf einem temporären Rechner wiederherstellen. Zum temporären Wiederherstellen der Daten können Sie eine BMR auf dem temporären Rechner ausführen. Wenn der temporäre Rechner verwendungsbereit ist, können Sie auf dem temporäre Rechner mit Ihrer Arbeit fortfahren.

Wenn der eigentliche Rechner verwendungsbereit ist, können Sie eine Migrations-BMR vom temporären Rechner auf den aktuellen Rechner ausführen.

Hinweis: Weitere Informationen zum Ausführen einer BMR finden Sie unter "So führen Sie eine Bare-Metal-Recovery (BMR) für Linux-Rechner aus".

Gehen Sie wie folgt vor:

1. Führen Sie einen der folgenden Vorgänge durch, um auf den Wiederherstellungsassistenten zuzugreifen:

   Von Arcserve UDP :

   a. Melden Sie sich bei Arcserve UDP an.

   b. Klicken Sie auf die Registerkarte **Ressourcen**.

   c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

   e. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

      Die Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche wird geöffnet. Das Auswahldialogfeld für den Wiederherstellungstyp wird in der Benutzeroberfläche des Agenten angezeigt.

   f. Wählen Sie den Wiederherstellungstyp aus, und klicken Sie auf **OK**.

      Hinweis: Sie werden automatisch beim Agentenknoten angemeldet, und der **Wiederherstellungsassistent** wird im Agentenknoten geöffnet.

   Von Arcserve Unified Data Protection Agent for Linux :

   a. Öffnen Sie die Arcserve Unified Data Protection Agent for Linux-Webbenutzeroberfläche.

      Hinweis: Während der Installation von Arcserve Unified Data Protection Agent for Linux haben Sie die URL erhalten, um auf den Server zugreifen und

ihn verwalten zu können.

b. Melden Sie sich bei Arcserve Unified Data Protection Agent for Linux an.

2. Klicken Sie auf **Wiederherstellen** im Menü **Assistent**, und wählen Sie **Bare-Metal-Recovery (BMR)** aus.

   Die Seite **Sicherungsserver** in **Wiederherstellungsassistent – BMR** wird geöffnet.

3. Geben Sie unter **Wiederherstellungsassistent – BMR** alle notwendigen Informationen ein, und speichern Sie den Assistenten.

4. Stellen Sie sicher, dass Sie das Kontrollkästchen **Instant BMR aktivieren** auf der Seite **Zielcomputer** des Assistenten ausgewählt haben.

5. Stellen Sie sicher, dass Sie das Kontrollkästchen **Daten nach Rechnerstart nicht automatisch wiederherstellen** auf der Seite **Zielcomputer** des Assistenten ausgewählt haben.

6. Führen Sie den BMR-Job aus.

   Der temporäre Rechner mithilfe der BMR wiederhergestellt, wobei die Option "Instant BMR" aktiviert ist. Sie können den temporären Rechner verwenden, bis der eigentliche Rechner bereit ist.

Ausführen der Migrations-BMR

Wenn der eigentliche Rechner bereit ist, führen Sie eine Migrations-BMR aus. Bei einer Migrations-BMR werden die ursprünglichen Daten aus der Sicherungssitzung und die neuen Daten vom temporären Rechner auf dem eigentlichen Rechner wiederhergestellt.

Gehen Sie wie folgt vor:

1. Klicken Sie im Menü **Assistent** auf **Wiederherstellen**, und wählen Sie **Migrations-BMR** aus.

   Die Seite **Sicherungsserver** des **Wiederherstellungsassistenten – Migrations-BMR** wird geöffnet.

2. Geben Sie im **Wiederherstellungsassistenten – Migrations-BMR** alle Details an.

   Hinweis: Weitere Informationen zum Ausführen einer BMR finden Sie unter "So führen Sie eine Bare-Metal-Recovery (BMR) für Linux-Rechner aus".

3. Stellen Sie sicher, dass auf der Seite **Sicherungsserver** des Assistenten die folgenden Informationen angegeben sind.

   a. Wählen Sie den Instant VM-Wiederherstellungsjob oder den Instant BMR-Job aus.

      Lokaler Server

      Gibt an, dass der Sicherungsserver lokal verwaltet wird. Der BMR-Job für den temporären Rechner wird auf dem lokalen Server ausgeführt.

      Remote-Server

      Gibt an, dass der Sicherungsserver remote verwaltet wird. Der BMR-Job für den temporären Rechner wird auf dem Remote-Server ausgeführt. Sie müssen die Remote-Server-Details angeben, um eine Verbindung zum Remote-Server herzustellen.

   b. Wählen Sie den Wiederherstellungsjob aus der Dropdown-Liste "Jobname" aus.

      Sobald verfügbar zeigt die Liste den Instant VM-Wiederherstellungsjob oder Instant BMR-Job an, der sich in der Jobphase "Ready to use" oder in der Jobphase "Power off" befindet.

4. Speichern Sie den BMR-Job.

   Auf der Startseite ändert sich die **Jobphase** auf der Registerkarte **Jobstatus** zu **Hier klicken, um Daten zu migrieren**.

5. (Optional) Starten Sie den temporären Rechner mithilfe einer Live-CD, wenn der ausgewählte Jobtyp "Instant BMR" ist.
6. Klicken Sie auf der Registerkarte **Jobstatus** auf **Hier klicken, um Daten zu migrieren**.

   Die Datenmigration beginnt.

   Sie haben die Migrations-BMR erfolgreich durchgeführt.

Überprüfen, dass der Zielknoten wiederhergestellt wurde

Überprüfen Sie nach Abschluss des Wiederherstellungsjobs, dass der Zielknoten mit den relevanten Daten wiederhergestellt wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu dem Zielcomputer, den Sie wiederhergestellt haben.
2. Stellen Sie sicher, dass der Zielcomputer sämtliche Informationen vom temporären Rechner enthält, einschließlich aller neuen Daten, die Sie auf dem temporären Rechner erstellt haben.

   Der Zielcomputer wurde erfolgreich überprüft.

   Die Migrations-BMR wurde erfolgreich für agentenbasierte Linux-Rechner durchgeführt.

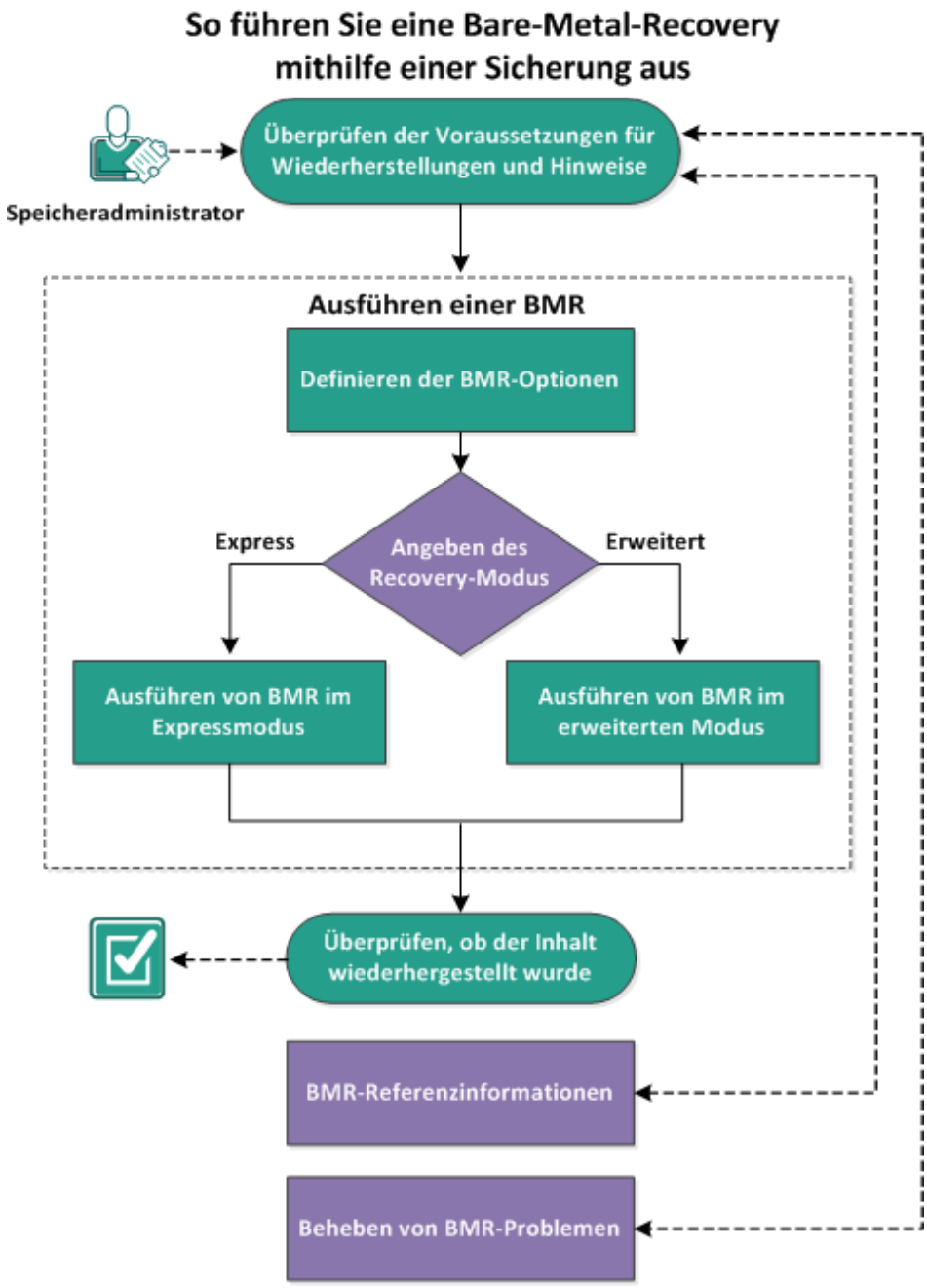
So führen Sie eine BMR mithilfe einer Sicherung aus

Eine Bare-Metal-Recovery ist eine Wiederherstellung Ihres Computersystems "von Null", einschließlich des Betriebssystems und Softwareanwendungen, mit einer darauffolgenden Wiederherstellung von Daten und Einstellungen. Durch eine Bare-Metal-Recovery können Sie Ihren Rechner mit minimalem Aufwand vollständig wiederherstellen. Dies ist sogar auf einer anderen Hardware möglich. BMR ist möglich, da Arcserve UDP Agent (Windows) während der Sicherung auf Blockebene nicht nur Daten, sondern auch Informationen erfasst werden, die sich auf folgende Anwendungen beziehen:

- Betriebssystem
- Installierte Anwendungen
- Konfigurationseinstellungen
- Erforderliche Treiber

Alle Informationen, die für eine vollständige Systemwiederherstellung "von Null" benötigt werden, werden in mehreren Blöcken gesichert und im Sicherungsziel gespeichert.

Die folgende Abbildung veranschaulicht den Prozess zur Ausführung von BMR mithilfe von Sicherungen:



Gehen Sie folgt vor, um eine BMR mithilfe einer Sicherung auszuführen:

1. Überprüfen der Voraussetzungen und Hinweise für BMR
2. Definieren der BMR-Optionen
   - Ausführen von BMR im Expressmodus
   - Ausführen von BMR im erweiterten Modus
3. Überprüfen des Erfolgs der BMR
4. BMR-Referenzinformationen
5. Beheben von BMR-Problemen

Überprüfen der Voraussetzungen und Hinweise für BMR

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine BMR ausführen:

- Sie müssen über eines der folgenden Images verfügen:
  - Ein auf eine CD/DVD gebranntes erstelltes ISO-Image für BMR
  - Ein auf einen tragbaren USB-Stick gebranntes erstelltes ISO-Image für BMR

  Hinweis: Mit Arcserve UDP Agent (Windows) können Sie mithilfe eines Bootkit-Hilfsprogramms ein WinPE-Image und ein Arcserve UDP Agent (Windows)-Image zu einem BMR-ISO-Image kombinieren. Dieses ISO-Image wird auf einen startfähigen Datenträger gebrannt. Sie können beide startfähigen Datenträger (CD/DVD oder USB-Stick) verwenden, um das neue Computersystem zu initialisieren und den Bare Metal Recovery-Prozess zu starten. Um sicherzustellen, dass Ihr gespeichertes Image immer die aktuellste Version ist, erstellen Sie jedes Mal ein neues ISO-Image, wenn Sie Arcserve UDP Agent (Windows) aktualisieren.
- Sie müssen über mindestens eine vollständige Sicherung verfügen.
- Auf dem virtuellen Rechner und auf dem Quellserver, den Sie wiederherstellen, muss mindestens 2 GB RAM installiert sein.
- Um virtuelle VMware-Rechner zu virtuellen VMware-Rechnern wiederherzustellen, die auf das Verhalten eines physischen Servers konfiguriert wurden, stellen Sie sicher, dass die Anwendung "VMware Tools" auf dem virtuellen Rechner des Ziels installiert ist.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Überprüfen Sie die folgenden Wiederherstellungshinweise:

- Der Prozess der Bare-Metal-Recovery ist bei den beiden Arten der Erstellung des Bootkit-Images praktisch identisch.

  Hinweis: Der BMR-Prozess kann keine Speicherplätze erstellen. Wenn der Quellrechner Speicherplätze hat, können Sie im Zuge der BMR keine Speicherplätze am Zielrechner erstellen. Sie können diese Volumes als normale Datenträger/Volumes wiederherstellen oder vor der Ausführung der BMR manuell Speicherplätze erstellen, um Daten in diesen Speicherplätzen wiederherzustellen.

- Dynamische Datenträger werden nur auf Datenträgerebene wiederhergestellt. Wenn Ihre Daten auf einem lokalen Volume eines dynamischen Datenträgers gesichert sind, können Sie diesen dynamischen Datenträger während der Bare-Metal-Recovery nicht wiederherstellen. Um in diesem Szenario eine Wiederherstellung während der BMR durchzuführen, müssen Sie eine der folgenden Aufgaben ausführen, und dann eine BMR vom kopierten Wiederherstellungspunkt aus durchführen:
  - Führen Sie eine Sicherung auf einem Volume oder auf einem anderen Laufwerk durch.
  - Führen Sie eine Sicherung auf der Remote-Freigabe durch.
  - Kopieren Sie einen Wiederherstellungspunkt in einen anderen Speicherort.

  Hinweis: Wenn Sie BMR bei mehreren dynamischen Datenträgern ausführen, kann die BMR wegen unerwarteter Fehler fehlschlagen (z. B. Fehler beim Starten, unerkannte dynamische Volumes, usw.). Wenn dies auftritt, sollten Sie nur den Systemdatenträger mithilfe von BMR wiederherstellen, und dann können Sie nach dem Rechnerneustart die anderen dynamischen Volumes auf einer normalen Umgebung wiederherstellen.
- (Optional) Überprüfen Sie die BMR-Referenzinformationen. Weitere Informationen finden Sie in den folgenden Themen:
  - Funktionsweise von Bare-Metal-Recovery
  - Betriebssysteme, die UEFI/BIOS-Konvertierung unterstützen
  - Verwalten des Menüs von BMR-Vorgängen

Überprüfen Sie die folgenden Hinweise:

- Wenn Sie auf eine neuere Version oder ein neueres Update von Arcserve UDP aktualisieren, müssen Sie das BMR-ISO-Image mithilfe der jeweils passenden Stufe des Windows AIK oder ADK neu erstellen, damit die neuesten Funktionen und Fehlerkorrekturen unterstützt werden. Nachdem eine BMR-ISO-Image erstellt wurde, kann jedoch die ISO-Datei für die gleiche BS-Stufe verwendet werden. Für folgende BS-Stufen können Sie das gleiche ISO-Image verwenden:
  - Mithilfe von Windows 7 WAIK erstelltes ISO-Image – funktioniert auf Windows 2003, Vista, 2008, 2008R2
  - Mithilfe von Windows 8/8.1 ADK erstelltes ISO-Image – funktioniert auf Windows 8, 8.1, Server 2012, Server 2012 R2
  - Mithilfe von Windows 10 ADK erstelltes ISO-Image – funktioniert unter Windows 10, Windows Server 2016 und Windows Server 2019

Definieren der BMR-Optionen

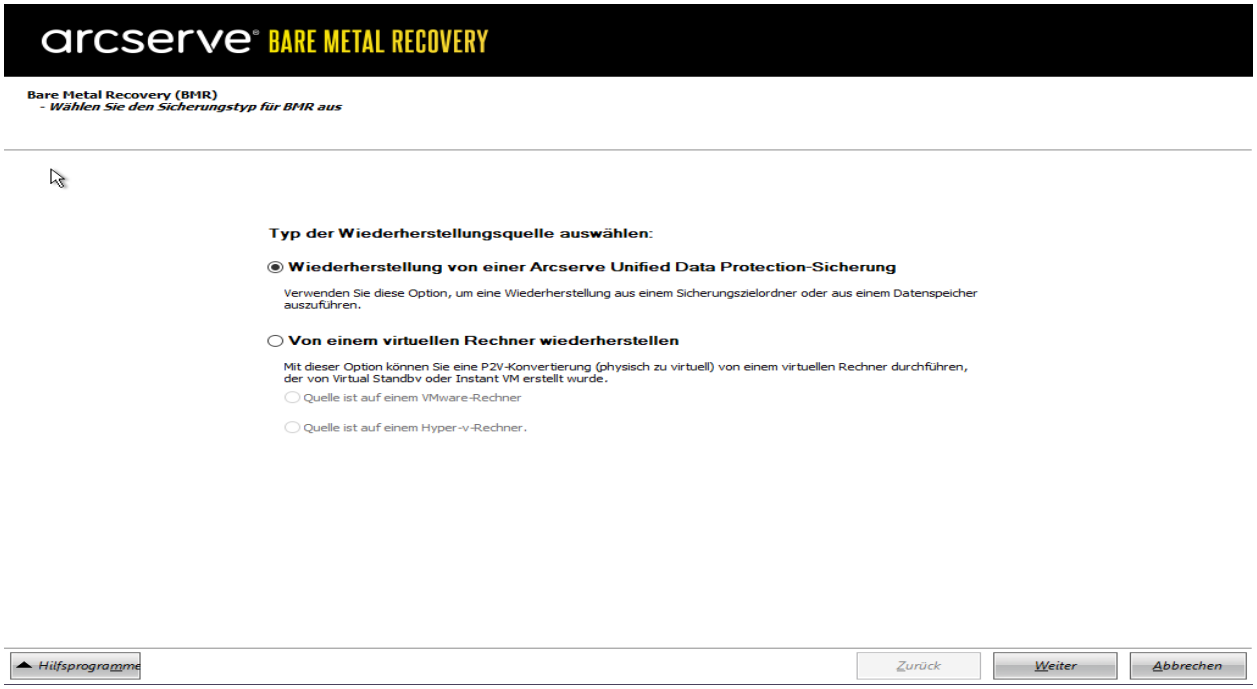
Bevor Sie den BMR-Prozess initiieren, müssen Sie eine Reihe von vorbereitenden BMR-Optionen angeben.

Gehen Sie wie folgt vor:

1. Legen Sie den Datenträger ein, auf dem das Bootkit-Image gespeichert ist, und starten Sie den Computer.
   - Wenn Sie ein auf eine CD/DVD gebranntes ISO-Image für BMR verwenden, legen Sie die CD/DVD ein.
   - Wenn Sie ein auf einen USB-Stick gebranntes ISO-Image für BMR verwenden, legen Sie den Stick ein.

   Der Bildschirm des **BIOS Setup-Hilfsprogramms** wird angezeigt.
2. Wählen Sie im Bildschirm des **BIOS Setup-Hilfsprogramms** die Option für CD-ROM-Laufwerk oder USB aus, um den Startprozess zu initiieren. Wählen Sie eine Architektur (x86 oder x64) aus, und drücken Sie die **Eingabetaste**, um fortzufahren.
3. Der Arcserve UDP Agent (Windows)-Bildschirm zur Sprachauswahl wird angezeigt. Wählen Sie eine Sprache aus, und klicken Sie auf **Weiter**, um fortzufahren.

Die Bare-Metal-Recovery wird gestartet und der erste Bildschirm des BMR-Assistenten wird angezeigt.



Im Bildschirm des BMR-Assistenten können Sie den BMR-Typ, den Sie ausführen möchten, auswählen:

- **Aus Arcserve Unified Data Protection-Sicherung wiederherstellen**

  Verwenden Sie diese Option, um eine Wiederherstellung entweder von einem Sicherungszielordner oder von einem Datenspeicher auszuführen.

  Mit dieser Option können Sie Daten wiederherstellen, die mithilfe von Arcserve UDP Agent (Windows) gesichert wurden. Diese Option wird in Verbindung mit Sicherungssitzungen verwendet, die mit Arcserve UDP Agent (Windows) oder mit der Arcserve UDP-Anwendung für hostbasierte VM-Sicherung ausgeführt werden.

  Wenn Sie diese Option auswählen, fahren Sie mit diesem Vorgang fort.

- **Aus einem virtuellen Rechner wiederherstellen**

  Verwenden Sie diese Option, um eine V2P-Wiederherstellung (virtuell-zu-physisch) von einer Virtual Standby-VM auszuführen. Virtuell-zu-physisch (V2P) ist ein Begriff, der sich auf das Migrieren eines Betriebssystems (BS), von Anwendungsprogrammen und von Daten von einem virtuellen Rechner oder von einer Datenträgerpartition zur Hauptfestplatte eines Computers bezieht. Beim Ziel kann es sich um einen oder mehrere Computer handeln.

- **Quelle ist auf einem VMware-Rechner**

  Ermöglicht es Ihnen, Daten für einen Rechner wiederherzustellen, für den eine virtuelle Konvertierung in einen virtuellen VMware-Rechner durchgeführt wurde. Diese Option wird in Verbindung mit der Arcserve Central Virtual Standby-Anwendung verwendet.

  Hinweis: Mit dieser Option können Sie nur Daten wiederherstellen, wenn die virtuelle Konvertierung in eine VMDK-Datei (für VMware) mit Arcserve Central Virtual Standby durchgeführt wurde.

  Wenn Sie diese Option auswählen, lesen Sie den Abschnitt Wiederherstellen mit einem virtuellen VMware Virtual Standby-Rechner, um mit diesem Vorgang fortzufahren.

  Weitere Informationen finden Sie in der Online-Hilfe zu Agent für Windows unter Wiederherstellen mit einem virtuellen VMware Virtual Standby-Rechner.

- **Quelle ist auf einem Hyper-V-Rechner**

  Ermöglicht es Ihnen, Daten für einen Rechner wiederherzustellen, für den eine virtuelle Konvertierung in einen virtuellen Hyper-V-Rechner durchgeführt wurde. Diese Option wird in Verbindung mit der Arcserve Central Virtual Standby-Anwendung verwendet.

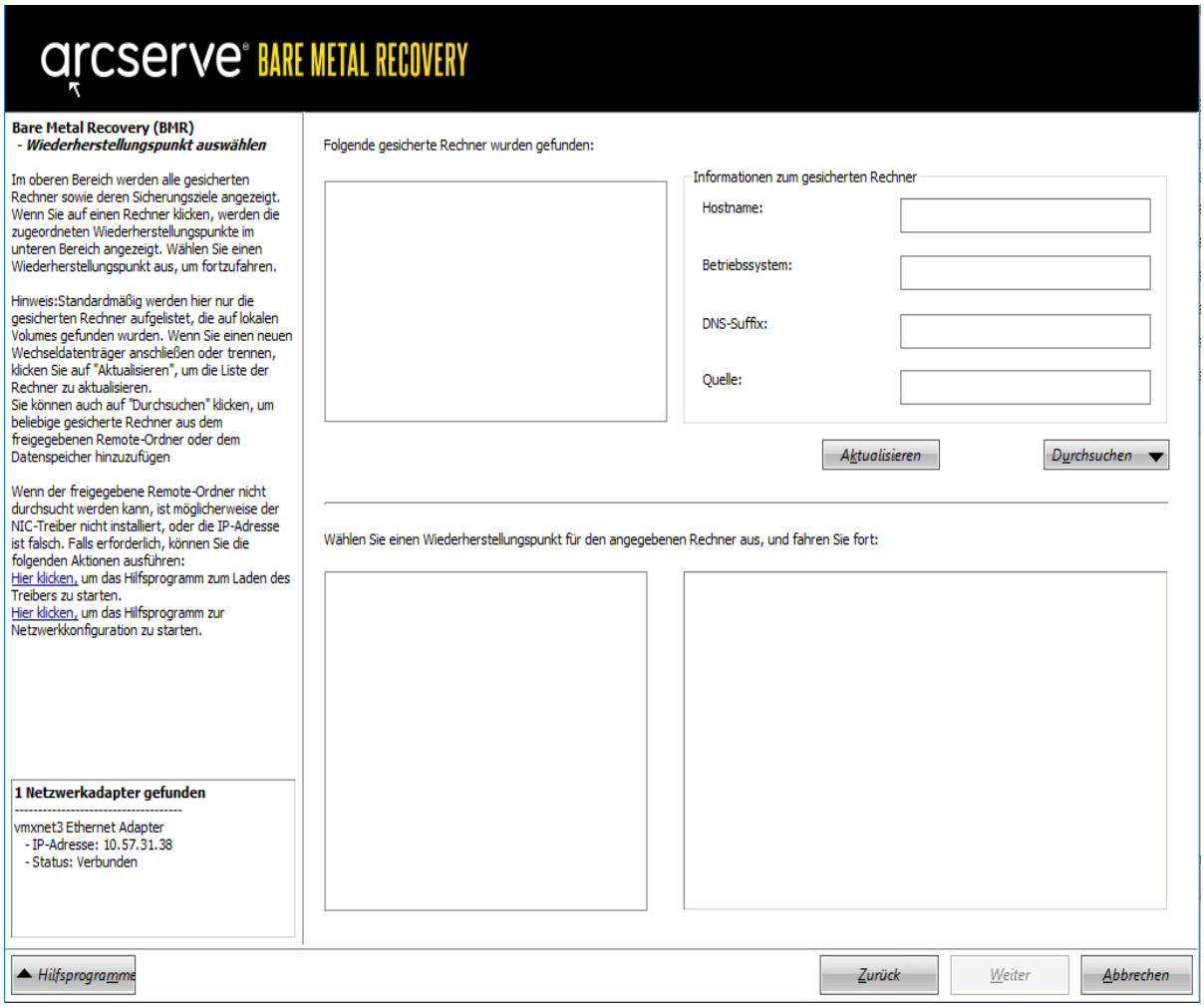
  Hinweis: Mit dieser Option können Sie nur Daten wiederherstellen, wenn die virtuelle Konvertierung in eine VHD-Datei (für Hyper-V) mit Arcserve Central Virtual Standby durchgeführt wurde.

  Wenn Sie diese Option auswählen, lesen Sie den Abschnitt Wiederherstellen mit einem virtuellen Hyper-V Virtual Standby-Rechner, um mit diesem Vorgang fortzufahren.

  Weitere Informationen finden Sie in der Online-Hilfe unter Wiederherstellen mit einem virtuellen Hyper-V Virtual Standby-Rechner.

4. Wählen Sie **Wiederherstellung von einer Arcserve Unified Data Protection-Sicherung aus**, und klicken Sie auf **Weiter**.

   Der Assistentenbildschirm **Wiederherstellungspunkt auswählen** wird angezeigt.



5. Klicken Sie im Fenster des Assistenten **Wiederherstellungspunkt auswählen** auf **Durchsuchen**, und wählen Sie entweder **Netzwerk/Lokalen Pfad durchsuchen** oder **Recovery Point Server durchsuchen** aus.

    a. Wenn Sie **Netzwerk/Lokalen Pfad durchsuchen** auswählen, wählen Sie den Rechner (oder das Volume) aus, der bzw. das Wiederherstellungspunkte für Ihr Sicherungs-Image enthält.

    Mit Arcserve UDP Agent (Windows) können Sie Wiederherstellungen von lokalen Laufwerken oder Netzwerkfreigaben durchführen.

    - Wenn Sie eine Wiederherstellung von einer lokalen Sicherung durchführen, erkennt der BMR-Assistent automatisch alle Volumes, die Wiederherstellungspunkte enthalten, und zeigt sie an.
    - Wenn Sie eine Wiederherstellung von einer Netzwerkfreigabe durchführen, suchen Sie den Remote-Speicherort der Wiederherstellungspunkte. Wenn mehrere Rechner Wiederherstellungspunkte enthalten, werden sie alle angezeigt.

Unter Umständen benötigen Sie Zugriffsinformationen (Benutzername und Kennwort) für den Remote-Rechner.

Hinweis: Damit Sie das Netzwerk nach den Wiederherstellungspunkten durchsuchen können, muss die Netzwerkverbindung aktiv und verfügbar sein. Über das Menü "Hilfsprogramme" können Sie gegebenenfalls Ihre Netzwerkkonfigurationsinformationen überprüfen bzw. aktualisieren sowie fehlende Treiber laden.

- Wenn das BMR-Modul kein lokales Ziel-Volume entdeckt, wird das Dialogfeld **Ordner auswählen** automatisch angezeigt. Geben Sie die Remote-Freigabe an, auf der sich die Sicherungen befinden.
- Wenn Sie ein iSCSI-Ziel wiederherstellen möchten, entdeckt das BMR-Modul dieses Ziel möglicherweise nicht. In diesem Fall müssen Sie folgende Schritte ausführen:

  1. Klicken Sie auf **Hilfsprogramme**, wählen Sie im Pop-up-Menü **Ausführen** aus, tippen Sie **cmd** und klicken Sie auf **OK**.

  2. Verwenden Sie im Fenster der Eingabeaufforderung folgende Windows iSCSI-Befehle, um iSCSI-Verbindungen einzurichten:

  > net start msiscsi

  > iSCSICLI QAddTargetPortal <Zielportaladresse>

  > iSCSICLI QLoginTarget <Zielname> [CHAP-Benutzername] [CHAP-Kennwort]

  Hinweis: CHAP = Challenge-Handshake Authentication Protocol

  Weitere Informationen zu Windows iSCSI-Befehlszeilenoptionen finden Sie unter Link.

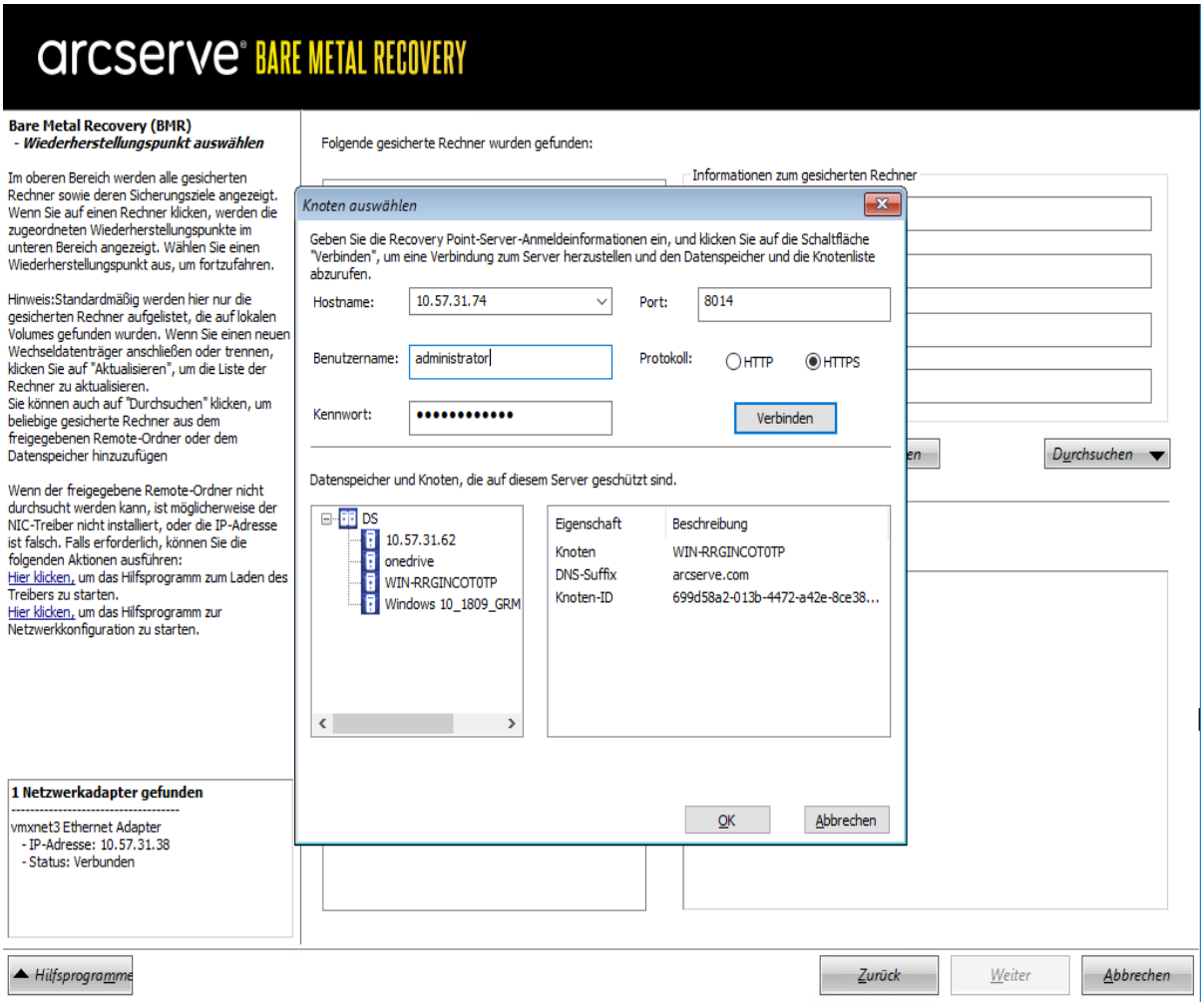
  Hinweis: Je nach eingesetzter iSCSI-Zielsoftware sind eventuell zusätzliche Schritte erforderlich. Konsultieren Sie für weitere Informationen das Handbuch für die jeweilige iSCSI-Zielsoftware.

  3. Im BMR-Fenster sollten die Datenträger/Volumes, die über den iSCSI-Datenträger verbunden sind, angezeigt werden. Der iSCSI-Datenträger kann nun als Quell-Volume oder Ziel-Volume für die Sicherung verwendet werden.

  Hinweis: BMR unterstützt keine Betriebssystem-Installationen auf iSCSI-Datenträgern. Es werden nur Daten-Datenträger unterstützt.

b. Wenn Sie **Browse the Recovery Point Server** (Recovery Point Server durchsuchen) auswählen, wird das Dialogfeld **Select Agent** (Agent auswählen) angezeigt. Geben Sie den **Hostnamen des Recovery Point Servers**, den

Benutzernamen, das **Kennwort**, den **Port** und das **Protokoll** an. Klicken Sie auf **Verbinden**.



6. Wählen Sie den Ordner oder den Agent-Namen unter "Datenspeicher" am Speicherort der Wiederherstellungspunkte für Ihre Sicherung aus, und klicken Sie auf **OK**.

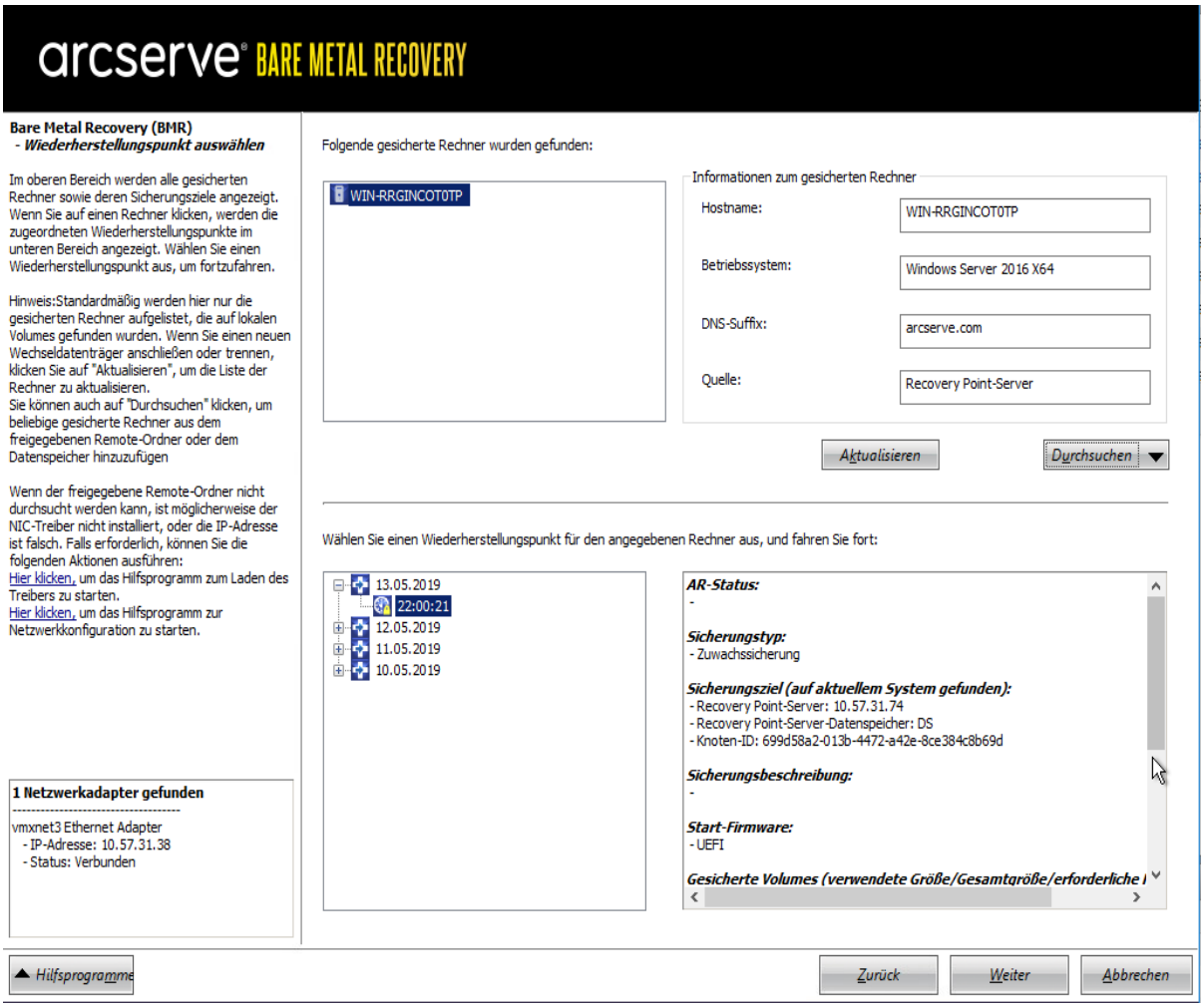
   Der BMR-Assistent zeigt jetzt folgende Informationen an:

   - Der Rechnername (im oberen linken Bereich).
   - Die verbundenen Sicherungsinformationen (im oberen rechten Bereich).
   - Alle entsprechenden Wiederherstellungspunkte (im unteren linken Bereich).

     Hinweis: Für unterstützte Betriebssysteme können Sie BMR von Sicherungen, die auf UEFI-Rechnern durchgeführt wurden, auf BIOS-kompatible Rechner und von Sicherungen, die auf BIOS-Rechnern durchgeführt wurden, auf UEFI-kompatible Rechner durchführen. In Betriebssysteme, die UEFI/BIOS-Kon-

vertierung unterstützen finden Sie eine vollständige Auflistung von Systemen, die die Konvertierung von Firmware unterstützen.

- Für Betriebssysteme, die keine Firmwarekonvertierung unterstützen, müssen Sie den Computer in UEFI-Modus booten, um eine BMR für ein UEFI-System auszuführen. BMR unterstützt keine Wiederherstellung eines Computers mit anderer Firmware. Um zu überprüfen, dass es sich bei der Start-Firmware um UEFI und nicht um BIOS handelt, klicken Sie auf **Hilfsprogramme**, **Info**.
- Wenn bei Betriebssystemen, die Firmwarekonvertierung unterstützen, nach der Auswahl eines Wiederherstellungspunkts entdeckt wird, dass der Quellrechner nicht dieselbe Firmware wie Ihr System ist, werden Sie gefragt, ob Sie UEFI in ein BIOS-kompatibles System oder BIOS in ein UEFI-kompatibles System konvertieren wollen.



Hinweis: Das Arcserve UDP Version 5.0 Update 2 unterstützt nur BMR auf einem kleineren Datenträger, wenn die Sitzungen von Arcserve UDP Version 5.0 Update 2 gesichert werden. Siehe Feld **Erforderliche Mindestgröße** für

die Ziel-Datenträgergröße. BMR auf einen kleineren Datenträger wird nur im **erweiterten Modus** unterstützt.

7. Wählen Sie den wiederherzustellenden Wiederherstellungspunkt aus.

   Die Informationen zum ausgewählten Wiederherstellungspunkt werden angezeigt (im rechten unteren Fensterbereich). Diese Anzeige beinhaltet Informationen wie den Typ der durchgeführten (und gespeicherten) Sicherung, das Sicherungsziel und die gesicherten Volumes.

   Wenn der Wiederherstellungspunkt verschlüsselte Sitzungen enthält (das Uhrsymbol neben dem Wiederherstellungspunkt hat eine Sperre), wird ein Bildschirm zur Kennworteingabe geöffnet. Geben Sie das Sitzungskennwort ein, und klicken Sie auf **OK**.

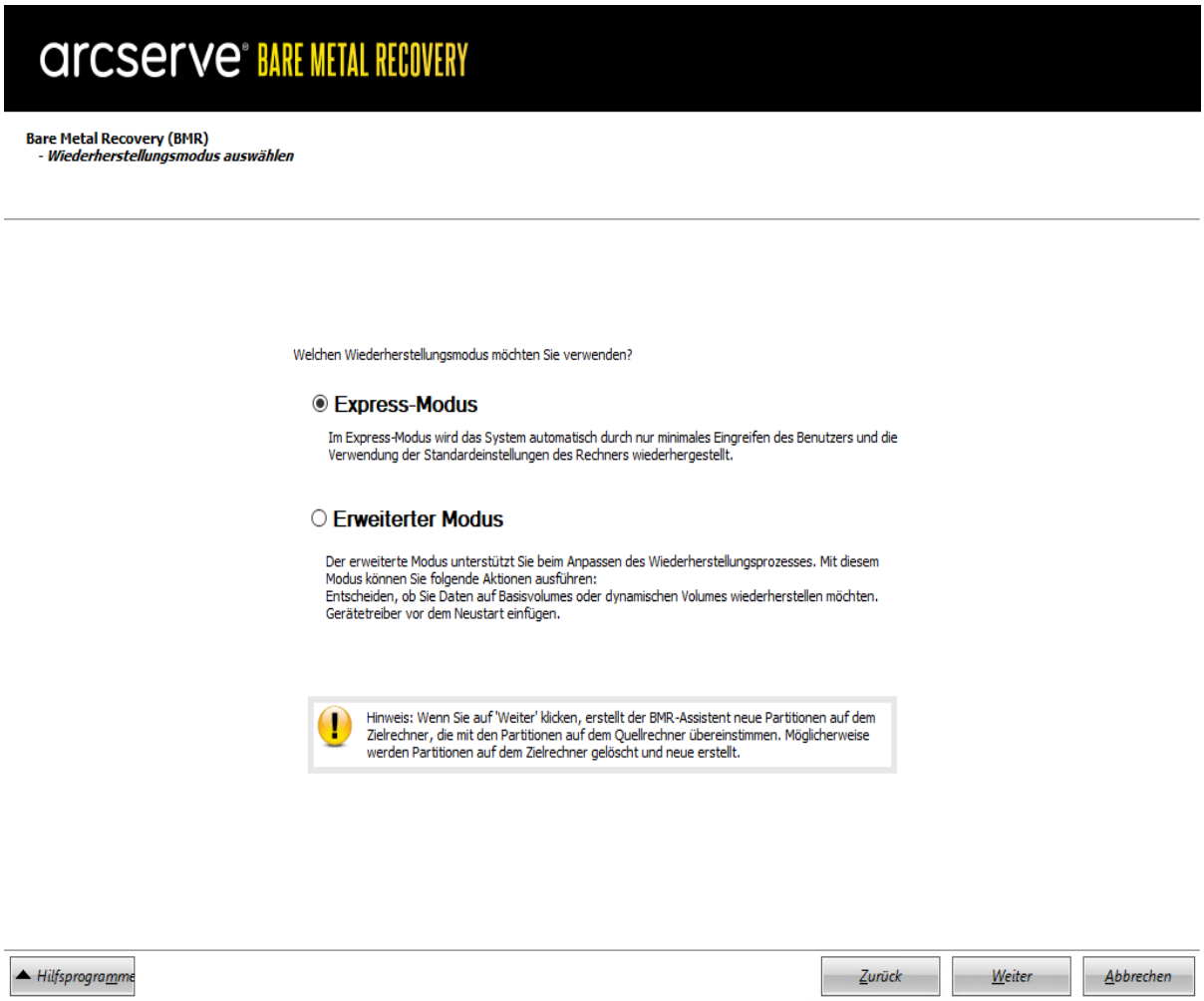
   Hinweise:

   Wenn Sie eine Wiederherstellung von einem Arcserve UDP-Recovery Point Server durchführen, werden Sie aufgefordert, ein Sitzungskennwort anzugeben.

   Wenn es sich bei Ihrem Rechner um einen Domänen-Controller handelt, unterstützt Arcserve UDP Agent (Windows) eine nicht verbindliche Wiederherstellung der Active Directory (AD)-Datenbankdatei während einer Bare-Metal-Recovery. (Wiederherstellung von MSCS-Clustern wird nicht unterstützt).

8. Überprüfen Sie den Wiederherstellungspunkt, den Sie wiederherstellen möchten, und klicken Sie auf **Weiter**.

   Im BMR-Assistenten werden die verfügbaren Wiederherstellungsmodi angezeigt.



Es stehen die Optionen **Erweiterter Modus** und **Express-Modus** zur Verfügung.

- Wenn Sie minimal in den Wiederherstellungsprozess eingreifen möchten, wählen Sie Express-Modus.
- Wenn Sie den Wiederherstellungsprozess personalisieren möchten, wählen Sie Erweiterter Modus.

  Standard: Express-Modus.

Ausführen von BMR im Expressmodus

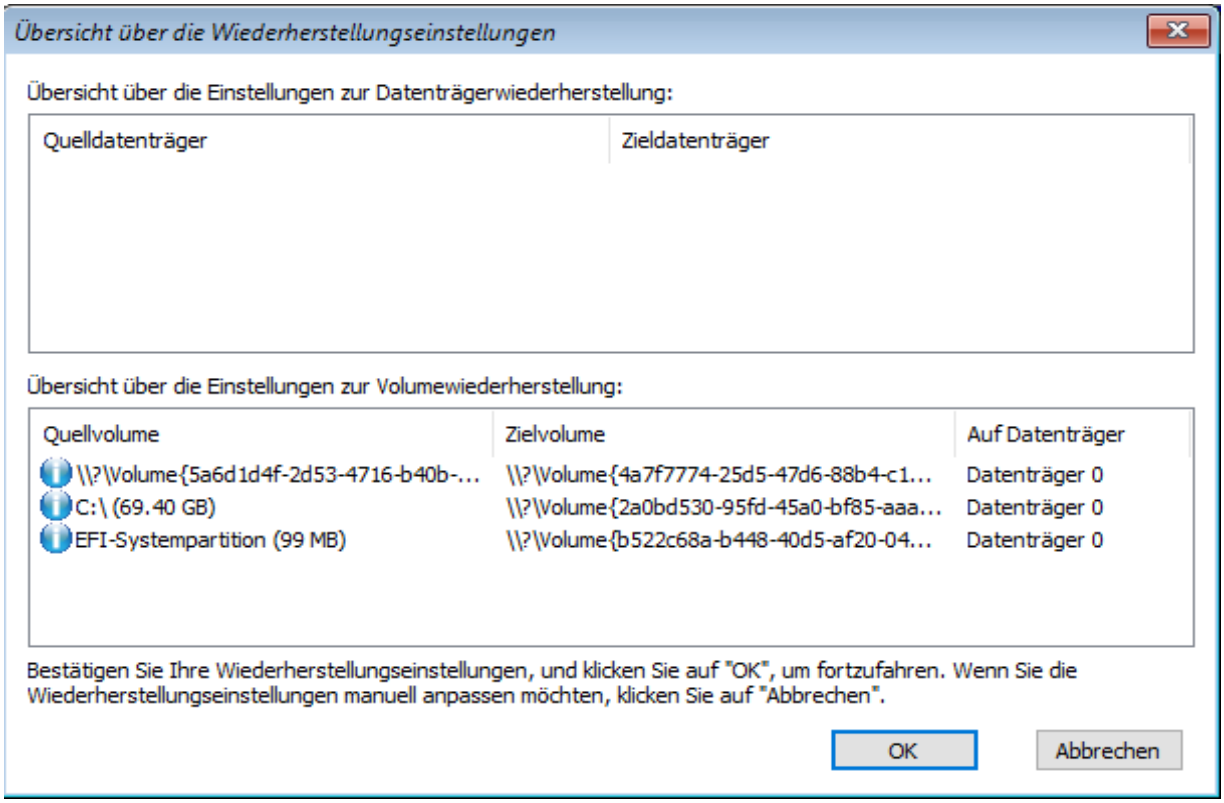
Der Express-Modus erfordert nur minimale Interaktion während des Wiederherstellungsprozesses.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Wiederherstellungsmodus auswählen Express-Modus** aus, und klicken Sie auf **Weiter**.

   Im Bildschirm **Übersicht über die Einstellungen zur Datenträgerwiederherstellung** wird eine Übersicht der wiederherzustellenden Volumes angezeigt.

   Hinweis: Die Laufwerkbuchstaben, die unten in der Spalte **Ziel-Volume** aufgelistet werden, werden von Windows Preinstallation Environment (WinPE) automatisch erstellt. Sie können von den Laufwerkbuchstaben der Spalte **Quell-Volume** abweichen. Auch wenn die Laufwerkbuchstaben nicht miteinander übereinstimmen werden die Daten im richtigen Volume ordnungsgemäß wiederhergestellt.

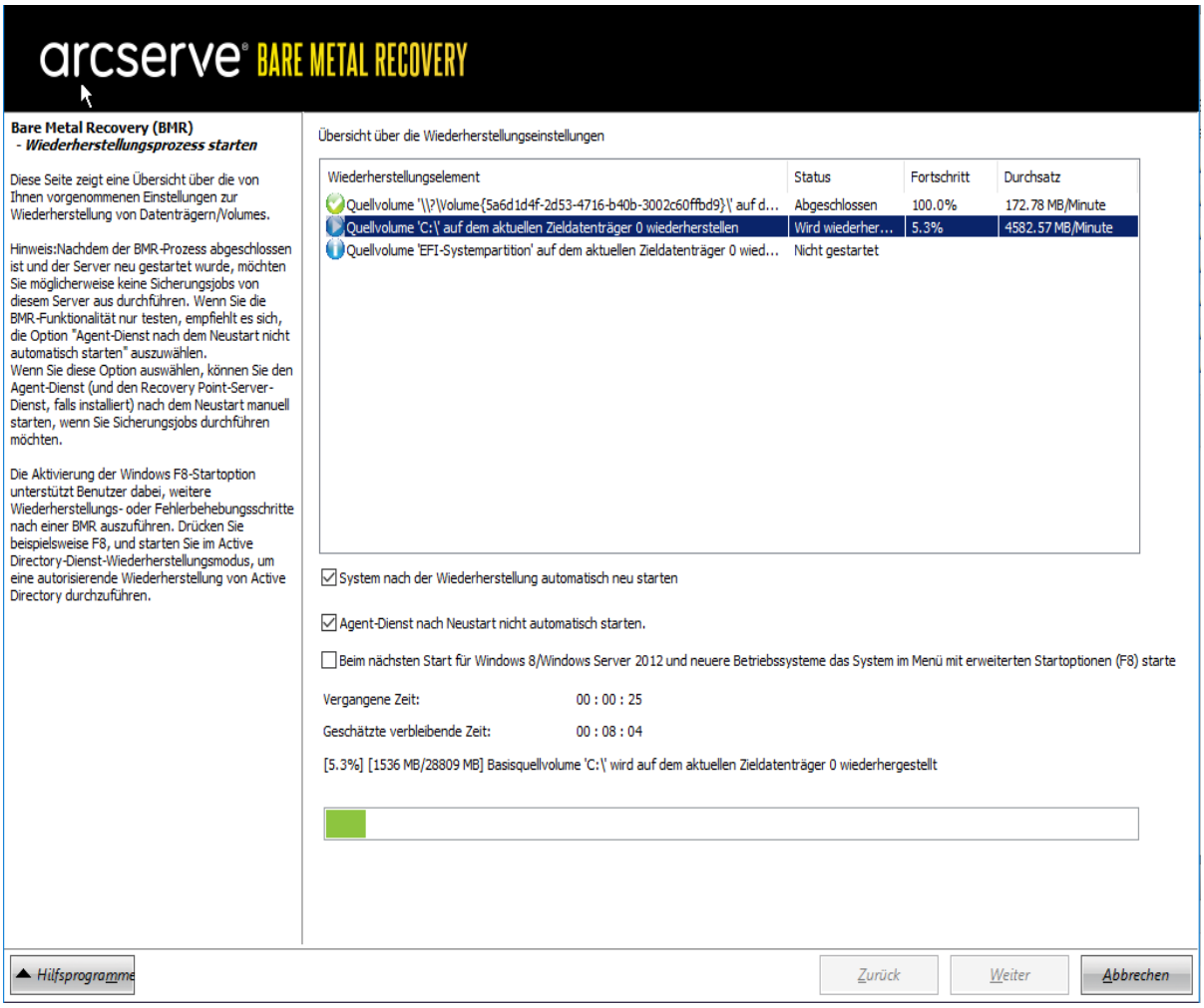


2. Nachdem Sie die Richtigkeit der Übersichtsinformationen überprüft haben, klicken Sie auf **OK**.

   Der Wiederherstellungsprozess beginnt. Im BMR-Assistenten wird der Wiederherstellungsstatus jedes Volume angezeigt.

- Dieser Vorgang kann, abhängig von der Größe des Volume, das wiederhergestellt wird, eine Weile dauern.
- Sie stellen durch diesen Prozess sämtliche Informationen, die Sie für diesen Wiederherstellungspunkt gespeichert hatten, Block für Block wieder her und erstellen auf dem Zielrechner eine Kopie des Quellrechners.
- Standardmäßig ist die Option, die nach der Wiederherstellung einen automatischen Systemneustart festlegt, aktiviert. Wenn nötig, können Sie diese Option löschen und den Neustart zu einem späteren Zeitpunkt manuell durchführen.

  Wichtig: Wenn Sie eine verbindliche Wiederherstellung eines Active Directory nach einer BMR ausführen, müssen Sie die Option **System nach der Wiederherstellung automatisch neu starten** deaktivieren. Weitere Informationen finden Sie unter So führen Sie eine verbindliche Wiederherstellung eines Active Directory nach einer BMR aus.
- Im Bedarfsfall können Sie "Agent-Dienst nach Neustart nicht automatisch starten" auswählen.
- Sie können den Vorgang auch jederzeit abbrechen.



3. Über das Menü **Hilfsprogramme** können Sie auf das BMR-**Aktivitätsprotokoll** zugreifen und es mithilfe der Option **Speichern** speichern.

   Der standardmäßige Speicherplatz für das Aktivitätsprotokoll ist folgender:

   X:\windows\system32\dr\log

   Hinweis: Um Windows-bedingten Fehlern vorzubeugen, sollten Sie nicht die Option **Speichern unter** im Fenster des BMR-Aktivitätsprotokolls verwenden, um das Aktivitätsprotokoll auf Ihrem Desktop zu speichern oder einen Ordner auf Ihrem Desktop zu erstellen.

4. Wenn Sie die Wiederherstellung auf einer abweichenden Hardware durchführen (z. B. wenn der SCSI-/FC-Adapter, der zur Verbindung mit den Festplatten verwendet wurde, geändert wurde), und im ursprünglichen System kein kompatibler Treiber gefunden wird, wird die Seite "Treibereinfügung" angezeigt, über die Sie sich mit den benötigten Treibern versorgen können.

Sie können das System durchsuchen und einzufügende Treiber auswählen, sodass sogar ein Rechner mit anderer Hardware nach einer Bare-Metal-Recovery wiederhergestellt werden kann.

Nach Abschluss der Bare-Metal-Recovery wird eine Bestätigungsmeldung angezeigt.

Ausführen von BMR im erweiterten Modus

In **Erweiterter Modus** können Sie den Wiederherstellungsprozess benutzerdefiniert anpassen.

Gehen Sie wie folgt vor:

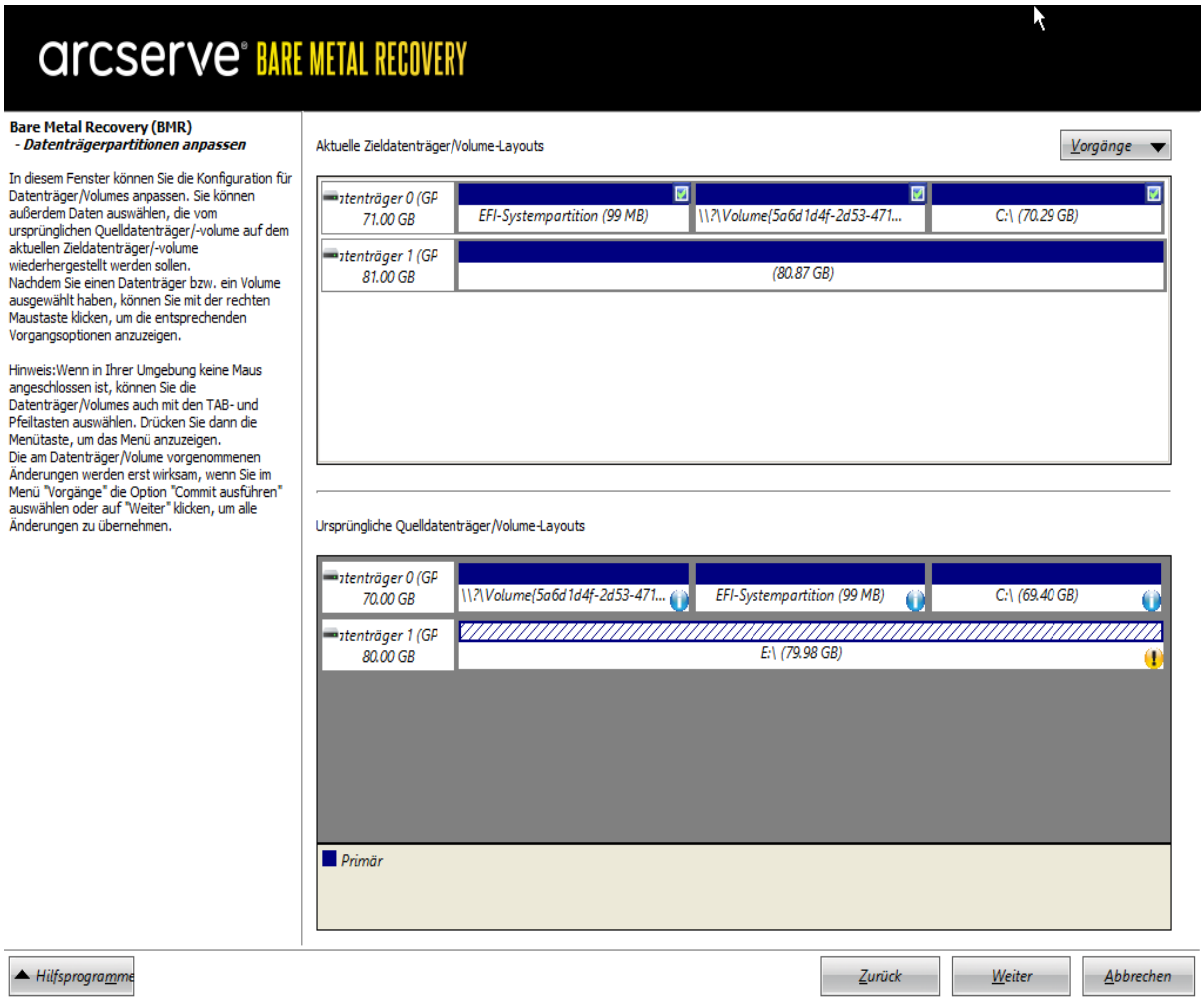
1. Wählen Sie im Dialogfeld **Wiederherstellungsmodus auswählen Erweiterter Modus** aus, und klicken Sie auf **Weiter**.

   Das BMR-Hilfsprogramm beginnt mit der Suche nach den wiederherzustellenden Rechnern und zeigt die entsprechenden Informationen zu Datenträgerpartitionen an.

   Im oberen Fensterbereich wird die Datenträgerkonfiguration des derzeitigen Rechners (Zielrechners) angezeigt. Im unteren Fensterbereich wird die Datenträgerkonfiguration angezeigt, die Sie am ursprünglichen Rechner (Quellrechner) eingestellt hatten.

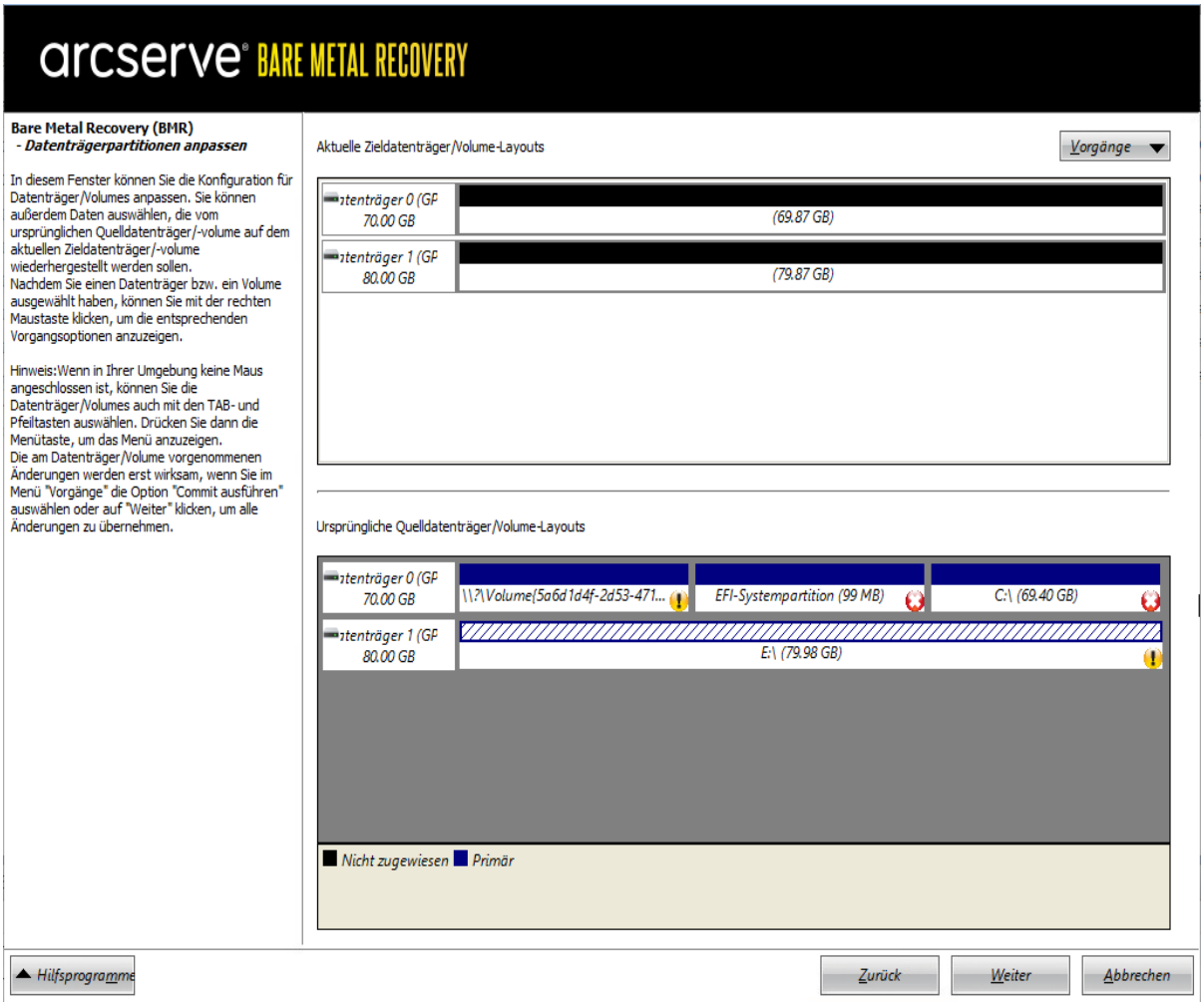
   Wichtig! Ein rotes X-Symbol, das für ein Quell-Volume im unteren Bereich angezeigt wird, gibt an, dass dieses Volume Systeminformationen enthält und dem Zieldatenträger nicht zugewiesen (zugeordnet) wurde. Diese Systeminformationen müssen dem Zieldatenträger zugewiesen werden und während der Bare-Metal-Recovery wiederhergestellt werden. Anderenfalls schlägt der Neustart fehl.

   Sie können Volumes auf einem kleineren Datenträger erstellen, der auf dem vorgeschlagenen Wert unter **Erforderlicher Mindestspeicherplatz** basiert. Im Beispiel ist die ursprüngliche Größe des Volumes 81.568 MB. Wenn Sie das Volume auf dem Zieldatenträger erstellen, dann ist die vorgeschlagene Mindestgröße 22.752 MB. In diesem Fall können Sie das ursprüngliche Volume mit einer Größe von 22.752 MB erstellen.



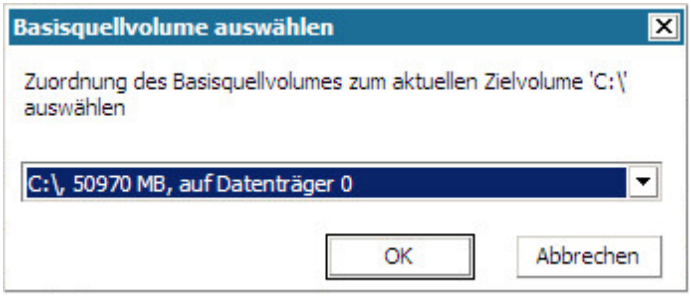
Hinweis: Wenn Sie eine BMR ausführen und das System-Volume auf einem Datenträger wiederherstellen, der nicht als Startdatenträger konfiguriert ist, kann der Rechner nicht gestartet werden, nachdem BMR abgeschlossen wurde. Stellen Sie sicher, dass Sie das System-Volume auf einem ordnungsgemäß konfigurierten Startdatenträger wiederherstellen.

Hinweis: Wenn eine Wiederherstellung auf einen anderen Datenträger bzw. auf ein anderes Volume durchgeführt wird, kann die Kapazität des neuen Datenträgers/Volumes dieselbe Größe haben, größer als der ursprüngliche Datenträger bzw. das ursprüngliche Volume oder kleiner als das ursprüngliche Datenträger/Volume sein. Eine Größenänderung ist bei dynamischen Datenträgern nicht möglich.



2. Wenn Ihnen die angezeigten aktuellen Datenträgerinformationen nicht richtig erscheinen, können Sie auf das Menü **Hilfsprogramm** zugreifen und nach fehlenden Treibern suchen.
3. Bei Bedarf können Sie im Fensterbereich des Zieldatenträgers/-Volume auf das Drop-down-Menü **Vorgänge** klicken, um die verfügbaren Optionen anzuzeigen. Weitere Informationen zu diesen Optionen finden Sie unter Verwalten des Menüs von BMR-Vorgängen.
4. Klicken Sie auf das entsprechende Ziel-Volume, und wählen Sie im Pop-up-Menü die Option **Volume zuordnen von** aus, um diesem Ziel-Volume ein Quell-Volume zuzuordnen.

   Das Dialogfeld **Basisquell-Volume auswählen** wird geöffnet.

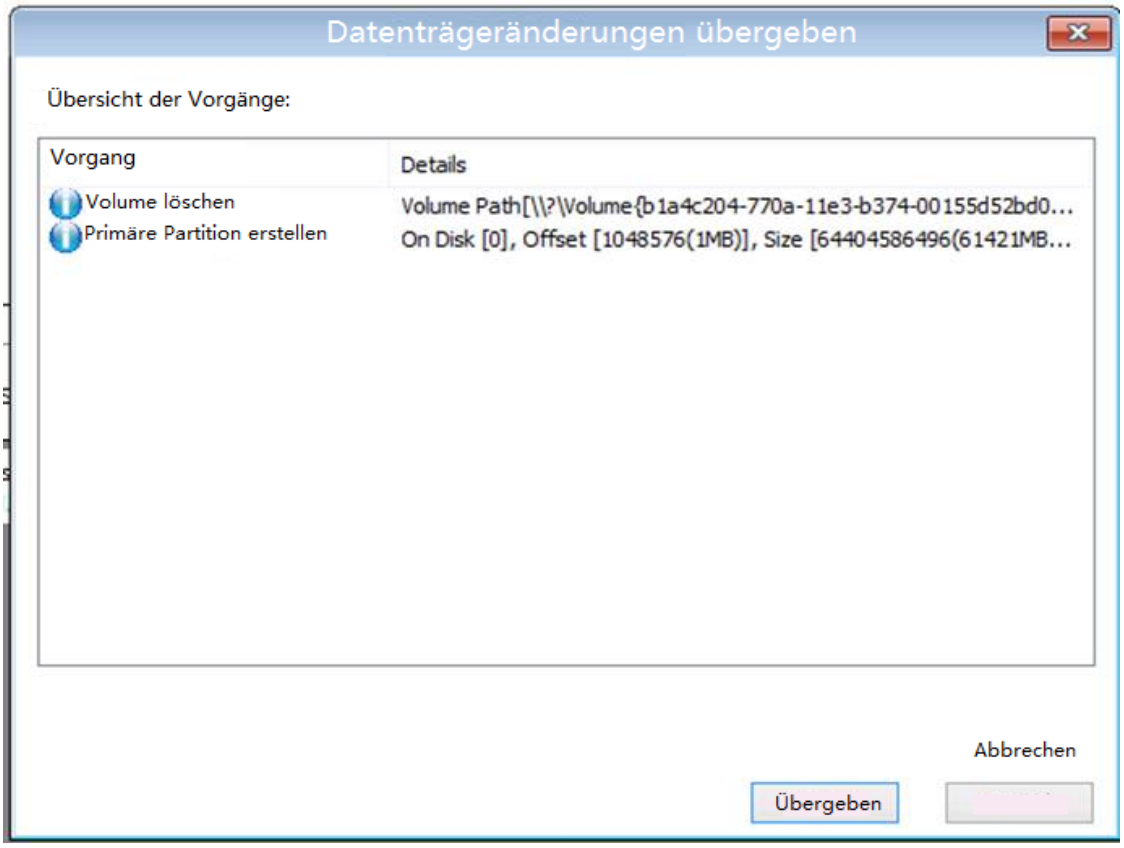


5. Klicken Sie im Dialogfeld **Basisquell-Volume auswählen** auf das Drop-down-Menü, und wählen Sie das verfügbare Quell-Volume aus, um es dem ausgewählten Ziel-Volume zuzuordnen. Klicken Sie auf **OK**.

   - Im Ziel-Volume zeigt ein grünes hakenförmiges Symbol an, dass eine Zuordnung zu diesem Ziel-Volume durchgeführt wurde.
   - Im Quell-Volume zeigt ein rotes x-förmiges Symbol an, dass dieses Quell-Volume einem Ziel-Volume zugeordnet wurde.

6. Wenn Sie sicher sind, dass alle Volumes, die Sie wiederherstellen möchten, und alle Volumes, die Systeminformationen enthalten, zu einem Ziel-Volume zugeordnet sind, klicken Sie auf **Weiter**.

   Im Bildschirm **Datenträgeränderungen übergeben** wird eine Übersicht über die ausgewählten Vorgänge angezeigt. Für jedes neu erstellte Volume werden die entsprechenden Informationen angezeigt.



7. Nachdem Sie die Richtigkeit der Übersichtsinformationen überprüft haben, klicken Sie auf **Übergeben**. (Wenn die Informationen nicht richtig sind, klicken Sie auf **Abbrechen**).

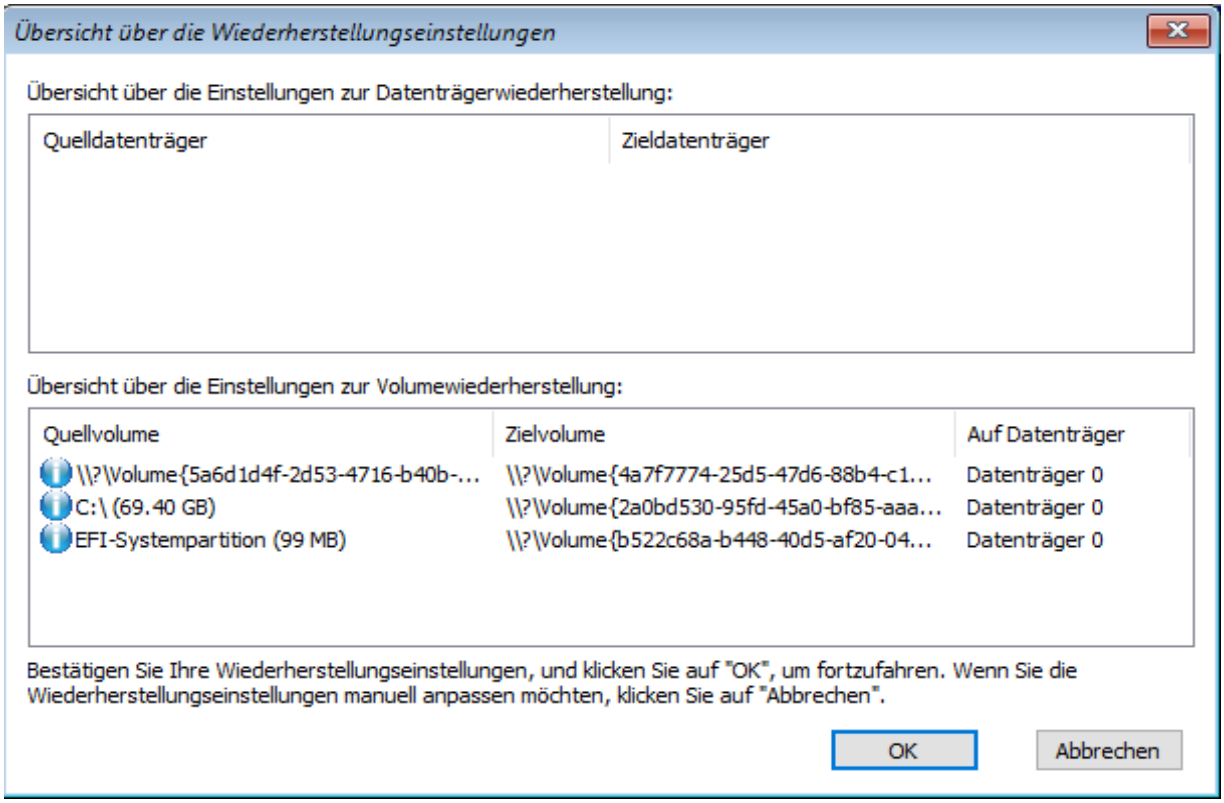
   Hinweis: Sämtliche Vorgänge, die die Festplatte betreffen, werden erst wirksam, wenn Sie sie übergeben haben.

   Auf dem Zielrechner werden die neuen Volumes erstellt und dem entsprechenden Quellrechner zugeordnet.

8. Wenn alle Änderungen abgeschlossen sind, klicken Sie auf **OK**.

   Im Bildschirm "Übersicht über die Einstellungen zur Datenträgerwiederherstellung" wird eine Übersicht der wiederherzustellenden Volumes angezeigt.

   Hinweis: Die Laufwerkbuchstaben, die unten in der Spalte "Ziel-Volume" aufgelistet werden, werden von Windows Preinstallation Environment (WinPE) automatisch erstellt. Sie können von den Laufwerkbuchstaben der Spalte "Quell-Volume" abweichen. Auch wenn die Laufwerkbuchstaben nicht miteinander übereinstimmen werden die Daten im richtigen Volume ordnungsgemäß wiederhergestellt.

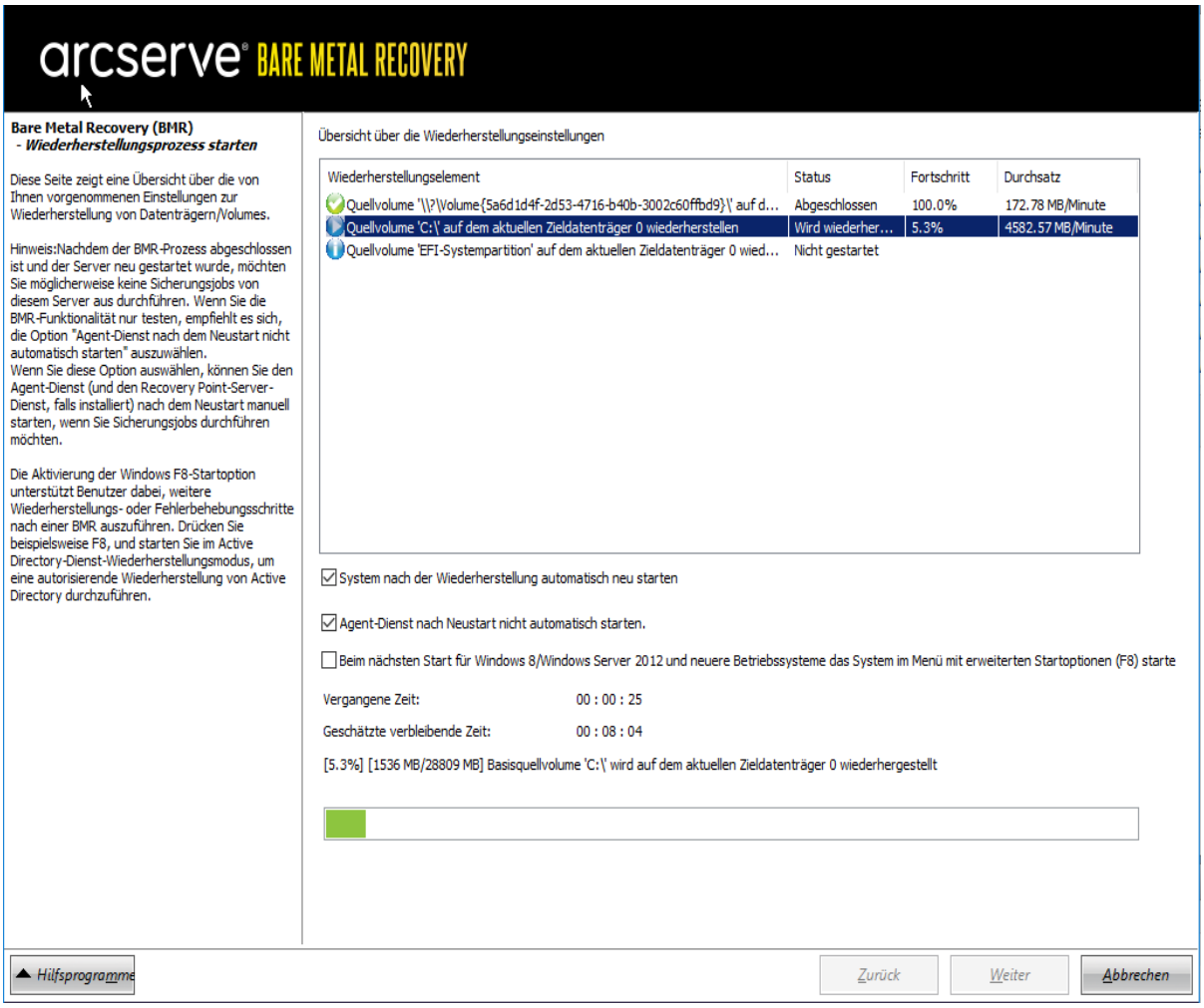


9. Nachdem Sie die Richtigkeit der Übersichtsinformationen überprüft haben, klicken Sie auf **OK**.

   Der Wiederherstellungsprozess beginnt. Im BMR-Assistenten wird der Wiederherstellungsstatus jedes Volume angezeigt.

- Dieser Vorgang kann, abhängig von der Größe des Volume, das wiederhergestellt wird, eine Weile dauern.
- Sie stellen durch diesen Prozess sämtliche Informationen, die Sie für diesen Wiederherstellungspunkt gespeichert hatten, Block für Block wieder her und erstellen auf dem Zielrechner eine Kopie des Quellrechners.
- Standardmäßig ist die Option, die nach der Wiederherstellung einen automatischen Systemneustart festlegt, aktiviert. Wenn nötig, können Sie diese Option löschen und den Neustart zu einem späteren Zeitpunkt manuell durchführen.

  Wichtig: Wenn Sie eine verbindliche Wiederherstellung eines Active Directory nach einer BMR ausführen, müssen Sie die Option **System nach der Wiederherstellung automatisch neu starten** deaktivieren. Weitere Informationen finden Sie unter So führen Sie eine verbindliche Wiederherstellung eines Active Directory nach einer BMR aus.
- Im Bedarfsfall können Sie "Agent-Dienst nach Neustart nicht automatisch starten" auswählen.
- Sie können den Vorgang auch jederzeit abbrechen.



10. Über das Menü **Hilfsprogramme** können Sie auf das BMR-**Aktivitätsprotokoll** zugreifen und es mithilfe der Option **Speichern** speichern.

    Der standardmäßige Speicherplatz für das Aktivitätsprotokoll ist folgender:

    X:\windows\system32\dr\log.

    Hinweis: Um Windows-bedingten Fehlern vorzubeugen, sollten Sie nicht die Option **Speichern unter** im Fenster des BMR-**Aktivitätsprotokolls** verwenden, um das Aktivitätsprotokoll auf Ihrem Desktop zu speichern oder einen Ordner auf Ihrem Desktop zu erstellen.

11. Wenn Sie die Wiederherstellung auf einer abweichenden Hardware durchführen (z. B. wenn der SCSI-/FC-Adapter, der zur Verbindung mit den Festplatten verwendet wurde, geändert wurde), und im ursprünglichen System kein kompatibler Treiber gefunden wird, wird die Seite "Treibereinfügung" angezeigt, über die Sie sich mit den benötigten Treibern versorgen können.

Sie können das System durchsuchen und einzufügende Treiber auswählen, sodass sogar ein Rechner mit anderer Hardware nach einer Bare-Metal-Recovery wiederhergestellt werden kann.

12. Nach Abschluss der Bare-Metal-Recovery wird eine Bestätigungsmeldung angezeigt.

Überprüfen des Erfolgs der BMR

Um zu überprüfen, ob die BMR erfolgreich war, führen Sie die folgenden Tasks aus:

- Starten Sie das Betriebssystem neu.
- Überprüfen Sie, ob alle Systeme und Anwendungen ordnungsgemäß funktionieren.
- Überprüfen Sie, ob alle Netzwerkeinstellungen richtig konfiguriert sind.
- Überprüfen Sie, ob das BIOS so konfiguriert ist, dass der Start vom Datenträger, auf dem das Boot-Volume wiederhergestellt wurde, durchgeführt wird.
- Beachten Sie nach Abschluss der BMR die folgenden Bedingungen:
  - Die erste Sicherung, die nach der BMR ausgeführt wird, ist eine Überprüfungssicherung.
  - Wenn Sie auf abweichender Hardware wiederhergestellt haben, müssen Sie die Netzwerkadapter nach dem Neustart des Rechners möglicherweise manuell konfigurieren.

    Hinweis: Wenn der Rechner neu startet, wird möglicherweise ein Fenster mit einer Windows-Wiederherstellung nach einem Fehler geöffnet, das anzeigt, dass Windows nicht erfolgreich heruntergefahren ist. Wenn dies auftritt, können Sie diese Warnung beruhigt ignorieren und Windows ganz normal weiter starten.
  - Bei dynamischen Datenträgern können Sie den Offline-Status des Datenträgers über die Datenträgerverwaltung manuell in online umändern (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).
  - Sie können dynamische Volumes auf dynamischen Datenträgern, die aufgrund von Redundanz fehlgeschlagen sind, über die Datenträgerverwaltung manuell neu synchronisieren (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).

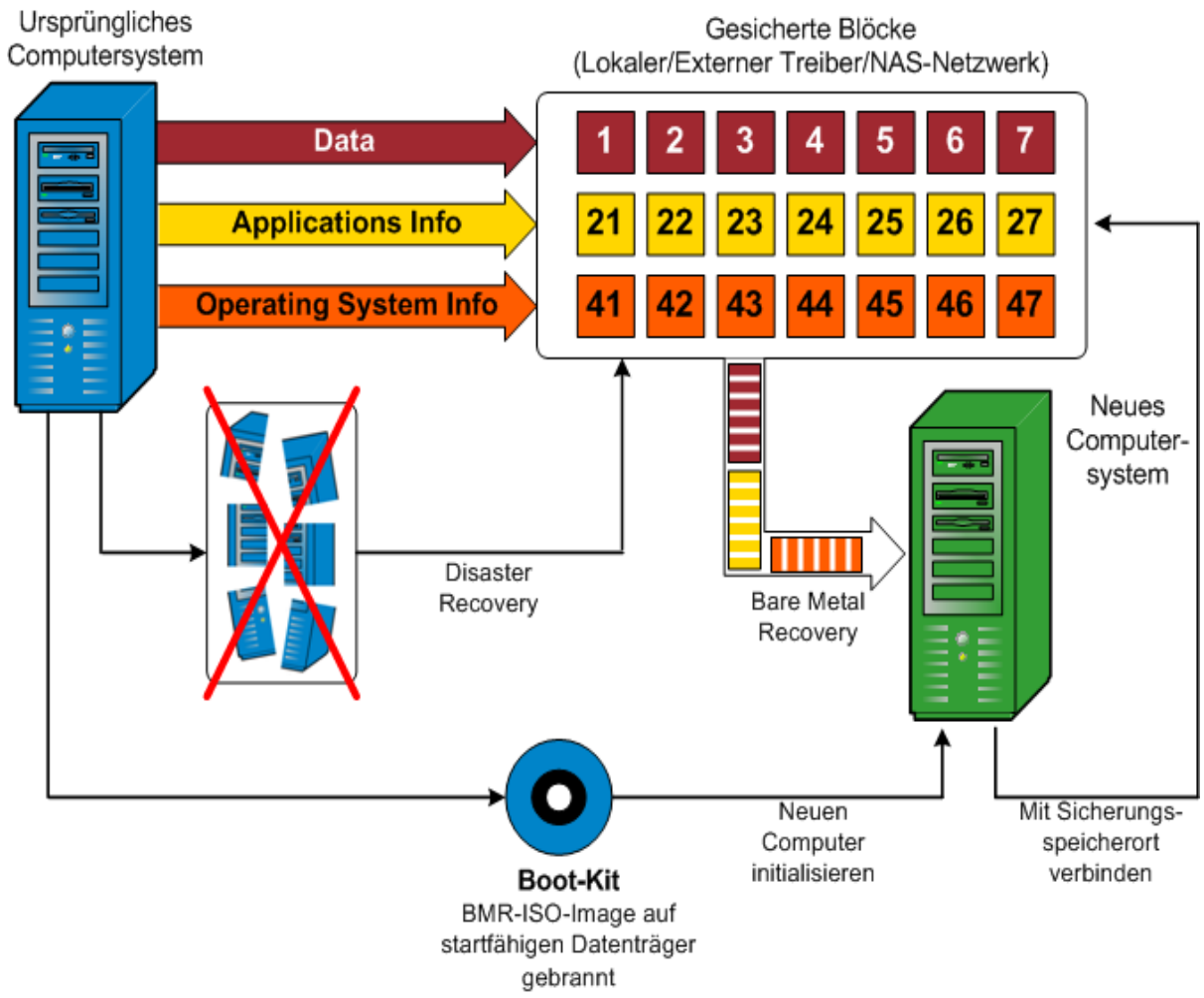
BMR-Referenzinformationen

- Funktionsweise von Bare-Metal-Recovery
- Betriebssysteme, die UEFI/BIOS-Konvertierung unterstützen
- Verwalten des Menüs von BMR-Vorgängen

Funktionsweise von Bare-Metal-Recovery

Bare-Metal-Recovery ist eine Wiederherstellung Ihres Computersystems "von Null", wobei Betriebssystem und Anwendungen neu installiert werden und Daten und Einstellungen wiederhergestellt werden. Die häufigsten Gründe für die Durchführung einer Bare-Metal-Recovery sind ein Festplattenausfall oder die Tatsache, dass eine Festplatte voll ist und ein Upgrade (eine Migration) auf eine größere Festplatte oder eine Migration zu neuerer Hardware erforderlich ist. Eine Bare-Metal-Recovery ist möglich, da Arcserve UDP Agent (Windows) während der Sicherung auf Blockebene nicht nur Daten, sondern auch sämtliche Informationen zum Betriebssystem sowie zu installierten Anwendungen, Konfigurationseinstellungen, benötigten Treibern usw. erfasst. Alle Informationen, die für eine vollständige Systemwiederherstellung "von Null" benötigt werden, werden in mehreren Blöcken gesichert und im Sicherungsziel gespeichert.

Hinweis: Dynamische Datenträger werden nur auf Datenträgerebene wiederhergestellt. Wenn Ihre Daten auf einem Volume eines dynamischen Datenträgers gesichert sind, können Sie diesen dynamischen Datenträger (einschließlich aller seiner Volumes) während der Bare-Metal-Recovery nicht wiederherstellen.



Bei einer Bare-Metal-Recovery initialisiert der Arcserve UDP Agent (Windows)-Startdatenträger das neue Computersystem und ermöglicht den Beginn der BMR. Zu Beginn der Bare-Metal-Recovery fordert Sie Arcserve UDP Agent (Windows) dazu auf, einen gültigen Speicherort auszuwählen oder anzugeben, von dem diese gesicherten Blöcke abgerufen werden sollen. Außerdem ist auch der Wiederherstellungspunkt für die Wiederherstellung anzugeben bzw. auszuwählen. Sie können auch aufgefordert werden, gültige Treiber für das neue System anzugeben. Sobald diese Verbindungs- und Konfigurationsinformationen angegeben sind, beginnt Arcserve UDP Agent (Windows) damit, das angegebene Sicherungs-Image vom Speicherort der Sicherung zu ziehen und alle gesicherten Blöcke im neuen System wiederherzustellen (leere Blöcke werden nicht wiederhergestellt). Wenn das Bare-Metal-Recovery-Image komplett wiederhergestellt ist, befindet sich der Rechner wieder im selben Status, in dem er sich beim Abschluss der letzten Sicherung befunden hat, und Arcserve UDP Agent (Windows)-Sicherungen können planmäßig fortgesetzt werden. (Die erste Sicherung nach Abschluss der Bare-Metal-Recovery ist eine Überprüfungssicherung).

Betriebssysteme, die UEFI/BIOS-Konvertierung unterstützen

Wenn entdeckt wird, dass das Betriebssystem Ihres Quellrechners nicht die gleiche Firmware wie Ihr System aufweist, werden Sie gefragt, ob Sie UEFI in ein BIOS-kompatibles System oder BIOS in ein UEFI-kompatibles System konvertieren möchten. Die folgende Tabelle listet alle Betriebssysteme und den Typ der unterstützten Konvertierung auf:

Betriebssystem (BS)	CPU	uEFI zu BIOS	BIOS zu uEFI
Windows Vista (kein SP)	x86	Nein	Nein
Windows Vista (kein SP)	x64	Nein	Nein
Windows Vista SP1	x86	Nein	Nein
Windows Vista SP1	x64	Ja	Ja
Windows Server 2008	x86	Nein	Nein
Windows Server 2008	x64	Ja	Ja
Windows Server 2008 R2	x64	Ja	Ja
Windows 7	x86	Nein	Nein
Windows 7	x64	Ja	Ja
Windows 8	x86	Nein	Nein
Windows 8	x64	Ja	Ja
Windows Server 2012	x64	Ja	Ja
Windows 8.1	x86	Nein	Nein
Windows 8.1	x64	Ja	Ja
Windows 10	x86	Nein	Nein
Windows 10	x64	Ja	Ja
Windows Server 2012 R2	x64	Ja	Ja
Windows Server 2016	x64	Ja	Ja
Windows Server 2019	x64	Ja	Ja

Verwalten des Menüs von BMR-Vorgängen

Das Menü von BMR-Vorgängen besteht aus den folgenden drei Arten von Vorgängen:

- Datenträgerspezifische Vorgänge
- Volume-/partitionsspezifische Vorgänge
- BMR-spezifische Vorgänge

Datenträgerspezifische Vorgänge:

Um datenträgerspezifische Vorgänge auszuführen, wählen Sie den Datenträger-Header aus, und klicken Sie auf **Vorgänge**.

Datenträger reinigen

Dieser Vorgang wird verwendet, um alle Partitionen eines Datenträgers zu bereinigen, und hat folgende Eigenschaften:

- Er ist eine alternative Methode, um alle Volumes von einem Datenträger zu löschen. Mit dem Vorgang **Datenträger reinigen** müssen Sie Volumes nicht einzeln hintereinander löschen.
- Er wird verwendet, um Nicht-Windows-Partitionen zu löschen. Aufgrund einer VDS-Einschränkung können Nicht-Windows-Partitionen nicht von der Benutzeroberfläche gelöscht werden, aber Sie können diesen Vorgang verwenden, um alle zu bereinigen.

  Hinweis: Während BMR können Sie – wenn der Zieldatenträger Nicht-Windows-Partitionen oder OEM-Partitionen hat – diese Partition nicht auswählen und nicht von der BMR-Benutzeroberfläche löschen. Üblicherweise würde dies auftreten, wenn Sie irgendwann Linux/UNIX auf dem Zieldatenträger installiert hatten. Gehen Sie folgendermaßen vor, um das Problem zu lösen:

- Wählen Sie den Datenträger-Header auf der BMR-Benutzeroberfläche aus, klicken Sie auf **Vorgänge**, und verwenden Sie den Vorgang **Datenträger reinigen**, um alle Partitionen auf dem Datenträger zu löschen.
- Öffnen Sie eine Eingabeaufforderung, und tippen Sie **Diskpart**, um die Diskpart-Befehlskonsole zu öffnen. Tippen Sie anschließend "select disk x", wobei "x" die Nummer des Datenträgers ist, und "clean", um alle Partitionen auf dem Datenträger zu löschen.

In MBR konvertieren

Dieser Vorgang wird verwendet, um einen Datenträger in MBR (Master Boot Record) zu konvertieren. Er ist nur verfügbar, wenn der ausgewählte

Datenträger ein GPT-Datenträger (GUID-Partitionstabelle) ist und keine Volumes auf diesem Datenträger vorhanden sind.

In GPT konvertieren

Dieser Vorgang wird verwendet, um einen Datenträger in GPT zu konvertieren. Er ist nur verfügbar, wenn der ausgewählte Datenträger ein MBR-Datenträger ist und keine Volumes auf diesem Datenträger vorhanden sind.

In "Basis" konvertieren

Dieser Vorgang wird verwendet, um einen Datenträger in einen Basisdatenträger zu konvertieren. Er ist nur verfügbar, wenn der ausgewählte Datenträger ein dynamischer Datenträger ist und keine Volumes auf diesem Datenträger vorhanden sind.

In "Dynamisch" konvertieren

Dieser Vorgang wird verwendet, um einen Datenträger in einen dynamischen Datenträger zu konvertieren. Er ist nur verfügbar, wenn der ausgewählte Datenträger ein Basisdatenträger ist.

Online-Datenträger

Dieser Vorgang wird verwendet, um einen Datenträger online zu stellen. Er ist nur verfügbar, wenn sich der ausgewählte Datenträger im Offline-Status befindet.

Datenträgereigenschaften

Dieser Vorgang wird verwendet, um detaillierte Datenträgereigenschaften anzuzeigen. Dieser Vorgang ist immer verfügbar. Wenn Sie ihn auswählen, wird ein Dialogfeld namens **Datenträgereigenschaften** angezeigt.

Volume-/partitionsspezifische Vorgänge:

Um Vorgänge für Volumes oder Partitionen auszuführen, wählen Sie den Textbereich des Datenträgers aus, und klicken Sie auf **Vorgänge**. Von diesem Menü aus können Sie neue Partitionen erstellen, um den Datenträgerpartitionen auf dem Quell-Volume zu entsprechen.

Primäre Partition erstellen

Dieser Vorgang wird verwendet, um eine Partition auf einem Basisdatenträger zu erstellen. Er ist nur verfügbar, wenn es sich beim ausgewählten Bereich um nicht zugeordneten Speicherplatz handelt.

Logische Partition erstellen

Dieser Vorgang wird verwendet, um eine logische Partition auf einem MBR-Basisdatenträger zu erstellen. Er ist nur verfügbar, wenn es sich beim ausgewählten Bereich um eine erweiterte Partition handelt.

Erweiterte Partition erstellen

Dieser Vorgang wird verwendet, um eine erweiterte Partition auf einem MBR--Basisdatenträger zu erstellen. Er ist nur verfügbar, wenn der Datenträger ein MBR-Datenträger ist und es sich beim ausgewählten Bereich um nicht zugeordneten Speicherplatz handelt.

Für das System reservierte Partition erstellen

Dieser Vorgang wird verwendet, um die für das System reservierte Partition auf einem BIOS-Firmwaresystem zu erstellen. Er erstellt eine Zuordnungsbeziehung mit der EFI-Systempartitionsquelle. Er ist nur verfügbar, wenn Sie ein UEFI-System in einem BIOS-System wiederherstellen.

Hinweis: Wenn Sie zu einem früheren Zeitpunkt UEFI in ein BIOS-kompatibles System konvertiert haben, verwenden Sie den Vorgang "Für das System reservierte Partition erstellen", um die Größe des Zieldatenträgers zu ändern.

EFI-Systempartition erstellen

Dieser Vorgang wird verwendet, um die EFI-Systempartition auf einem GPT-Basisdatenträger zu erstellen. Er ist nur verfügbar, wenn es sich bei der Firmware des Zielcomputers um UEFI handelt und der ausgewählte Datenträger ein GPT-Basisdatenträger ist.

Hinweis: Wenn Sie zu einem früheren Zeitpunkt BIOS in ein UEFI-kompatibles System konvertiert haben, verwenden Sie den Vorgang "EFI-Systempartition erstellen", um die Größe des Zieldatenträgers zu ändern.

Hinweis: In Systemen, die UEFI unterstützen, muss sich die Startpartition auf einer Festplatten mit GUID-Partitionstabellen (GPT) befinden. Wenn Sie einen MBR-Datenträger (Master Boot Record) verwenden, müssen Sie diesen Datenträger in einen GPT-Datenträger konvertieren und anschließend den Vorgang "EFI-Systempartition erstellen" verwenden, um die Größe des Zieldatenträgers zu ändern.

Größe des Volume ändern

Dieser Vorgang wird verwendet, um die Größe eines Volume zu ändern. Dies ist eine Alternative zu den Windows-Methoden "Volume erweitern" bzw. "Volume verkleinern". Er ist nur verfügbar, wenn es sich beim ausgewählten Bereich um eine gültige Datenträgerpartition handelt.

Volume löschen

Dieser Vorgang wird verwendet, um ein Volume zu löschen. Er ist nur verfügbar, wenn es sich beim ausgewählten Bereich um ein gültiges Volume handelt.

Erweiterte Partition löschen

Dieser Vorgang wird verwendet, um eine erweiterte Partition zu löschen. Er ist nur verfügbar, wenn es sich beim ausgewählten Bereich um eine erweiterte Partition handelt.

Volume-Eigenschaften

Dieser Vorgang wird verwendet, um detaillierte Volume-Eigenschaften anzuzeigen. Wenn Sie diesen Vorgang auswählen, wird ein Dialogfeld namens **Volume-Eigenschaften** angezeigt.

BMR-spezifische Vorgänge:

Diese Vorgänge sind spezifisch für BMR. Um BMR-Vorgänge auszuführen, wählen Sie den Header oder den Textbereich des Datenträgers aus, und klicken Sie auf **Vorgänge**.

Datenträger zuordnen von...

Dieser Vorgang wird verwendet, um eine Zuordnungsbeziehung zwischen dem Quelldatenträger und dem dynamischen Zieldatenträger zu erstellen. Er ist nur verfügbar, wenn der ausgewählte Datenträger ein dynamischer Datenträger ist.

Hinweis: Wenn Sie eine Zuordnung zu einem anderen Datenträger durchführen, muss die Kapazität jedes zugeordneten Ziel-Volume gleich oder größer als die des entsprechenden Quell-Volumes sein.

Volume zuordnen von...

Dieser Vorgang wird verwendet, um eine Zuordnungsbeziehung zwischen dem Quell-Volume und dem Basisziel-Volume zu erstellen. Er ist nur verfügbar, wenn das ausgewählte Volume ein Basis-Volume ist.

Hinweis: Wenn Sie eine Zuordnung zu einem anderen Datenträger durchführen, muss die Kapazität jedes zugeordneten Ziel-Volume gleich oder größer als die des entsprechenden Quell-Volumes sein.

Commit ausführen

Dieser Vorgang ist immer verfügbar. Alle Vorgänge werden zwischengespeichert und verursachen keine Änderungen des Zieldatenträgers, bis Sie den Vorgang **Commit ausführen** auswählen.

Zurücksetzen

Dieser Vorgang ist immer verfügbar. Der Vorgang **Zurücksetzen** wird verwendet, um Ihre Vorgänge aufzuheben und den Standardstatus des Datenträgerlayouts wiederherzustellen. Dieser Vorgang bereinigt alle zwischengespeicherten Vorgänge. Zurücksetzen bedeutet, die Informationen zu Quell- und Zieldatenträgerlayout neu aus der Konfigurationsdatei und

dem derzeitigen BS zu laden und alle vom Benutzer geänderten Informationen zum Datenträgerlayout zu verwerfen.

Beheben von BMR-Problemen

Wenn ein Problem erkannt wird, generiert Arcserve UDP Agent (Windows) eine Meldung, die Ihnen dabei hilft, das Problem zu identifizieren und zu beheben. Diese Meldungen sind im **Aktivitätsprotokoll** von Arcserve UDP Agent (Windows) enthalten, auf das über die Option **Protokolle anzeigen** auf der Startseite des Produkts zugegriffen werden kann. Wenn versucht wird, eine ungültige Aktion durchzuführen, zeigt Arcserve UDP Agent (Windows) außerdem üblicherweise eine Pop-up-Meldung an, damit Sie das Problem schnell identifizieren und lösen können.

- Langsamer Durchsatz während der BMR
- Nach der BMR werden dynamische Volumes nicht vom Betriebssystem erkannt
- Neustart von virtuellem Hyper-V-Rechner nach Bare-Metal-Recovery nicht möglich
- Neustart von virtuellem VMware-Rechner nach Bare-Metal-Recovery nicht möglich
- Server kann nicht gestartet werden, nachdem BMR ausgeführt wurde
- BMR-Job kann nicht an Recovery Point Server übergeben werden

Langsamer Durchsatz während der BMR

Dieses Problem wird kann durch SATA-Controller verursacht werden, bei denen "AHCI" aktiviert ist.

Während der BMR installiert Arcserve UDP Agent (Windows) Treiber für kritische unbekannte Geräte. Treiber, die bereits auf dem Gerät installiert sind, werden von Arcserve UDP Agent (Windows) nicht aktualisiert. Bei einigen Geräten verfügt Windows 7PE über die entsprechenden Treiber, die aber möglicherweise nicht die besten Treiber sind, was dazu führen kann, dass die BMR zu langsam ausgeführt wird.

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

- Überprüfen Sie, ob der Treiberordner die neuesten Laufwerktreiber enthält. Wenn dies der Fall ist und Sie eine Wiederherstellung auf dem ursprünglichen Rechner durchführen, installieren Sie den neuen Treiber aus dem Treiberordner. Wenn Sie eine Wiederherstellung auf einem alternativen Rechner durchführen, laden Sie aus dem Internet die aktuellsten Laufwerktreiber herunter und laden Sie sie, bevor Sie die Wiederherstellung der Daten starten. Um den Treiber zu laden, können Sie das Hilfsprogramm "drvload.exe" verwenden, das in Windows PE enthalten ist.
- Ändern Sie die Betriebsart des Gerätes von "AHCI" (Advanced Host Controller Interface) in Kompatibilitätsmodus. (Kompatibilitätsmodus gibt einen höheren Durchsatz an).

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Nach der BMR werden dynamische Volumes nicht vom Betriebssystem erkannt

Um dynamische Datenträger in einem konsistenten Status halten zu können, synchronisiert das Windows-Betriebssystem auf jedem dynamischen Datenträger automatisch die Metadaten des "Logical Disk Manager" (LDM). Wenn BMR einen dynamischen Datenträger wiederherstellt und ihn online stellt, werden die LDM-Metadaten auf diesem Datenträger automatisch vom Betriebssystem aktualisiert. Dies kann dazu führen, dass ein dynamisches Volume nicht vom Betriebssystem erkannt wird und nach dem Neustart fehlt.

Um dieses Problem zu beheben, sollten Sie bei einer BMR mit mehreren dynamischen Datenträgern keine Vorgänge vor der BMR durchführen, wie z. B. Volume reinigen oder löschen usw.

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Neustart von virtuellem Hyper-V-Rechner nach Bare-Metal-Recovery nicht möglich

Wenn Sie eine Bare-Metal-Recovery auf einem Hyper-V-Rechner durchgeführt haben, der aus mehr als einem mit einem Integrated Drive Electronics (IDE)-Controller verbundenen Datenträger besteht, und der Server nicht neu gestartet werden kann, führen Sie zur Fehlerbehebung folgenden Vorgang durch:

1. Stellen Sie sicher, dass der Datenträger, der das Systemvolume enthält, der Masterdatenträger ist.

   Das Hyper-V-BIOS sucht nach dem Systemvolume auf dem Masterdatenträger (Datenträger 1), der mit dem Masterkanal verbunden ist. Wenn das Systemvolume nicht auf dem Masterdatenträger gespeichert ist, startet der virtuelle Rechner nicht neu.

   Hinweis: Stellen Sie sicher, dass der Datenträger, der das Systemvolume enthält, mit einem IDE-Controller verbunden ist. Hyper-V kann nicht von einem SCSI-Datenträger gestartet werden.

2. Wenn nötig, ändern Sie die Hyper-V-Einstellungen. Verbinden Sie den Datenträger, der das Systemvolume enthält, mit dem IDE-Masterkanal, und starten Sie den virtuellen Rechner neu.

   Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Neustart von virtuellem VMware-Rechner nach Bare-Metal-Recovery nicht möglich

Wenn Sie eine Bare-Metal-Recovery auf einem VMware-Rechner durchgeführt haben, der aus mehr als einem mit einem Integrated Drive Electronics (IDE)-Controller oder einem SCSI-Adapter verbundenen Datenträger besteht, und der Server nicht neu gestartet werden kann, führen Sie zur Fehlerbehebung folgenden Vorgang durch:

1. Stellen Sie sicher, dass der Datenträger, der das Systemvolume enthält, der Masterdatenträger ist.

   Das VMware-BIOS sucht nach dem Systemvolume auf dem Masterdatenträger (Datenträger 0), der mit dem Masterkanal verbunden ist. Wenn sich das Systemvolume nicht auf dem Masterdatenträger befindet, startet der virtuelle Rechner nicht neu.

2. Wenn nötig, ändern Sie die VMware-Einstellungen. Verbinden Sie den Datenträger, der das Systemvolume enthält, mit dem IDE-Masterkanal, und starten Sie den virtuellen Rechner neu.

3. Wenn es sich um einen SCSI-Datenträger handelt, stellen Sie sicher, dass sich der Datenträger, der das Boot-Volume enthält, als erster mit dem SCSI-Adapter verbindet. Anderenfalls weisen Sie den Boot-Datenträger aus dem VMware-BIOS zu.

4. Da das VMware-BIOS während dem Starten nur acht Datenträger erkennt, stellen Sie sicher, dass sich der Datenträger mit dem Boot-Volume unter den letzten acht Datenträgern befindet. Wenn vor dem Datenträger mit dem Boot-Volume mehr als sieben Datenträger mit dem SCSI-Adapter verbunden sind, kann der virtuelle Rechner nicht gestartet werden.

   Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Der Server kann nicht gestartet werden, nachdem eine BMR ausgeführt wurde.

Problem

Wenn es sich beim Quellrechner um einen Active Directory-Server handelt, der eine BMR auf einen physischen Rechner mit abweichender Hardware oder auf einen virtuellen Rechner auf einem Hyper-V-Server ausführt, wird der Server nicht gestartet, und es wird ein blauer Bildschirm mit folgender Meldung angezeigt:

STOPP: c00002e2 Verzeichnisdienste konnten aufgrund von folgendem Fehler nicht gestartet werden: Ein Gerät, das an das System angehängt wurde, funktioniert nicht. Fehlerstatus: 0xc0000001.

Lösung

Starten Sie das System zur BMR-PE-Umgebung neu, benennen Sie alle *.log-Dateien im Ordner "C:\Windows\NTDS" um, und starten Sie das System neu. Benennen Sie zum Beispiel die Datei "edb.log" in "edb.log.old" um, und starten Sie das System neu.

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

BMR-Job kann nicht an Recovery Point Server übergeben werden

Bei einer Wiederherstellung von einem RPS-Server für denselben Knoten (Agent-Sicherung oder hostbasierte Sicherung) wird nur ein BMR-Job unterstützt. Dies wird vom Job-Monitor auf dem RPS-Server gesteuert.

Wenn der Rechner, auf dem der BMR-Job ausgeführt wird, unerwartet heruntergefahren oder neu gestartet wird, wartet der Job-Monitor auf der Seite des RPS-Servers 10 Minuten lang. Danach tritt eine Zeitüberschreitung ein. Während dieses Zeitraums können Sie für denselben Knoten über denselben RPS-Server keinen weiteren BMR-Job starten.

Wenn Sie die BMR über die BMR-Benutzeroberfläche abbrechen, tritt dieses Problem nicht auf.

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Auf dem BMR-Zielrechner wird nach dem Start das Fenster "System-Wiederherstellungsoptionen" angezeigt, nachdem eine BMR durchgeführt wurde

Problem

Wenn Sie auf einem virtuellen Rechner auf einem ESX-Server eine BMR durchführen, wird auf dem BMR-Zielcomputer manchmal nach dem Start das Fenster "System-Wiederherstellungsoptionen" angezeigt.

Lösung

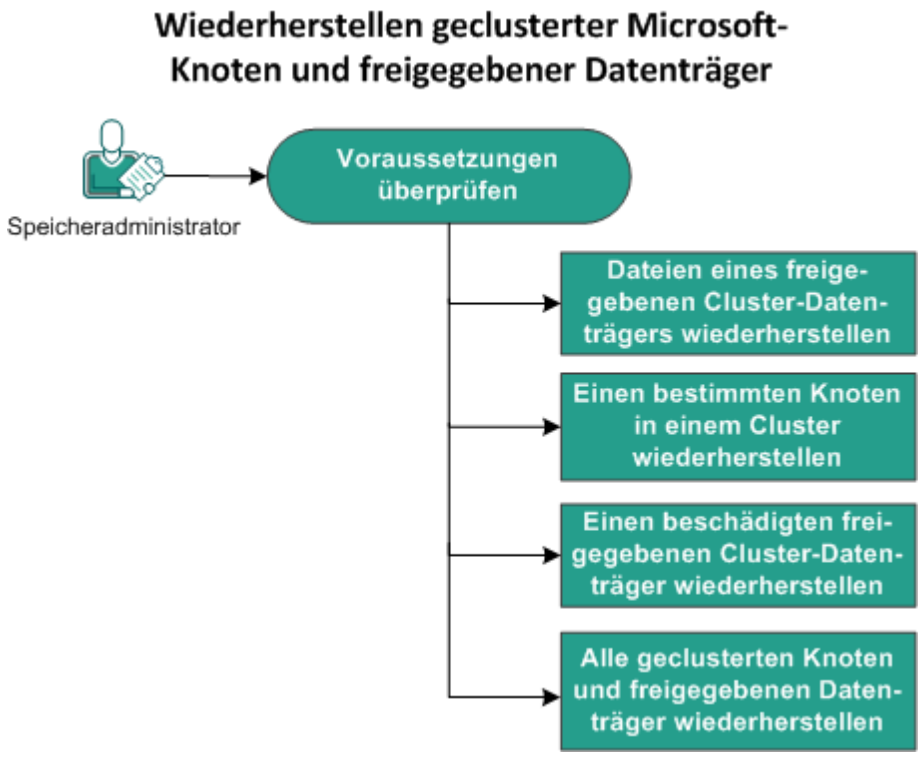
Um dieses Problem zu beheben, sollten Sie auf dem Instant VM-Rechner bestimmte VSS-Writer mit VMware-Tools deaktivieren und dann erneut eine BMR ausführen.

So stellen Sie geclusterte Microsoft-Knoten und freigegebene Datenträger wieder her

Wenn Sie eine geclusterte Umgebung verwenden und die geclusterten Knoten und freigegebenen Datenträger nicht ordnungsgemäß funktionieren, können Sie die Knoten und Datenträger auf einfache Weise wiederherstellen. Sie können folgende Elemente wiederherstellen:

- Einzelne Dateien und Ordner auf einem freigegeben Datenträger
- Spezifische Knoten in einem Cluster
- Vollständigen freigegeben Datenträger
- Vollständiges Cluster-Setup (alle geclusterten Knoten sowie den freigegebenen Datenträger)

Das folgende Diagramm veranschaulicht den Prozess zum Wiederherstellen von geclusterten Knoten und freigegeben Festplatten:



Befolgen Sie diese Schritte, um geclusterte Microsoft-Knoten und freigegebene Datenträger wiederherzustellen:

- Überprüfen der Voraussetzungen
- Wiederherstellen von Dateien auf einem freigegebenen Cluster-Datenträger
- Wiederherstellen eines spezifischen Knotens in einem Cluster

- Wiederherstellen eines beschädigten freigegebenen Cluster-Datenträgers
- Wiederherstellen des vollständigen geclusterten Knotens und des freigegebenen Datenträgers

Überprüfen der Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Sie haben einen gültigen Wiederherstellungspunkt für die Wiederherstellung.
- Sie haben ein gültiges ISO-Image für eine BMR.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Wiederherstellen von Dateien auf einem freigegebenen Cluster-Datenträger

Der freigegebene Datenträger gehört zu einem der Knoten des Clusters. Wenn Sie Dateien von der freigegebenen Festplatte (nicht dem Quorum-Datenträger des Clusters) wiederherstellen, müssen Sie den übergeordneten Knoten des freigegebenen Datenträgers suchen. Wenn Sie den übergeordneten Knoten identifiziert haben, können Sie Dateien auf dem übergeordneten Knoten des freigegebenen Datenträgers wiederherstellen.

Hinweis: Nach einem Failover müssen Sie den Wiederherstellungspunkt eines anderen Agenten durchsuchen, um den gewünschten Wiederherstellungspunkt ausfindig zu machen.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Agenten an, der den freigegebenen Datenträger besitzt.
2. Öffnen Sie den Wiederherstellungsassistenten, und wählen Sie "Wiederherzustellende Dateien/Ordner suchen" aus.

   Hinweis: Weitere Informationen zum Wiederherstellen der Dateien und Ordner finden Sie in "So stellen Sie Dateien/Ordner wieder her".
3. Wählen Sie im Wiederherstellungsassistenten alle Dateien, die Sie am ursprünglichen Speicherort wiederherstellen möchten, aus.
4. Schließen Sie die Konfigurationen im Wiederherstellungsassistenten ab, und übergeben Sie den Job.

   Die Dateien werden wiederhergestellt.
5. Melden Sie sich beim übergeordneten Knoten des freigegebenen Datenträgers an, und überprüfen Sie, ob die Dateien wiederhergestellt wurden.

   Die Dateien des freigegebenen Datenträgers werden wiederhergestellt.

Wiederherstellen eines spezifischen Knotens in einem Cluster

Wenn ein spezifischer Knoten in einem Cluster außer Betrieb ist, können Sie eine BMR speziell für diesen Knoten ausführen. Normalerweise befindet sich der freigegebene Datenträger in diesem Szenario in einem guten Zustand und benötigt keine Wiederherstellung.

Gehen Sie wie folgt vor:

1. Bereiten Sie das BMR-Image vor (auf CD, DVD oder USB-Stick).
2. Entfernen Sie alle Verbindungen zwischen dem Knoten, den Sie wiederherstellen möchten, und dem freigegebenen Datenträger.

   Beispiel: Unterbrechen Sie die Fibre-Channel-Verbindung.
3. Führen Sie eine BMR für den Cluster-Knoten aus.

   Hinweis: Weitere Informationen zum Ausführen einer Bare-Metal-Recovery finden Sie in "So führen Sie eine BMR mithilfe einer Sicherung aus".

   Der spezifische Knoten im Cluster wird wiederhergestellt.
4. Überprüfen Sie den Status des wiederhergestellten Knotens in der Cluster-Verwaltungskonsole, und stellen Sie sicher, dass er als Teil des Clusters agiert.

   Der spezifische Knoten im Cluster wird wiederhergestellt.

Wiederherstellen eines beschädigten freigegebenen Cluster-Datenträgers

Der freigegebene Datenträger gehört zu einem der Knoten des Clusters. Wenn der freigegebene Datenträger beschädigt oder fehlerhaft ist, können Sie die betroffenen Dateien oder Ordner des freigegebenen Datenträgers wiederherstellen, ohne die geclusterten Knoten wiederherzustellen. Normalerweise befinden sich der Quorum-Datenträger und alle Cluster-Knoten in diesem Szenario in einem guten Zustand.

Gehen Sie wie folgt vor:

1. Ersetzen Sie den beschädigten Datenträger manuell, und konfigurieren Sie den freigegebenen Cluster-Datenträger neu.
2. Identifizieren Sie den Agenten, der den freigegebenen Datenträger besitzt, und melden Sie sich bei diesem Agenten an.
3. Öffnen Sie den Wiederherstellungsassistenten, und wählen Sie "Wiederherzustellende Dateien/Ordner suchen" aus.

   Hinweis: Weitere Informationen zum Wiederherstellen der Dateien und Ordner finden Sie in "So stellen Sie Dateien/Ordner wieder her".
4. Wählen Sie im Wiederherstellungsassistenten alle Dateien, die Sie am ursprünglichen Speicherort wiederherstellen möchten, aus.
5. Schließen Sie die Konfigurationen im Wiederherstellungsassistenten ab, und übergeben Sie den Job.

   Der freigegebene Datenträger wird wiederhergestellt.
6. Überprüfen Sie den Status des freigegebenen Datenträgers in der Cluster-Verwaltungskonsole, und stellen Sie sicher, dass er als Teil des Clusters agiert.

   Der freigegebene Datenträger wird wiederhergestellt.

Wiederherstellen des vollständigen geclusterten Knotens und des freigegebenen Datenträgers

Wenn das gesamte geclusterte Setup beschädigt ist oder nicht ordnungsgemäß funktioniert, können Sie den vollständigen Cluster wiederherstellen. Das Wiederherstellen des vollständigen Clusters ist ein zweiteiliger Prozess. Zunächst stellen Sie einzelne geclusterte Knoten mithilfe von BMR wieder her. Danach stellen Sie die Dateien und Ordner des freigegebenen Datenträgers wieder her.

Hinweis: Quorum-Datenträger sollten nicht mit dem Wiederherstellungsassistenten in Arcserve UDP Agent (Windows) wiederhergestellt, sondern über die Clusterverwaltungskonsole neu erstellt werden.

Gehen Sie wie folgt vor:

1. Bereiten Sie das BMR-Image vor (auf CD, DVD oder USB-Stick).
2. Entfernen Sie alle Verbindungen zwischen dem Knoten, den Sie wiederherstellen möchten, und dem freigegebenen Datenträger.

   Beispiel: Unterbrechen Sie die Fibre-Channel-Verbindung.
3. Führen Sie eine BMR für den Cluster-Knoten aus.

   Hinweis: Weitere Informationen zum Ausführen einer Bare-Metal-Recovery finden Sie in "So führen Sie eine BMR mithilfe einer Sicherung aus".

   Der spezifische Knoten im Cluster wird wiederhergestellt.
4. Überprüfen Sie den Status des wiederhergestellten Knotens in der Cluster-Verwaltungskonsole, und stellen Sie sicher, dass er als Teil des Clusters agiert.

   Der spezifische Knoten im Cluster wird wiederhergestellt.
5. Wiederholen Sie die Schritte, um alle geclusterten Knoten wiederherzustellen.

   Alle geclusterten Knoten werden wiederhergestellt. Stellen Sie nun den freigegebenen Datenträger wieder her.
6. Ersetzen Sie den beschädigten Datenträger manuell, und konfigurieren Sie den freigegebenen Cluster-Datenträger neu.
7. Identifizieren Sie den Agenten, der den freigegebenen Datenträger besitzt, und melden Sie sich bei diesem Agenten an.
8. Öffnen Sie den Wiederherstellungsassistenten, und wählen Sie "Wiederherzustellende Dateien/Ordner suchen" aus.

   Hinweis: Weitere Informationen zum Wiederherstellen der Dateien und Ordner finden Sie in "So stellen Sie Dateien/Ordner wieder her".

9. Wählen Sie im Wiederherstellungsassistenten alle Dateien, die Sie am ursprünglichen Speicherort wiederherstellen möchten, aus.
10. Schließen Sie die Konfigurationen im Wiederherstellungsassistenten ab, und übergeben Sie den Job.

    Der freigegebene Datenträger wird wiederhergestellt.
11. Überprüfen Sie die Dateien des freigegebenen Datenträgers, und stellen Sie sicher, dass die Dateien wiederhergestellt wurden.

    Der gesamte Cluster ist wiederhergestellt.

Wiederherstellen eines Active Directory

Sie müssen eine gesicherte Active Directory-Sitzung wiederherstellen, wenn folgende Szenarien vorliegen:

- Sie möchten ein Attribut des Active Directory-Objekts von einer verfügbaren gesicherten Active Directory-Sitzung wiederherstellen (nicht nur die letzte gesicherte Sitzung).
- Sie möchten das Active Directory-Objekt von einer verfügbaren gesicherten Active Directory-Sitzung wiederherstellen (nicht nur die letzte gesicherte Sitzung).
- Sie möchten mehrere Active Directory-Attribute und -Objekte von einer verfügbaren gesicherten Active Directory-Sitzung wiederherstellen (nicht nur die letzte gesicherte Sitzung).

Wichtig! Um eine Granular-Wiederherstellung eines Active Directory durchzuführen ist eine agentenbasierte Sicherung erforderlich.

Liste aktiver Directory-Objekte, die durch eine Wiederherstellung auf Objektebene wiederhergestellt wurden		
Organisationseinheit	Website	Lost-and-found-Klasse
Benutzer	Standort-Container	In Domain-Klasse erstellen
Gruppe	Standort-Link	DNS-Zonenklasse
Computer	Standort-Linkbrücke	Domain-Klasse
Kontakt	Standorteinstellungen	Domain-DNS-Klasse
Verbindung	Subnet-Container	DMD-Klasse
Freigegebener Ordner	Vertrauenswürdige Domain	Klasse der Organisationseinheit
Drucker	Konfigurationsklasse	Containerecifiers-Klasse

In diesem Szenario wird beschrieben, wie Sie ein Active Directory wiederherstellen können.

Führen Sie folgende Aufgaben aus, um ein Active Directory wiederherzustellen:

1. Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise
2. Wiederherstellen eines Active Directory
3. Überprüfen, ob das Active Directory wiederhergestellt wurde

Überprüfen der Voraussetzungen für Wiederherstellungen und Hinweise

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Wiederherstellung ausführen:

- Sie haben bereits die Volumes unterstützt, die den Active Directory-Datenbankordner und den Ordner der Protokolldateien enthalten.
- Sie haben Arcserve UDP Agent (Windows) auf dem Domänencontroller installiert haben.
- Sie haben eine agentenbasierte Sicherung durchgeführt.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Überprüfen Sie die folgenden Wiederherstellungshinweise:

- Um bei einem Wiederherstellungspunkt, für den kein Dateisystemkatalog erstellt wurde, sicherzustellen, dass Sie wiederherzustellende Dateien/Ordner suchen und auswählen können, sollte dem Konto bzw. der Gruppe vor der Erstellung der Sicherung Lese-und Schreibzugriff für alle Ordner/Dateien auf allen Volumes gewährt werden.
- Sie können eine Active Directory-Wiederherstellung nur unter Arcserve UDP Agent (Windows) ausführen.

Wiederherstellen eines Active Directory

Nachdem Sie das Active Directory in verschiedenen Volumes installiert und eine Sicherung für beide Volumes ausgeführt haben, möchten Sie möglicherweise die Volumes mit dem Active Directory wiederherstellen. Dieses Szenario beschreibt, wie Sie gesicherte Active Directory-Volumes wiederherstellen können.

Hinweis: Stellen Sie sicher, dass Sie die Voraussetzungen abgeschlossen und Active Directory-Volumes gesichert haben.

Gehen Sie wie folgt vor:

1. Verwenden Sie eine der folgenden Vorgangsweisen, um auf das Dialogfeld zur Auswahl der Wiederherstellungsmethoden zuzugreifen:

   In Arcserve UDP:

   a. Melden Sie sich bei Arcserve UDP an.

   b. Klicken Sie auf die Registerkarte **Ressourcen**.

   c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

   e. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

      Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

      Hinweis: Sie werden automatisch im Agent-Knoten angemeldet, und das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird im Agent-Knoten geöffnet.

   In Arcserve UDP Agent (Windows):

   a. Melden Sie sich bei Arcserve UDP Agent (Windows) an.

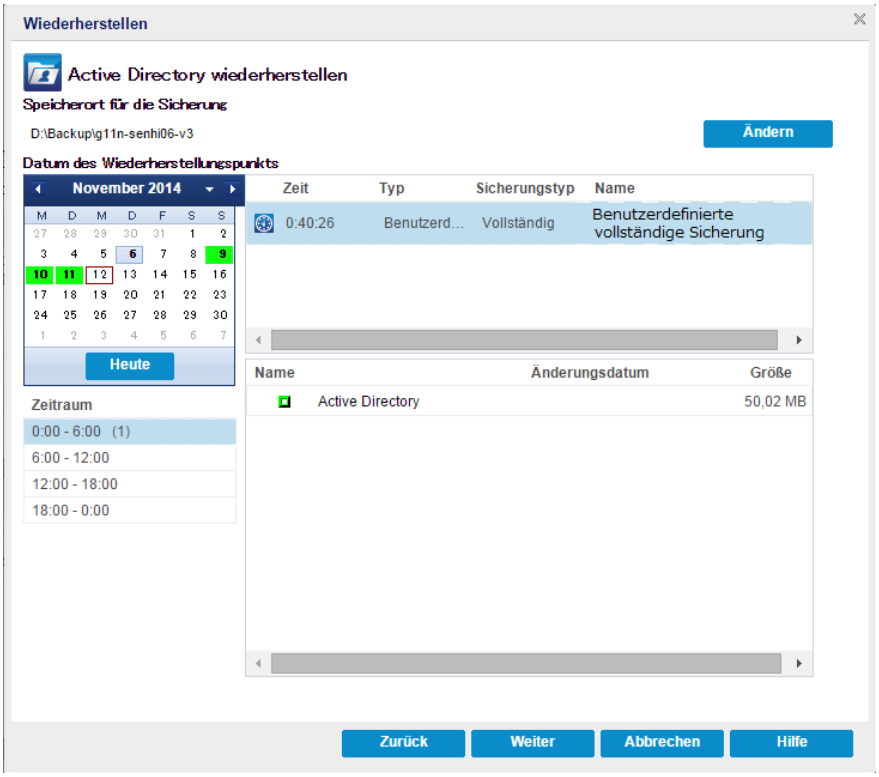
   b. Wählen Sie auf der Startseite **Wiederherstellen** aus.

   Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

2. Klicken Sie im Fenster "Wiederherstellen" auf "Active Directory wiederherstellen".

   Das Dialogfeld "Active Directory wiederherstellen" wird geöffnet.

3. Führen Sie im Fenster "Active Directory wiederherstellen" die folgenden Schritte aus:



a. Wählen Sie im Kalender das Sicherungsdatum für das Active Directory aus, das Sie wiederherstellen möchten.

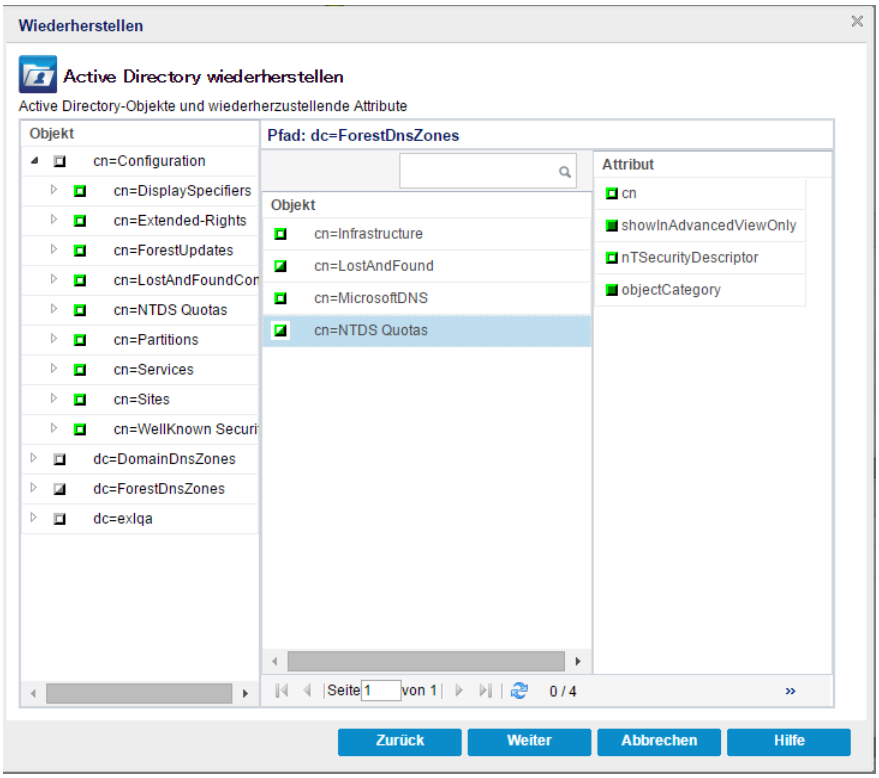
b. Wählen Sie im Zeitbereich die Sicherungszeit aus.

c. Wählen Sie auf dem Bildschirm „Active Directory wiederherstellen“ einen Wiederherstellungspunkt aus, der mit Zeit, Typ, Sicherungstyp und Name gekennzeichnet ist.

d. Wählen Sie im Namensabschnitt eine Active Directory-Sicherungssitzung aus, die wiederhergestellt werden soll.

4. Klicken Sie auf "Weiter".

5. Aktivieren Sie die folgenden Optionen, um die Objekte, den Pfad und die Attribute, die wiederhergestellt werden soll, zu definieren:



a. Wählen Sie aus der Spalte "Objekt" den Namen eines Objekts aus. Die Pfade, die sich auf das ausgewählte Objekt beziehen, werden angezeigt.

b. Wählen Sie einen Pfad aus der Spalte "Pfad" aus. Die Attribute, die sich auf den ausgewählten Pfad beziehen, werden angezeigt.

   Hinweis: Sie können das Symbol "Suchen" verwenden, um nach dem Pfad zu suchen.

c. Wählen Sie von der Spalte "Attribut" ein oder mehrere Attribute aus.

6. Klicken Sie auf "Weiter".

   Das Dialogfeld "Wiederherstellungsoptionen" wird geöffnet.

7. Wählen Sie von den Wiederherstellungsoptionen die folgenden Objekte entsprechend Ihrer Anforderung aus:

   a. Wenn das ausgewählte Objekt nach der Sicherung umbenannt wurde, klicken Sie auf die Option "Mit ursprünglichem Namen der umbenannten Objekte wiederherstellen" um das umbenannte Objekt wiederherzustellen.

      Hinweis: Wenn Sie diese Option nicht auswählen, wird das Objekt nicht wiederhergestellt.

   b. Wenn das ausgewählte Objekt nach der Sicherung in einen anderen Container verschoben wurde, klicken Sie auf die Option "Restore to original loca-

tion of Moved Objects" (Am ursprünglichen Speicherort der verschobenen Objekte wiederherstellen), um das verschobene Objekt wiederherzustellen.

Hinweis: Wenn Sie diese Option nicht auswählen, wird das Objekt nicht wiederhergestellt.

c. Wenn das ausgewählte Objekt nach der Sicherung dauerhaft gelöscht wurde, klicken Sie auf die Option "Restore with the new object ID of Deleted Objects" (Mit neuer Objekt-ID von gelöschten Objekten wiederherstellen), um das dauerhaft gelöschte Objekt wiederherzustellen.

Hinweis: Mit dieser Option können Sie das wiederhergestellte Objekt mit der neuen Objekt-ID beibehalten.

8. Klicken Sie auf "Weiter".

   Das Dialogfeld "Wiederherstellungsübersicht" wird angezeigt

9. Überprüfen Sie die Details, und führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf "Zurück", wenn Sie die Details ändern möchten.
   - Klicken Sie auf "Fertig stellen", um die Wiederherstellung auszuführen.

   Eine Statusmeldung wird angezeigt, die angibt, wann der Wiederherstellungsjob fertiggestellt ist. Wenn die Wiederherstellung nicht erfolgreich ist, zeigen Sie die Protokolle an, und versuchen Sie es erneut.

Überprüfen, ob das Active Directory wiederhergestellt wurde

Nach dem Abschluss der Wiederherstellung können Sie das Hilfsprogramm für Active Directory-Benutzer und -Computer verwenden, um zu überprüfen, dass das Active Directory (Objekt und/oder Attribut) am angegebenen Ziel wiederhergestellt wurde.

Hinweis: Das Active Directory-Hilfsprogramm ist automatisch mit dem Active Directory installiert.

Wiederherstellen von Active Directory-Daten mithilfe des Dienstprogramms "Arcserve UDP Active Directory Objekt Level Restore"

Nachdem Sie Active Directory auf verschiedenen Volumes installiert und eine Sicherung für beide Volumes mit einem Host-basierten agentenlosen Sicherungstask durchgeführt haben, können Sie Objekte und Attribute aus Active Directory granular wiederherstellen. In diesem Szenario wird beschrieben, wie Sie die gesicherten Active Directory-Objekte und -Attribute von den Volumes, die sie beinhalten, wiederherstellen können.

Bevor Sie eine Wiederherstellung durchführen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Das Dienstprogramm "Active Directory Object Level Restore" finden Sie im folgenden Speicherort:

  <Arcserve UDP-Installationspfad>\Engine\BIN\

  Hinweis: Das Tool wir zusammen mit Arcserve UDP Agent installiert.

- Der Wiederherstellungsjob wird vom hostbasierten Sicherungs-Proxy-Rechner ausgeführt.

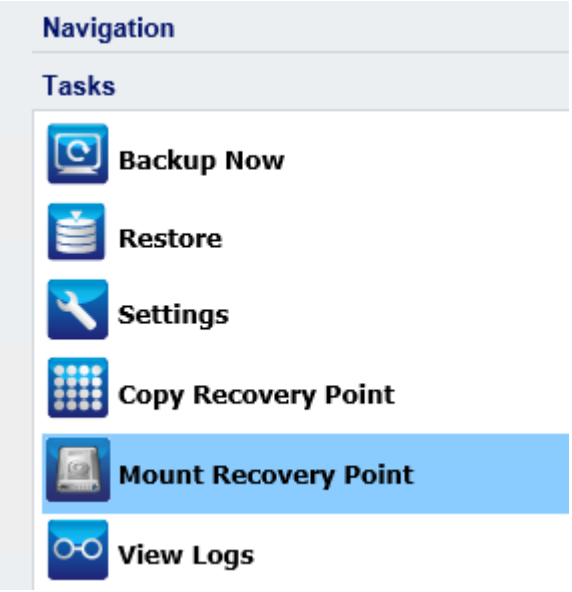
  Hinweis: Wenn der Wiederherstellungsjob auf einem anderen Rechner ausgeführt werden soll, suchen Sie im Sicherungsziel nach dem gewünschten Wiederherstellungspunkt.

- Zum Ausführen des Wiederherstellungsjobs wird der Pfad zur Active Directory-Datenbank (NTDS.dit) ermittelt.

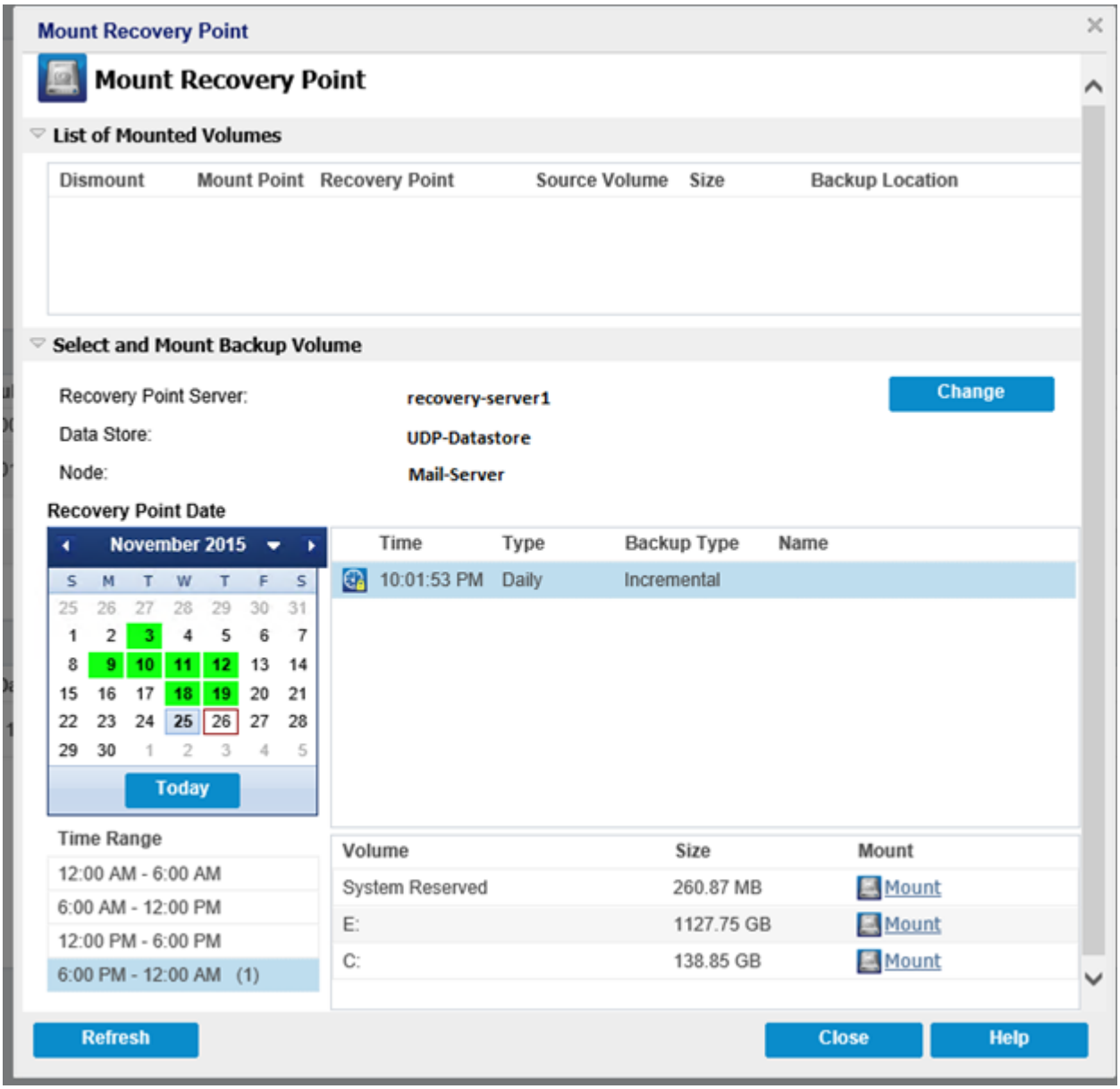
  Hinweis: Standardmäßig lautet der Pfad zu NTDS.dit "C:\Windows\NTDS\NTDS.dit".

Gehen Sie wie folgt vor:

1. Wählen Sie in der Arcserve UDP Agent-Konsole auf dem hostbasierten Sicherungs-Proxy-Rechner den Task Wiederherstellungspunkt laden aus. Das Dialogfeld Wiederherstellungspunkt laden wird geöffnet.

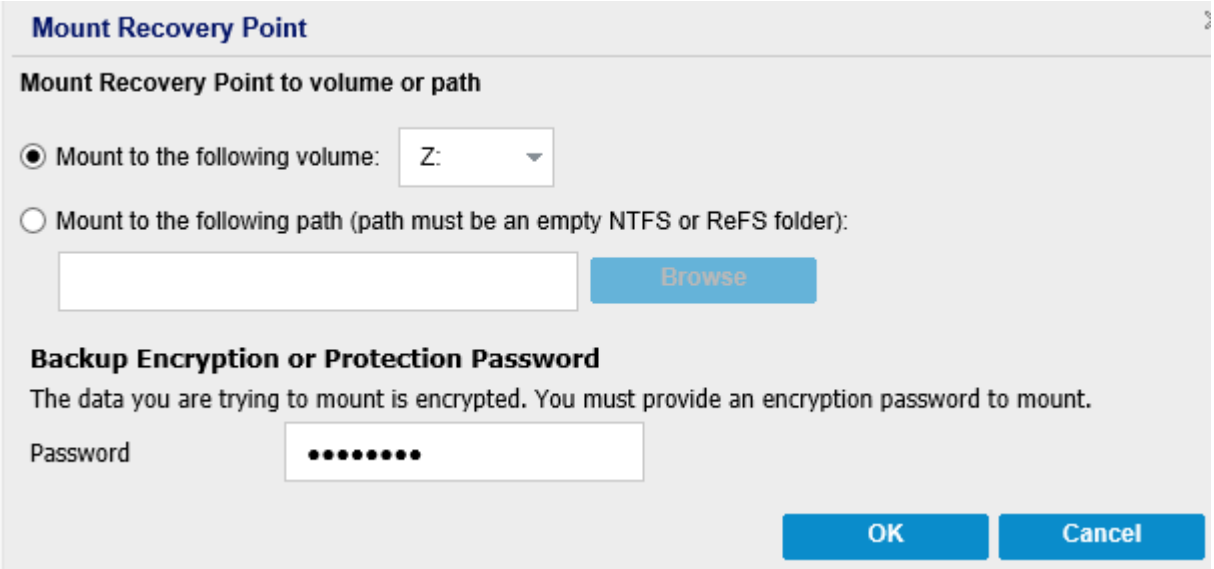


2. Wählen Sie das Datum des Wiederherstellungspunkts aus.
3. Klicken Sie für das Volume, das die Active Directory-Datenbank enthält, auf **Laden**.



Hinweis: Wenn der Server, der den Job ausführt, nicht der HBBU-Proxy ist, klicken Sie auf **Ändern**, um den entsprechenden Recovery Point Server, Datenspeicher und Active Directory-Server auszuwählen.

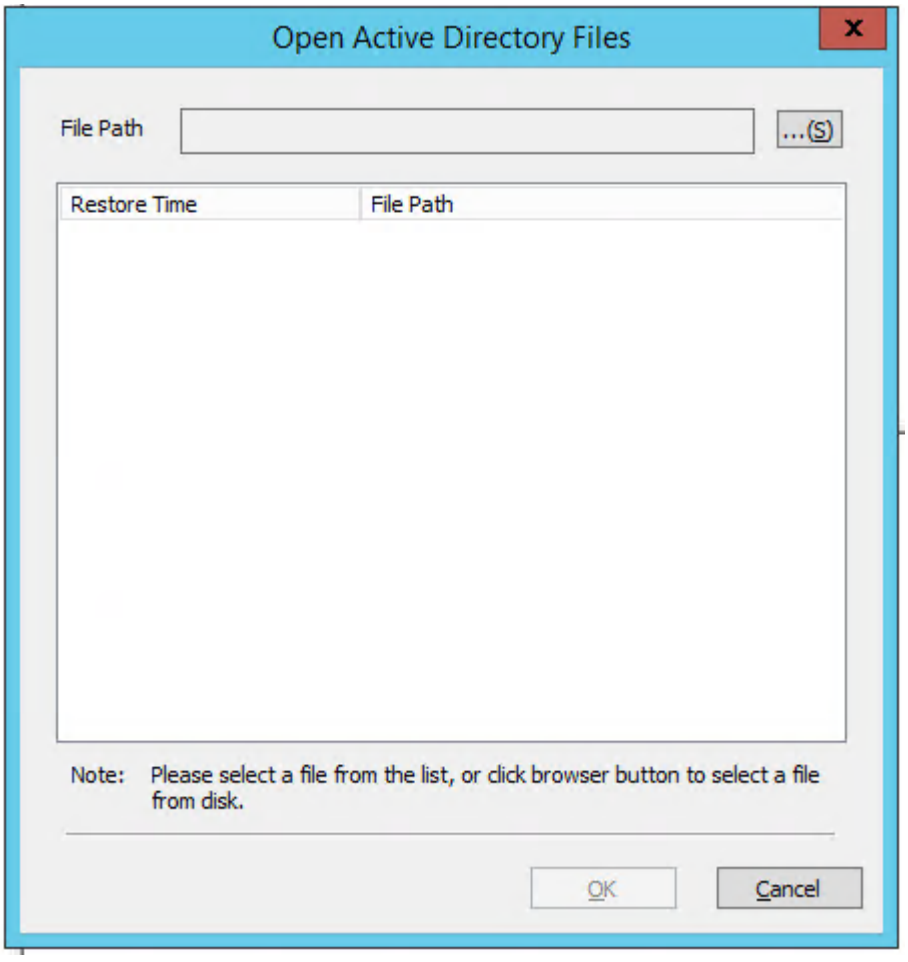
4. Wählen Sie den Laufwerksbuchstaben aus, um das Volume zu laden, und klicken Sie auf **OK**.



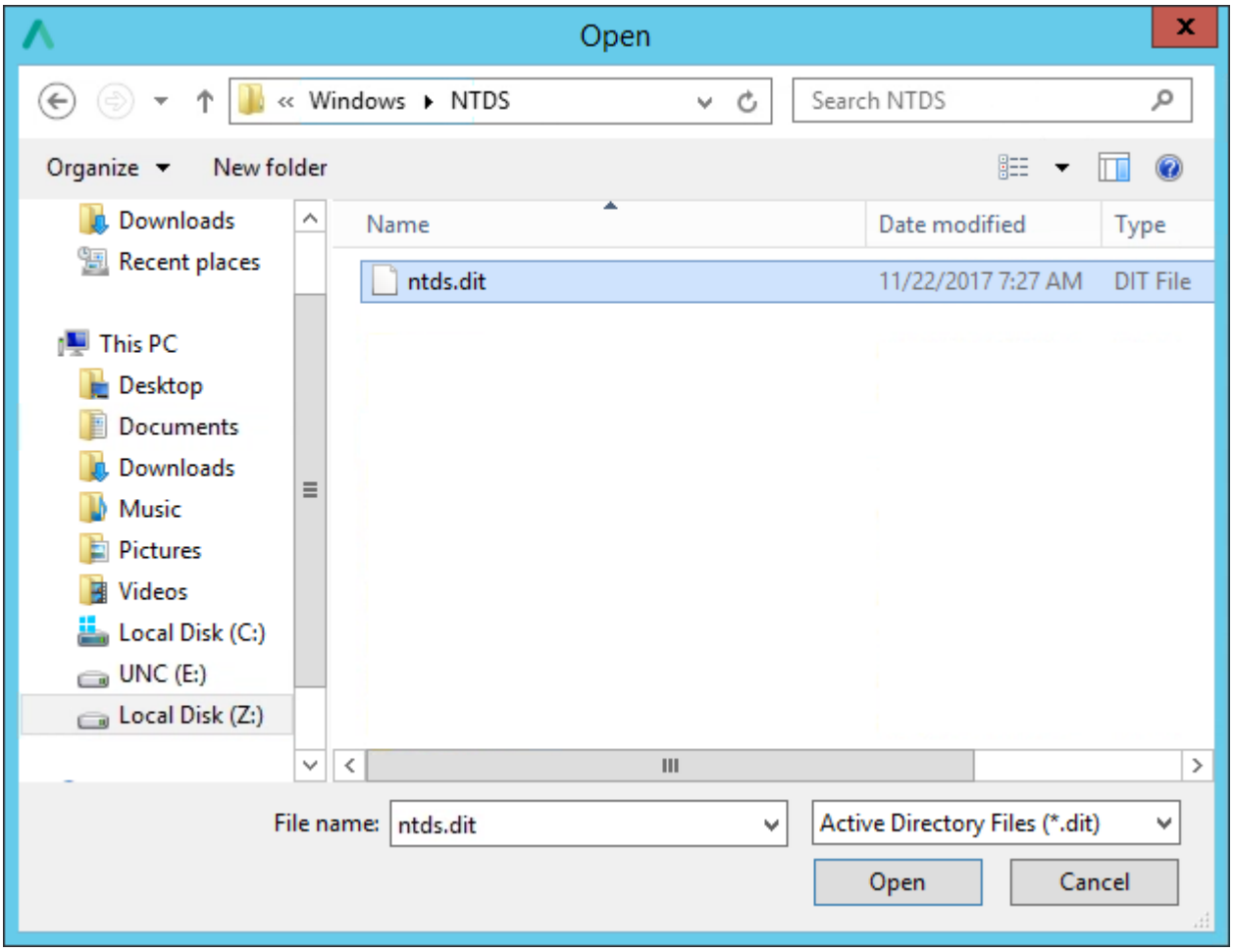
5. Starten Sie das Dienstprogramm "Active Directory Object Level Restore" vom folgendem Speicherort aus:

   <Arcserve UDP-Installationspfad>\Engine\BIN\AD_restore.exe

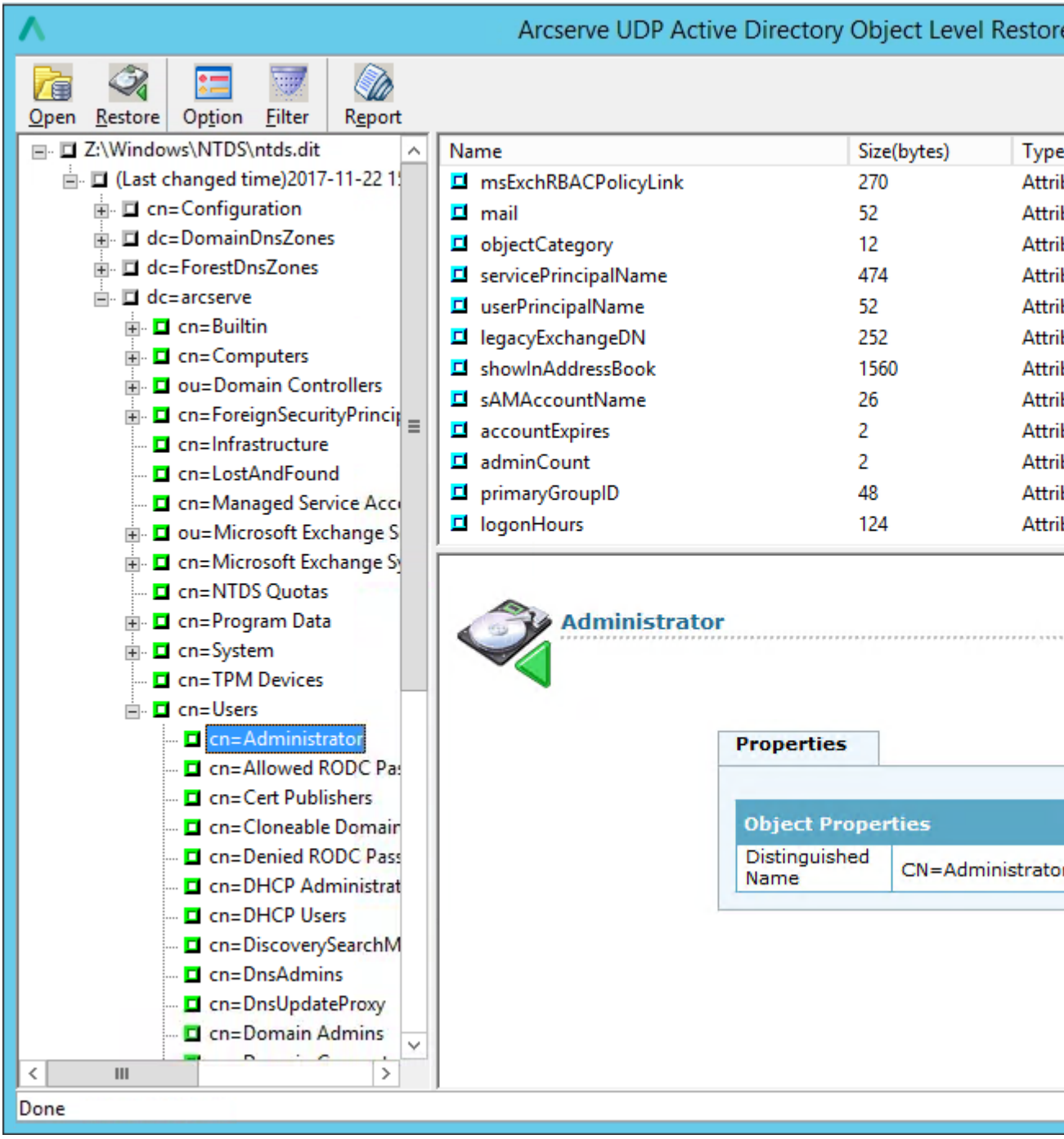
6. Klicken Sie auf **Öffnen**, um das Auswahlfenster zu öffnen.



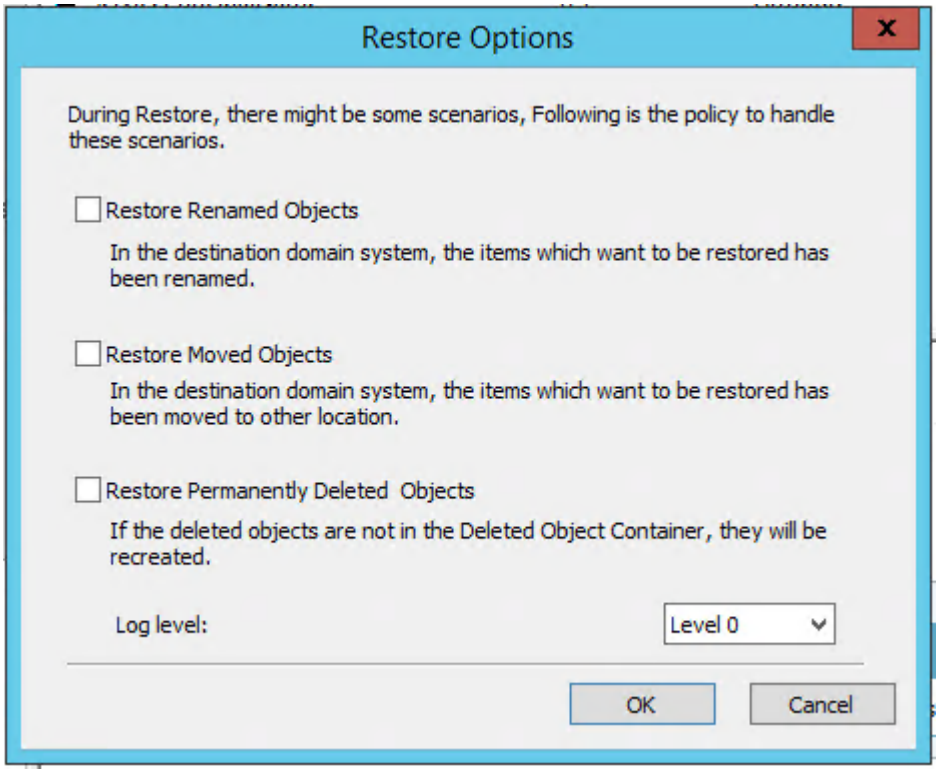
7. Klicken Sie auf das Symbol ...(S), und durchsuchen Sie die Active Directory-Datenbank (NTDS.dit) auf dem bereitgestellten Wiederherstellungspunkt, klicken Sie auf **Öffnen**, und klicken Sie dann auf **OK**.



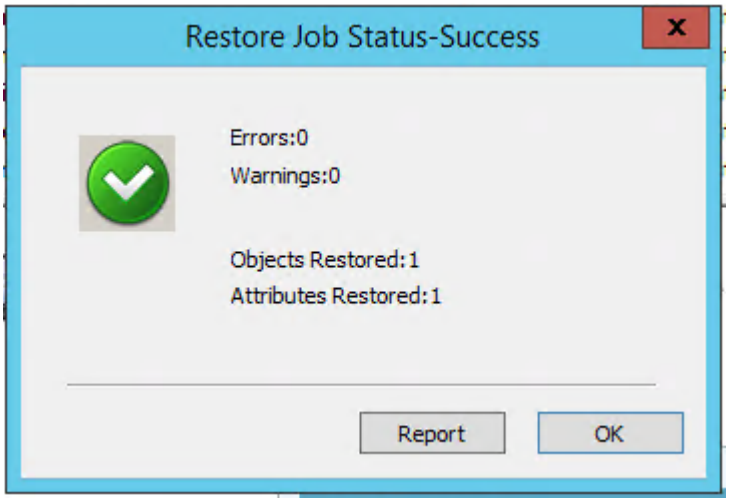
8. Suchen Sie nach den Active Directory-Objekten oder -Attributen, die Sie wiederherstellen möchten, und wählen Sie diese aus.



9. Klicken Sie auf **Optionen**, um das Standardverhalten bei Bedarf zu ändern.



10. Wenn Sie fertig sind, klicken Sie auf **OK**, um den Wiederherstellungsjob auszuführen.
11. Nach Abschluss des Wiederherstellungsjobs wird ein Ergebnisfenster angezeigt. Klicken Sie auf **Bericht**, wenn Sie die Details anzeigen möchten, oder klicken Sie zum Schließen auf **OK**.



Hinweise:

- Standardmäßig verwendet das Dienstprogramm den aktuellen, bei Windows angemeldeten Benutzer zum Herstellen der Verbindung.

- Wenn ein Fehler gemeldet wird, sollten Sie sich mit einem Konto mit Domänen-Administratorrechten beim Computer anmelden, um die Wiederherstellung durchzuführen.

12. Wenn der Wiederherstellungsjob abgeschlossen ist, entladen Sie das Volume, das für die Wiederherstellung verwendet wurde.
13. Um das Volume zu entladen, klicken Sie in der Arcserve UDP Agent-Konsole auf dem hostbasierten Sicherungs-Rechner auf **Wiederherstellungspunkt laden**, und klicken Sie dann auf **Entladen**.

Wiederherstellen von Microsoft Office 365-Daten

In diesem Abschnitt werden die folgenden Themen behandelt:

Wiederherstellen von Exchange Online-Postfachdaten

Sie können Exchange Online-Postfachdaten (E-Mails, Kalender, Kontakte, Notizen, Aufgaben usw.) über einen beliebigen Computer aus der Microsoft-Cloud wiederherstellen. Sie können Daten von einem Wiederherstellungspunkt am ursprünglichen Speicherort oder an einem alternativen Speicherort wiederherstellen.

Führen Sie die folgenden Aufgaben aus, um Exchange Online-Postfachdaten wiederherzustellen:

1. Auswählen der wiederherzustellenden Exchange Online-Postfachelemente
2. Definieren der Wiederherstellungsoptionen
3. Wiederherstellbare Elemente wiederherstellen
4. Wiederherstellen des Inhalts des Wiederherstellungspunkts
5. Überprüfen, ob der Inhalt wiederhergestellt wurde

Auswählen der wiederherzustellenden Exchange Online-E-Mail-Elemente

Sie können Exchange Online-E-Mail-Daten von einem Wiederherstellungspunkt aus wiederherstellen. Wenn Sie ein Wiederherstellungsdatum auswählen und dann die Uhrzeit angeben, werden alle zugeordneten Wiederherstellungspunkte für diesen Zeitraum angezeigt. Sie können die Inhalte (einschließlich Anwendungen) für die Wiederherstellung suchen und auswählen.

Gehen Sie wie folgt vor:

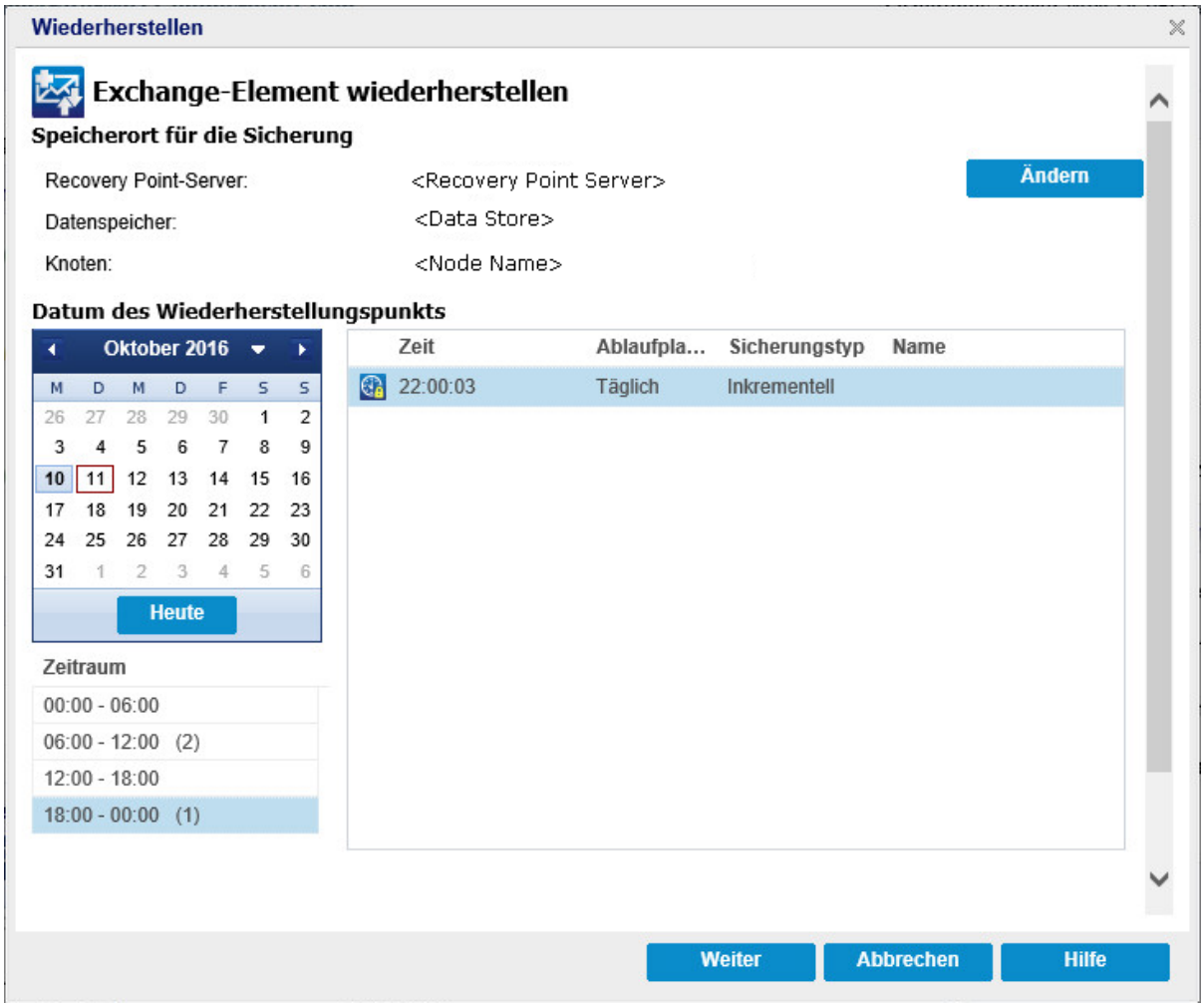
1. Melden Sie sich bei Arcserve UDP an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

   Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.
4. Wählen Sie im mittleren Fensterbereich den Exchange Online-Knoten aus, und klicken Sie dann auf **Aktionen**.
5. Klicken Sie im Drop-down-Menü **Aktionen** auf Wiederherstellen.

   Das Dialogfeld Exchange-Element wiederherstellen wird geöffnet.

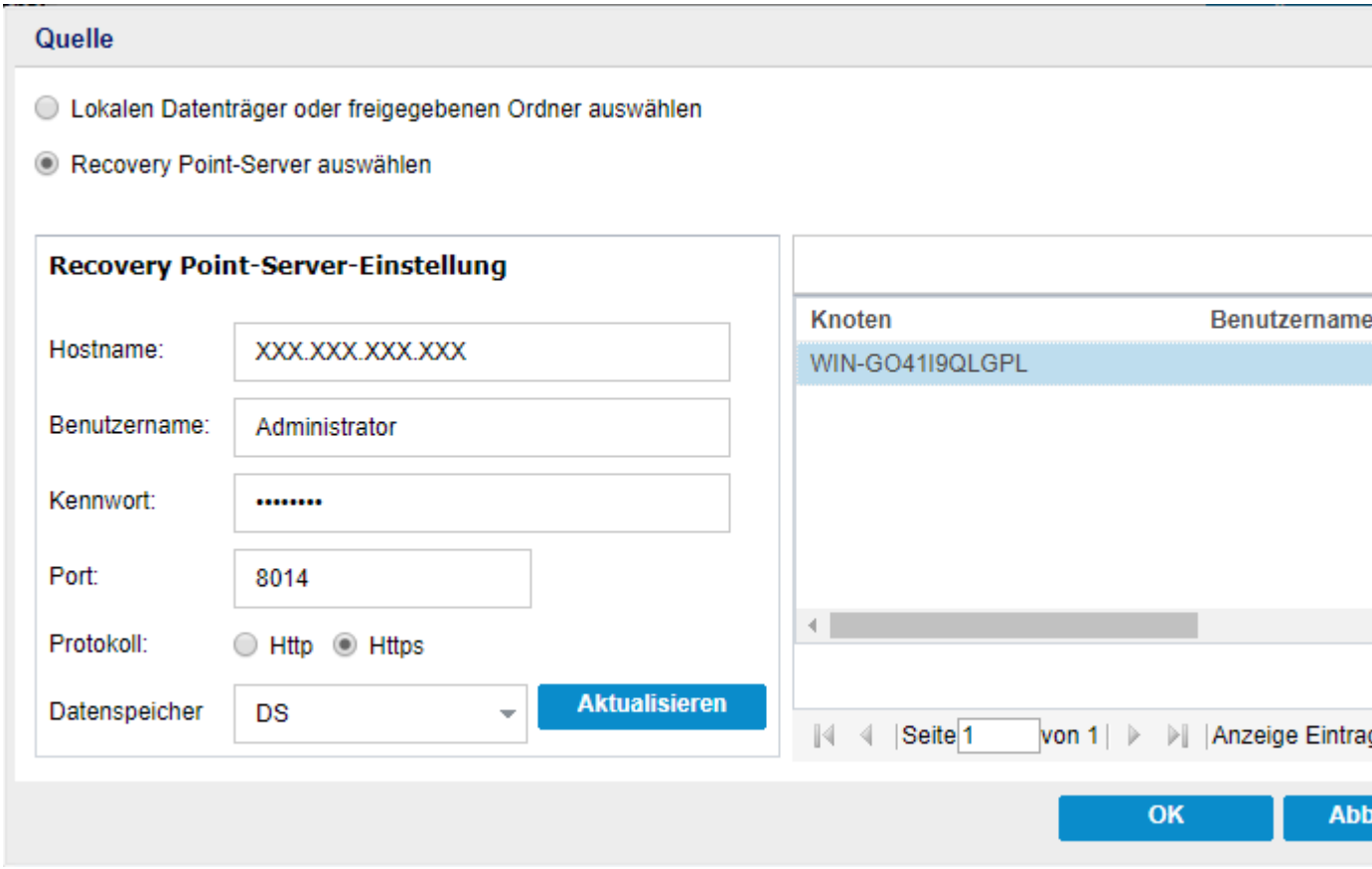
   Hinweis: Sie werden automatisch in den Agent-Knoten eingeloggt und das Dialogfeld Exchange-Element wiederherstellen wird geöffnet.

   Die Details zum Recovery Point Server werden im Sicherungsspeicherort angezeigt.



6. (Optional) Klicken Sie auf **Ändern**, wenn Sie den Speicherort für die Sicherung ändern möchten.

   Das Dialogfeld Quelle wird geöffnet. Sie können den Sicherungsspeicherort in diesem Dialogfeld auswählen.



Hinweis: Wenn Sie dem Plan einen Task "Kopie auf Band" hinzufügen und nun den Wiederherstellungspunkt "Kopie auf Band" wiederherstellen möchten, wählen Sie den Wiederherstellungspunkt aus der Sicherung auf Kopie auf Band aus. Weitere Informationen finden Sie unter Durchsuchen der Kopie auf Band nach Wiederherstellungspunkten.

7. Um die Quelle anzugeben, wählen Sie eine der folgenden Optionen aus, und klicken Sie dann auf **OK**.

   Lokalen Datenträger oder freigegebenen Ordner auswählen

   Hinweis: In Arcserve UDP empfehlen wir nicht die Auswahl der Option **Lokalen Datenträger oder freigegebenen Ordner auswählen**.

   Auswählen des Recovery Point-Servers

   a. Geben Sie die Details für die Einstellungen des Recovery Point Servers an, und klicken Sie dann auf **Aktualisieren**.

      Alle Agenten werden in der Spalte "Data Protection Agent" im Dialogfeld Quelle aufgelistet.

   b. Wählen Sie den Agenten in der angezeigten Liste aus, und klicken Sie auf **OK**.

Die Wiederherstellungspunkte werden im Dialogfeld Exchange-Element wiederherstellen aufgelistet.

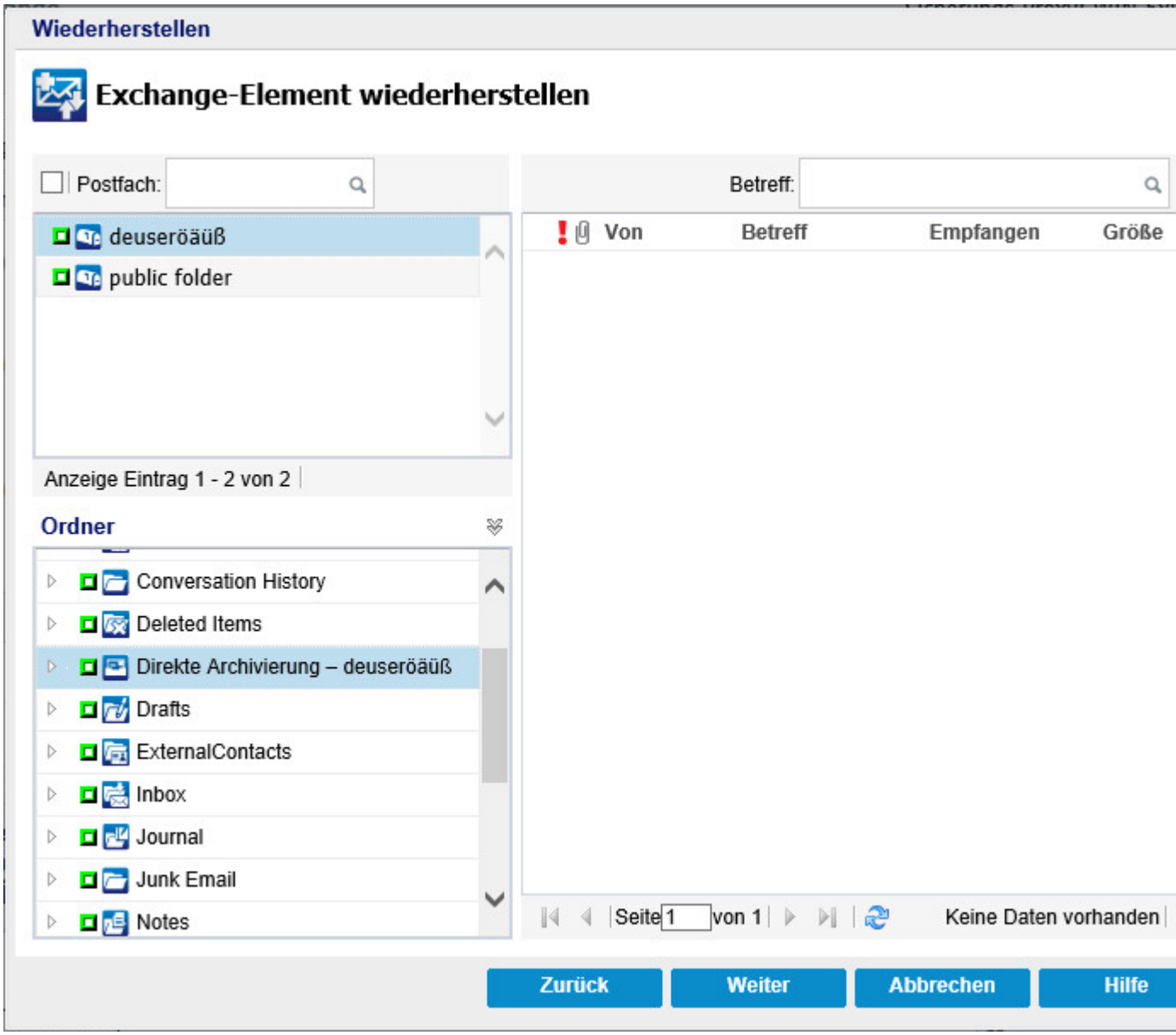
Hinweis: Vom Wiederherstellungspunkt Ordner aus sehen Sie möglicherweise viele Ordner mit demselben Namen zusammen mit den Exchange Online-Knoten. Dies geschieht, weil die Knoten-GUID geändert wird und ein neuer Wiederherstellungspunkt-Ordner erstellt wird, wenn Sie einen Knoten löschen und wieder zum Prüfplan hinzufügen.

8. Wählen Sie das Kalenderdatum des wiederherzustellenden Sicherungs-Images aus, und klicken Sie dann auf **Weiter**.

   Alle Daten, die Wiederherstellungspunkte für die angegebene Sicherungsquelle enthalten, werden grün hervorgehoben.

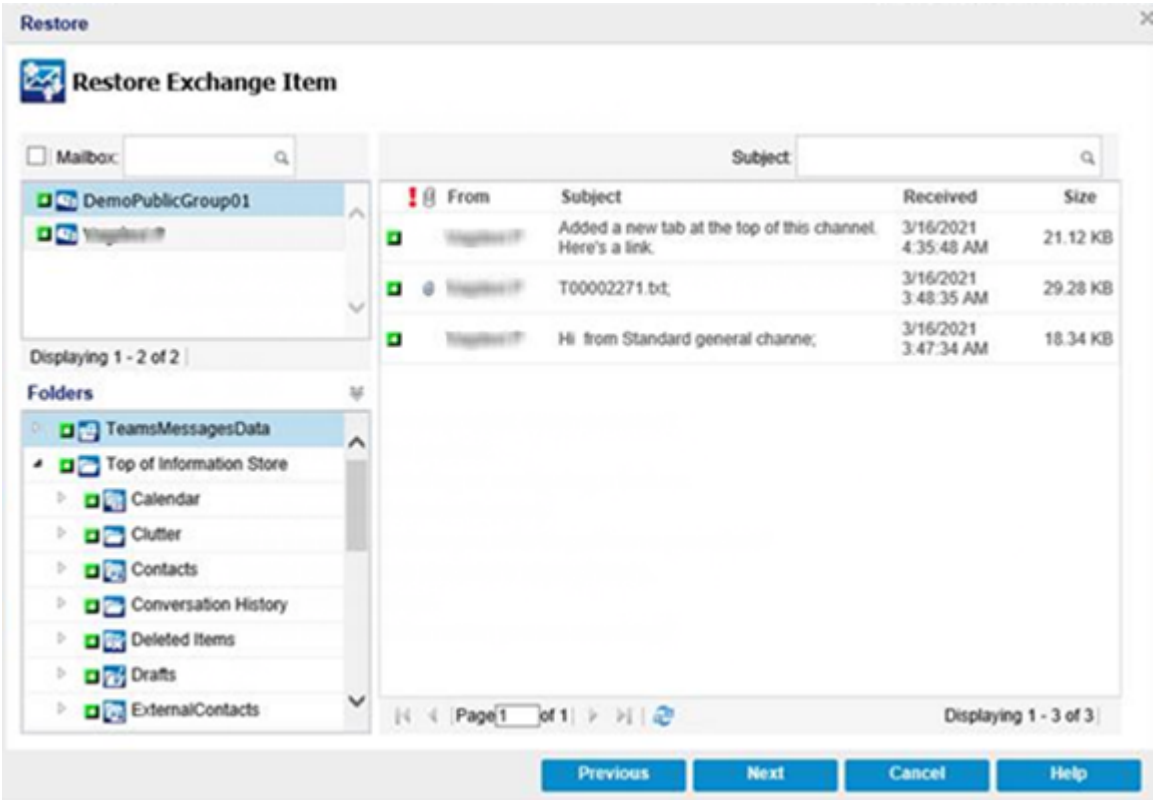
   Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp (vollständige Sicherung, Zuwachssicherung oder Überprüfungssicherung) und der Name der Sicherung angezeigt.

9. Wählen Sie im Fenster Postfach das Postfach aus, das Sie wiederherstellen möchten.



Alle E-Mail-Elemente in Verbindung mit dem Postfach werden im Fensterbereich Ordner angezeigt.

Hinweis: Bei der Sicherung von Office 365 Exchange Online-Gruppen unterscheidet sich die Ordnerstruktur für das Gruppenpostfach vom Benutzerpostfach. Die Gruppenpostfachordner werden oben im Ordner "Informationsspeicher" angezeigt. Wenn der Benutzer beispielsweise AD-Gruppenpostfächer/Verteilerlisten sichert, werden alle gesicherten Ordner unter "Oben im Informationsspeicher" angezeigt.



10. Wählen Sie die entsprechenden E-Mail-Elemente oder -Ordner (einschließlich des gesamten Postfachs, E-Mails, Kalendern, Kontakten, Notizen, Aufgaben usw.) aus, die Sie aus Ordner wiederherstellen möchten, und klicken Sie dann auf **Weiter**.

    Hinweise:

    - Sie können den gesamten Inhalt oder Teile des Inhalts des wiederherzustellenden Exchange-Objekts auswählen. Um Teile des Inhalts auszuwählen, erweitern Sie das Objekt, und klicken Sie auf das Kontrollkästchen des Inhalts.
    - Sie können mehrere wiederherzustellende Exchange-Objekte auswählen.

    Das Dialogfeld Wiederherstellungsoptionen wird geöffnet.

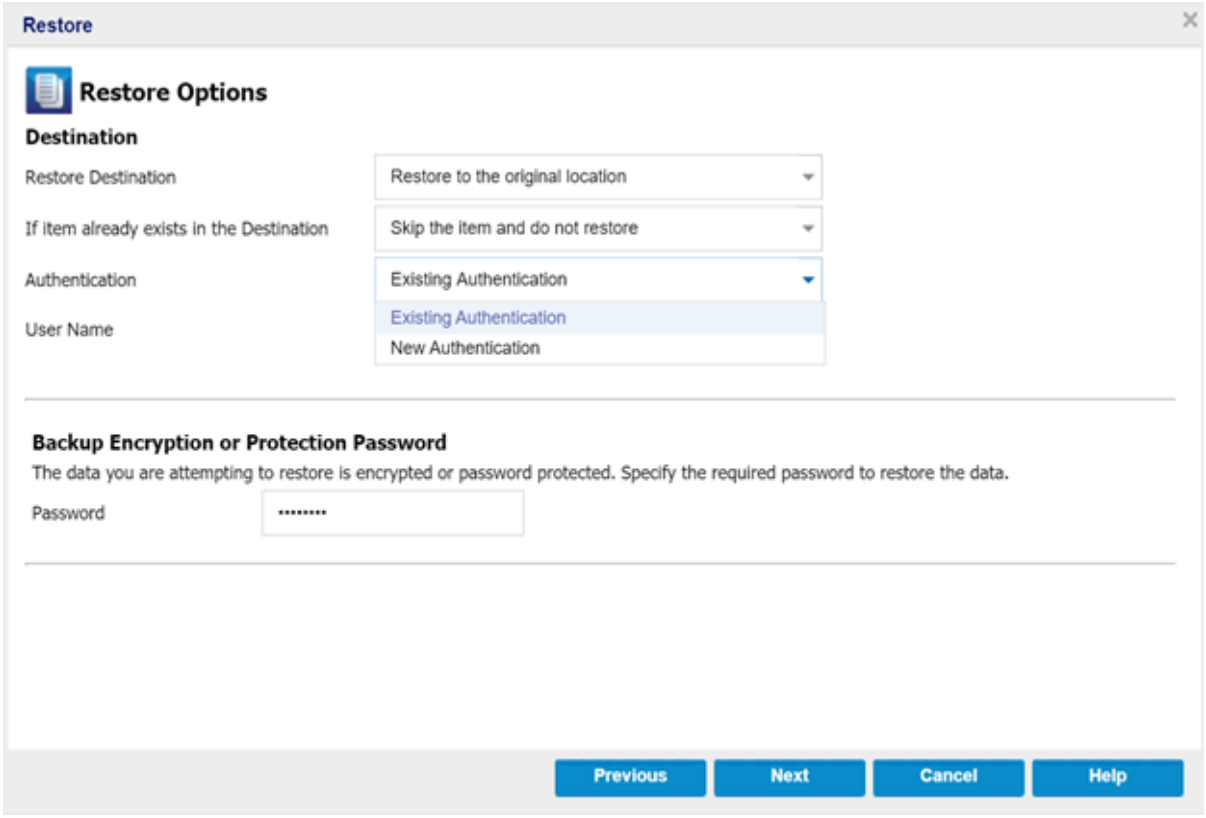
    Die Exchange Online-E-Mail-Elemente, die wiederhergestellt werden sollen, sind ausgewählt. Nun können Sie die Wiederherstellungsoptionen definieren.

Definieren der Wiederherstellungsoptionen

Nachdem Sie die wiederherzustellenden Exchange Online-Informationen angegeben haben, legen Sie die Wiederherstellungsoptionen für die ausgewählten Inhalte fest.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Wiederherstellungsoptionen** das Wiederherstellungsziel aus.



Es sind folgende Zieloptionen verfügbar:

Am ursprünglichen Speicherort wiederherstellen

Stellt die E-Mail-Daten am selben Speicherort wieder her, an dem Sie eine Sicherung vorgenommen haben.

Hinweise:

- Wenn Sie ein E-Mail-Element am ursprünglichen Speicherort unter Verwendung der Überschreibungsoption zweimal wiederherstellen, wird nach der zweiten Wiederherstellung das erste wiederhergestellte E-Mail-Element nicht überschrieben. Dadurch werden die zwei ähnliche

E-Mail-Objekte am ursprünglichen Speicherort angezeigt.

- Wenn Sie E-Mail-Nachrichten am ursprünglichen Speicherort mit der Option "Überspringen" wiederherstellen, und im ursprünglichen Ordner bereits ein Element vorhanden ist, das dem wiederhergestellten ähnelt, zeigt der Sicherungsjob das Ergebnis "Unvollständig" an.

An einem anderen Speicherort wiederherstellen

Stellt die E-Mail-Daten in einem anderen Postfach oder einem anderen Ordner im ursprüngliche Postfach wieder her. Wenn Sie diese Option auswählen, können Sie das Ziel auswählen.

2. Geben Sie eine der folgenden Optionen aus der Drop-down-Liste **Wenn das Element auf dem Ziel bereits vorhanden ist** an:

Objekt überspringen und nicht wiederherstellen

Elemente werden übersprungen und nicht wiederhergestellt.

Standard: Elemente werden übersprungen und nicht wiederhergestellt.

Das Element im Ziel überschreiben

Das Element im Ziel wird überschrieben.

Hinweis: Die Drop-down-Liste **Wenn das Element auf dem Ziel bereits vorhanden ist** ist verfügbar, wenn Sie die Option **Am ursprünglichen Speicherort wiederherstellen** in der Drop-down-Liste **Wiederherstellungsziel** auswählen.

Authentifizierung

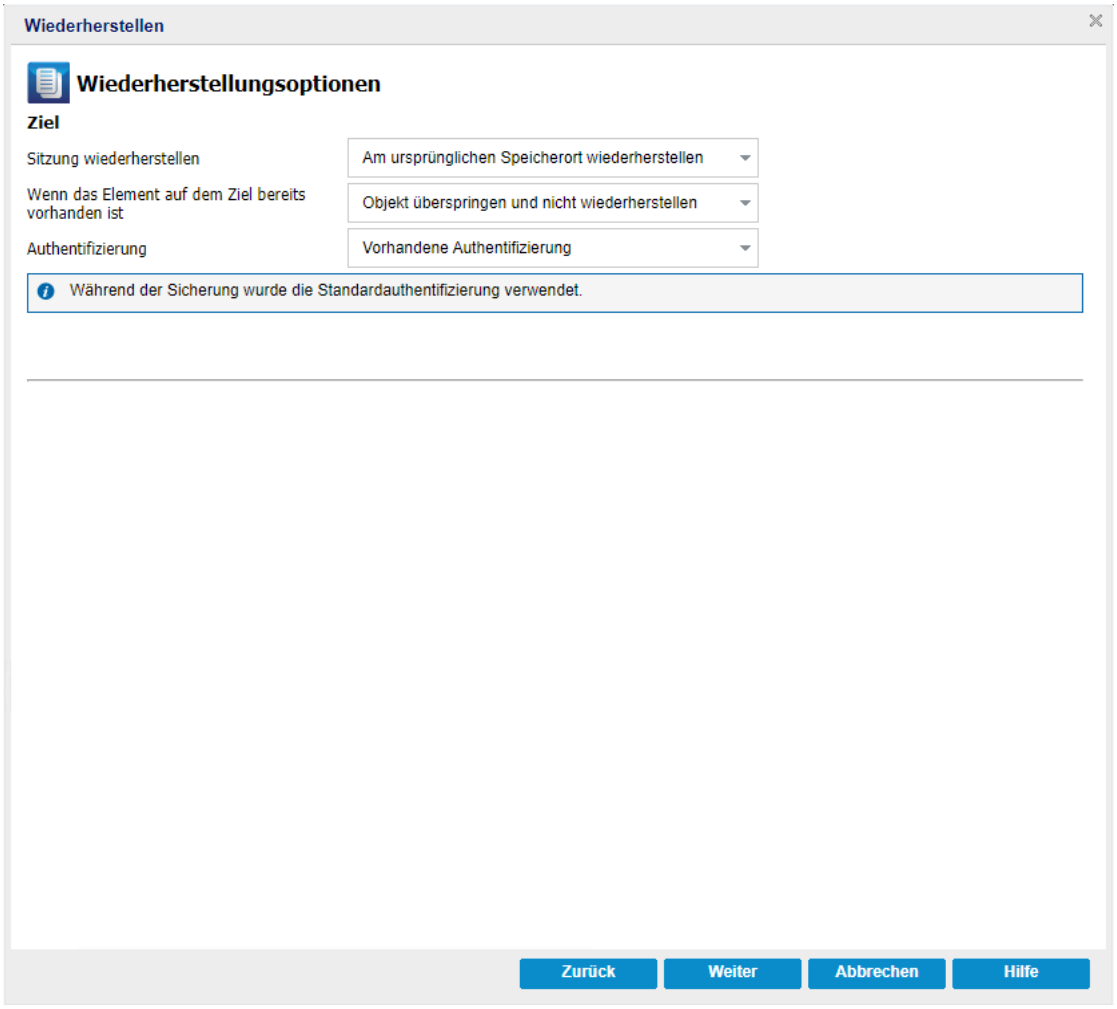
Validiert und identifiziert das Benutzerkonto. Wählen Sie eine der folgenden Optionen:

- **Vorhandene Authentifizierung**

  Wenn Sie "Vorhandene Authentifizierung" auswählen, wird der Authentifizierungstyp verwendet, der während der Knotenerstellung ausgewählt wurde.

  - Wenn es sich bei der Knotenauthentifizierung um die Standardauthentifizierung handelt, werden Parameter wie Benutzername, Kennwort und Sicherungsverschlüsselung oder Schutzkennwort [falls verschlüsselt] automatisch geladen, um mit der Wiederherstellung fortzufahren.
  - Wenn es sich bei der Knotenauthentifizierung um die moderne Authentifizierung handelt, werden Parameter wie Benutzername

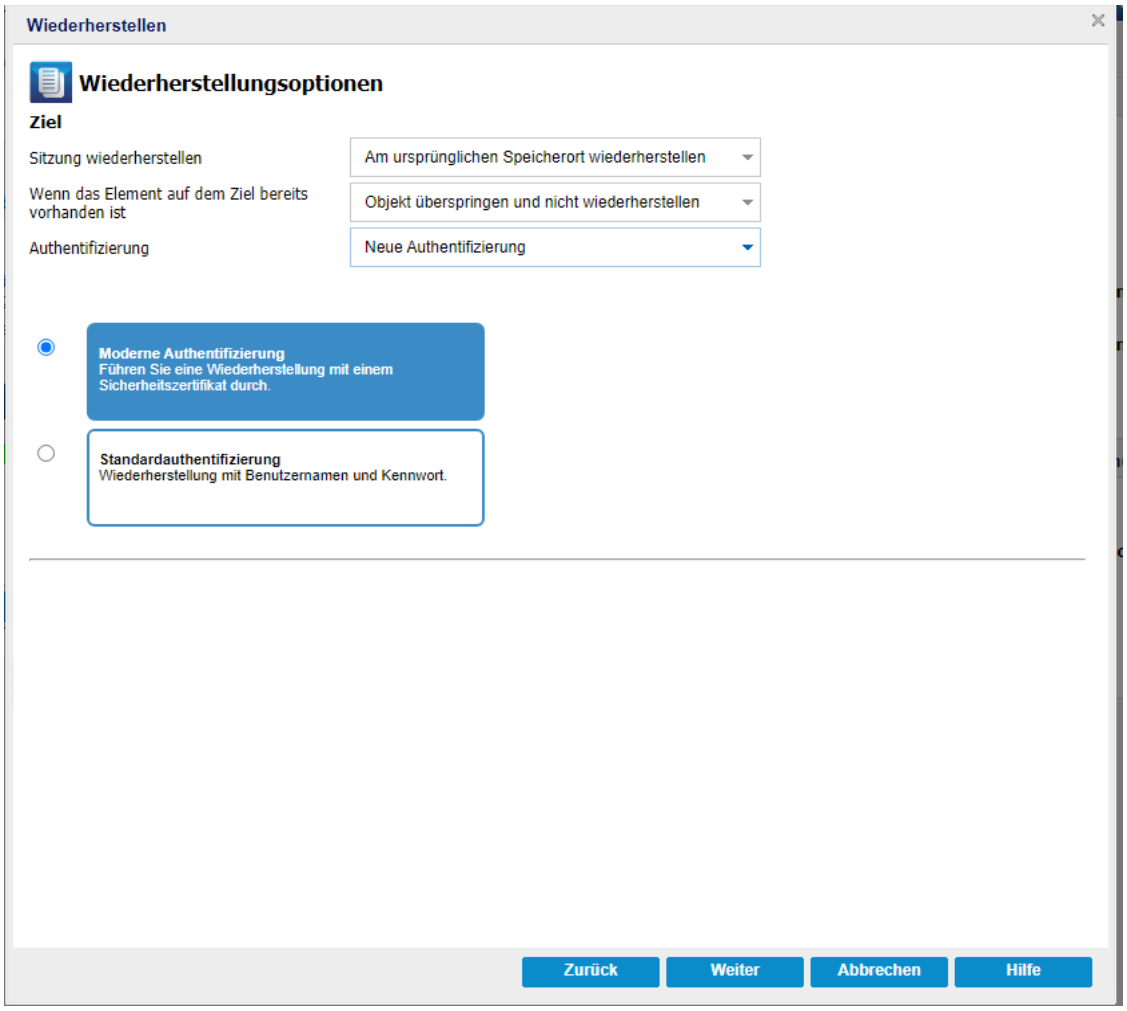
und Sicherungsverschlüsselung oder Schutzkennwort [falls verschlüsselt] automatisch geladen, um mit der Wiederherstellung fortzufahren.



- **Neue Authentifizierung**

  Während der Wiederherstellung können Sie eine der folgenden Optionen auswählen, um den Authentifizierungstyp zu ändern:

  - Moderne Authentifizierung
  - Standardauthentifizierung



3. Gehen Sie folgendermaßen vor, um die Authentifizierung anzuwenden:

   Moderne Authentifizierung

   Bei der modernen Authentifizierung können Sie eine Wiederherstellung mithilfe eines Sicherheitszertifikats ausführen.

   Sicherheitszertifikat verwenden

   Hinweis: Standardmäßig wählt der Sicherungsplan die Option **Sicherheitszertifikat verwenden** für die moderne Authentifizierung aus.

   Gehen Sie wie folgt vor:

   a. Informationen zur Authentifizierung mithilfe eines selbstsignierten Zertifikats finden Sie unter Herunterladen des Zertifikats von UDP und Hochladen in Azure

   b. Geben Sie die Anwendungs-ID und den Benutzernamen ein.

c. Um die erforderlichen Rollen und Berechtigungen anzuwenden, aktivieren Sie das Kontrollkästchen **Ermöglichen Sie Arcserve UDP, die erforderlichen Azure-Rollen und -Berechtigungen für diese Anwendung festzulegen**, und klicken Sie dann auf **Weiter**.

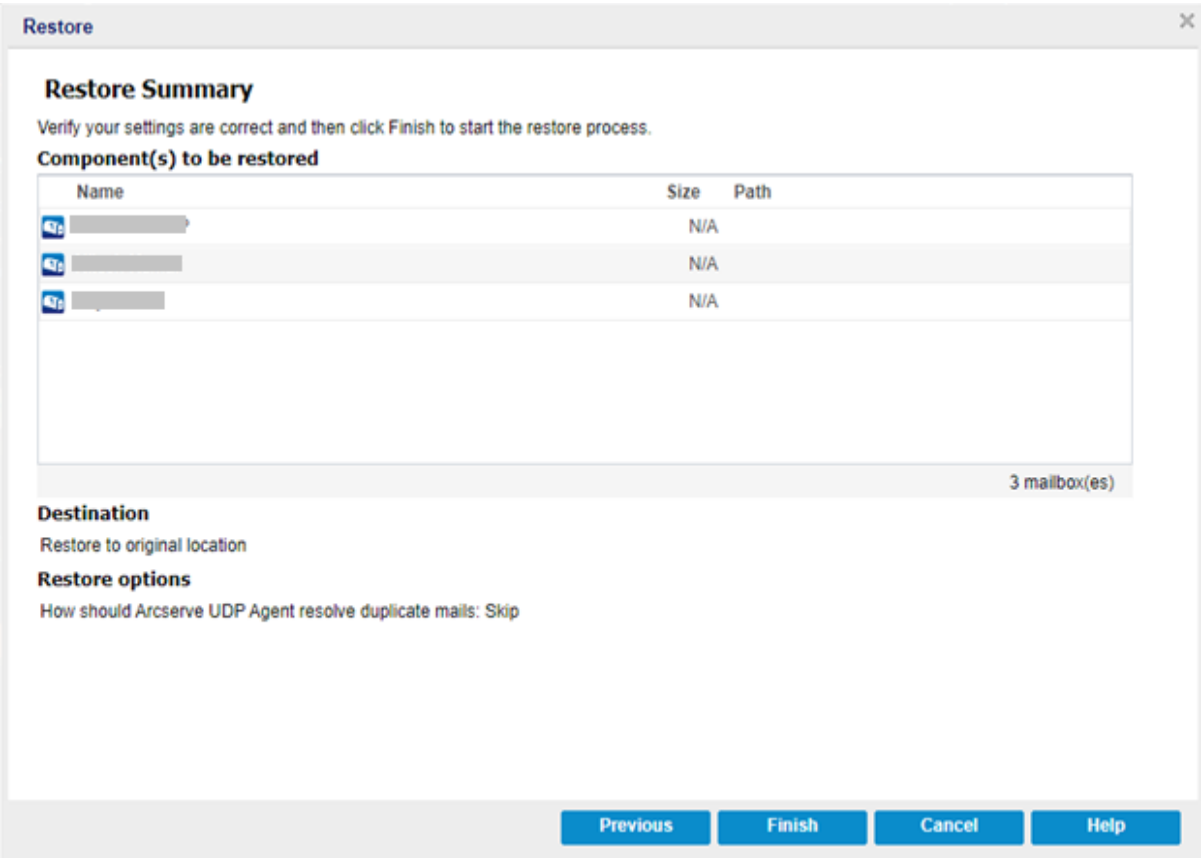
Standardauthentifizierung

Um bei Verwendung der Standardauthentifizierung mit der Wiederherstellung fortzufahren, geben Sie Benutzername und Kennwort ein.

Hinweis: Diese Option schlägt fehl, wenn Sie die moderne Authentifizierung für den Mandanten oder das Konto aktiviert haben.

4. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsübersicht** wird geöffnet.



5. Überprüfen Sie die Einstellungen im Fenster "Wiederherstellungs-Übersicht", und klicken Sie dann auf **Fertig stellen**.

Die Wiederherstellungsoptionen für die Wiederherstellung von Exchange Online-Informationen sind festgelegt.

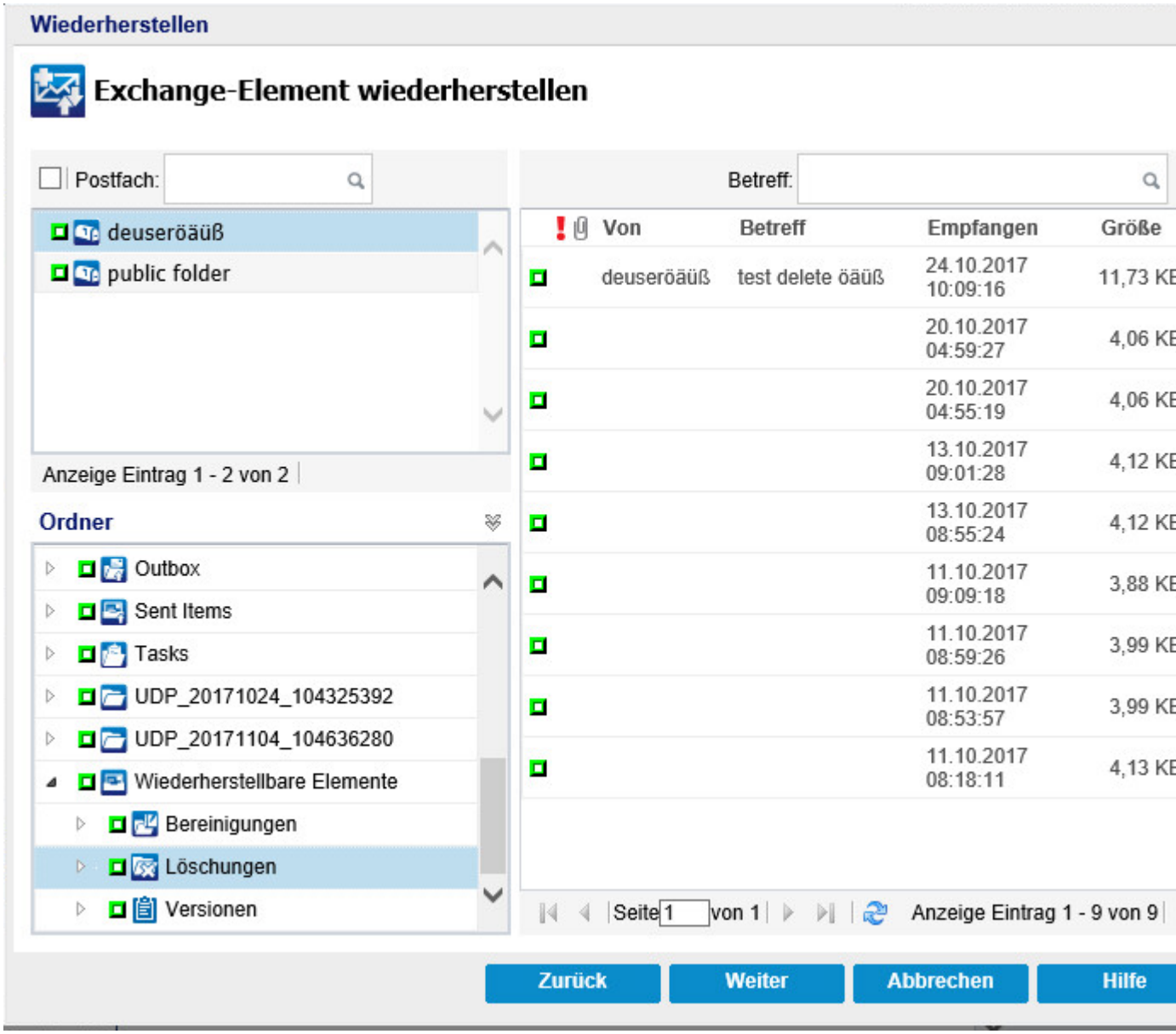
Wiederherstellbare Elemente wiederherstellen

Sie können wiederherstellbare Elemente aus dem Postfach wiederherstellen, das die In-Place-Hold- und Litigation-Hold-Funktion ermöglicht – vom Exchange Online-Knoten-UI bis zum Durchsuchen einer Backup-Sitzung. Informationen zur Aktivierung dieser Funktion finden Sie unter Angeben der Quelle.

Nachdem Sie die Funktion aktiviert haben, können Sie mit dem Wiederherstellungsassistenten wiederherstellbare Elemente wiederherstellen.

Gehen Sie wie folgt vor:

1. Im Dialogfeld **Exchange-Element wiederherstellen** wählen Sie die erforderlichen Ordner unter **Wiederherstellbare Elemente** aus und klicken anschließend auf **Weiter**.



Der Bildschirm der Wiederherstellungsoption wird angezeigt.

2. Führen Sie auf dem Bildschirm der Wiederherstellungsoption die folgenden Schritte aus und klicken Sie auf **Weiter**:

   - Wählen Sie ein Ziel für die Wiederherstellung aus.
   - Überspringen oder überschrieben Sie, wenn das Element bereits im Ziel vorhanden ist.

     Sie können eine originale oder alternative Wiederherstellung durchführen.

     Originale Wiederherstellung

     Die Elemente unter „Wiederherstellbare Elemente“ werden im Ordner *UDP_RecoverableItems_yyyyMMdd_HHmmssfff* wiederhergestellt, der

im Zielpostfach erstellt wird. Die Wiederherstellungsoptionen „Überspringen“ und „Überschreiben“ sind nicht für diese Elemente anwendbar.

Alternative Wiederherstellung

Bei einem Benutzerpostfach werden ausgewählte Elemente in einem Zielverzeichnis mit einem Ordner mit einzigartigem Zeitstempel wiederhergestellt, beispielsweise mit dem Namen */restore_yyyyMMdd-mmssff*.

- Geben Sie die Benutzer-ID und das Passwort des Ziels an, in dem Sie die Wiederherstellung durchführen möchten.

Die ausgewählten wiederherstellbaren Elemente werden wiederhergestellt.

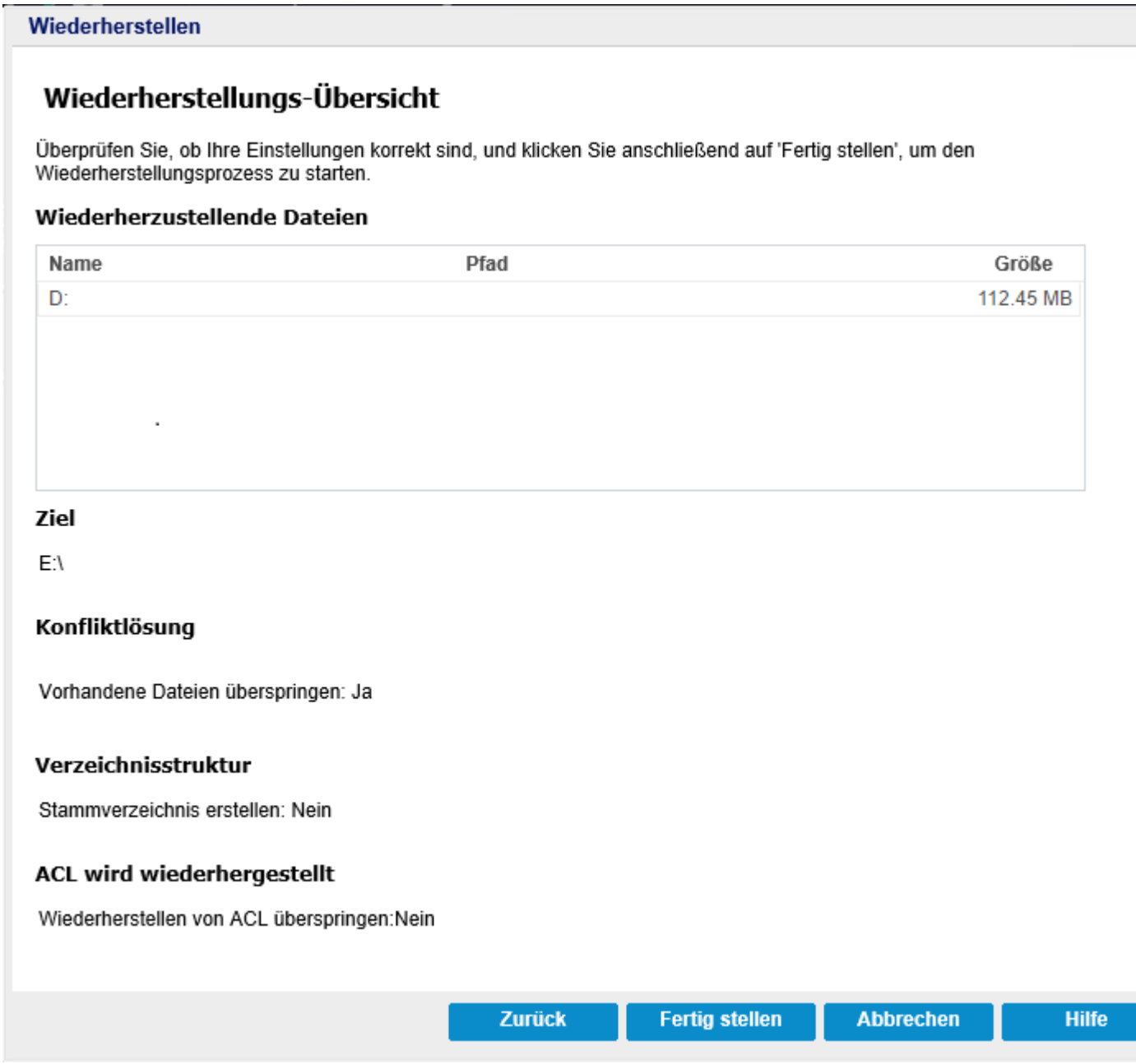
Der Wiederherstellungspunktinhalt wird wiederhergestellt.

Wiederherstellen des Inhalts des Wiederherstellungspunkts

Nachdem Sie die Wiederherstellungsoptionen definiert haben, überprüfen Sie, dass Ihre Einstellungen korrekt sind, und bestätigen Sie den Wiederherstellungsprozess. Die **Wiederherstellungs-Übersicht** ist hilfreich, um sämtliche Wiederherstellungsoptionen, die Sie festgelegt haben, zu überprüfen und bei Bedarf zu ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Informationen im Dialogfeld **Wiederherstellungs-Übersicht**, um die Richtigkeit aller Wiederherstellungsoptionen und Einstellungen sicherzustellen.



- Wenn die Übersichtsinformationen Fehler enthalten, klicken Sie auf **Zurück**, und ändern Sie die inkorrekten Einstellungen im entsprechenden Dialogfeld.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsjob zu starten.

Der Wiederherstellungspunktinhalt wird wiederhergestellt.

Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen Sie nach dem Abschluss der Wiederherstellung, dass der Inhalt auf dem angegebenen Ziel wiederhergestellt wurde.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Zielpostfach an.
2. Überprüfen Sie das Postfachelement, das Sie wiederhergestellt haben.
3. Überprüfen die wiederhergestellten Inhalte.

   Der wiederhergestellte Inhalt wurde erfolgreich überprüft.

So stellen Sie SharePoint Online-Websitesammlungsdaten wieder her

Sie können SharePoint Online-Listen/-Bibliotheken oder -Listenelemente auf der Website oder der übergeordneten SharePoint-Website wiederherstellen. Sie können die Daten unter Verwendung eines neuen Namens auf der ursprünglichen Website wiederherstellen, die Daten am ursprünglichen Speicherort wiederherstellen und von den Wiederherstellungspunkten auf Datenträger exportieren.

Führen Sie die folgenden Tasks aus, um SharePoint Online-Listenelemente wiederherzustellen:

1. Auswählen der SharePoint Online-Website-Listenelemente für die Wiederherstellung
2. Definieren der Wiederherstellungsoptionen
3. Überprüfen, ob der Inhalt wiederhergestellt wurde

Auswählen der SharePoint Online-Website-Listenelemente für die Wiederherstellung

Sie können SharePoint Online-Listenelementdaten von einem Wiederherstellungspunkt wiederherstellen. Wenn Sie ein Wiederherstellungsdatum auswählen und dann die Uhrzeit angeben, werden alle zugeordneten Wiederherstellungspunkte für diesen Zeitraum angezeigt. Sie können die Inhalte (einschließlich Anwendungen) für die Wiederherstellung suchen und auswählen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve UDP an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

   Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   Oder

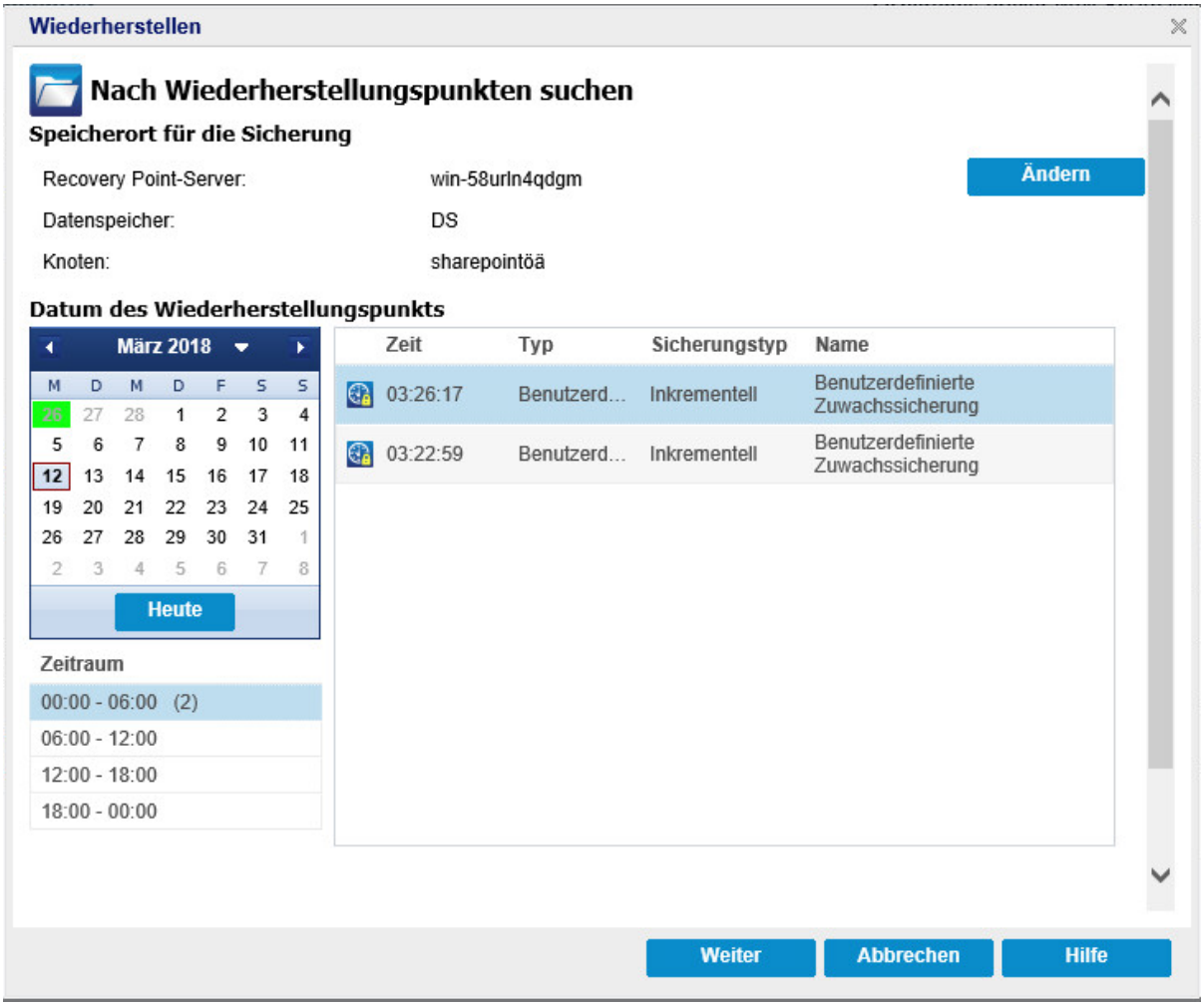
   Wählen Sie die Gruppe **SharePoint Online-Knoten**.

   Alle hinzugefügten SharePoint-Knoten werden im mittleren Fensterbereich angezeigt.
4. Wählen Sie im mittleren Fensterbereich den SharePoint Online-Knoten aus, und klicken Sie auf **Aktionen**.
5. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

   Das Dialogfeld **SharePoint-Element wiederherstellen** wird geöffnet.

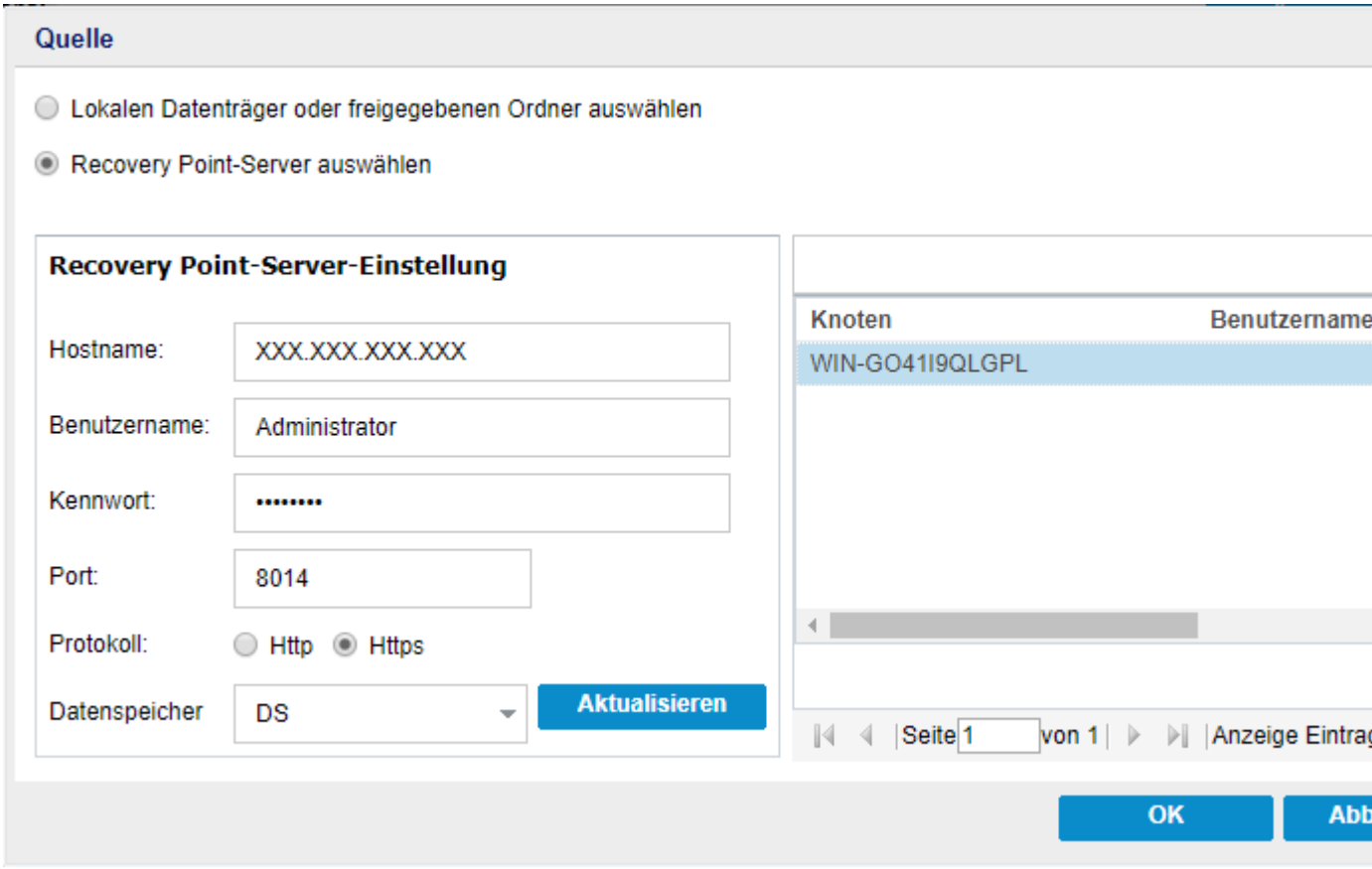
   Hinweis: Sie werden automatisch beim Agent-Knoten angemeldet, und das Dialogfeld **SharePoint-Element wiederherstellen** wird geöffnet.

   Speicherort für die Sicherung zeigt die **Recovery Point Server**-Details an.



6. (Optional) Klicken Sie auf **Ändern**, um den Speicherort für die Sicherung zu ändern.

   Das Dialogfeld **Quelle** wird geöffnet. Sie können den Sicherungsspeicherort in diesem Dialogfeld auswählen.



Hinweis: Wenn Sie dem Plan einen Task "Kopie auf Band" hinzufügen und nun den Wiederherstellungspunkt "Kopie auf Band" wiederherstellen möchten, wählen Sie den Wiederherstellungspunkt aus der Sicherung auf Kopie auf Band aus. Weitere Informationen finden Sie unter Durchsuchen der Kopie auf Band nach Wiederherstellungspunkten.

7. Um die Quelle anzugeben, wählen Sie eine der folgenden Optionen, und klicken Sie auf **OK**.

   Lokalen Datenträger oder freigegebenen Ordner auswählen

   Hinweis: In Arcserve UDP empfehlen wir nicht die Auswahl der Option **Lokalen Datenträger oder freigegebenen Ordner auswählen**.

   Recovery Point Server auswählen

   a. Geben Sie die Details für die Einstellungen des Recovery Point-Servers an, und klicken Sie auf **Aktualisieren**.

      Alle Agenten werden in der Spalte "Data Protection Agent" im Dialogfeld **Quelle** aufgelistet.

b. Wählen Sie den Agenten aus der angezeigten Liste/Bibliothek aus, und klicken Sie auf **OK**.

   Die Wiederherstellungspunkte werden im Dialogfeld **SharePoint-Element wiederherstellen** aufgelistet.

8. Geben Sie das Datum des Sicherungs-Images an, das Sie wiederherstellen möchten, und klicken Sie auf **Weiter**.

   Alle Daten, die Wiederherstellungspunkte für die angegebene Sicherungsquelle enthalten, werden grün hervorgehoben.

   Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp (vollständig oder inkrementell) und Name der Sicherung angezeigt.

9. Erweitern Sie im Dialogfeld **SharePoint Online-Elemente wiederherstellen** die Websitesammlung.

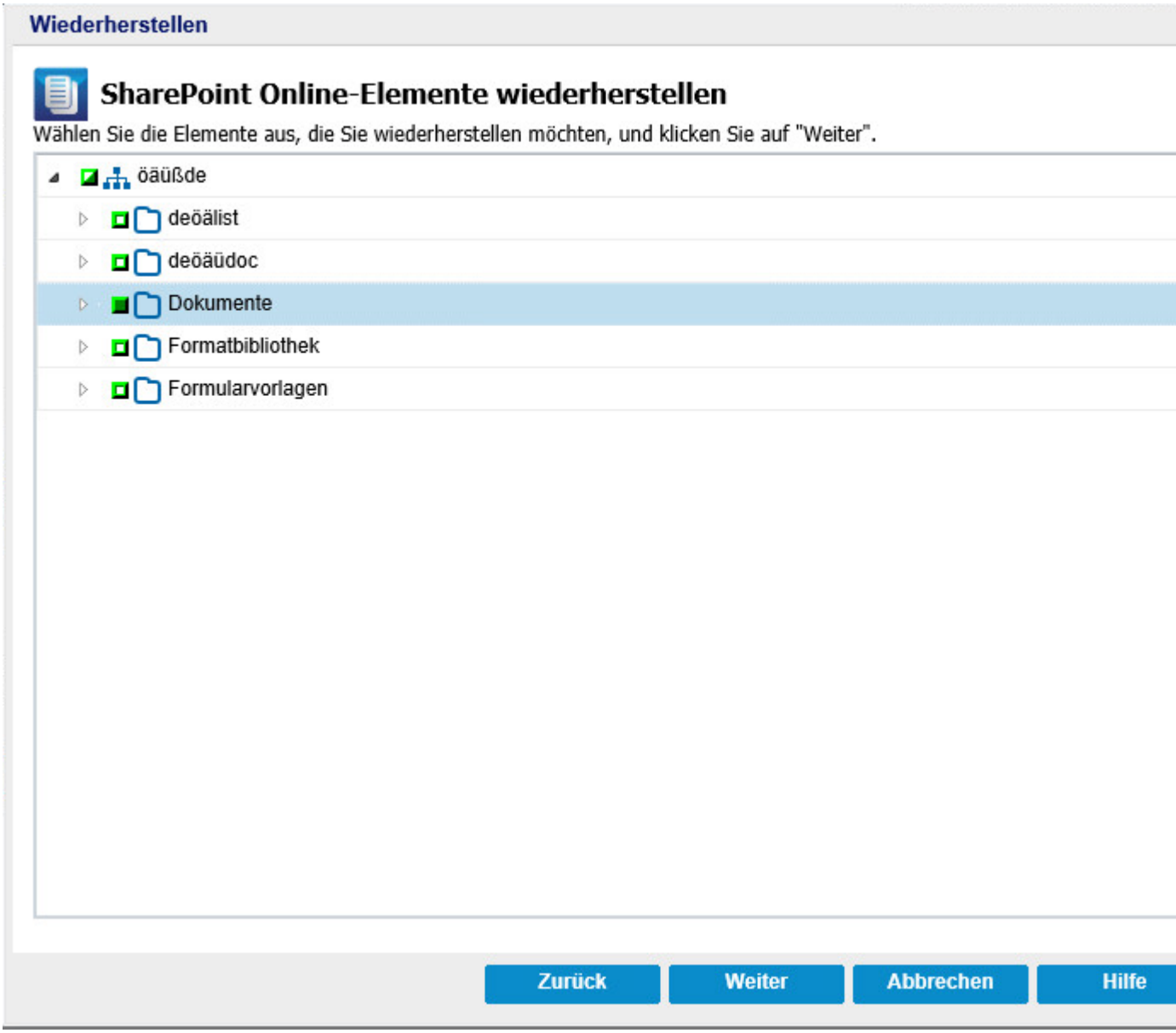
   Alle Listen/Bibliotheken und Elemente werden angezeigt.

10. Wählen Sie die Listen/Bibliotheken in der Websitesammlung, die Sie wiederherstellen möchten, aus der SharePoint-Websitesammlung, und klicken Sie auf **Weiter**.

    Hinweise:

    - Sie können den gesamten Inhalt oder Teile des Inhalts des wiederherzustellenden SharePoint-Objekts auswählen. Um Teile des Inhalts auszuwählen, erweitern Sie das Objekt, und klicken Sie auf das Kontrollkästchen des Inhalts.
    - Sie können mehrere SharePoint-Listen/-Bibliotheken oder -Listenelemente wiederherstellen.

    Das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet.



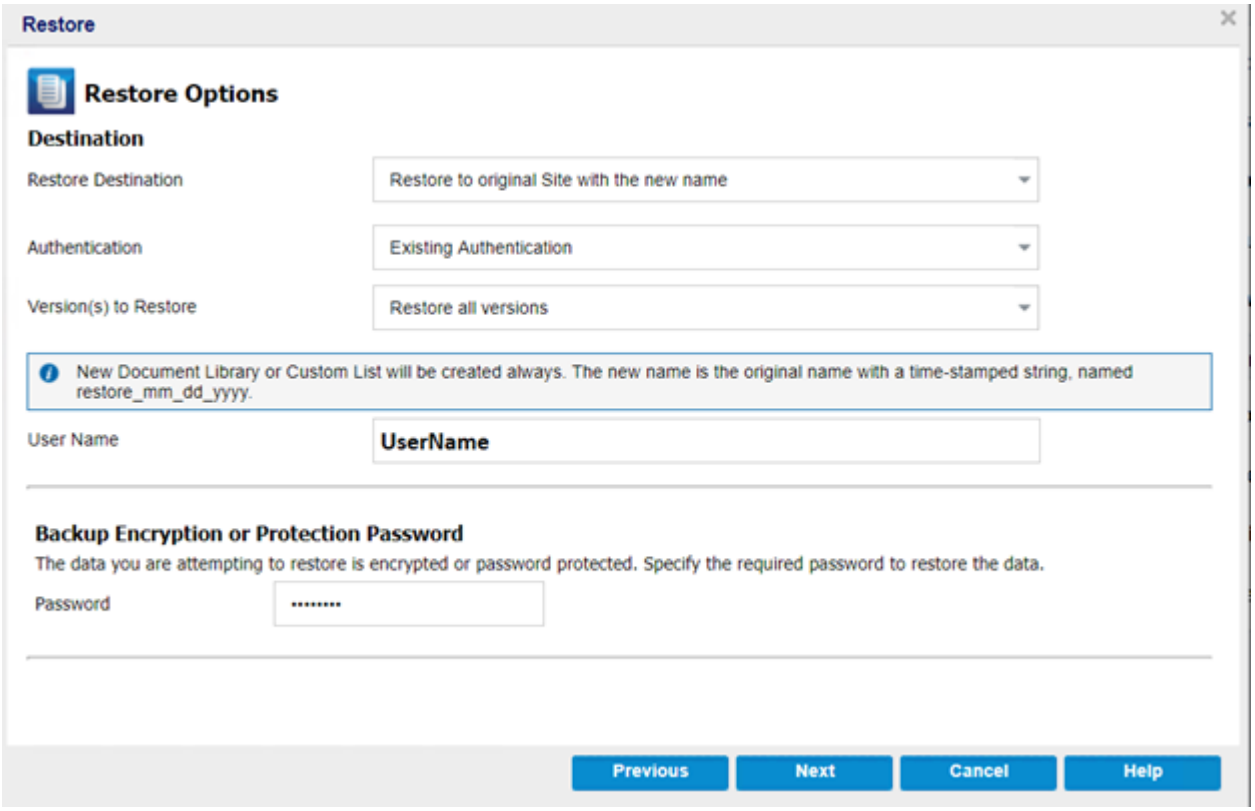
Die SharePoint Online-Listen/Bibliotheken oder -Listenelemente für die Wiederherstellung werden ausgewählt. Nun können Sie die Wiederherstellungsoptionen definieren.

Definieren der Wiederherstellungsoptionen

Nachdem Sie die wiederherzustellenden SharePoint Online-Informationen angegeben haben, legen Sie die Wiederherstellungsoptionen für die ausgewählten Inhalte fest.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Wiederherstellungsoptionen** das Wiederherstellungsziel aus.



Es sind folgende Zieloptionen verfügbar:

Auf ursprüngliche Website mit dem neuen Namen wiederherstellen

Stellt die Daten der Liste/Bibliothek und der Listenelemente auf derselben Website mit einem neuen Listennamen her, von der Sie die Sicherung erstellt haben.

Wiederherstellen am ursprünglichen Speicherort

Stellt die Daten der Liste/Bibliothek und der Listenelemente am selben Speicherort wieder her, an dem Sie die Sicherung erstellt haben.

2. Geben Sie eine der folgenden Optionen aus der Drop-down-Liste **Wenn das Element auf dem Ziel bereits vorhanden ist** an:

Bei aktivierter Versionierung als neue Version anfügen

Diese Option funktioniert, wenn Ihre Versionseinstellung in der Bibliothekseinstellung auf der SharePoint-Website aktiviert ist. Wenn Sie diese Option auswählen, wird die neue Version an die aktuellen Versionen der Listenelemente angehängt, wenn die Listenelemente vorhanden sind.

Objekt überspringen und nicht wiederherstellen

Elemente werden übersprungen und nicht wiederhergestellt.

Das Element im Ziel überschreiben

Das Element im Ziel wird überschrieben.

Auf Datenträger exportieren

Stellt die Listen/Bibliotheken oder Listenelemente in der Websitesammlung im Ordner oder freigegebenen Ordner auf dem Datenträger wieder her.

Hinweis: Wenn Sie für die Listenwiederherstellung die Wiederherstellungsoption "Auf Datenträger exportieren" auswählen, werden nur Anhänge der Liste auf den Datenträger exportiert.

Authentifizierung

Validiert und identifiziert das Benutzerkonto. Wählen Sie eine der folgenden Optionen:

- **Vorhandene Authentifizierung**

  Wenn Sie "Vorhandene Authentifizierung" auswählen, wird der Authentifizierungstyp verwendet, der während der Knotenerstellung ausgewählt wurde.

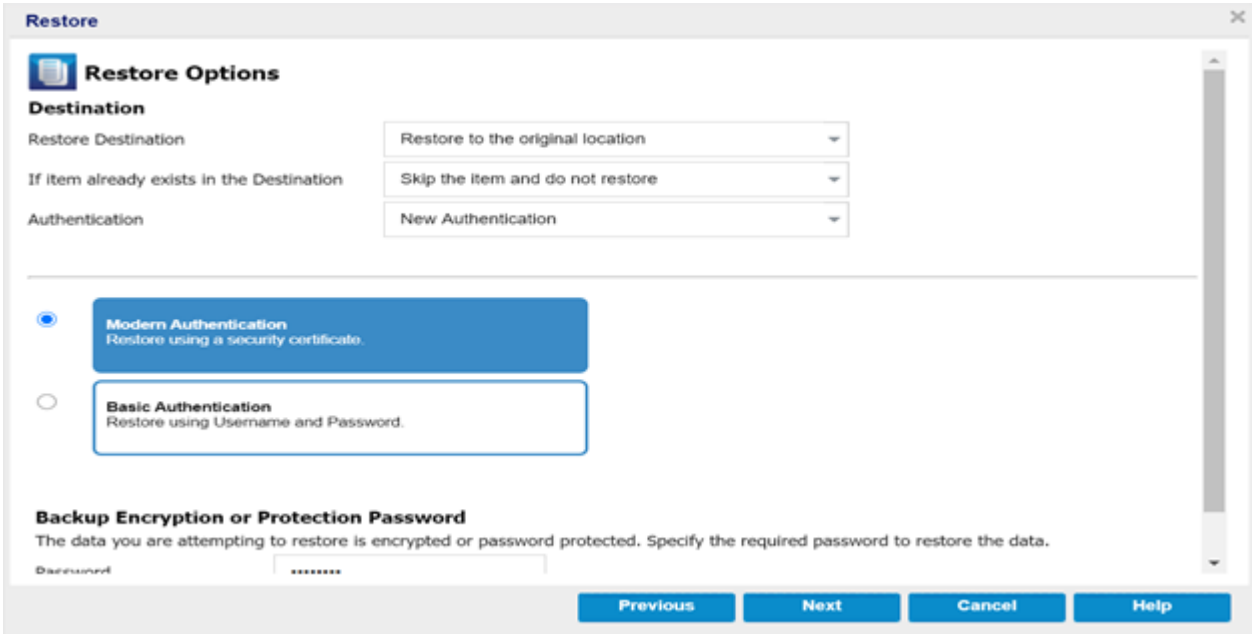
  - Wenn es sich bei der Knotenauthentifizierung um die Standardauthentifizierung handelt, werden Parameter wie Benutzername, Kennwort und Sicherungsverschlüsselung oder Schutzkennwort [falls verschlüsselt] automatisch geladen, um mit der Wiederherstellung fortzufahren.
  - Wenn es sich bei der Knotenauthentifizierung um die moderne Authentifizierung handelt, werden Parameter wie Benutzername und Sicherungsverschlüsselung oder Schutzkennwort [falls verschlüsselt] automatisch geladen, um mit der Wiederherstellung fortzufahren.

- **Neue Authentifizierung**

  Während der Wiederherstellung können Sie eine der folgenden Optionen auswählen, um den Authentifizierungstyp zu ändern:

  - Moderne Authentifizierung

- Standardauthentifizierung



3. Gehen Sie folgendermaßen vor, um die Authentifizierung anzuwenden:

Moderne Authentifizierung

Bei der modernen Authentifizierung können Sie eine Wiederherstellung mithilfe eines Sicherheitszertifikats ausführen.

Sicherheitszertifikat verwenden

Hinweis: Standardmäßig wählt der Sicherungsplan die Option **Sicherheitszertifikat verwenden** für die moderne Authentifizierung aus.

Gehen Sie wie folgt vor:

a. Informationen zur Authentifizierung mithilfe eines selbstsignierten Zertifikats finden Sie unter Herunterladen des Zertifikats von UDP und Hochladen in Azure

b. Geben Sie die Anwendungs-ID und den Benutzernamen ein.

c. Um die erforderlichen Rollen und Berechtigungen anzuwenden, aktivieren Sie das Kontrollkästchen **Ermöglichen Sie Arcserve UDP, die erforderlichen Azure-Rollen und -Berechtigungen für diese Anwendung festzulegen**, und klicken Sie dann auf **Weiter**.

Standardauthentifizierung

Um bei der Standardauthentifizierung mit der Wiederherstellung fortzufahren, geben Sie Benutzername und Kennwort ein.

Hinweis: Diese Option schlägt fehl, wenn Sie die moderne Authentifizierung für den Mandanten oder das Konto aktiviert haben.

4. Geben Sie die Listenelementversionen an, die Sie wiederherstellen möchten, wenn Ihre Versionseinstellung in der Bibliothekseinstellung auf der SharePoint-Website aktiviert wird.

   Alle Versionen wiederherstellen

   Stellt alle Versionen bei Sicherung wieder her.

   Nur die neueste Version wiederherstellen

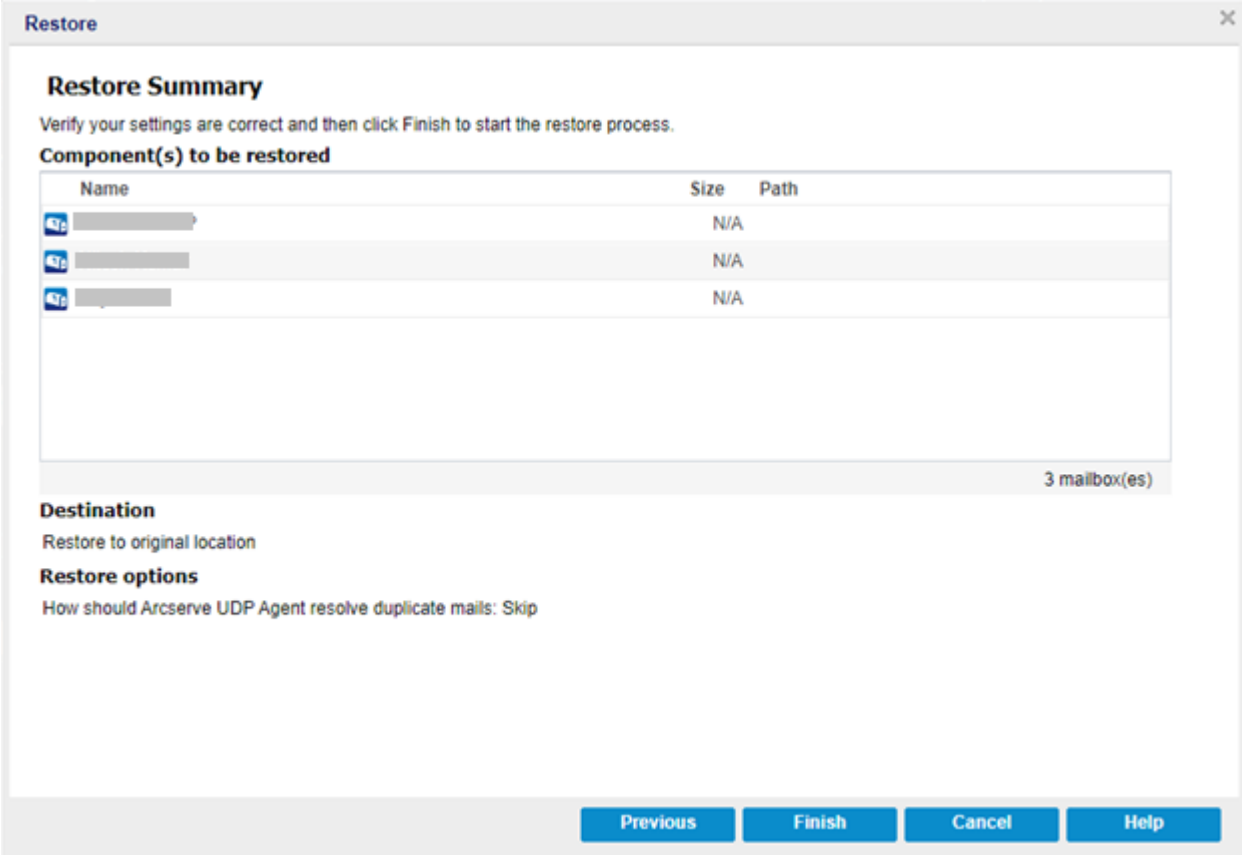
   Stellt nur die neuste Version bei Sicherung wieder her.

   Nur die neueste Hauptversion wiederherstellen

   Stellt nur die neueste Hauptversion bei Sicherung wieder her.

5. Geben Sie das Sitzungskennwort an, falls vorhanden.
6. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsübersicht** wird geöffnet.



   Sie können die Wiederherstellungsinformationen aus dem Dialogfeld "Wiederherstellungsübersicht" wiederherstellen.

7. Klicken Sie auf **Fertig stellen**, um den Wiederherstellungsjob zu senden.

Die Wiederherstellungsoptionen für die Wiederherstellung von SharePoint Online-Informationen sind festgelegt.

Überprüfen, ob der Inhalt wiederhergestellt wurde

Überprüfen Sie nach dem Abschluss der Wiederherstellung, dass der Inhalt auf dem angegebenen Ziel wiederhergestellt wurde.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der SharePoint-Websitesammlung an.
2. Überprüfen Sie die Listen/Bibliotheken und die Listenelemente.
3. Überprüfen die wiederhergestellten Inhalte.

   Der wiederhergestellte Inhalt wurde erfolgreich überprüft.

So stellen Sie OneDrive Daten wieder her

Sie können OneDrive Daten (Dateien, Ordner usw.) mit jedem Computer wiederherstellen. Sie können die Wiederherstellung mit der Wiederherstellungsoption oder auch mit der Option "Mount Volume" aus der Benutzeroberfläche des Agenten durchführen.

Führen Sie die folgenden Aufgaben aus, um OneDrive Daten, die Option "Wiederherstellung" wiederherzustellen:

1. Wählen Sie die wiederherzustellenden OneDrive Elemente aus
2. Definieren der Wiederherstellungsoptionen
3. Wiederherstellungsübersicht anzeigen

   Oder sonst

   Stellen Sie OneDrive Daten mit der Option "Mount Volume" wieder her.

OneDrive-Elemente für die Wiederherstellung auswählen

Sie können OneDrive-Daten von einem Wiederherstellungspunkt aus wiederherstellen. Wenn Sie ein Wiederherstellungsdatum auswählen und dann die Uhrzeit angeben, werden alle zugeordneten Wiederherstellungspunkte für diesen Zeitraum angezeigt. Sie können die Inhalte (einschließlich Anwendungen) für die Wiederherstellung suchen und auswählen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve UDP an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

   Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.
4. Wählen Sie im mittleren Bereich den OneDrive-Knoten aus und klicken Sie auf **Aktionen**.
5. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

   Hinweis: Sie sind automatisch am Agentenknoten angemeldet und der Dialog **Knoten** wird geöffnet.

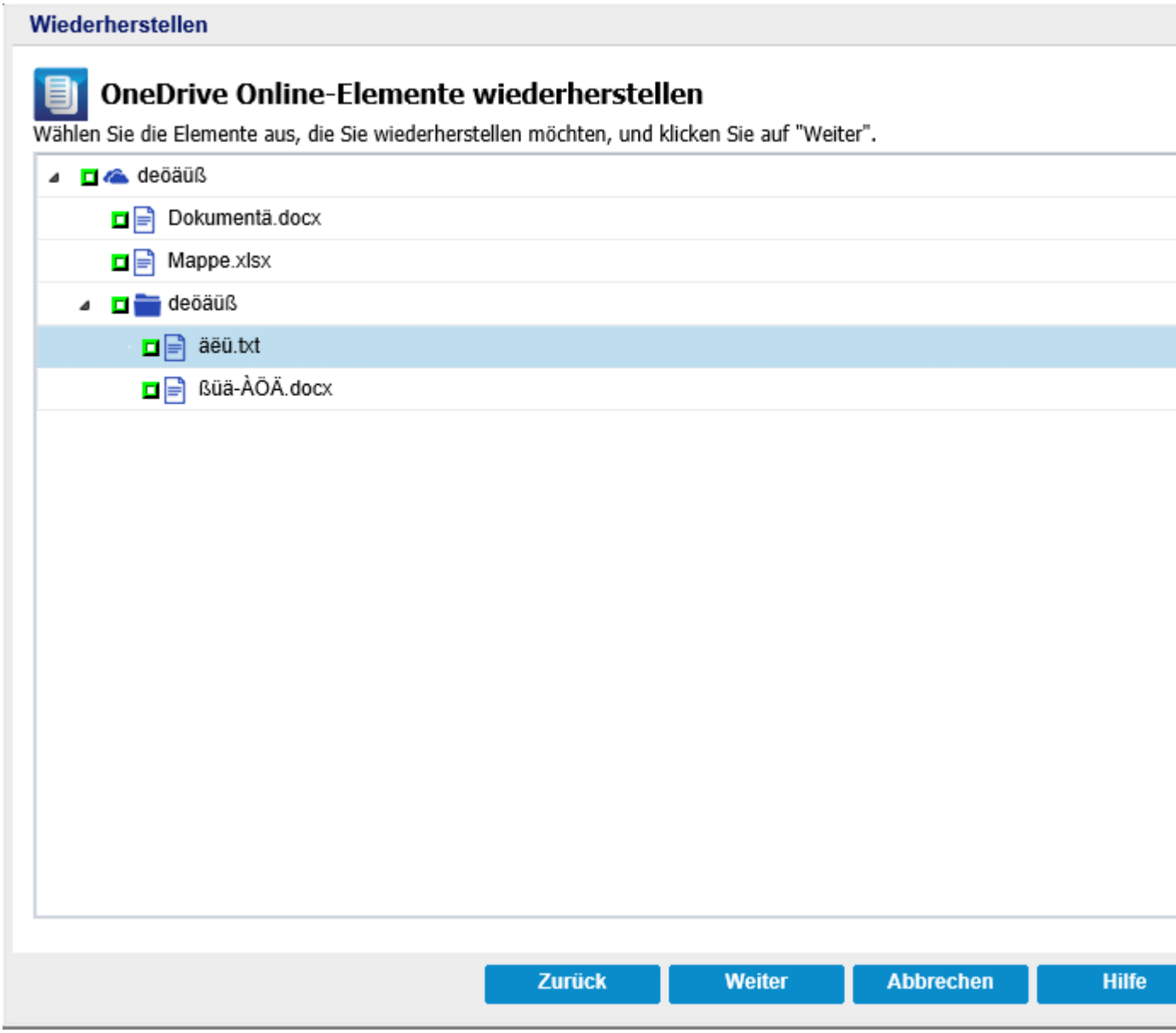
   Sie können die Details von **Wiederherstellungspunkte durchsuchen** im Sicherungsspeicherort einsehen. Der Name des ausgewählten *Wiederherstellungspunkt-Server* wird angezeigt. Wenn erwünscht, klicken Sie auf **Ändern** und ändern Sie **Einstellungen des Wiederherstellungspunkt-Servers** im **Source** Pop-up-Fenster.

   Hinweis: Wenn Sie dem Plan einen Task "Kopie auf Band" hinzufügen und nun den Wiederherstellungspunkt "Kopie auf Band" wiederherstellen möchten, wählen Sie den Wiederherstellungspunkt aus der Sicherung auf Kopie auf Band aus. Weitere Informationen finden Sie unter Durchsuchen der Kopie auf Band nach Wiederherstellungspunkten.
6. Geben Sie das Datum des Sicherungs-Images an, das Sie wiederherstellen möchten, und klicken Sie auf **Weiter**.

   Alle Daten, die Wiederherstellungspunkte für die angegebene Sicherungsquelle enthalten, werden grün hervorgehoben.

   Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp (vollständig oder inkrementell) und Name der Sicherung angezeigt.

7. Aktivieren Sie im Bereich **OneDrive-Knotenelemente wiederherstellen** die Kontrollkästchen für verwandte Elemente oder Ordner, die Sie aus Ordnern wiederherstellen möchten, und klicken Sie auf **Weiter**.



Hinweise:

- Sie können den gesamten Inhalt oder einen Teilinhalt des OneDrive-Objekts für die Wiederherstellung auswählen. Um Teile des Inhalts auszuwählen, erweitern Sie das Objekt, und klicken Sie auf das Kontrollkästchen des Inhalts.
- Sie können mehrere OneDrive-Objekte für die Wiederherstellung auswählen.

Das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet.

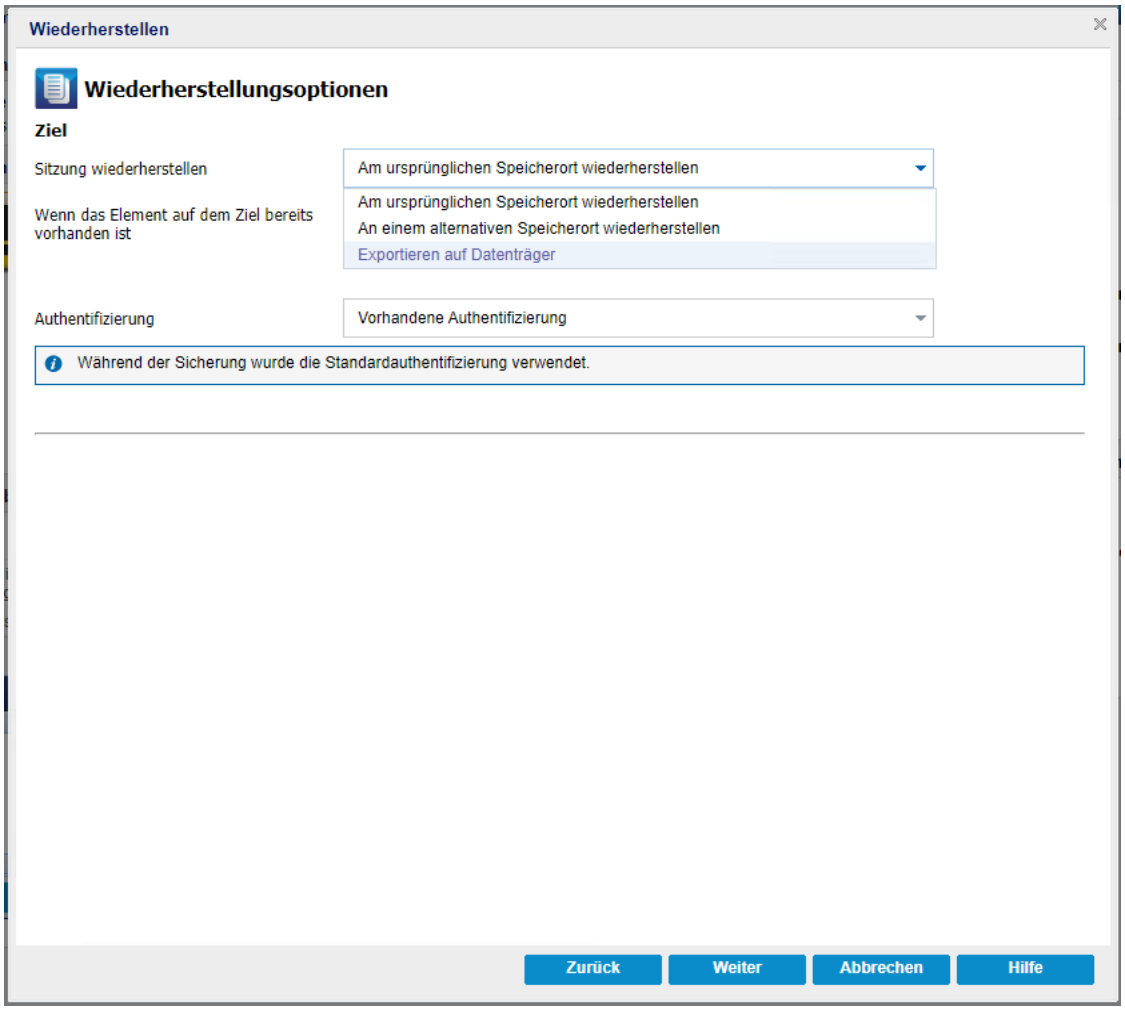
Die wiederherzustellenden OneDrive Knotenelemente sind ausgewählt. Nun können Sie die Wiederherstellungsoptionen definieren.

Definieren der Wiederherstellungsoptionen

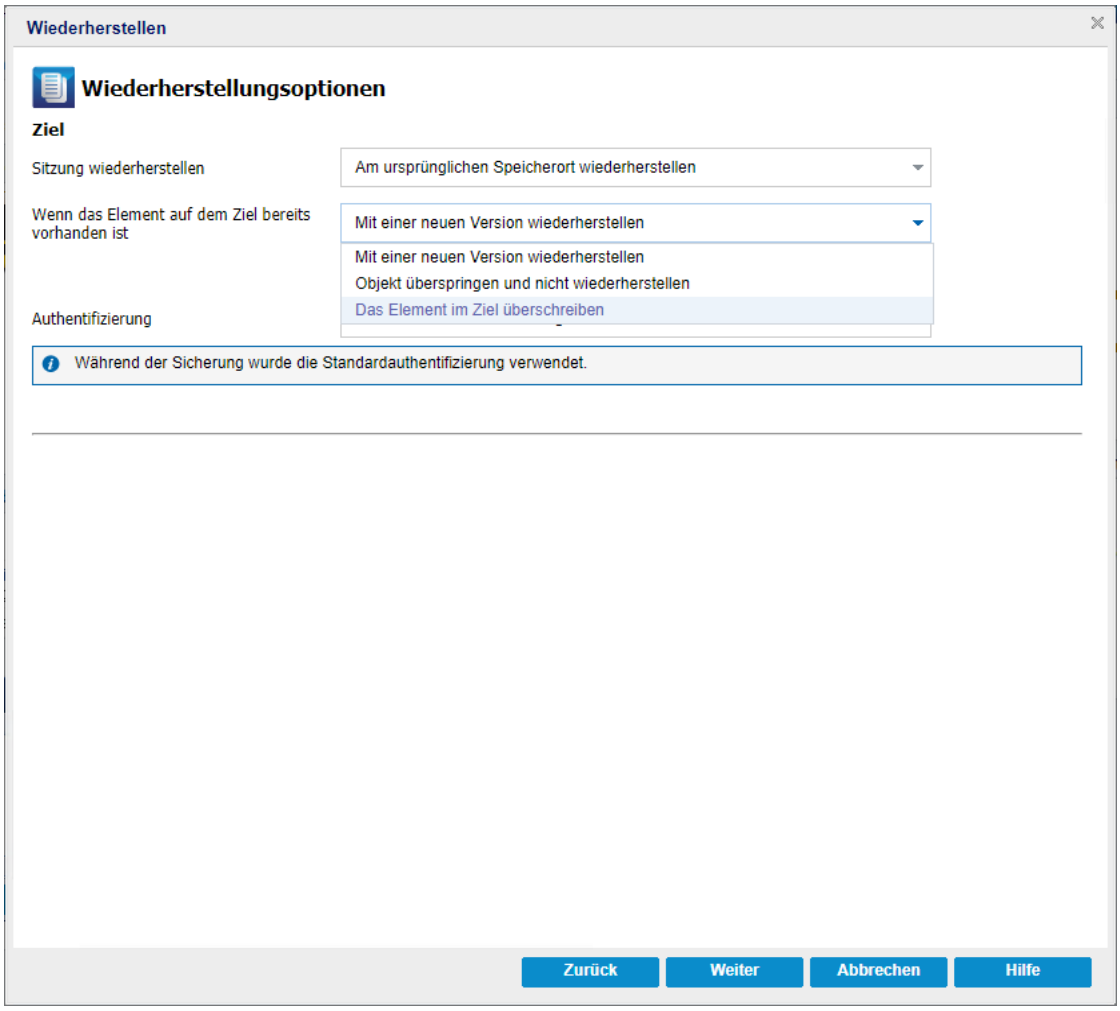
Nachdem Sie die wiederherzustellenden OneDrive-Informationen angegeben haben, definieren Sie die Wiederherstellungsoptionen für den ausgewählten Inhalt.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Wiederherstellungsoptionen** das Wiederherstellungsziel aus.



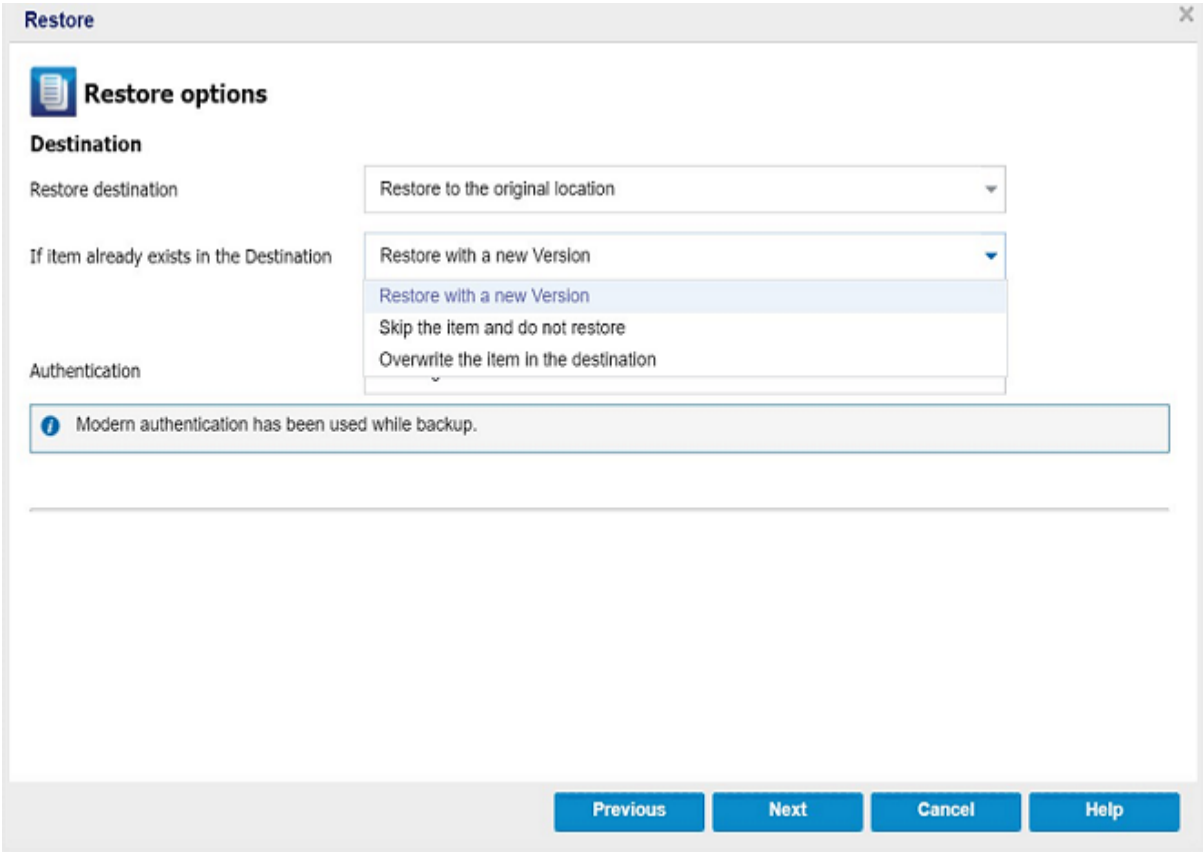
Es sind folgende Zieloptionen verfügbar:



Wiederherstellen am ursprünglichen Speicherort

Stellt die Dateien oder Ordner am selben Speicherort wieder her, an dem Sie eine Sicherung ausgeführt haben.

Wenn Sie die Option **Am ursprünglichen Speicherort wiederherstellen** auswählen, wählen Sie aus der Drop-down-Liste **Wenn das Element bereits vorhanden im Ziel ist** eine der folgenden Optionen aus:



Mit einer neuen Version wiederherstellen

Hängt eine neue Version an die vorhandene (n) Datei(en) an.

Diese Option ist standardmäßig aktiviert.

Objekt überspringen und nicht wiederherstellen

Elemente werden übersprungen und nicht wiederhergestellt.

Das Element im Ziel überschreiben

Das Element im Ziel wird überschrieben.

An einem anderen Speicherort wiederherstellen

Stellt die Dateien, Ordner oder Konten auf einem Konto am alternativen Speicherort wieder her. Wenn Sie diese Option auswählen, können Sie das Ziel auswählen.

Hierarchie der Quelle

Behält die Hierarchiestruktur beim Erstellen von Sicherungsplänen wie in der Quelle angegeben bei.

Hinweis: Diese Option wird nur angezeigt, wenn "An einem alternativen Speicherort wiederherstellen" ausgewählt ist.

Auf Datenträger exportieren

Stellt einen Ordner oder Freigabe-Ordner auf der Festplatte wieder her.

2. Um das Benutzerkonto zu validieren und zu identifizieren, wählen Sie im Drop-down-Menü **Authentifizierung** eine der folgenden Optionen aus:

Vorhandene Authentifizierung

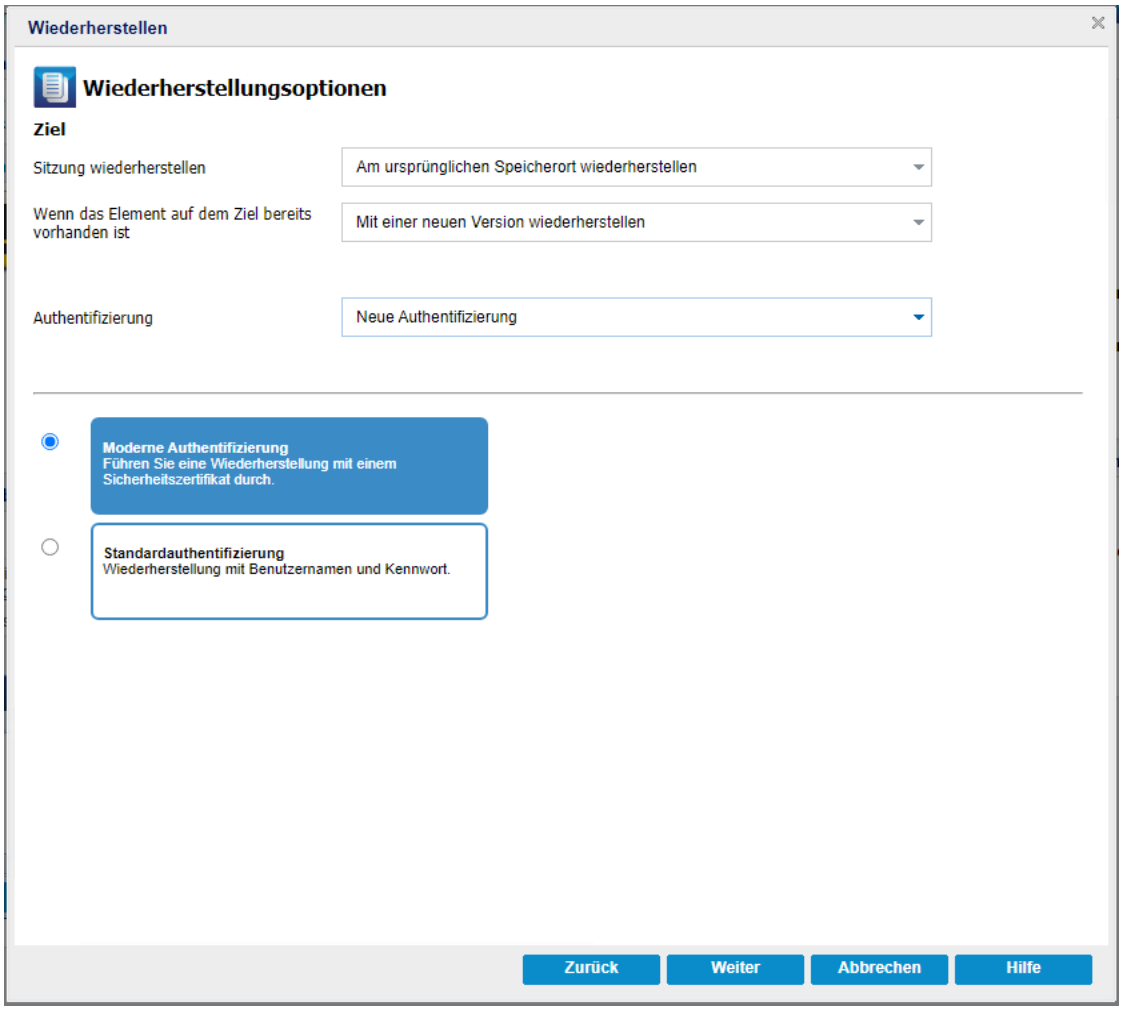
Wenn Sie "Vorhandene Authentifizierung" auswählen, wird der Authentifizierungstyp verwendet, der während der Knotenerstellung ausgewählt wurde.

- Wenn es sich bei der Knotenauthentifizierung um die Standardauthentifizierung handelt, werden Parameter wie Benutzername, Kennwort und Sicherungsverschlüsselung oder Schutzkennwort [falls verschlüsselt] automatisch geladen, um mit der Wiederherstellung fortzufahren.
- Wenn es sich bei der Knotenauthentifizierung um die moderne Authentifizierung handelt, werden Parameter wie Benutzername und Sicherungsverschlüsselung oder Schutzkennwort [falls verschlüsselt] automatisch geladen, um mit der Wiederherstellung fortzufahren.

Neue Authentifizierung

Während der Wiederherstellung können Sie eine der folgenden Optionen auswählen, um den Authentifizierungstyp zu ändern:

- Moderne Authentifizierung
- Standardauthentifizierung



3. Gehen Sie folgendermaßen vor, um die neue Authentifizierung anzuwenden:

   Moderne Authentifizierung

   Bei der modernen Authentifizierung können Sie eine Wiederherstellung mithilfe eines Sicherheitszertifikats ausführen.

   Gehen Sie wie folgt vor:

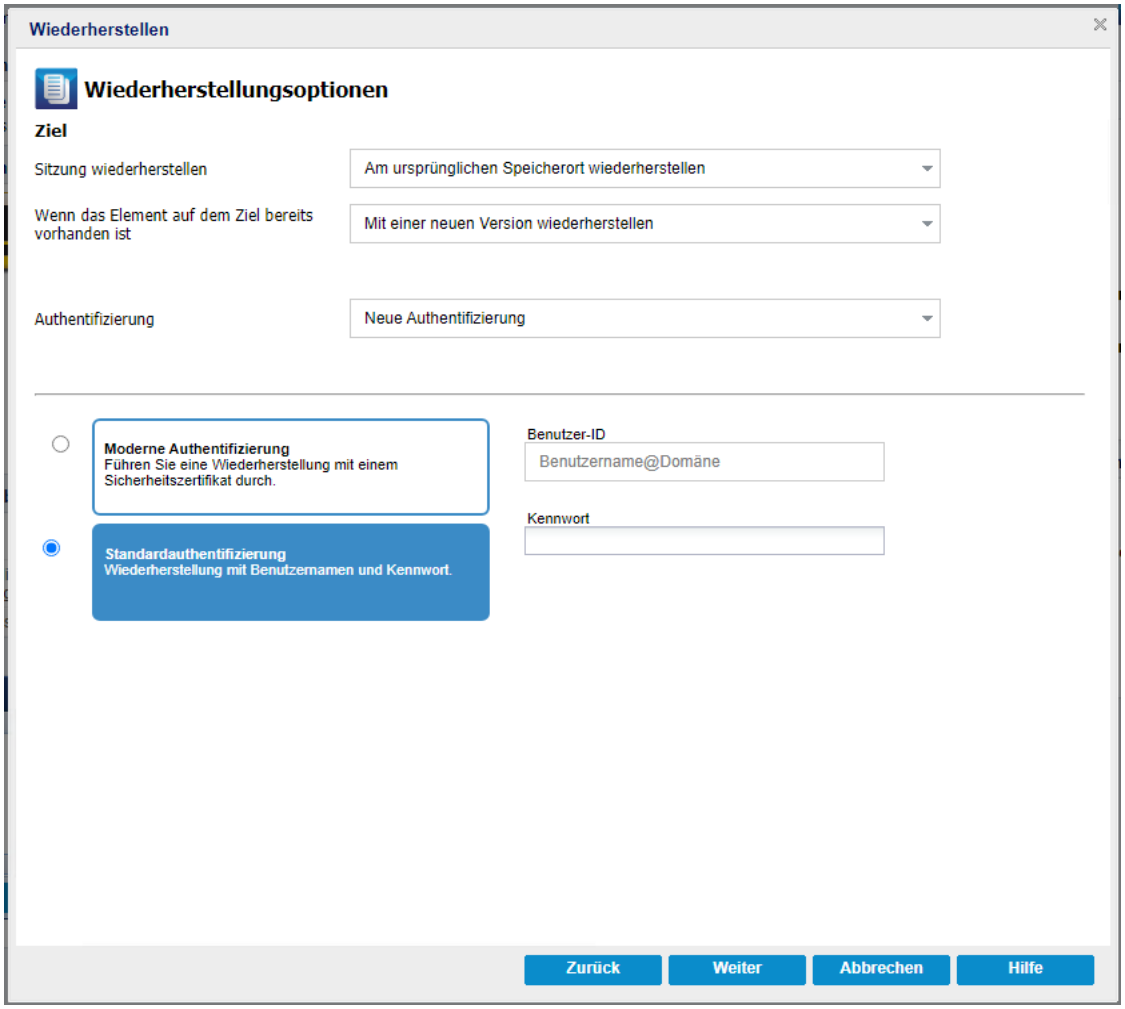
   a. Informationen zur Authentifizierung mit dem selbstsignierten Zertifikat finden Sie unter Herunterladen des Zertifikats von UDP und Hochladen des Zertifikats in Azure.

   b. Geben Sie die Anwendungs-ID und den Benutzernamen ein.

   c. Um die erforderlichen Rollen und Berechtigungen anzuwenden, aktivieren Sie das Kontrollkästchen **Ermöglichen Sie Arcserve UDP, die erforderlichen Azure-Rollen und -Berechtigungen für diese Anwendung festzulegen**, und klicken Sie dann auf **Weiter**.

   Standardauthentifizierung

Um bei Verwendung der Standardauthentifizierung mit der Wiederherstellung fortzufahren, geben Sie Benutzer-ID und Kennwort ein.



4. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsübersicht** wird geöffnet.

5. Überprüfen Sie im Dialogfeld "Wiederherstellungs-Übersicht" Ihre Einstellungen, und klicken Sie dann auf **Fertig stellen**.

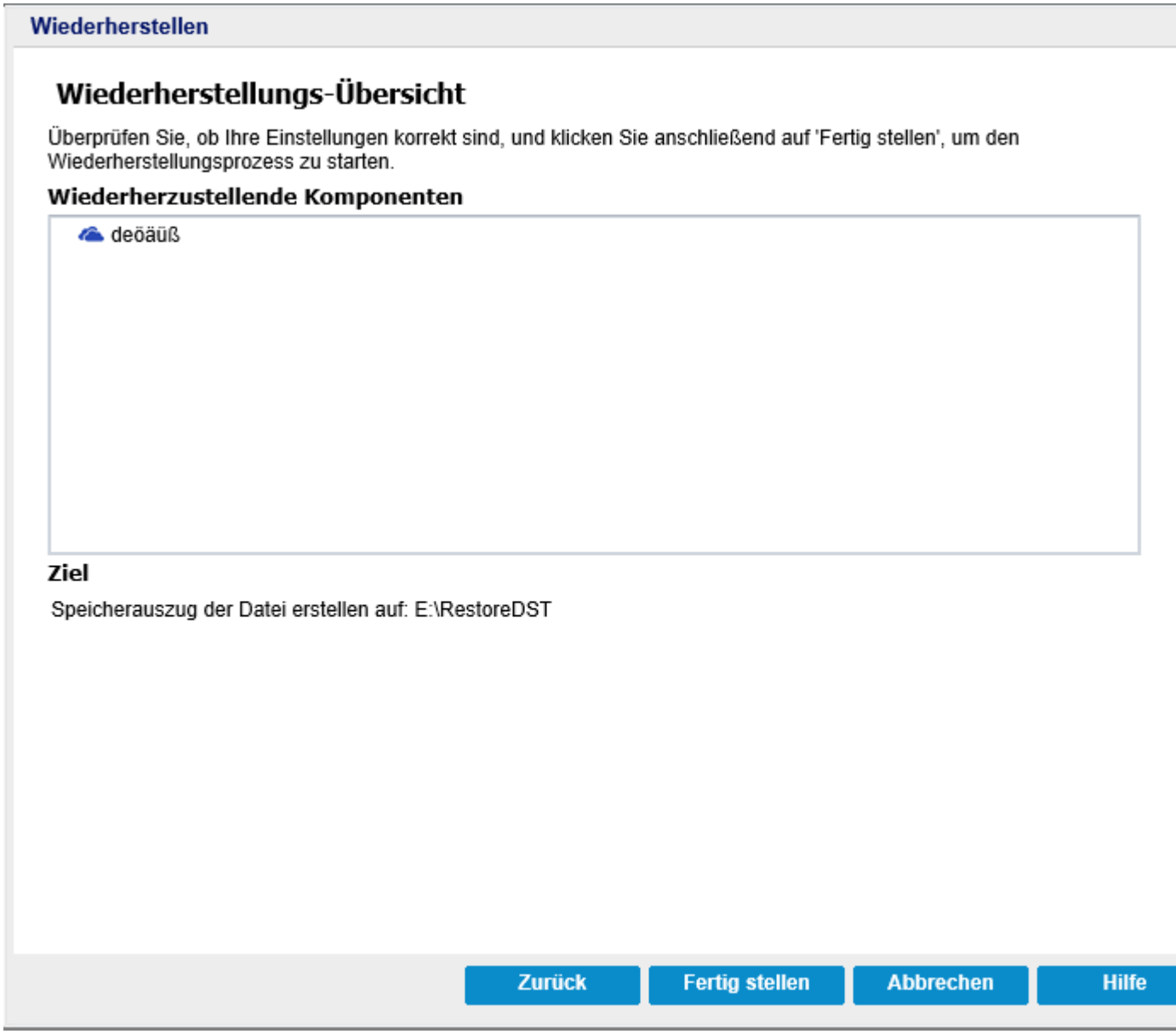
   Die Wiederherstellungsoptionen sind definiert, um die OneDrive-Informationen wiederherzustellen. Sie können jetzt die Wiederherstellungs-Übersicht anzeigen.

Wiederherstellungsübersicht anzeigen

Nachdem Sie die Wiederherstellungsoptionen definiert haben, überprüfen Sie, dass Ihre Einstellungen korrekt sind, und bestätigen Sie den Wiederherstellungsprozess. **Wiederherstellungs-Übersicht** hilft Ihnen dabei, alle Optionen und Ziel-Wiederherstellungspfade zu überprüfen, die Sie festgelegt haben. Wenn Sie Änderungen vornehmen möchten, klicken Sie auf **Zurück**.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Informationen im Dialogfeld **Wiederherstellungsübersicht**, um die Richtigkeit aller Wiederherstellungsoptionen und Einstellungen sicherzustellen.



- Wenn die zusammengefassten Informationen falsch sind, klicken Sie auf **Zurück** und gehen Sie zurück zum entsprechenden Dialogfeld, um die Einstellungen zu ändern.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsjob zu starten.

Der Wiederherstellungspunktinhalt wurde wiederhergestellt.

Wiederherstellen von OneDrive-Daten mit der Mount Volume Option

OneDrive Protection verwendet das universelle Sicherungs-Sitzungsformat. Sie können die Sicherungssitzung als Laufwerksbuchstaben einbinden und dann die Datei/-den Ordner vom eingelegten Volume kopieren.

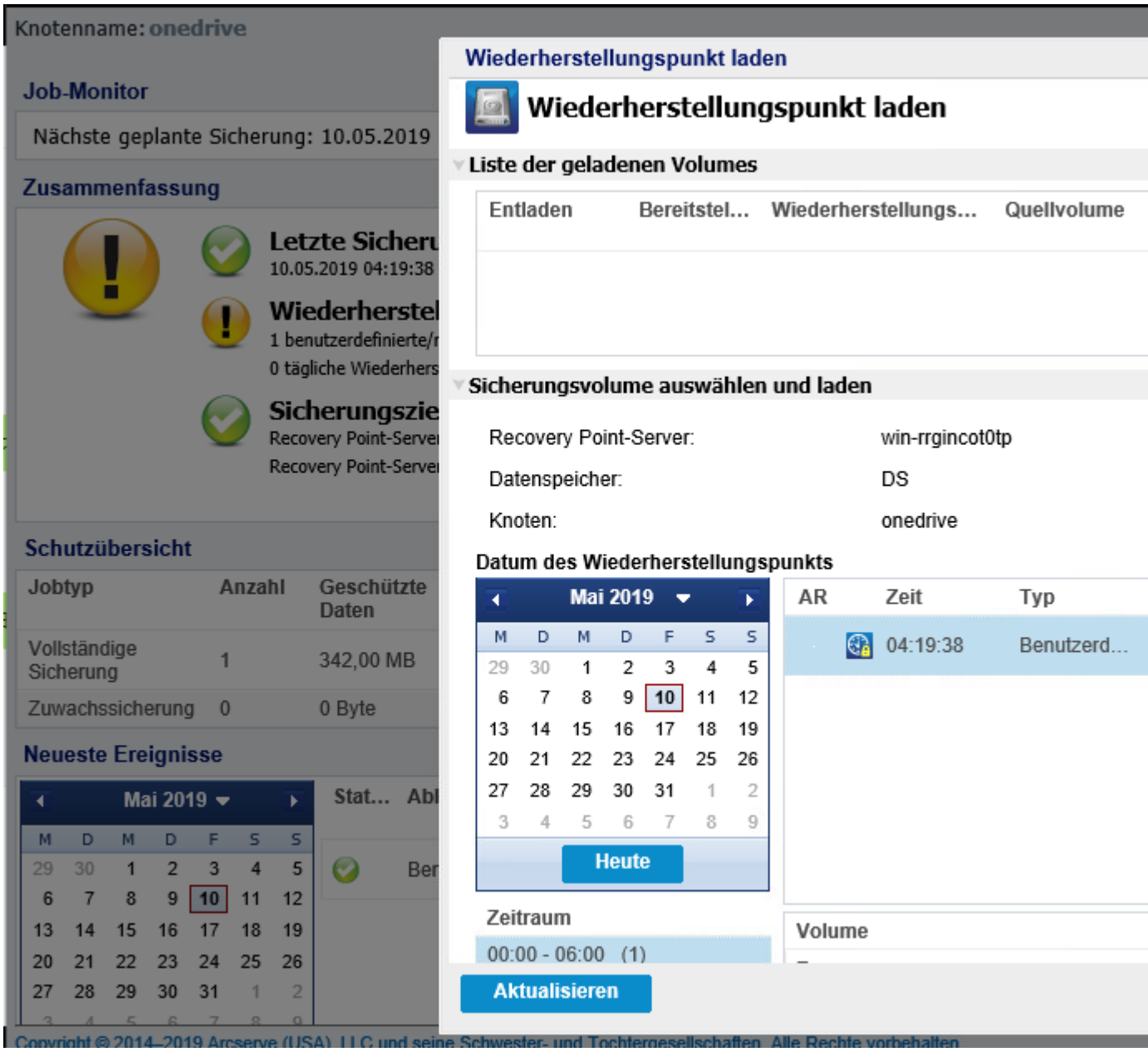
Gehen Sie wie folgt vor:

1. Melden Sie sich bei Arcserve UDP an.
2. Klicken Sie auf die Registerkarte **Ressourcen**.
3. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

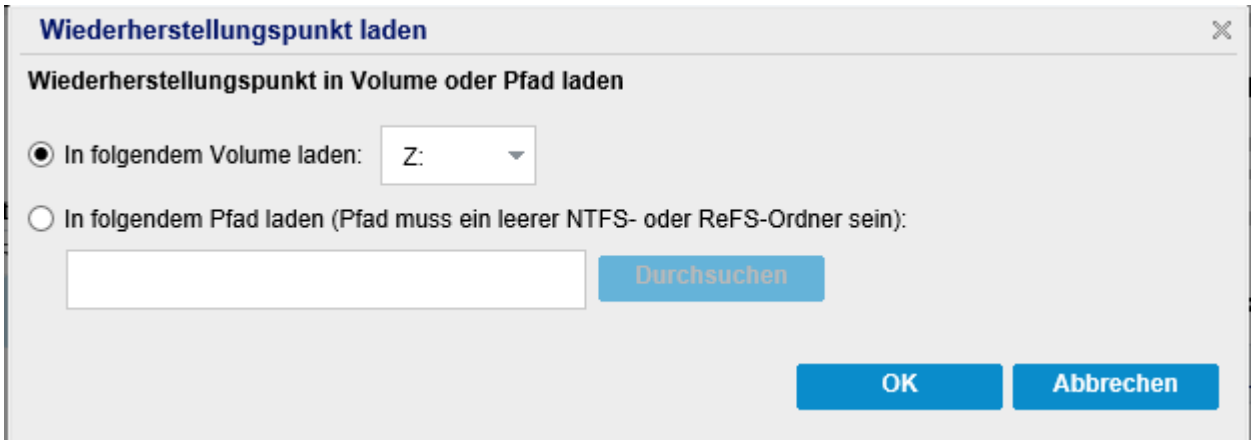
   Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.
4. Wählen Sie im mittleren Bereich den OneDrive-Knoten aus und klicken Sie auf **Aktionen**.
5. Klicken Sie auf **Bei Agent anmelden** im **Aktionen** Drop-Down-Menü aus.

   Hinweis: Sie werden automatisch beim Agentenknoten angemeldet. Sie können vollständige Details über den Knoten anzeigen auch im rechten Bereich die Liste der Aufgaben, die Sie ausführen können.
6. Klicken Sie im rechten Fensterbereich unter **Aufgaben** auf **Laden des Wiederherstellungspunkts**.

   Das Dialogfeld **Wiederherstellungspunkt laden** wird geöffnet. In diesem Dialogfeld können Sie die Sicherungssitzung auswählen.



7. Wählen Sie das Ziel aus und laden Sie die Sitzung als Laufwerksbuchstaben oder Mount in einen leeren NTFS-Ordner.



Sie können das Volume durchsuchen. Im Volume speicherte Arcserve UDP alle Metadaten von OneDrive. Jedes Konto hat einen zugehörigen Ordner im Stammvolumen. Der Ordner wird entsprechend dem Namen des Benutzerkontos benannt.

Sie können den unter diesem Kontonamen erstellten Ordner öffnen und überprüfen, ob die OneDrive-Daten gesichert sind.

Durchsuchen Sie "Auf Band-Wiederherstellungspunkt kopieren" zur Wiederherstellung

Dieser Abschnitt enthält Informationen zur Auswahl eines Wiederherstellungspunkts aus den Sicherungen "Kopieren auf Band".

Befolgen Sie diese Schritte:

1. Laden Sie die Wiederherstellungspunkte mit dem Arcserve Backup-Manager herunter, und kopieren Sie sie auf einen lokalen Datenträger.
2. Klicken Sie im Dialogfeld "Wiederherstellen" auf die Schaltfläche **Ändern**.
3. Wählen Sie die Option **Lokalen Datenträger oder freigegebenen Ordner auswählen** aus.
4. Klicken Sie auf **Durchsuchen**, um zum Speicherort des Ordners zu navigieren, in den die Wiederherstellungspunkte in Schritt 1 kopiert werden.
5. Wählen Sie in der Liste der Wiederherstellungspunkte einen Wiederherstellungspunkt aus, und klicken Sie auf **OK**.

   Der ausgewählte Wiederherstellungspunkt wird im Dialogfeld "Wiederherstellen" angezeigt.

So führen Sie eine Wiederherstellung zu einem bestimmten Zeitpunkt durch

Point-In-Time Restore unterstützt die Wiederherstellung der SQL-Datenbank für einen bestimmten Zeitraum zwischen N und N+1 Wiederherstellungspunkten. Mit Point-In-Time können Administratoren die Transaktionen wiederherstellen, die zwischen zwei Wiederherstellungspunkten in der SQL-Datenbank erfolgt sind. Bedenken Sie zum Beispiel, dass Sie einen Wiederherstellungspunkt am 16.03.2019 12:14:14:04:177 und einen nachfolgenden Wiederherstellungspunkt am 29.03.2019 22:03:14:177 haben. Mit Point-In-Time können Sie die Transaktionen wiederherstellen, die zwischen den zwei Wiederherstellungspunkten erfolgt sind. Auf diese Weise können Administratoren ausschließlich die erforderlichen Transaktionen aus einer großen Menge an gesicherten Daten wiederherstellen.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen
2. Überprüfen der Hinweise
3. Durchführen einer Wiederherstellung zu einem bestimmten Zeitpunkt

Voraussetzungen

Beachten Sie die folgenden Voraussetzungen, bevor Sie eine Wiederherstellung zu einem bestimmten Zeitpunkt durchführen:

- MS SQL-Datenbankserver muss auf dem Windows-Agent-Rechner installiert sein.
- Sie benötigen mindestens zwei Wiederherstellungspunkte für die Wiederherstellung zu einem bestimmten Zeitpunkt.
- Sie müssen Point-In-Time bei jeder Wiederherstellung manuell aktivieren.

Hinweise

Beachten Sie die folgenden Hinweise, bevor Sie eine Wiederherstellung zu einem bestimmten Zeitpunkt durchführen:

- Sie können die Wiederherstellung zu einem bestimmten Zeitpunkt nur mithilfe des Befehlszeilenhilfsprogramms PIT.EXE durchführen.
- Sie benötigen zwei zusammenhängende Wiederherstellungspunkte, um eine Wiederherstellung zu einem bestimmten Zeitpunkt durchzuführen.

- Die Wiederherstellung zu einem bestimmten Zeitpunkt unterstützt nur die agentenbasierte Sicherung. Hostbasierte Sicherung wird nicht unterstützt.
- Point-In-Time unterstützt ausschließlich die Wiederherstellung am ursprünglichen Speicherort. Die Wiederherstellung an einem alternativen Speicherort und Speicherauszug auf Datenträger werden nicht unterstützt.
- Die Sicherung des Transaktionsprotokolls der SQL-Datenbank wird im selben Verzeichnis der SQL-Protokolldatei gespeichert, bevor der Snapshot erstellt wird.
- Der erste Wiederherstellungspunkt bietet die SQL-Wiederherstellung auf Datenbankebene. Nach der Wiederherstellung zu einem bestimmten Zeitpunkt, wird die SQL-Datenbank auf den Wiederherstellungsstatus festgelegt. Sie können den Wiederherstellungspunkt sichern, wenn Point-in-Time deaktiviert ist.
- Um eine Wiederherstellung zu einem bestimmten Zeitpunkt durchzuführen, müssen Sie den Zeitpunkt zwischen N und N+1 Wiederherstellungspunkten auswählen. Ein Zeitpunkt vor dem Wiederherstellungspunkt N und nach dem Wiederherstellungspunkt N+1 ist nicht zulässig. Wenn Sie einen Zeitpunkt festlegen, der nicht zwischen dem Wiederherstellungspunkt N und N+1 liegt, schlägt der Sicherungsjob fehl und führt zur Beschädigung der Datenbank.
- Die Option "Protokoll verkürzen" ist in den Point-In-Time Backup- und Wiederherstellungsplänen standardmäßig deaktiviert. Wenn aktiviert, werden nach dem Kürzen der Sicherungs-Transaktionsprotokolle die Protokolle abgeschnitten und die nächste Point-In-Time-Sicherung übersieht einige Transaktionen.

Durchführen einer Wiederherstellung zu einem bestimmten Zeitpunkt

1. Führen Sie die Datei **PIT.EXE** aus.

   Das Point-In-Time-Befehlszeilenhilfsprogramm wird geöffnet, und es wird die PIT$-Eingabeaufforderung angezeigt.

   Weitere Informationen finden Sie unter Grundlegendes zum Point-In-Time-Befehlszeilenhilfsprogramm.

2. Führen Sie in der Eingabeaufforderung **set pitbackup=1** aus.

   Die Sicherung zu einem bestimmten Zeitpunkt ist aktiviert.

3. Führen Sie über die **Arcserve UDP-Konsole** eine Sicherung der SQL-Datenbank durch.

Der Wiederherstellungspunkt N wird erstellt.

4. Stellen Sie sicher, dass die folgenden Dateien im Ordner **Katalog** erstellt werden:
   - Wenn der SQL Server-Instanz Name MSSQLSERVER (Standard Instanzname) lautet:
     - ***_<DatabaseName>.idx.pit***

       Enthält eine feste Größe der Zeitpunktzusammenfassung.
     - ***_<DatabaseName>.cat.pit***

       Enthält eine variable Größe der Zeitpunktdetails.
     - ***_<DatabaseName>.map.pit***

       Enthält die Zuordnung zwischen der internen Zeichenfolge und der interne Zeichenfolgenidentität.
   - Wenn der Name der SQL Server-Instanz ein anderer ist als MSSQLSERVER (nicht der Standard-Instanzname):
     - ***<SQLInstanceName>_<DatabaseName>.idx.pit***

       Enthält eine feste Größe der Zeitpunktzusammenfassung.
     - ***<SQLInstanceName>_<DatabaseName>.cat.pit***

       Enthält eine variable Größe der Zeitpunktdetails.
     - ***<SQLInstanceName>_<DatabaseName>.map.pit***

       Enthält die Zuordnung zwischen der internen Zeichenfolge und der interne Zeichenfolgenidentität.
5. Führen Sie über die **Arcserve UDP-Konsole** eine weitere Sicherung der SQL-Datenbank durch.

   Der Wiederherstellungspunkt N+1 wird erstellt.
6. Führen Sie in der Eingabeaufforderung ***set pitrestore=1*** aus.

   Die Wiederherstellung zu einem bestimmten Zeitpunkt ist aktiviert.
7. Führen Sie in der Eingabeaufforderung die folgenden SQL-Abfragen aus, um Zeitpunktangaben der Sicherungssitzung N+1 anzuzeigen:
   - *Query <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<Ordnername der Sicherungssitzung N+1>*

     Zeigt eine Zusammenfassung aller Zeitpunkte in Sicherung an.
8. Führen Sie in der Eingabeaufforderung ***set pittime="<MM/DD/YYYY HH:MM:SS:ss>"*** aus.

9. Führen Sie in der **Arcserve UDP-Konsole** eine Wiederherstellung auf Datenbankebene am ursprünglichen Speicherort unter Verwendung des Wiederherstellungspunkts N durch.

   Die Wiederherstellung zu einem bestimmten Zeitpunkt wurde erfolgreich abgeschlossen. Stellen Sie sicher, dass die erwarteten Daten in der Datenbank wiederhergestellt wurden.

Grundlegendes zum Point-In-Time-Befehlszeilenhilfsprogramm

Das Point-In-Time-Befehlszeilenhilfsprogramm steht unter dem Pfad *<Arcserve UDP Installed path>\BIN* mit dem Dateinamen *PIT.exe* zur Verfügung.

Die Eingabeaufforderung im Befehlszeilenhilfsprogramm ist **PIT$**.

Nachfolgend sind die verfügbaren Optionen aufgeführt, die Sie im Befehlszeilenhilfsprogramm ausführen können:

HELP

Zeigt alle Optionen an, die in PIT.exe zur Verfügung stehen.

COMMAND /?

Zeigt die Verwendung des Befehls an.

CONFIG

Verwendet die Einstellung in der Registrierung.

OPTION

Gibt die globale Option an. VALUE ist immer eine Hexadezimalzahl.

SEQ

Gibt die Sequenznummer in der DB/TLog-Sicherung.

TIMEOUT

Gibt das Verbindungs-Timeout in Sekunden an.

DEVICE

Gibt den Typ des Sicherungsgeräts an, das immer ein Datenträger ist.

DATABASE

Gibt den Namen der Datenbank an. Geben Sie den Wert im folgenden Format ein: *[server]\[instance]\<Datenbank>*.

LOGBACKUP

Gibt den Pfad der TLog-Sicherung an.

LOGRESTORE

Gibt den Pfad der TLog-Wiederherstellung an.

DBBACKUP

Gibt den Pfad der TLog-Sicherung an.

DBRESTORE

Gibt den Pfad der TLog-Wiederherstellung an.

CATALOG

Gibt den Pfad des Katalogs an.

STOPAT

Gibt den Zeitpunkt für die Wiederherstellung an.

NORECOVERY

Deaktiviert(1) oder aktiviert(0) die automatische Wiederherstellung nach der UDP-DB-Wiederherstellung.

PITBACKUP

Aktiviert(1) oder deaktiviert(0) die Sicherung zu einem bestimmten Zeitpunkt für UDP.

Beispiel: set pitbackup=1

PITRESTORE

Aktiviert(1) oder deaktiviert(0) die Wiederherstellung zu einem bestimmten Zeitpunkt für UDP.

Beispiel: *set pitrestore=1*

PITTEMP

Temporärer Ordner für die Wiederherstellung zu einem bestimmten Zeitpunkt

PITTIME

Gibt den Zeitpunkt für die Wiederherstellung zu einem bestimmten Zeitpunkt an.

Beispiel: set pittime="<MM/DD/YYYY HH:MM:SS:ss>

PITNOSTAGE

Gibt die Verwendung des Protokolls im geladenen Volume an, anstelle der Wiederherstellung in einen temporären Ordner.

BACKUPOPT

Gibt die Sicherungsoption für die Steuerung von VSS an.

RESTOREOPT

Gibt die Wiederherstellungsoption für die Steuerung von VSS an.

Nachfolgend sind die SQL-Abfragen aufgeführt, die Sie im Befehlszeilenhilfsprogramm ausführen können:

- *Query <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<Ordnername der Sicherungssitzung N+1>*

  Zeigt eine Zusammenfassung aller Zeitpunkte in Sicherung an.

- *Query /d <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<Ordnername der Sicherungssitzung N+1>*

  Zeigt alle Zeitpunktdetails in Sicherung an.

- *Query /i N <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<Ordnername der Sicherungssitzung N+1>*

  Zeigt eine Zeitpunktzusammenfassung von N in der Sicherung an.

- *Query /d /i N <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<Ordnername der Sicherungssitzung N+1>*

  Zeigt die Zeitpunktdetails von N in der Sicherung an.

So stellen Sie ein Cluster Shared Volume wieder her

Jedes Mal, wenn Arcserve UDP eine erfolgreiche Sicherung ausführt, wird gleichzeitig ein Snapshot-Image Ihrer Sicherung (ein Wiederherstellungspunkt) erstellt. Diese Sammlung an Wiederherstellungspunkten ermöglicht es Ihnen, das Sicherungs-Image, das Sie wiederherstellen möchten, zu finden und genau anzugeben. Wenn Sie zu einem späteren Zeitpunkt den Verdacht haben, dass gesicherte Informationen verloren gegangen, korrupt oder nicht zuverlässig sein könnten, können Sie diese Informationen suchen und aus einer früheren Version wiederherstellen, deren Qualität außer Frage steht.

Der nächste Schritt?

1. Überprüfen der Voraussetzungen und Hinweise
2. Festlegen der wiederherzustellenden CSV-Informationen
   a. Festlegen des wiederherzustellenden CSV und Inhalts
   b. Definieren der Wiederherstellungsoptionen
3. Wiederherstellen des CSV-Inhalts

Überprüfen der Voraussetzungen und Hinweise

Überprüfen Sie, dass die folgenden Voraussetzungen gegeben sind, bevor Sie eine Wiederherstellung ausführen:

- Sie haben mindestens einen Wiederherstellungspunkt zur Wiederherstellung zur Verfügung.
- Sie haben ein gültiges und zugreifbares Wiederherstellungspunktziel, von dem aus Sie den Inhalt des Wiederherstellungspunkts wiederherstellen können.
- Sie haben einen gültigen und zugreifbaren Zielspeicherort, auf dem Sie den Inhalt des Wiederherstellungspunkts wiederherstellen können.
- Überprüfen Sie die Kompatibilitätsmatrix, die die unterstützten Betriebssysteme, Datenbanken und Browser enthält.

Überprüfen Sie die folgenden Wiederherstellungshinweise:

- Wenn die Wiederherstellung auf einem Remote-Ziel erfolgt und alle Laufwerksbuchstaben (A – Z) besetzt sind, gelingt die Wiederherstellung auf einem Remote-Pfad nicht. Arcserve UDP Agent (Windows) benötigt einen Laufwerksbuchstaben, um den Pfad des Remote-Ziels zu laden.
- (Optional) Erfahren Sie, wie die Wiederherstellung funktioniert. Weitere Informationen erhalten Sie unter Funktionsweise von Wiederherstellungen auf Dateiebene.
- (Optional) Überprüfen Sie die Dateien, die während der Wiederherstellung übersprungen wurden. Weitere Informationen finden Sie unter "Dateien, die während der Wiederherstellung übersprungen wurden".
- Wenn Sie versuchen, eine optimierte Sicherungssitzung auf einem nichtleeren Volume (unoptimierte Wiederherstellung) wiederherzustellen, kann der Wiederherstellungsjob mehr Zeit kosten als die geschätzte Zeit, die im Job-Monitor angezeigt wird. Die Datenmenge, die bearbeitet wird, und die vergangene Zeit können größer werden auf der Basis der Daten, die auf dem Volume optimiert werden.

Beispiel:

Die Sicherungsvolumegröße beträgt 100 GB und nach Optimierung ist die Volumegröße auf 50 GB reduziert.

Wenn Sie eine unoptimierte Wiederherstellung dieses Volume ausführen, zeigt der Wiederherstellungsjob-Monitor 100 % an, nachdem er 50 GB wiederhergestellt hat, aber es dauert länger, um die ganzen 100 GB wiederherzustellen.

- Folgende Aktivitätsprotokollmeldung wird angezeigt, wenn die Systemdateien wiederhergestellt werden:

  "Systemdateien wurden übersprungen. Im Bedarfsfall können Sie die Option "Bare-Metal-Recovery (BMR)" verwenden, um sie wiederherzustellen."

Funktionsweise von Wiederherstellungen auf Dateiebene

Bei einer Sicherung auf Blockebene besteht jede gesicherte Datei aus mehreren erfassten Blöcken, die sie definieren. Zusätzlich wird eine Katalogdatei mit einer Liste der gesicherten Dateien, der einzelnen Blöcke, die für jede Datei verwendet wurden, und der Wiederherstellungspunkte, die für diese Datei zur Verfügung stehen, erstellt. Wenn Sie eine bestimmte Datei wiederherstellen möchten, können Sie Ihre Sicherung durchsuchen, um die Datei und den Wiederherstellungspunkt auszuwählen. Arcserve UDP erfasst die Versionen der Blöcke, die für den Wiederherstellungspunkt der ausgewählten Datei verwendet wurden, fasst sie zusammen und stellt die Datei wieder her.

Hinweis: Sie können auch Wiederherstellungen ohne Katalogdateien von katalogfreien Sicherungs-Wiederherstellungspunkten ausführen.

Das folgende Ablaufschema veranschaulicht den Prozess, mit dem Arcserve UDP eine spezifische Datei wiederherstellt:

Dateien, die während der Wiederherstellung übersprungen wurden

Bei Wiederherstellungen mit Arcserve UDP Agent (Windows) werden bestimmte Dateien möglicherweise absichtlich übersprungen.

Die Dateien und Ordner in der folgenden Tabelle werden während einer Wiederherstellung übersprungen, wenn die folgenden zwei Bedingungen vorhanden sind:

- Dateien werden übersprungen, wenn solche Dateien vor der Wiederherstellung vorhanden sind und die Konfliktoption "Vorhandene Dateien überspringen" ist.
- Dateien und Ordner, die in der folgenden Tabelle aufgelistet sind, werden übersprungen, weil sie keine wichtige Komponente für Windows oder Arcserve UDP Agent (Windows) sind.

BS	Ordner oder Speicherort	Datei oder Ordnername	Bemerkungen

Alle	Stammordner von jedem Volume	CAVolTrc.dat	Wird von dem Arcserve UDP-Treiber für die Nachverfolgung verwendet.
		cavoltrcsnapshot.dat	
		System Volume Information*	Wird verwendet, um Dateien/Ordner von einem Windows-System zu speichern, zum Beispiel Volume-Schattenkopie-Dateien.
		RECYCLER*	Wird nur auf NTFS-Partitionen verwendet. Es enthält einen Papierkorb für jeden Benutzer, der sich beim Computer anmeldet, sortiert nach Sicherheitskennung (SID).
		$Recycle.Bin*	Wenn Sie eine Datei in Windows NT Explorer oder im Arbeitsplatz löschen, dann wird die Datei im Papierkorb gespeichert, bis Sie den Papierkorb leeren oder die Datei wiederherstellen.
	Alle Ordner enthalten Bilddateien	Thumbs.db	Speichert Miniaturansicht -Bilder für Windows Explorer Miniaturansicht.
	Stammordner des Volume	PageFile.sys	Windows-Auslagerungsdatei des virtuellen Speichers.
		Hiberfil.sys	Ruhezustanddatei wird verwendet, um die Systemdaten zu speichern, wenn ein Computer in den Ruhezustand geht.

Die folgenden Dateien und Ordner werden nur übersprungen, wenn Sie eine Wiederherstellung am ursprünglichen Speicherort durchführen:

BS	Ordner oder Speicherort	Datei oder Ordnername	Bemerkung
Alle	Der Ordner ist im Wertdatensatz hier angegeben: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Alle Dateien/Ordner (rekursiv)	Der Ordner enthält eine zwischengespeicherte DLL-Datei, die für SFC (System File Checker) verwendet wird, und die Inhalte des Verzeichnisses des System-DLL-Cache werden mithilfe von SFC neu erstellt.
	%SystemRoot%\SYSTEM32\dllCache		
	Stammordner von quorum_device	MSCS*	Wird für Microsoft Cluster Server verwendet.

	%SystemRoot%\SYSTEM32\	perf?00?.dat	Leistungsdaten, die vom Windows-Leistungsindikator verwendet werden.
		perf?00?.bak	
		CATROOT*	Wird für WFP (Windows File Protection) verwendet. Es werden digitale Signaturen der Betriebssystem-installationen (wie z. B. DLL, EXE, SYS, OCX usw.) erfasst, um sie vor Löschung oder vor Ersatz von älteren Versionen zu schützen.
	%SystemRoot%\inetsrv\	metabase.bin	Binäre Metabasis-Datei von früheren IIS-Versionen vor 6.0.
	Datei oder Ordner, der im Wert angegeben ist, mit Ausnahme von "Gemeinsamer SIS-Speicher" unter "HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup"	Alle Dateien/Ordner (rekursiv)	Dateien und Ordner sollten nicht gesichert und nicht wiederhergestellt werden. Weitere Informationen finden Sie unter Link.
XP W2-003	System-Volume	NTLDR	Der Haupt-Boot-Loader.
		BOOT.INI	Enthält die Boot-Konfiguration (falls nicht vorhanden, wird NTLDR standardmäßig auf \Windows auf der ersten Partition der ersten Festplatte gesetzt).

		NTDETECT.COM	Ist erforderlich, um ein NT-basiertes BS zu starten. Erkennt grundlegende Hardware-Informationen, die für einen erfolgreichen Start erforderlich sind.
Vista und höher	Stammordner des System-Volume	boot*	Boot-Ordner für Windows.
		bootmgr	Datei "Windows-Start-Manager"
		EFI\Microsoft\Boot*	Wird für EFI-Boot verwendet.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Speichert ETW-Ablaufverfolgungsdateien (mit der Erweiterung .etl) für Ablaufverfolgungssitzungen der Ereignisse in Echtzeit.
		config\RegBack*	Sicherung der aktuellen Registrierungstabelle.
Win-8 und höher	System-Volume	swapfile.sys	Systemcontroller-Datei, normalerweise ca. 256 MB. Wird von Anwendungen im Metro-Stil verwendet, die nicht in die herkömmlichen Paging-Merkmale (wie z. B. Verwendungsmuster, Wachstum, Reser-

			vierung von Speicherplatz) von pagefile.sys passen.
		BOOTNXT	Wird verwendet, um von einem BS aus zu starten, das nicht Windows 8 ist. Wird erstellt, wenn die Startoptionen aktiviert werden, und wird von Windows aktualisiert.

Das Aktivitätsprotokoll stellt folgende Informationen bereit:

- Datums- und Uhrzeitinformationen: jobxxxx Systemdateien wurden übersprungen. Sie können bei Bedarf die Bare-Metal-Recovery-Option (BMR) verwenden, um sie wiederherzustellen.
- Datums- und Uhrzeitinformationen: jobxxxx Dateien oder Verzeichnisse wurden übersprungen. Übersprungene Dateien oder Verzeichnisse finden Sie hier: C:\Programme\Arcserve\Unified Data Protection\Engine\Logs\Restore-<JJJJMMTT>-<hhmmss>-<Prozess-ID>-<Job-ID>.log.

Festlegen der wiederherzustellenden CSV-Informationen

Arcserve UDP bietet eine Option zur Wiederherstellung von Daten von einem Wiederherstellungspunkt. Das Ziel eines Wiederherstellungsjobs besteht darin, schnell zu erkennen, welche Daten benötigt werden, und sie vom entsprechenden Sicherungsdatenträger abzurufen. Für jeden Wiederherstellungsjob ist eine Quelle und ein Ziel erforderlich.

Der nächste Schritt?

1. Festlegen des wiederherzustellenden CSV und Inhalts
2. Definieren der Wiederherstellungsoptionen

Festlegen des wiederherzustellenden CSV und Inhalts

Verwenden Sie die Option **Nach Wiederherstellungspunkten suchen**, um von einem Wiederherstellungspunkt aus wiederherzustellen. Wenn Sie ein Wiederherstellungsdatum auswählen und dann die Uhrzeit angeben, werden alle

zugeordneten Wiederherstellungspunkte für diesen Zeitraum angezeigt. Sie können die Inhalte (einschließlich Anwendungen) für die Wiederherstellung suchen und auswählen.

Gehen Sie wie folgt vor:

1. Verwenden Sie eine der folgenden Vorgangsweisen, um auf das Dialogfeld zur Auswahl der Wiederherstellungsmethoden zuzugreifen:

   Von der Arcserve UDP-Konsole:

   a. Melden Sie sich bei **Arcserve UDP** an.

   b. Klicken Sie auf die Registerkarte **Ressourcen**.

   c. Wählen Sie im linken Fensterbereich **Alle Knoten** aus.

      Alle hinzugefügten Server werden im mittleren Fensterbereich angezeigt.

   d. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf **Aktionen**.

   e. Klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

      Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

      Hinweis: Sie werden automatisch beim Agentenknoten angemeldet, und das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird im Agentenknoten geöffnet.

   Über Arcserve UDP Agent (Windows):

   a. Melden Sie sich bei Arcserve UDP Agent (Windows) an.

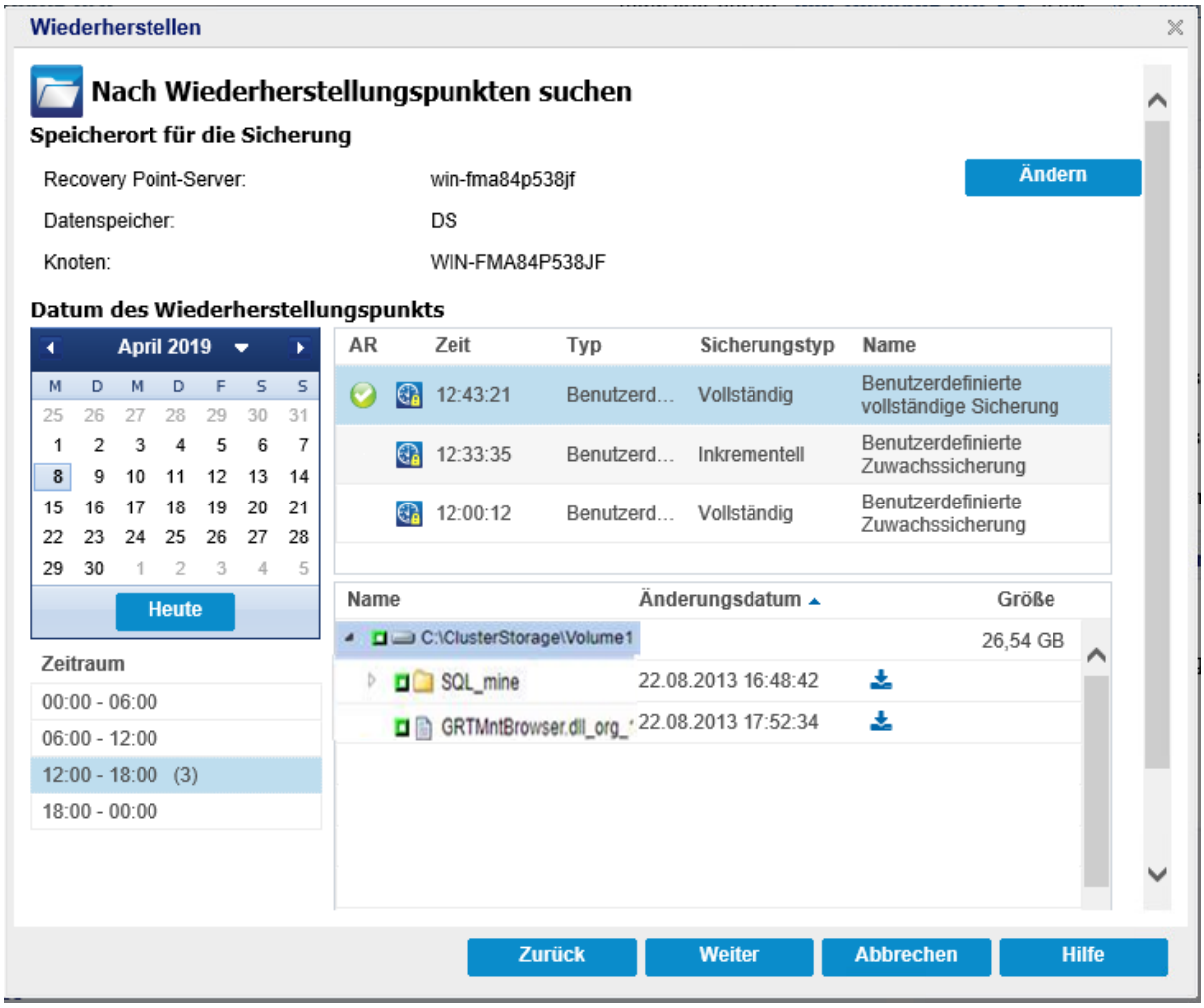
   b. Wählen Sie auf der Startseite **Wiederherstellen** aus.

   Das Dialogfeld zur Auswahl der Wiederherstellungsmethoden wird geöffnet.

2. Klicken Sie auf die Option **Nach Wiederherstellungspunkten suchen**.

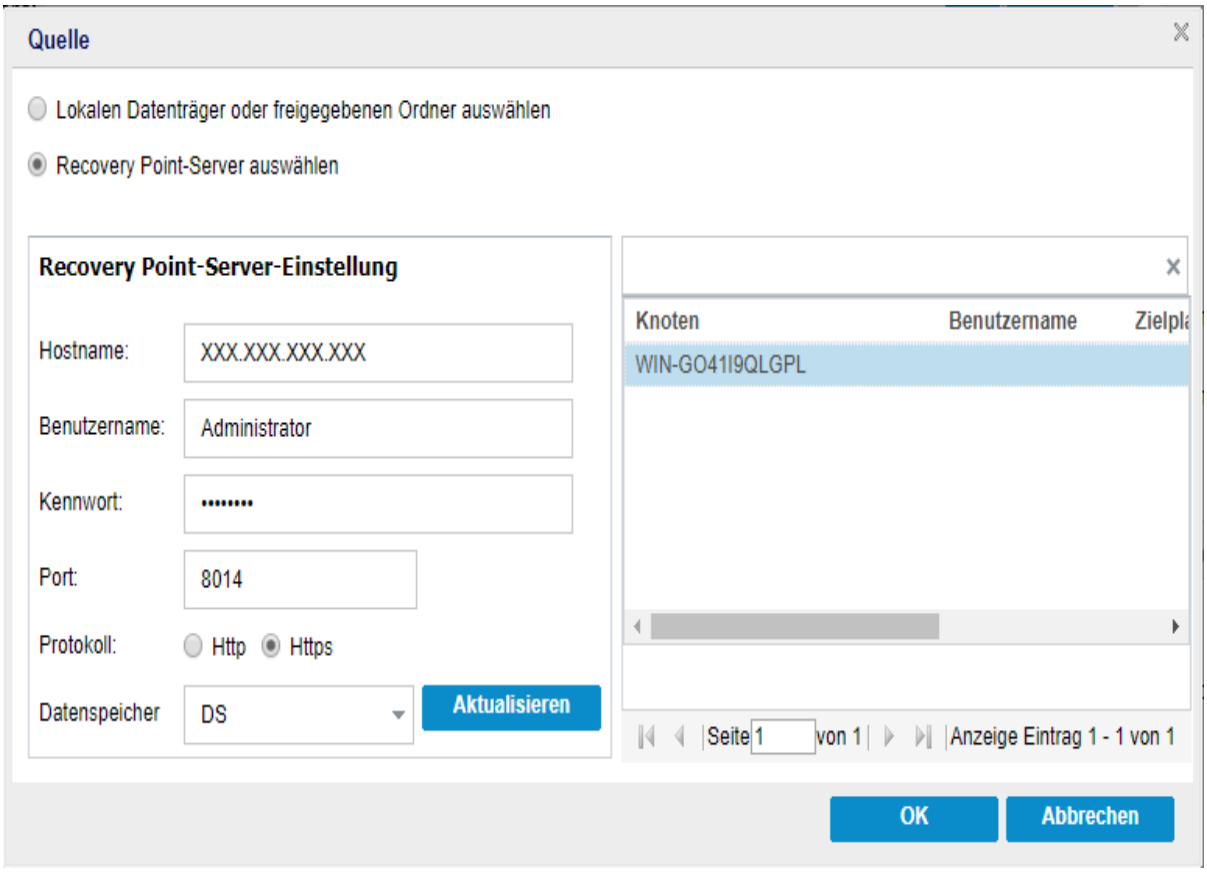
   Das Dialogfeld **Nach Wiederherstellungspunkten suchen** wird angezeigt. Die Details zum **Recovery Point Server** werden im **Sicherungsspeicherort** angezeigt.

   AR gibt das Ausführungsergebnis an, wenn Assured Recovery für die Sitzung ausgeführt wurde.



3. Klicken Sie auf **Ändern**, um den Speicherort für die Sicherung zu aktualisieren.

   Das Dialogfeld **Quelle**, in dem Sie den Sicherungsspeicherort auswählen können, wird geöffnet.



4. Wählen Sie eine der folgenden Quellen aus:

   Lokalen Datenträger oder freigegebenen Ordner auswählen

   a. Legen Sie den Speicherort fest, unter dem Ihre Sicherungs-Images gespeichert werden, und wählen Sie die entsprechende Sicherungsquelle aus.

      Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen. Wenn erforderlich, müssen Sie **Benutzernamen** und **Kennwort** angeben, um Zugriff auf diesen Quellspeicherort zu erhalten.

      Das Dialogfeld **Speicherort für die Sicherung auswählen** wird geöffnet.

   b. Wählen Sie den Ordner, in dem die Wiederherstellungspunkte gespeichert sind, aus, und klicken Sie auf **OK**.

      Das Dialogfeld **Speicherort für die Sicherung auswählen** wird geschlossen, und der Sicherungsspeicherort wird im Dialogfeld **Quelle** angezeigt.

   c. Klicken Sie auf **OK**.

      Die Wiederherstellungspunkte werden im Dialogfeld **Nach Wiederherstellungspunkten suchen** aufgelistet.

      Auswählen des Recovery Point-Servers

d. Geben Sie die Details für die Einstellungen des Recovery Point-Servers an, und klicken Sie auf **Aktualisieren**.

   Alle Agenten werden in der Spalte "Data Protection Agent" im Dialogfeld Quelle aufgelistet.

e. Wählen Sie den Agenten aus der angezeigten Liste aus, und klicken Sie auf **OK**.

   Die Wiederherstellungspunkte werden im Dialogfeld **Nach Wiederherstellungspunkten suchen** aufgelistet.

5. Geben Sie das Datum des Sicherungs-Images an, das Sie wiederherstellen möchten.

   Alle Daten, die Wiederherstellungspunkte für die angegebene Sicherungsquelle enthalten, werden grün hervorgehoben.

   Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp (vollständige Sicherung, Zuwachssicherung oder Überprüfungssicherung) und der Name der Sicherung angezeigt.

6. Wählen Sie einen wiederherzustellenden Wiederherstellungspunkt aus.

   Der Sicherungsinhalt (einschließlich aller Anwendungen) für die ausgewählten Wiederherstellungspunkte wird angezeigt.

   Hinweis: Wenn eine Uhr mit einem Schlosssymbol angezeigt wird, bedeutet dies, dass der Wiederherstellungspunkt verschlüsselte Informationen enthält und möglicherweise ein Kennwort zur Wiederherstellung benötigt wird.

7. Wählen Sie das CSV Volume für die Wiederherstellung aus.

   - Bei einer Wiederherstellung auf Volume-Ebene können Sie angeben, ob das gesamte Volume oder ausgewählte Dateien/Ordner wiederhergestellt werden sollen.
   - Bei einer Wiederherstellung auf Anwendungsebene können Sie festlegen, ob die gesamte Anwendung, oder ausgewählte Komponenten, Datenbanken, Instanzen etc. wiederhergestellt werden sollen.

8. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet.

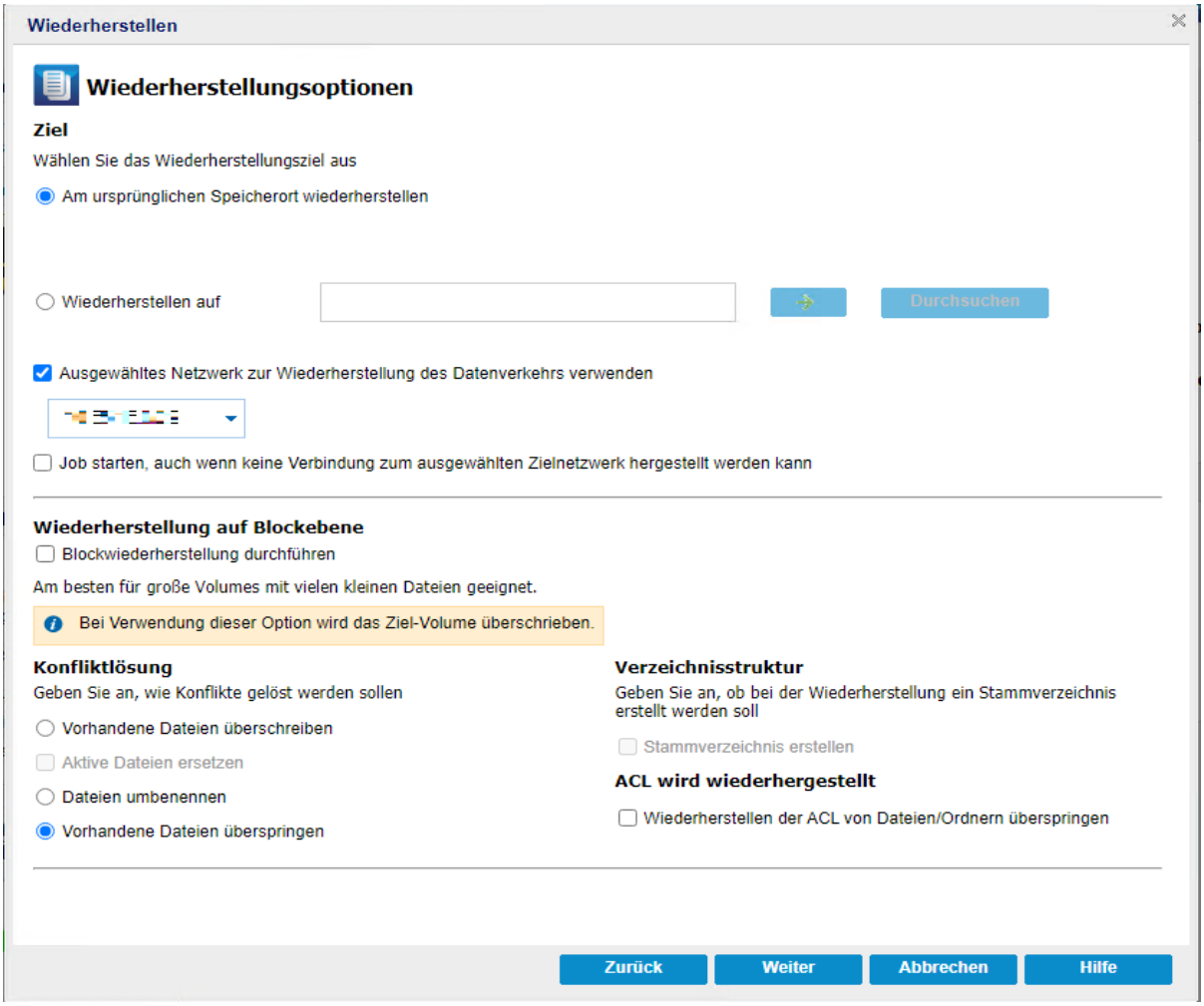
   Wiederherstellungspunkt und wiederherzustellender Inhalt werden festgelegt.

Definieren der Wiederherstellungsoptionen

Nachdem Sie Wiederherstellungspunkt und wiederherzustellenden Inhalt festgelegt haben, definieren Sie die Kopieroptionen für den ausgewählten Wiederherstellungspunkt.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld **Wiederherstellungsoptionen** das Wiederherstellungsziel aus.



Es sind folgende Zieloptionen verfügbar:

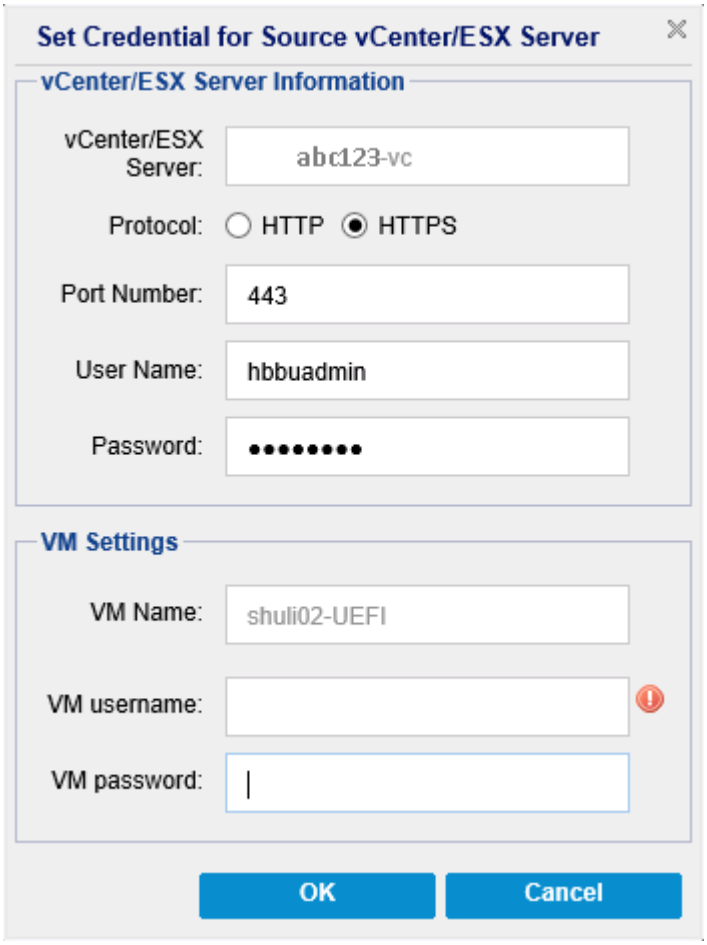
Am ursprünglichen Speicherort wiederherstellen

Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

Hinweis: Wenn Sie die Recovery Point-Sicherung mithilfe der hostbasierten agentenlosen Sicherung durchgeführt haben, wird die Datei bei der Wiederherstellung am ursprünglichen Speicherort auf dem virtuellen Rechner

wiederhergestellt. In diesem Fall wird ein Dialogfeld geöffnet. Sie können die Anmeldeinformationen des Hypervisors und des Betriebssystems des virtuellen Rechners eingeben.

Für VMware-VM:



Hinweis: Um Dateien innerhalb des virtuellen Rechners zu erstellen und schreiben zu können, beachten Sie die folgenden Anforderungen für die Einstellungen und die Kontoberechtigung des virtuellen Rechners:

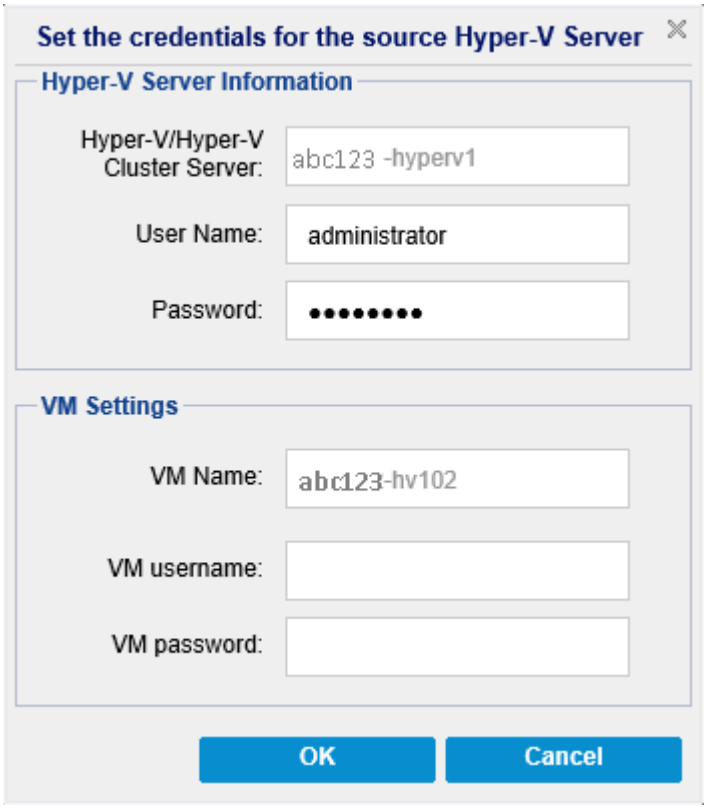
- VMware-Tools ist installiert und wird ausgeführt.
- Firewall muss Datei- und Druckerfreigabe zulassen.
- Das Konto ist ein integrierter lokaler Administrator, integrierter Domänenadministrator oder ein Domänenkonto, das Mitglied der lokalen Administratorengruppe ist. Wenn andere Konten verwendet werden:
  - Deaktivieren Sie den Remote-Zugriff auf UAC. Informationen zum Deaktivieren des Remote-Zugriffs auf UAC finden Sie in Importieren von virtuellen Rechnern mit einem zusätzlichen

Administratorkonto.

- Deaktivieren Sie UAC in der lokalen Sicherheitsrichtlinie, indem Sie die Einstellung zur Ausführung aller Administratoren im Administrator-Genehmigungsmodus unter secpol.msc-> lokale Richtlinien-> Sicherheitsoptionen deaktivieren. (Secpol.msc ist der Editor für Sicherheitsrichtlinien von Microsoft).

  Wichtig: Versuchen Sie nicht, die UAC im Dialogfeld "Einstellungen zur Benutzerkontensteuerung" zu deaktivieren, das über die Systemsteuerung geöffnet wird.

Für Hyper-V-VM:



Hinweis: Um Dateien innerhalb des virtuellen Rechners zu erstellen und schreiben zu können, beachten Sie die folgenden Anforderungen für die Einstellungen und die Kontoberechtigung des virtuellen Rechners:

- Hyper-V-Integrationsdienste sind installiert und werden ausgeführt.
- Firewall muss Datei- und Druckerfreigabe zulassen.

- Das Konto ist ein integrierter lokaler Administrator, integrierter Domänenadministrator oder ein Domänenkonto, das Mitglied der lokalen Administratorengruppe ist. Wenn andere Konten verwendet werden:

  Deaktivieren Sie den Remote-Zugriff auf UAC. Informationen zum Deaktivieren des Remote-Zugriffs auf UAC finden Sie in Importieren von virtuellen Rechnern mit einem zusätzlichen Administratorkonto.

- Wenn das VM-Gast-BS Clientversion-Windows (z. B. Windows 10) ist, muss Firewall manuell so konfiguriert werden, dass Windows-Verwaltungsinstrumentation (WMI) zugelassen wird.

Wiederherstellen auf

Stellt am angegebenen Speicherort wieder her. Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.

2. Legen Sie die Option für die **Konfliktlösung** fest, die von Arcserve UDP ausgeführt werden soll, wenn während der Wiederherstellung Konflikte auftreten.

   Es sind folgende Optionen verfügbar:

   Vorhandene Dateien überschreiben

   Überschreibt (ersetzt) alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind. Alle Objekte werden aus den Sicherungsdateien wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.

   Aktive Dateien ersetzen

   Ersetzt alle aktiven Dateien nach einem Neustart. Wenn der Arcserve UDP Agent (Windows) während des Wiederherstellungsversuchs feststellt, dass die vorhandene Datei derzeit verwendet wird, wird diese nicht sofort ersetzt. Um Probleme zu vermeiden, wird das Ersetzen der aktiven Dateien stattdessen verzögert, bis der Computer das nächste Mal gestartet wird. Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt.

   Diese Option ist nur verfügbar, wenn Sie die Option **Vorhandene Dateien überschreiben** auswählen.

   Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien im Wiederherstellungsprozess übersprungen.

   Dateien umbenennen

Erstellt eine neue Datei, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit demselben Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten sind dann in einer neuen Datei wiederhergestellt.

Vorhandene Dateien überspringen

Überspringt alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, und überschreibt (ersetzt) sie nicht. Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

Standard: Vorhandene Dateien überspringen

3. Geben Sie die **Verzeichnisstruktur** an, um während der Wiederherstellung ein Stammverzeichnis zu erstellen.

Stammverzeichnis erstellen

Legt fest, dass Arcserve UDP eine ggf. vorhandene Stammverzeichnisstruktur des erfassten Sicherungs-Images im Zielpfad der Wiederherstellung neu erstellt.

Wenn diese Option nicht ausgewählt wird, wird die Datei oder der Ordner direkt im Zielordner wiederhergestellt.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt" und "C:\Ordner1\Unterordner2\B.txt" erfasst und als Wiederherstellungsziel "D:\Wiederherstellen" ausgewählt.

- Wenn Sie die Wiederherstellung der Dateien "A.txt" und "B.txt" einzeln festgelegt haben, werden die Dateien in "D:\Wiederherstellen\A.txt" und "D:\Wiederherstellen\B.txt" wiederhergestellt (das Stammverzeichnis über der ausgewählten Dateiebene wird nicht wiederhergestellt).
- Wenn Sie eine Wiederherstellung auf "Unterordner2"-Ebene auswählen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Unterordner2\A.txt" und "D:\Wiederherstellen\Unterordner2\B.txt" (das Stammverzeichnis über der ausgewählten Ordnerebene wird nicht wiederhergestellt).

Wenn diese Option ausgewählt ist, wird der gesamte Stammverzeichnispfad für die Dateien/Ordner (einschließlich des Volume-Namens) im Zielordner neu erstellt. Wenn Dateien/Ordner vom selben Volume-Name wiederhergestellt werden sollen, ist dieser Volume-Name nicht im Wiederherstellungsziel-Stammverzeichnispfad enthalten. Wenn Dateien/Ordner von einem anderen Volume-Name wiederhergestellt werden sollen, enthält der Wiederherstellungsziel-Stammverzeichnispfad diesen Volume-Namen.

Beispiel: Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt", "C:\Ordner1\Unterordner2\B.txt" und E:\Ordner3\Unterordner4\C.txt erfasst, und bei der Wiederherstellung "D:\Wiederherstellen" als Wiederherstellungsziel ausgewählt.

- Wenn Sie nur die Datei "A.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Ordner1\Unterordner2\A.txt" (das gesamte Stammverzeichnis wird ohne den Volume-Namen erneut erstellt).
- Wenn Sie die Dateien "A.txt" und "C.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\C\Ordner1\Unterordner2\A.txt" und "D:\Wiederherstellen\ E\Ordner3\Unterordner4\C.txt" (das gesamte Stammverzeichnis wird mit dem Volume-Namen erneut erstellt).

4. Wählen Sie unter **ACL wird wiederhergestellt** die Option **Wiederherstellen der ACL von Dateien/Ordnern überspringen** aus, um die ursprüngliche Berechtigung für die wiederhergestellten Dateien/Ordner zu überspringen. Bei Auswahl der Option können Sie stattdessen die Berechtigungen des Zielordners erben. Wenn Sie die Option nicht auswählen, werden die ursprünglichen Berechtigungen beibehalten.
5. Wenn die Daten, die Sie wiederherstellen möchten, verschlüsselt sind, geben Sie bei Bedarf das **Verschlüsselungskennwort der Sicherung** an.

   Es ist kein Kennwort erforderlich, wenn Sie versuchen, die Wiederherstellung über denselben Arcserve UDP Agent (Windows)-Rechner durchzuführen, auf dem die verschlüsselte Sicherung ausgeführt wurde. Wenn Sie jedoch versuchen, die Wiederherstellung über einen anderen Arcserve UDP Agent (Windows)-Rechner durchzuführen, ist ein Kennwort erforderlich.

   Hinweis: Wenn eine Uhr mit einem Schlosssymbol angezeigt wird, bedeutet dies, dass der Wiederherstellungspunkt verschlüsselte Informationen enthält und möglicherweise ein Kennwort zur Wiederherstellung benötigt wird.
6. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Wiederherstellungsübersicht** wird geöffnet.

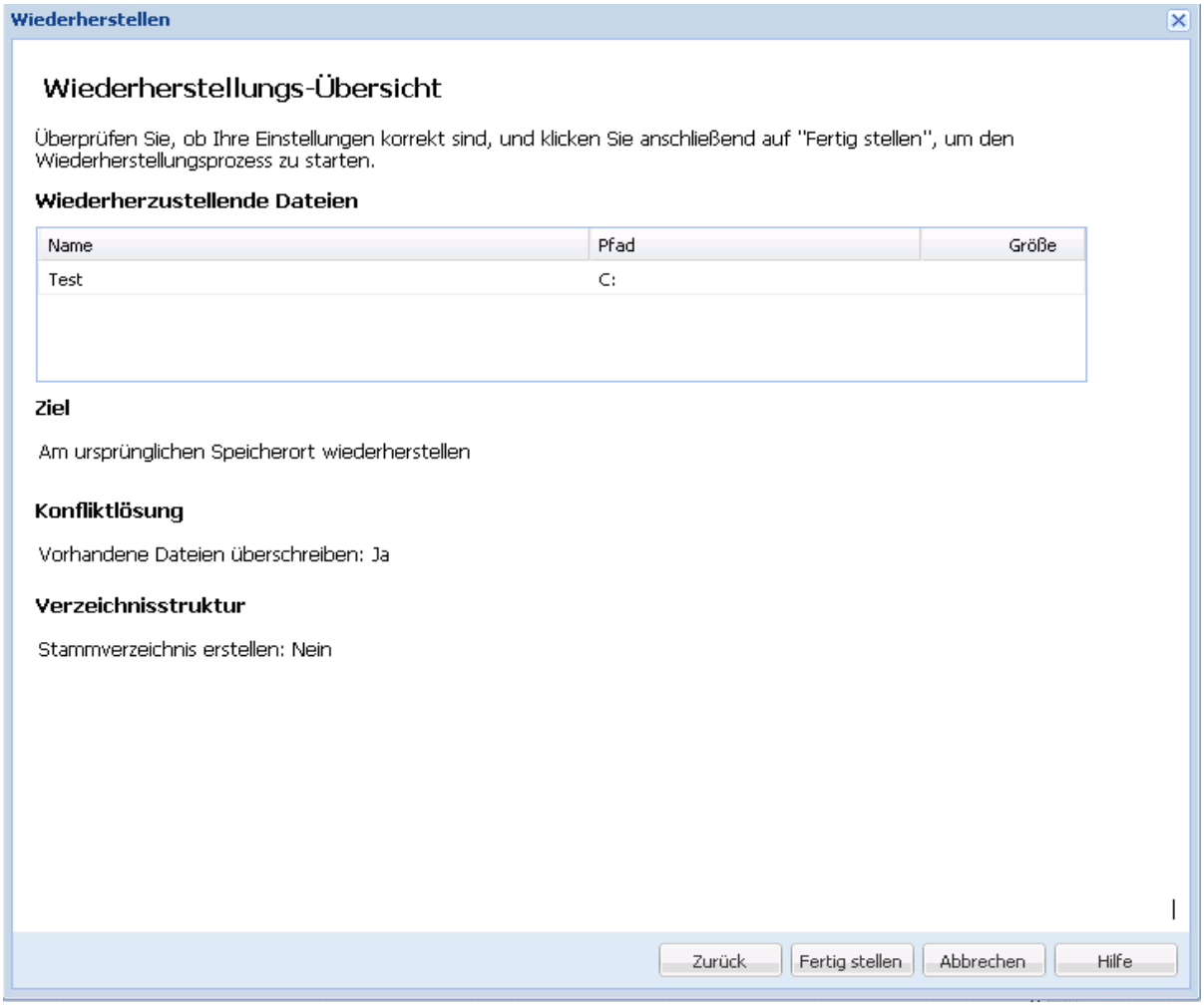
   Die Wiederherstellungsoptionen sind für die Wiederherstellung von einem Wiederherstellungspunkt aus festgelegt.

Wiederherstellen des CSV-Inhalts

Nachdem Sie die Wiederherstellungsoptionen definiert haben, überprüfen Sie, dass Ihre Einstellungen korrekt sind, und bestätigen Sie den Wiederherstellungsprozess. Die **Wiederherstellungsübersicht** ist hilfreich, um sämtliche Wiederherstellungsoptionen, die Sie festgelegt haben, zu überprüfen und bei Bedarf zu ändern.

Gehen Sie wie folgt vor:

1. Überprüfen Sie die Informationen im Dialogfeld **Wiederherstellungsübersicht**, um die Richtigkeit aller Wiederherstellungsoptionen und Einstellungen sicherzustellen.



- Wenn die Übersichtsinformationen Fehler enthalten, klicken Sie auf **Zurück**, und ändern Sie die inkorrekten Einstellungen im entsprechenden Dialogfeld.
- Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf **Fertig stellen**, um den Wiederherstellungsprozess zu starten.

Der Wiederherstellungspunktinhalt wurde wiederhergestellt.

Kapitel 2: Verwalten von Bandsicherung und -wiederherstellung

Mit Arcserve UDP können Sie Daten auf einem Band sichern und die gesicherten Daten vom Band auf einem Knoten wiederherstellen.

In diesem Abschnitt werden die folgenden Themen behandelt:

So sichern Sie Deduplizierungsdatenspeicher auf einem Band

Verwenden Sie die folgenden Methoden, um einen Deduplizierungsdatenspeicher auf einem Band zu sichern:

- Sichern Sie UDP-Knoten auf Band. Weitere Informationen finden Sie im Abschnitt Methode 1: Sichern der neuesten UDP-Sicherungssitzung auf Band im Arcserve Backup-Administrationshandbuch.
- Sichern Sie Arcserve UDP-Daten aus Datenspeichern. Weitere Informationen finden Sie im Abschnitt Methode 2: Sichern von Arcserve-UDP-Daten aus Datenspeichern im Arcserve Backup-Administrationshandbuch.

So stellen Sie einen Deduplizierungsdatenspeicher von einem Band wieder her

Wenn Sie bereits einen Deduplizierungsdatenspeicher von einem Recovery Point Server (RPS) auf einem Bandgerät gesichert haben, können Sie den Datenspeicher wiederherstellen. Für diesen Vorgang werden Arcserve Backup und Arcserve UDP in Verbindung miteinander verwendet, um einen Deduplizierungsdatenspeicher von einem Band wiederherzustellen. Arcserve Backup wird verwendet, um ihn vom Band an einem angegebenen Ziel wiederherzustellen, und dann wird Arcserve UDP verwendet, um ihn an einen RPS zu importieren.

Die folgenden zwei Prozesse sind am Wiederherstellungsprozess beteiligt:

1. Der erste Prozess verwendet Arcserve Backup, um die Sitzungen vom Bandmedium auf einem Volume wiederherzustellen. Es wird empfohlen, die Sitzungen an einem alternativen Standort wiederherzustellen.
2. Der zweite Prozess verwendet Arcserve UDP, um den wiederhergestellten Datenspeicher an den RPS zu importieren.

   Hinweis: Sie müssen den **Sicherungszielordner** des Deduplizierungsdatenspeichers angeben, wenn Sie den Speicherort während des Imports durchsuchen.

   Das folgende Diagramm veranschaulicht, wie ein Arcserve-Deduplizierungsdatenspeicher von einem Band wiederhergestellt wird:

Der nächste Schritt?

1. Überprüfen der Voraussetzungen
2. Wiederherstellen von einem Band an einem alternativen Speicherort
3. Wiederhergestellten Datenspeicher an den RPS importieren

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie mit der Wiederherstellung beginnen:

- Sie müssen einen RPS-Datenspeicher auf dem Band gesichert haben.
- Sie müssen bei Bedarf das Sitzungskennwort eingeben.
- Sie müssen den Benutzernamen und das Kennwort für das Wiederherstellungsziel angeben.

Wiederherstellen von einem Band an einem alternativen Speicherort

Um die Sitzung vom Banddatenträger an einem alternativen Speicherort wiederherzustellen, müssen Sie Arcserve Backup Manager verwenden.

Wenn die Wiederherstellung erfolgreich war, können Sie dann die wiederhergestellten Datenspeicher mit Arcserve UDP an den RPS importieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich über Arcserve Backup beim Arcserve Backup-Manager an.
2. Klicken Sie im Navigationsbereich **Schnellstart** auf **Wiederherstellen**, und wählen Sie dann im mittleren Bereich die Registerkarte **Quelle**.
3. Wählen Sie im Drop-Down-Menü **Wiederherstellung nach Sitzung**, und wählen Sie die Sitzung, die Sie wiederherstellen möchten.
4. Klicken Sie auf die Registerkarte **Ziel**.
5. Deaktivieren Sie das Kontrollkästchen **Dateien am ursprünglichen Speicherort wiederherstellen**.
6. Erweitern Sie **Windows-Systeme** und navigieren Sie zu dem Speicherort, an dem Sie wiederherstellen möchten.
7. Klicken Sie auf die Registerkarte **Ablaufplan**, und wählen Sie **einmal** für die Option **Wiederholungsmethode**.
8. Klicken Sie auf **Übergeben**.

   Das Dialogfeld **Datenträger wiederherstellen** wird angezeigt.
9. Überprüfen Sie den Wiederherstellungsdatenträger, und klicken Sie auf **OK**.

   Das Dialogfeld **Benutzername und Kennwort der Sitzung** wird angezeigt.
10. Geben Sie den Benutzernamen und das Kennwort für den Wiederherstellungsspeicherort und das Sitzungskennwort für die Wiederherstellungspunkte an, falls erforderlich.
11. Klicken Sie auf **OK**.

    Das Dialogfeld "**Job übergeben**" wird angezeigt.
12. Geben Sie die erforderlichen Informationen im Dialogfeld **Job übergeben** ein, und klicken Sie auf **OK**.

    Der Wiederherstellungsjob wird übergeben.

    Nachdem der Wiederherstellungsjob abgeschlossen ist, werden Arcserve UDP-Datenspeicherdateien am Speicherort angezeigt, den Sie angegeben haben.

Wiederhergestellten Datenspeicher an den RPS importieren

Um den wiederhergestellten Datenspeicher an den RPS zu importieren, müssen Sie die Arcserve UDP-Konsole verwenden. Mit der Funktion **Datenspeicher importieren** können Sie einen Datenspeicher zum Recovery Point Server hinzufügen. Sie können alle vorhandenen Datenspeicher zu einem Recovery Point Server importieren.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird angezeigt.
3. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf einen Recovery Point Server.
   - Wählen Sie einen Recovery Point Server aus, und klicken Sie im mittleren Menü auf die Drop-down-Liste **Aktionen**.
4. Klicken Sie auf **Datenspeicher importieren**.

   Die Seite **Datenspeicher importieren** wird angezeigt.
5. Führen Sie folgende Aktionen durch, und klicken Sie auf **Weiter**:
   a. Klicken Sie auf **Durchsuchen** und wählen Sie den **Ordner des Sicherungsziels** aus, aus dem Sie den Datenspeicher importieren möchten.
   b. Wenn erforderlich, geben Sie das **Verschlüsselungskennwort** ein.

      Hinweis: Wenn der Datenspeicher nicht verschlüsselt ist, können Sie dieses Feld leer lassen.

   Nach der Authentifizierung des **Ordners des Sicherungsziels** wird die Seite **Datenspeicher importieren** angezeigt. Sie enthält die Details zum Datenspeicher.

   Hinweis: Das Importieren des wiederhergestellten Datenspeichers wird nicht unterstützt, wenn sich der ursprüngliche Datenspeicher im selben RPS befindet. Sie müssen den ursprünglichen Datenspeicher löschen, bevor Sie den wiederhergestellten Datenspeicher importieren, oder Sie müssen den Datenspeicher alternativ dazu den Datenspeicher auf einen anderen RPS importieren.
6. Bei Bedarf ändern Sie die Datenspeicherdetails, und klicken Sie auf **Speichern**.

Wenn der wiederhergestellte Datenspeicher importiert wird, liest Arcserve UDP weiter die Index-, Hash- und Datenziele aus den Konfigurationseinstellungen des Datenspeichers und zeigt die tatsächlichen Pfade, unter denen sich der Datenspeicher ursprünglich befand. Nachdem der Importvorgang abgeschlossen ist, müssen diese Pfadziele in die neuen wiederhergestellten Pfade geändert werden.

Hinweis: Sie können die Verschlüsselungsoption für vorhandene Datenspeicher nicht aktivieren oder deaktivieren.

Der Datenspeicher wird zum Recovery Point Server hinzugefügt und im Dialogfeld **Ziele: Recovery Point Server** angezeigt.

Nach erfolgreichem Abschluss des Importvorgangs wird ein grünes Häkchen neben dem entsprechenden Namen des Datenspeichers angezeigt.

Sie haben erfolgreich einen Deduplizierungsdatenspeicher von einem Band wiederhergestellt.

Kapitel 3: Verwenden der PowerShell-Schnittstelle

In diesem Abschnitt werden die folgenden Themen behandelt:

So verwenden Sie die PowerShell-Schnittstelle

Arcserve UDP verfügt über PowerShell-Funktionen, die es Ihnen ermöglichen, einen Sicherungsjob zu übergeben, eine Wiederherstellung durchzuführen und über die Befehlszeile eine VM wiederherzustellen. Die PowerShell-Schnittstelle heißt UDPPowerCLI.ps1.

Überprüfen der Voraussetzungen

Überprüfen Sie folgende Voraussetzungen, bevor Sie die PowerShell-Schnittstelle verwenden:

- Sie müssen über Windows 2008 R2 Server oder eine höhere Version verfügen.
- Auf Ihrem Server muss PowerShell 3 oder höher installiert sein.

Verwenden der PowerShell-Schnittstelle für Arcserve UDP

Das Hilfsprogramm PowerShell ist in die Installationsdatei von Arcserve UDP eingebunden.

Bei der Installation von Arcserve UDP wird die Datei normalerweise am folgenden Speicherort installiert:

C:\Programme\Arcserve\Unified Data Protection

In solchen Fällen auf der Konsole wird UDPPowerCLI.ps1 an folgendem Speicherort installiert:

C:\Programme\Arcserve\Unified Data Protection\Management\PowerCLI

Auf RPS oder Agent wird UDPPowerCLI.ps1 an folgendem Speicherort installiert:

C:\Programme\Arcserve\Unified Data Protection\Engine\PowerCLI

Hilfe bei der Nutzung der PowerShell-Schnittstelle erhalten Sie über folgende Optionen:

- Aktualisieren Sie die PowerShell Ausführungsrichtlinie, um Skripte ausführen zu können. Sie können z. B. die Ausführungsrichtlinie auf **Set-ExecutionPolicy RemoteSigned** aktualisieren.

  Hinweis: Weitere Informationen zum Ändern der Ausführungsrichtlinie finden Sie auf der Website von Microsoft.

- Führen Sie den folgenden PowerShell-Befehl, um die detaillierten Hilfemeldungen und Beispiele für die Skripts zu erhalten:

  ```
  Auf der Konsole:
  ```

  Hilfe erhalten Sie unter: C:\Programme\Arcserve\Unified Data Protection\Management\PowerCLI\UDPPowerCLI.ps1' -full

  Auf RPS oder Agent:

  Hilfe erhalten Sie unter: C:\Programme\Arcserve\Unified Data Protection\Engine\PowerCLI\UDPPowerCLI.ps1' -full

PowerShell-Syntax und -Parameter

SYNTAX 1

```
UDPPowerCLI.ps1 -Command <CreatePswFile> -Password
<System.Security.SecureString> -PasswordFile <string>
[<CommonParameters>]
```

SYNTAX 2

```
UDPPowerCLI.ps1 -Command <Backup> [-UDPC-
onsoleServerName <String>] [-UDPConsoleProtocol <{htt-
p|https}>] [-UDPConsolePort <int>] [-
UDPConsoleUserName [<String>]] [-UDPConsolePassword
<System.Security.SecureString>] [-UDPC-
onsolePasswordFile <String>] [-UDPConsoleDomainName
<String>] -planName <String> -nodeName <String> [-
backupJobType <String>] [-jobDescription <String>] [-
waitJobFinish <String String>] [-timeOut <int>] [-
jobType <{ agentbase|agentless|uncpath} String>] [-
backupScheduleType <String>] [<CommonParameters>]
```

SYNTAX 3

```
UDPPowerCLI.ps1 -Command <Restore> [-UDPC-
onsoleServerName <String>] [-UDPConsoleProtocol
<String>] [-UDPConsolePort <int>] [-UDPConsoleUserName
<String>] [-UDPConsolePassword <Sys-
tem.Security.SecureString>] [-UDPConsolePasswordFile
<String>] [-UDPConsoleDomainName <String>] [-UDPA-
gentServerName <String>] [-UDPAgentProtocol <String>]
[-UDPAgentPort <int>] [-UDPAgentUserName <String>] [-
UDPAgentPassword <System.Security.SecureString>] [-
UDPAgentPasswordFile <String>] [-UDPAgentDomainName
<String>] [-RestoreDirectoryPath <String>] [-Resto-
reFilePath <String>] [-BackupSessionNumber <int>] [-
VmName <String>] -RestoreDestination <String> [-Resto-
reDestinationUserName <String>] [-Resto-
reDestinationPassword <System.Security.SecureString>]
[-CreateRootFolder <String>] [-ChangeFileName
<String>] [-ReplaceActiveFilesFlag <String>] [-Over-
writeExistFiles <String>] [<CommonParameters>]
```

SYNTAX 4

```
UDPPowerCLI.ps1 -command <RecoverVM> [-UDPC-
onsoleServerName <String>] [-UDPConsoleProtocol
<String>] [-UDPConsolePort <int>] [-UDPConsoleUserName
<String>] [-UDPConsolePassword <Sys-
tem.Security.SecureString>] [-UDPConsolePasswordFile
```

```
<String>] [-UDPConsoleDomainName <String>] [-UDPA-
gentServerName <String>] [-UDPAgentProtocol <String>]
[-UDPAgentPort <int>] [-UDPAgentUserName <String>] [-
UDPAgentPassword <System.Security.SecureString>] [-
UDPAgentDomainName <String>] [-UDPAgentPasswordFile
<String>] [-BackupSessionNumber <int>] -RecoverVmName
<String> [-OverwriteExistingVM <String>] [-PoweronVM
<String>] [<CommonParameters>]
```

BESCHREIBUNG

Ein Hilfsprogramm zum Verbinden mit dem Arcserve UDP-Konsolendienst sowie zur Übermittlung von Sicherungs- und Wiederherstellungsjobs.

PARAMETER

-Command <String>

Gibt den Befehl an, der verwendet wird. Derzeit werden folgende Zeichenfolgen unterstützt:

- CreatePswFile
- Sichern
- Datenbank
- RecoverVM

Erforderlich? **True**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-Password <System.Security.SecureString>

Gibt das Kennwort an, das Sie für die Erstellung der Kennwortdatei verwenden möchten.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPConsoleServerName <String>

Gibt den DNS-Namen des UDP-Servers (des Servers, auf dem Sie die Konsole installiert haben) an, zu dem Sie eine Verbindung herstellen möchten. Wenn dieser Wert nicht angegeben wird, verwendet das Cmdlet den Standardwert bzw. den DNS-Namen des lokalen Rechners.

Erforderlich? **false**

Position? **benannt**

Standardwert **$env: COMPUTERNAME**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPConsolePort <int>

Geben Sie die Portnummer an, die Sie für die Verbindung verwenden möchten. Wenn dieser Wert nicht angegeben wird, verwendet das Cmdlet den Standardwert von 8015.

Erforderlich? **false**

Position? **benannt**

Standardwert **8015**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPConsoleProtocol <String>

Gibt das Protokoll auf dem Server an, das Sie für die Verbindung verwenden möchten. Das Protokoll kann entweder http oder https sein. Wenn dieser Wert nicht angegeben wird, verwendet das Cmdlet den Standardwert http.

Erforderlich? **false**

Position? **benannt**

Standardwert **http**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPConsoleUserName <String>

Gibt den Benutzernamen an, den Sie für die Kommunikation mit dem UDP-Server verwenden möchten. Wenn der Benutzername nicht angegeben ist, verwendet das Cmdlet den Benutzernamen an, der derzeit für die Anmeldung beim System verwendet wird.

Erforderlich? **false**

Position? **benannt**

Standardwert **$env:UserName**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPConsolePassword <System.Security.SecureString>

Gibt das Kennwort an, das Sie für die Verbindung zum UDP-Server verwenden möchten.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-PasswordFile <String>

Legt fest, die Kennwortdatei zu generieren.

Erforderlich? **True**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPConsolePasswordFile <String>

Gibt die UDP-Kennwortdatei an, die Sie für die Verbindung zum UDP-Server verwenden möchten.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPAgentServerName <String>

Gibt den DNS-Namen des UDP-Agentenservers an, zu dem Sie für die Wiederherstellung eine Verbindung herstellen möchten.

Erforderlich? **false**

Position? **benannt**

Standardwert **$env: COMPUTERNAME**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPAgentProtocol <String>

Gibt das Internetprotokoll an, das Sie für die Verbindung zum UDP-Agentenserver verwenden möchten. Dies kann entweder http oder https sein. Wenn dieser Wert nicht angegeben wird, verwendet das Cmdlet den Standardwert http.

Erforderlich? **false**

Position? **benannt**

Standardwert **http**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPAgentPort <int>

Gibt die Portnummer an, die Sie für die Verbindung zum UDP-Agentenserver verwenden möchten. Wenn dieser Wert nicht angegeben wird, verwendet das Cmdlet den Standardwert von 8014.

Erforderlich? **false**

Position? **benannt**

Standardwert **8014**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPAgentUserName <String>

Gibt den Benutzernamen an, den Sie für die Verbindung zum UDP-Agentenserver verwenden möchten. Wenn der Benutzername nicht angegeben ist, verwendet das Cmdlet den Benutzernamen an, der derzeit für die Anmeldung beim System verwendet wird.

Erforderlich? **false**

Position? **benannt**

Standardwert **$env:UserName**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPAgentPassword <System.Security.SecureString>

Gibt das Kennwort an, das Sie für die Verbindung zum UDP-Agentenserver verwenden möchten.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPAgentPasswordFile <String>

Gibt das UDP-Agenten-Kennwort an, das Sie für die Verbindung zum UDP-Agentenserver verwenden möchten.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPAgentDomainName <String>

Gibt den Namen der Domäne an, in der sich der angegebene UDP-Agent-Benutzer befindet.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-NodeName <String>

Wählen Sie den Namen des zu sichernden Knotens aus.

Erforderlich? **True**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-RestoreFilePath <String>

Gibt die Datei an, die Sie wiederherstellen möchten.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-RestoreDirectoryPath <String>

Gibt das Verzeichnis an, das Sie wiederherstellen möchten.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-BackupSessionNumber <int>

Gibt die Sitzungsnummer an, die für die Wiederherstellung verwendet werden soll.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-VmName <String>

Gibt den Hostnamen eines virtuellen Rechners für das Wiederherstellen von Dateien oder Verzeichnissen aus der Sicherungssitzung an.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-RestoreDestination <String>

Gibt den Pfad des Verzeichnisses an, in dem die Dateien wiederhergestellt werden.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-RestoreDestinationUserName <String>

Gibt den Benutzernamen des Zielrechners an, auf dem Sie die Daten wiederherstellen möchten. Der Benutzername gehört zu dem Benutzer, der sich auf dem Zielrechner anmelden kann.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-RestoreDestinationPassword <System.Security.SecureString>

Gibt das Kennwort an, das Sie für die Anmeldung am Zielrechner verwenden.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-CreateRootFolder <String>

Legt fest, dass Arcserve UDP die Stammverzeichnisstruktur des erfassten Sicherungs-Images, soweit vorhanden, am Zielpfad wiederherstellt. Wenn diese Option nicht ausgewählt wird, wird die Datei oder der Ordner direkt im Zielordner wiederhergestellt. Sie können eine der folgenden Zeichenfolgen verwenden:

- True
- False

Erforderlich? **false**

Position? **benannt**

Standardwert **False**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-ChangeFileName <String>

Erstellt eine neue Datei, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit demselben Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten sind dann in einer neuen Datei wiederhergestellt. Sie können eine der folgenden Zeichenfolgen verwenden:

- True
- False

Erforderlich? **false**

Position? **benannt**

Standardwert **False**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-ReplaceActiveFilesFlag <String>

Ersetzt alle aktiven Dateien nach einem Neustart. Wenn Arcserve Unified Data Protection Agent für Windows während eines Wiederherstellungsversuchs entdeckt, dass die vorhandene Datei derzeit verwendet oder auf sie zugegriffen wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt). Diese Option ist nur verfügbar, wenn der Parameter **OverwriteExistingFiles** True ist. Sie können eine der folgenden Zeichenfolgen verwenden:

- True
- False

Erforderlich? **false**

Position? **benannt**

Standardwert **False**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-OverwriteExistingFiles <String>

Überschreibt (ersetzt) alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind. Alle Objekte werden aus den Sicherungsdateien

wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind. Sie können eine der folgenden Zeichenfolgen verwenden:

- True
- False

Erforderlich? **false**

Position? **benannt**

Standardwert **False**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-UDPConsoleDomainName <String>

Gibt den Namen der Domäne an, in der sich der angegebene Benutzer befindet. Wenn dieser Wert nicht angegeben ist, verwendet das Cmdlet den Domänennamen des lokalen Rechners bzw. den DNS-Namen des lokalen Rechners ist, falls dieser sich nicht in einer Domäne befindet.

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-PlanName <String>

Gibt den Plannamen an, durch den die Einstellung des Sicherungsjobs definiert wird.

Erforderlich? **True**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-BackupJobType <String>

Gibt den Typ des Sicherungsjobs an. Einer der folgenden Werte kann verwendet werden: Full (für eine vollständige Sicherung), Incr (für eine inkrementelle Sicherung) oder Rsyn (für eine Resync-Sicherung). Folgende Zeichenfolgen werden unterstützt:

- Vollständige Sicherung
- Incr
- Rsyn

Erforderlich? **True**

Position? **benannt**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-JobDescription <String>

Gibt die Beschreibung für den Sicherungsjob an.

Erforderlich? **True**

Position? **benannt**

Standardwert **PowerCLIJo**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-RecoverVmName <String>

Gibt den Hostnamen des virtuellen Rechners an, der wiederhergestellt werden soll.

Erforderlich? **True**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-OverwriteExistingVM <String>

Gibt an, dass beim Wert "true" der vorhandene virtuelle Rechner vom Wiederherstellungsjob überschrieben wird. Der Standardwert ist "false". Sie können eine der folgenden Zeichenfolgen verwenden:

- True
- False

Erforderlich? **false**

Position? **benannt**

Standardwert **False**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-PoweronVM <String>

Gibt an, dass beim Wert "true" der virtuelle Rechner nach der Wiederherstellung aktiviert wird. Der Standardwert ist "false". Sie können eine der folgenden Zeichenfolgen verwenden:

- True
- False

Erforderlich? **false**

Position? **benannt**

Standardwert **False**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-waitJobFinish <{true|false} String>

Gibt an, dass der Befehl beim Wert "true" weitere Anweisungen abwartet, bis der Sicherungsjob abgeschlossen ist. Der Standardwert ist "false". Sie können eine der folgenden Zeichenfolgen verwenden:

- True
- False

Erforderlich? **false**

Position? **benannt**

Standardwert **False**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-timeOut <int>

Gibt die maximale Wartezeit (in Sekunden) bis zum Abschluss der Sicherung an.

Erforderlich? **false**

Position? **benannt**

Standardwert **600**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-jobType <String>

Gibt den Typ des Sicherungsjobs für verschiedene Knotentypen an. Der Standardwert ist agentbase. Verwenden Sie eine der folgenden Zeichenfolgen:

- agentbase
- agentless
- uncpath

Erforderlich? **false**

Position? **benannt**

Standardwert **agentbase**

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

-backupScheduleType <String>

Gibt den Ablaufplan-Sicherungsjob an, übergibt den angegebenen Ablaufplan-Sicherungsjob sofort und wird nur einmal ausgeführt. Folgende Zeichenfolgen werden unterstützt:

- Täglich
- Wöchentlich
- Monatlich

Erforderlich? **false**

Position? **benannt**

Standardwert

Pipeline-Eingabe akzeptieren? **false**

Platzhalterzeichen akzeptieren? **false**

<CommonParameters>

Dieses Cmdlet unterstützt die gemeinsamen Parameter wie **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer** und **OutVariable**. Weitere Informationen finden Sie unter about_CommonParameters.

EINGABEN

AUSGABEN

- 0 oder 1

Wenn ein Job erfolgreich übergeben wurde, gibt der Befehl 0 und andernfalls 1 zurück.

PowerShell-Beispiele

System.Security.SecureString Kennworttyp

Hinweis: Wenn Sie über ein konfiguriertes PowerShell-Skript in Arcserve UDP 6.5 verfügen, das ein Nur-Text-Kennwort verwendet, ändern Sie es so, dass $SecurePassword verwendet wird, oder verwenden Sie die Kennwortdatei.

Beschreibung

Der Befehl wird verwendet, um das Kennwort mit System.Security.SecureString zu erstellen, und wird auch von allen anderen Befehle verwendet. Der System.Security.SecureString-Typ ist ein vom System vordefinierter Typ. Er lässt sich auf vielerlei Arten generieren. Die folgenden beiden Typen werden häufig für verschiedene Zwecke verwendet:

- Dieser Befehl erfordert die Eingabe des Kennworts auf der PowerShell Console. Er erfordert die Interaktion mit den Endbenutzer. In der Regel könnten wir nach dem Ausführen dieses Befehls den Befehl *CreatePswFile* ausführen, um das Kennwort in eine Kennwort-Datei zu schreiben. Und die Kennwortdatei dann automatisch für die Ausführung von PowerShell-Skripts verwenden.

  ```
  $SecurePassword = Read-Host - AsSecureString
  ```

- Dieser Befehl erfordert das Kennwort mit reinem Text. Er kann direkt für die automatische Ausführung von PowerShell-Skripts automatisch verwendet werden.

  ```
  $SecurePassword = ConvertTo-SecureString
  "<PlainPassword>" - AsPlainText - Force
  ```

- (Optional) Nachdem Sie einen der vorherigen Befehle zum Zuweisen eines Kennworts ausgeführt haben, führen Sie den Befehl CreatePswFile aus, um das Kennwort in eine Kennwortdatei zu schreiben. Verwenden Sie anschließend die Passwortdatei, um die PowerShell-Skripte automatisch auszuführen.

  Der Befehl verschlüsselt das sichere Kennwort und speichert es in der Kennwortdatei.

  ```
  C:\PS>UDPPowerCLI.ps1 -Command CreatePswFile -
  Password $SecurePassword -PasswordFile
  myUDPPasswordFile
  ```

Beispiel 1

Beschreibung

Der Befehl verschlüsselt das sichere Kennwort und speichert es in der Kennwort-Datei.

```
C:\PS>UDPPowerCLI.ps1 -Command CreatePswFile -Password
$SecurePassword -PasswordFile myUDPPasswordFile
```

Beispiel 2

Beschreibung

Auf dem lokalen Server wird durch den Befehl eine Verbindung mit dem UDP-Konsolen-Dienst per HTTP-Protokoll über Port 8015 hergestellt und dann ein Zuwachssicherungsjob für den Plan mit dem Namen *myplan* übermittelt.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPC-
onsoleUserName myUsr -UDPConsolePassword $Se-
curePassword -PlanName myPlan -BackupJobType Incr
```

Beispiel 3

Beschreibung

Auf dem lokalen Server wird durch den Befehl eine Verbindung mit dem UDP-Konsolen-Dienst per HTTP-Protokoll über Port 8015 hergestellt und dann ein Zuwachssicherungsjob für den Knoten mit dem Namen *myNodeName* übermittelt.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPC-
onsoleUserName myUsr -UDPConsolePasswordFile myUDPPass-
wordFile -NodeName myNodeName -BackupJobType Incr
```

Beispiel 4

Beschreibung

Mit dem Befehl wird eine Verbindung zum UDP-Konsolen-Dienst auf dem Server mit dem Namen *myServer* per HTTPS-Protokoll über Port 8018 hergestellt, anschließend ein vollständiger Sicherungsjob für den Plan mit dem Namen *myPlan* übermittelt, und danach eine Jobbeschreibung als *myJob* festgelegt.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPC-
onsoleServerName myServer -UDPConsoleProtocol https -
UDPConsolePort 8018 -UDPConsoleUserName myUsr -UDPC-
onsolePassword $SecurePassword -UDPConsoleDomainName
myDomain -PlanName myPlan -BackupJobType Full -JobDe-
scription myJob
```

Beispiel 5

Beschreibung

Mit dem Befehl wird eine Verbindung zum UDP-Agentendienst auf dem Server mit dem Namen *yourUDPAgentServer* per HTTP-Protokoll über Port 8014 her-

gestellt und dann ein Zuwachssicherungsjob für *yourUDPAgentServer* übermittelt.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -BackupJobType
Incr
```

Beispiel 6

Beschreibung

Der Befehl verkürzt den Namen des Parameters.

```
C:\PS>UDPPowerCLI.ps1 -Cmd Backup -Svr myServer -Ptc
https -Prt 8018 -Usr myUsr -Psw $SecurePassword -Dmn
myDomain -Pln myPlan -Jbt Full -Jbd myJob
```

Beispiel 7

Beschreibung

Mit dem Befehl wird eine Verbindung zum Server mit dem Namen *yourUDPAgentServer* mithilfe des Benutzernamens der Umgebung, dem Standard-HTTP-Protokoll und Port 8014 hergestellt. Mit dem Befehl wird zudem überprüft, ob die Sicherungssitzungsnummer aus der Sicherungskonfiguration von *yourUDPAgentServer* 1 ist und dann das Verzeichnis am ursprünglichen Speicherort wiederhergestellt. Dabei ist für die Option "Wiederherstellung" die Option "Vorhandene Dateien überschreiben" ausgewählt.

```
C:\PS>UDPPowerCLI.ps1 -Command restore -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
RestoreDirectoryPath 'c:\Test' -BackupSessionNumber 1
```

Beispiel 8

Beschreibung

Mit dem Befehl wird eine Verbindung zu dem Server mit dem Namen *YourUDPAgentServer* mit dem HTTPS-Protokoll und Port 8018 hergestellt. Mit dem Befehl wird zudem überprüft, ob die Sicherungssitzungsnummer aus der Sicherungskonfiguration von *yourUDPAgentServer* 1 ist und dann die Datei "1.txt" an einem anderen Speicherort wiederhergestellt. Dabei ist für die Option "Wiederherstellung" die Option "Vorhandene Dateien überschreiben und Stammverzeichnis erstellen" ausgewählt.

```
C:\PS>UDPPowerCLI.ps1 -Command restore -UDPA-
gentServerName yourUDPAgentServer -UDPAgentUserName
UDPAgentUsername -UDPAgentPasswordFile myUDPA-
gentPasswordFile -UDPAgentProtocol 'https' -UDPA-
gentPort 8018 -UDPAgentDomainName UDPAgentdomainName -
```

```
BackupSessionNumber 1 -RestoreFilePath 'C:\1.txt' -
RestoreDestination 'C:\restore' -Resto-
reDestinationUserName remoteAccessUser -Resto-
reDestinationPassword remoteAccessPsw -
CreateBaseFolder 'true'
```

Beispiel 9

Beschreibung

Mit dem Befehl wird eine Verbindung zum Server mit dem Namen *yourUDPAgentServer* mithilfe des Benutzernamens der Umgebung, dem Standard-HTTP-Protokoll und Port 8014 hergestellt. Dann wird über den Standardport 8015 und das HTTP-Protokoll eine Verbindung zum UDP-Server hergestellt, um zu überprüfen, ob die Nummer der Sicherungssitzung 1 ist. Schließlich wird das Verzeichnis an einem alternativen Speicherort wiederhergestellt; dabei ist die Wiederherstellungsoption zum Überschreiben der vorhandenen Datei und zum Erstellen eines Stammverzeichnisses ausgewählt.

```
C:\PS>UDPPowerCLI.ps1 -Command restore -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
RestoreDirectoryPath 'c:\Test' -BackupSessionNumber 1
-RestoreDestination 'C:\restore' -Resto-
reDestinationUserName remoteAccessUser -Resto-
reDestinationPassword remoteAccessPsw -
UDPConsoleServerName yourUDPServer -vmname sour-
ceVMName -UDPConsolePasswordFile myUDPPasswordFile -
domainname yourUDPDomainName -OverwriteExistFiles
'true' -CreateRootFolder 'true'
```

Beispiel 10

Beschreibung

Mit dem Befehl wird eine Verbindung zum Server mit dem Namen *yourUDPAgentServer* mithilfe des Benutzernamens der Umgebung, dem Standard-HTTP-Protokoll und Port 8014 hergestellt. Dann wird über den Standardport 8015 und das HTTP-Protokoll eine Verbindung zum UDP-Server hergestellt, um zu überprüfen, ob die Nummer der Sicherungssitzung 1 ist. Schließlich wird die VM am ursprünglichen Speicherort wiederhergestellt; dabei ist die Option zur VM-Wiederherstellung zum Überschreiben der vorhandenen VM und zum Einschalten der VM nach Wiederherstellung ausgewählt.

```
C:\PS>UDPPowerCLI.ps1 -Command RecoverVM -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
BackupSessionNumber 1 -UDPConsoleServerName yourUDPSer-
ver -recovervmname sourceVMName -
```

```
UDPConsolePasswordFile myUDPPasswordFile -UDPC-
onsoleDomainName yourUDPDomainName -Over-
writeExistingVM 'true' -PoweronVM 'true'
```

Beispiel 11

Beschreibung

Der Befehl sendet sofort wöchentliche Sicherungsjobs an UDP Agent und wird nur einmal ausgeführt.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPA-
gentServerName myServer -UDPAgentPassword $Se-
curePassword -UDPAgentDomainName myDomainName -
UDPAgentUserName UDPAgentUsername -BackupJobType Incr
-backupScheduleType 'weekly' -jobDescription
'PowerCLIJob'
```

Beispiel 12

Beschreibung

Mit dem Befehl wird der Sicherungsjob übergeben, und das Zeitlimit in Sekunden für die Wartezeit festgelegt, bis der Job abgeschlossen ist.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPC-
onsoleServerName myServer -UDPConsolePasswordFile
myUDPPasswordFile -UDPConsoleDomainName myDomainName -
nodeName myNodeName -UDPConsoleUserName myAdmin -
BackupJobType Incr -jobDescription 'PowerCLIJob'
waitJobFinish 'true' -timeout 600 -jobType 'agentbase'
```

Konfigurationsdatei und Eigenschaften von PowerCLI

Sie können die folgende Konfigurationsdatei und die folgenden Eigenschaften für UDP-PowerCLI anpassen:

Name der Konfigurationsdatei: *PowerCLIConfiguration.properties*

Installationsort der Konfigurationsdatei:

- *C:\Programme\Arcserve\Unified Data Protection\Management\Configuration*
- *C:\Programme\Arcserve\Unified Data Protection\Engine\Configuration*

Format der Konfigurationsdatei:

Enable24HoursSetting=yes

LogPath=D:\PowerCLILogPath

RotationSizeInMB=2

RetentionPeriodInDays=5

RetainNoOfFiles=6

Konfigurationseigenschaften:

Eigenschaftsname	Beschreibung	Standardwert	Zulässiger Wert
Enable24HoursSetting	▪ Wenn der Wert auf "Yes" festgelegt ist, wird der Zeitstempel der Protokolldatei im 24-Stunden-Format geschrieben. ▪ Wenn der Wert auf "No" festgelegt ist, wird der Zeitstempel der Protokolldatei im 12-Stunden-Format geschrieben.	Ja	Yes oder No
LogPath	▪ Der Speicherort des Ordners für die PowerCLI-Protokolldatei(en). ▪ Wenn der Speicherort nicht angegeben wird, wird die Protokolldatei am Standardspeicherort abgelegt. ▪ LogPath unterstützt relative und absolute Pfade. ▪ Symbole außer \ /: *? <> | sind für Datei- oder Ordnernamen zulässig.	-	-
RotationSizeInMB	▪ Wenn der in "RotationSizeInMB" angegebene Grenzwert erreicht ist, wird die PowerCLI-Protokolldatei in "(Rotated)" mit einem Datums- und Zeitstempel umbenannt.	0	Minimum = 1 Maximum = 1024
RetentionPeriodInDays	▪ Wenn die rotierten Dateien älter sind als der in "RetentionPeriodInDays" angegebene Wert, werden die	0	Minimum = 5 Maximum = 365

	alten Protokolldateien gelöscht.		
RetainNoOfFiles	▪ Wenn mehr rotierte Protokolldateien vorhanden sind als in "RetainNoOfFiles" angegeben, werden die zusätzlichen Dateien gelöscht.	0	Minimum = 5 Maximum = 1000

Hinweise:

- Wenn Sie für Konfigurationseigenschaften andere als die zulässigen Werte angeben, zeigt PowerCLI einen Fehler an, und die Ausführung wird beendet.
- Wenn Sie Standardwerte für Konfigurationseigenschaften angeben, wird die Ausführung von PowerCLI fortgesetzt und mit dem Standardverhalten ausgeführt.

Kapitel 4: Schützen von Oracle-Systemen mit Recovery Manager (RMAN)

Recovery Manager (RMAN) ist ein Oracle-Hilfsprogramm, das Sicherungsjobs und Wiederherstellungstasks für Datenbanken ausführt und die Verwaltung von Sicherungsstrategien automatisiert. Mit dieser Funktion können Sie die Datenbankdateien problemlos sichern und wiederherstellen.

In diesem Abschnitt werden die folgenden Themen behandelt:

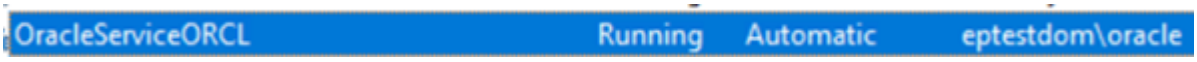
Überprüfen der Voraussetzungen für Oracle-Datenbank mit RMAN (Windows und Linux)

Voraussetzungen für die Konfiguration, wenn Oracle unter Windows installiert ist

Plan hinzufügen

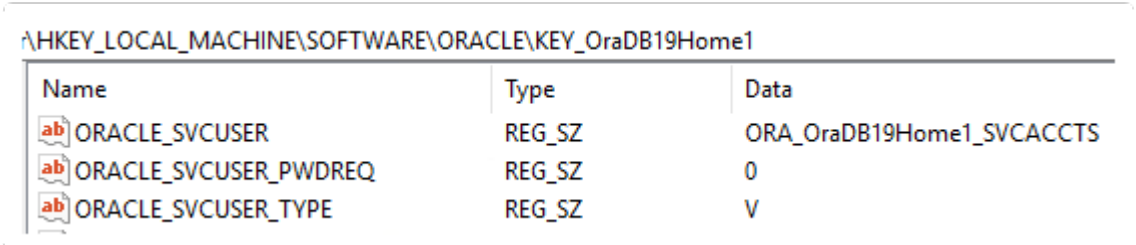
- Die Windows Oracle-Knoten, die UDP-Konsole und der RPS müssen sich in derselben Domäne befinden.
- Die UDP-Konsole und die RPS-Systeme müssen installiert und mit einem Domänenadministrator ("<Domäne>\administrator") oder einem gleichwertigen Konto verwendet werden.
- Wenn Sie sich bei der UDP-Konsole anmelden, gehen Sie wie folgt vor:
  1. Der Benutzer "<Domäne>\Administrator" wird zur lokalen Gruppe "ORA_DBA" in den Windows-Oracle-Knoten hinzugefügt.
  2. Fügen Sie den Oracle-Knoten unter Verwendung der Benutzer-ID "<Domäne>\Domänennutzer" zur UDP-Konsole hinzu.

  Hinweis: Sie können in UDP alle Benutzer außer Administratoren verwenden. Die entsprechenden Berechtigungen müssen jedoch angegeben werden.
- Unterstützt die unten aufgeführten Oracle-Konten, die während Oracle-Installationen verwendet werden (sowohl eigenständig als auch RAC).
  - Domänenbenutzer: Notieren Sie sich den Domänenbenutzer, dem der Oracle-Dienst gehört (Dienstkonto). Beispiel: eptestdom\oracle.

  - Virtuelles Konto: Wenn Oracle mit einem virtuellen Konto installiert wird, überprüfen Sie die Parameter in der Registrierung des Oracle-Servers, bevor Sie eine Datenbank zum UDP-Plan hinzufügen.

    Hinweis: Standardmäßig sind die virtuellen Konten in Windows aktiviert.

- Stellen Sie sicher, dass der Listener entsprechend konfiguriert ist. Dies hilft, die Oracle-Datenbank zu schützen, und stellt eine Verbindung zu sqlplus und RMAN für diese Datenbank her.

  Beispiel: "rman target / " muss auf die richtige Datenbank verweisen.

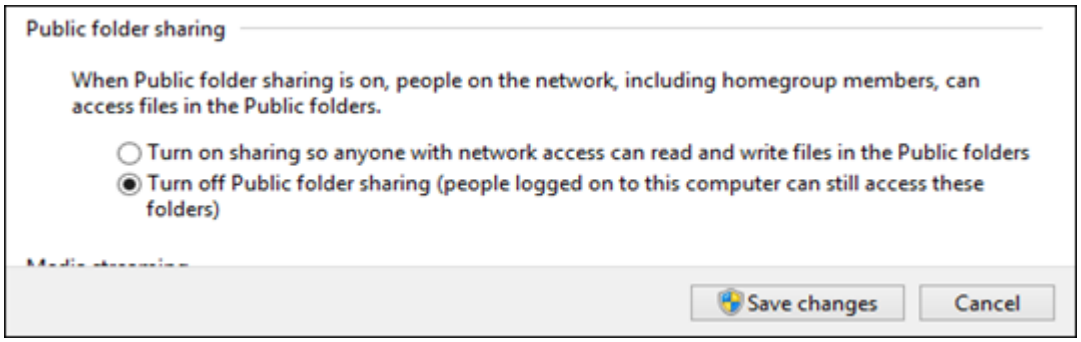
Sichern

- Wenn Sie die Oracle-Datenbank(en) sichern, stellen Sie sicher, dass diese den Status OPEN aufweisen und der ARCHIVELOG-Modus aktiviert ist. Weitere Informationen finden Sie unter How to enable ARCHIVELOG mode.
- Für die erfolgreiche Durchführung von Oracle RMAN-Sicherungen mit Arcserve UDP müssen Sie die systemeigene Windows-Authentifizierung aktivieren. Um zu überprüfen, ob die Windows-Authentifizierung aktiviert ist, stellen Sie sicher, dass die folgende Zeile in der Datei "sqlnet.ora" im Pfad "ORACLE-STAMMVERZEICHNIS/network/admin" hinzugefügt wurde.

  SQLNET.AUTHENTICATION_SERVICES= (NTS)
- Die Freigabe des öffentlichen Ordners ist deaktiviert, um einen sicheren Zugriff auf die Datenbank(en) zu ermöglichen.

  Um die Verwendung des öffentlichen Ordners für die Netzwerkfreigabe zu deaktivieren, gehen Sie folgendermaßen vor:

  1. Gehen Sie zum Netzwerk- und Freigabecenter, und klicken Sie dann auf **Erweiterte Freigabeeinstellungen ändern**.
  2. Suchen Sie im linken Fensterbereich nach der Einstellung "Freigabe des öffentlichen Ordners" für die aktive Netzwerkadresse, und klicken Sie dann auf **"Freigabe des öffentlichen Ordners" deaktivieren (an diesem Computer angemeldete Benutzer können weiterhin auf diese Ordner zugreifen)**.
  3. Klicken Sie auf **Änderungen speichern**.



Tabellen wiederherstellen

Wiederherstellungen von Tablespaces und auf Tabellenebene verwenden eine zusätzliche Datenbank, für die folgende Berechtigungen erforderlich sind:

- **Domänenbenutzer für Oracle-Installation:** Fügen Sie den Oracle-Benutzer des Dienstkontos der Gruppe "Administratoren" in den Oracle-Knoten hinzu. In unserem Beispiel wird "eptestdom\oracle" der lokalen Administratorgruppe hinzugefügt.
- **Virtuelles Konto für Oracle-Installation:** Öffnen Sie den Registrierungsschlüssel "HKLM\SYSTEM\CurrentControlSet\services\eventlog\Application", klicken Sie mit der rechten Maustaste, und fügen Sie der Gruppe Berechtigungen wie "ORA_OraDB18Home1_SVCACCTS" hinzu.

Auf alternativem Knoten wiederherstellen

- Auf dem Zielsystem ist dieselbe Version von Oracle mit derselben Konfiguration installiert.
- Die Datenbank wird mit derselben SID wie der (ursprüngliche) Quellrechner installiert.
- Die Oracle-Datenbank auf dem Zielknoten muss heruntergefahren sein.

Firewall-Einstellungen für den Zugriff auf Oracle-Knoten (Windows)

netsh advfirewall firewall add rule name="AS ora" dir=in action=allow program="C:\ **path\to\oracle\home**\bin\oracle.exe" enable=yes	
netsh advfirewall firewall add rule name="AS tns" dir=in action=allow program="C:**path\to\oracle\home**\tnslsnr.exe" enable=yes	
netsh advfirewall firewall add rule name="AS ora" dir=out action=allow program="C:\ **path\to\oracle\home**\bin\oracle.exe" enable=yes	
netsh advfirewall firewall add rule name="AS tns" dir=out action=allow program="C:**path\to\oracle\home**\bin\tnsls-	

nr.exe" enable=yes	
netsh advfirewall firewall add rule name="ora_1521" dir=in action=allow protocol=TCP local-port=**1521**	
netsh advfirewall firewall add rule name="ora_1521" dir=out action=allow protocol=TCP local-port=**1521**	Die Portnummer kann sich je nach konfiguriertem Port ändern.

Voraussetzungen für die Konfiguration, wenn Oracle auf Linux installiert ist

Plan hinzufügen

- Der Oracle-Knoten "/etc/hosts" muss über einen Eintrag für FQDN und "resolv.conf" mit dem entsprechenden DNS-Eintrag verfügen.
- Für jede zu schützende Datenbank muss ein Eintrag in der Datei "/etc/oratab" vorhanden sein.

  Hinweis: Stellen Sie in einer RAC-Umgebung sicher, dass der Inhalt für beide Knoten aktualisiert wird.

  Die Syntax der Datei "/etc/oratab" lautet wie folgt:

  <EINDEUTIGER_DATENBANKNAME>:<ORACLE-STAMMVERZEICHNIS>:<AKTIV/INAKTIV>

  Beispiel: ORCL:/u01/app/oracle/ORCL/:Y

Sichern

- Wenn Sie die Oracle-Datenbank(en) sichern, stellen Sie sicher, dass diese den Status OPEN aufweisen und der ARCHIVELOG-Modus aktiviert ist. Weitere Informationen finden Sie unter How to enable ARCHIVELOG mode.
- Installieren Sie smbclient mithilfe des folgenden Befehls:

  #yum install smbclient
- Stellen Sie sicher, dass der Listener entsprechend konfiguriert ist. Dies hilft, die Oracle-Datenbank zu schützen und eine Verbindung zu sqlplus und RMAN für diese Datenbank herzustellen.

  Beispiel: Überprüfen Sie "lsnrctl status" für die Datenbanken, die für einen bestimmten Listener verfügbar sind.

  Der Befehl "rman target / " muss mit der richtigen für die Sicherung angegebenen Datenbank verbunden sein.

Assured Recovery-Jobs

- Stellen Sie sicher, dass sich die zu sichernden Oracle-Datenbanken im Status "MOUNT" oder "OPEN" befinden.

Auf öffentlichen und privaten Schlüsseln basierende Authentifizierung

Hinweis: Die auf öffentlichen und privaten Schlüsseln basierende Authentifizierung wurde für die Ausführung von Linux-RMAN-Skripten implementiert. Dadurch werden Klartext-Kennwörter bei der Ausführung von Remote-Skripten auf einem Linux-Oracle-Server vom Recovery Point Server (RPS) vermieden.

1. Gehen Sie auf dem RPS-Knoten wie folgt vor:
    a. Stellen Sie sicher, dass das Installationsprogramm das Verzeichnis *PrivateKey* unter folgendem Pfad erstellt hat:

    Installieren Sie Path\Arcserve\Unified Data Protection\Engine\BIN\OracleRMAN\PrivateKey

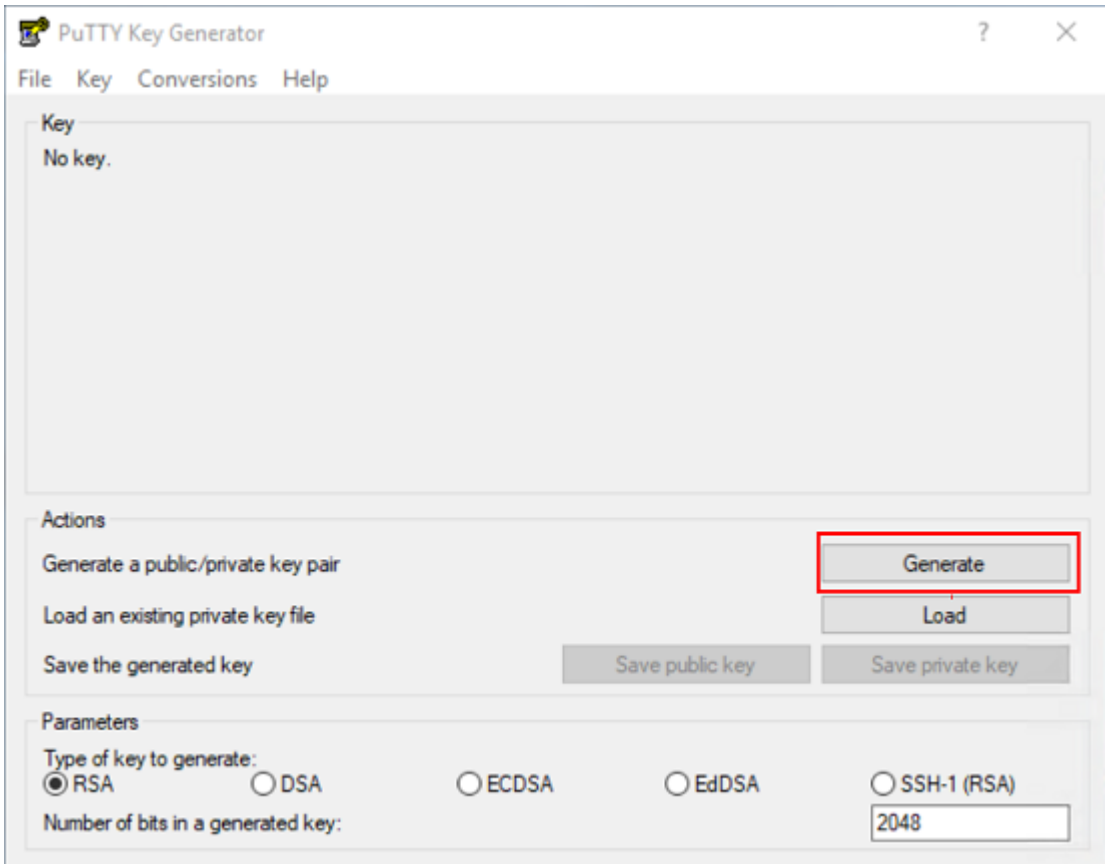
    b. Installieren Sie PuTTY (Version 0.73 oder höher), und führen Sie dann einen der folgenden Schritte aus, um den PuTTY Key Generator zu öffnen:

    - Führen Sie unter "cmd.exe" den Befehl *puttygen* aus.
    - Gehen Sie zu **Programme** > **PuTTY** > **PuTTYgen**.

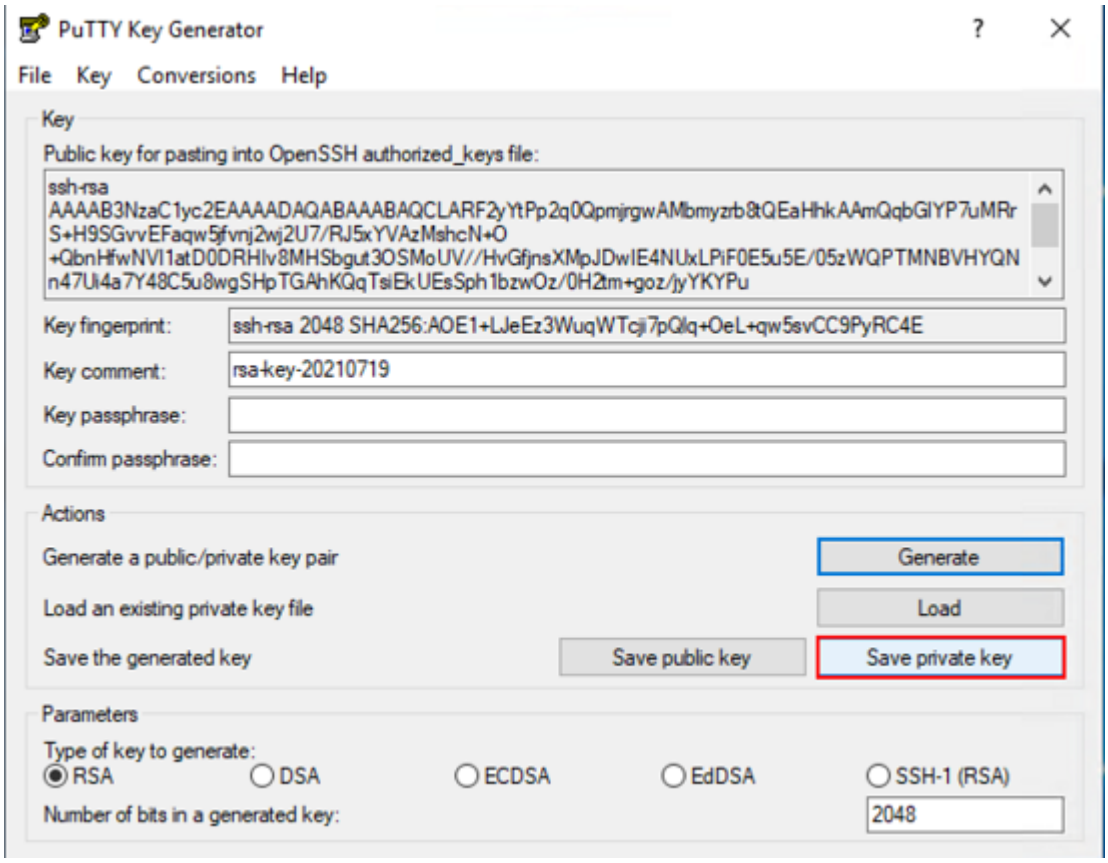
    Das Dialogfeld "PuTTY-Schlüsselgenerator" wird angezeigt.

    c. Klicken Sie im Dialogfeld "PuTTY Key Generator" auf **Erzeugen**.

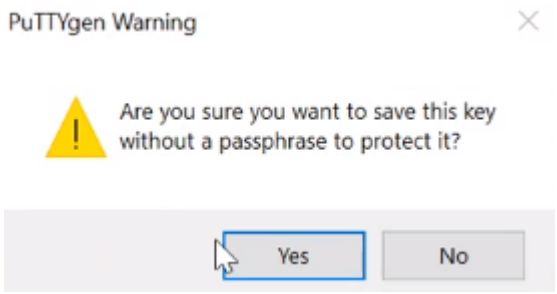
    Der öffentliche und der private Schlüssel werden generiert.



d. Klicken Sie auf **Privaten Schlüssel speichern**.



e. Klicken Sie im Dialogfeld "PuTTYgen-Warnung" auf **Ja**, um den privaten Schlüssel ohne Passphrase zu speichern.



f. Navigieren Sie beim Speichern des privaten Schlüssels zum folgenden Pfad, geben Sie den Dateinamen ein, und klicken Sie dann auf **Speichern**:

Installieren Sie Path\Arcserve\Unified Data Protection\Engine\BIN\OracleRMAN\PrivateKey

Hinweise:

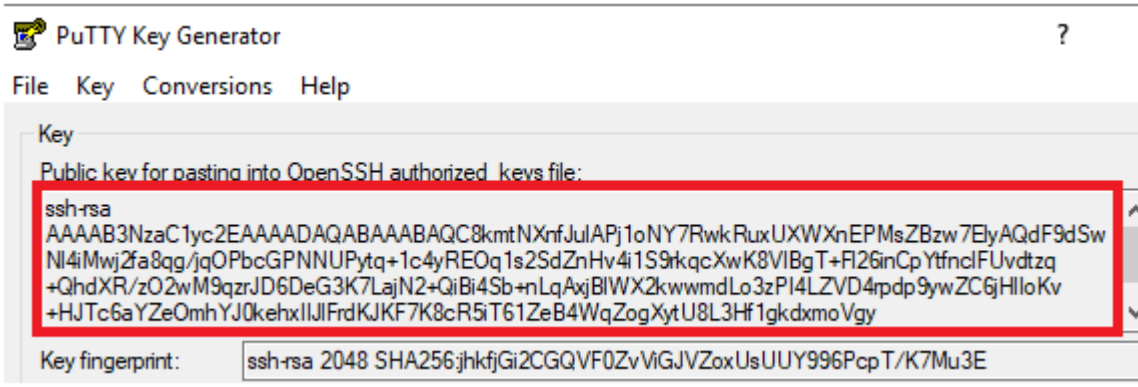
- Der Dateiname muss im Format "PrivateKeyFile.ppk" vorliegen. Sie können einen beliebigen Namen angeben.

- Speichern Sie den privaten Schlüssel mit der Erweiterung ".ppk" unter folgendem Pfad:

  Engine\Bin\OracleRMAN\PrivateKey

- Kopieren Sie den öffentlichen Schlüssel manuell aus dem Dialogfeld "PuTTY-Schlüsselgenerator", und speichern Sie ihn im Textformat im folgenden Ordner für zukünftige Verweise, falls er zu anderen Linux-Oracle-Servern hinzugefügt werden muss:

  Engine\Bin\OracleRMAN\PrivateKey



g. Öffnen Sie den Pfad *Engine\Bin* auf "cmd.exe".

h. Führen Sie den folgenden Befehl aus, um den privaten Schlüssel mit dem Befehlszeilenhilfsprogramm RMANCryptUtil.exe zu verschlüsseln:

   RMANCryptUtil.exe "C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\<Name des generierten privaten Schlüssels>.ppk"

   Die verschlüsselte Datei mit dem privaten Schlüssel wird mit der Erweiterung **.enc** am folgenden Speicherort generiert:

   Engine\Bin\OracleRMAN\PrivateKey

   Ein Beispiel für den Dateinamen: PrivateKey.ppk.enc

   Der verschlüsselte private Schlüssel (.enc), der mit RMANCryptutil generiert wird, wird im Ordner "Privater Schlüssel" gespeichert.

i. Kopieren Sie die **.enc**-Schlüssel zu anderen RPS-Knoten und UDP-Konsolen.

j. Erstellen Sie auf dem UDP-Konsolen-Knoten den Ordner "PrivateKey" wie folgt, und kopieren Sie dann den .enc-Schlüssel in den Ordner "PrivateKey":

   UDP\Engine\Bin\OracleRMAN\PrivateKey

k. Kopieren Sie den öffentlichen Schlüssel von der PuTTYgen-Benutzeroberfläche, und verweisen Sie auf Schritt 2, um den öffentlichen Schlüssel im Linux-Oracle-Knoten hinzuzufügen.

2. Führen Sie auf dem Linux-Knoten, auf dem Oracle installiert ist, die folgenden Vorgänge aus:

   a. Stellen Sie sicher, dass der *.ssh*-Ordner im Stammverzeichnis (~) verfügbar ist. Wenn das *.ssh*-Verzeichnis nicht verfügbar ist, erstellen Sie das Verzeichnis mit dem folgenden Befehl und den Standardberechtigungen:

      mkdir ~.ssh

   b. Überprüfen Sie mithilfe des folgenden Befehls, ob der *sshd*-Dienst auf dem Linux-Server ausgeführt wird:

      service sshd status

      Hinweis: Wenn *sshd* nicht installiert ist, installieren Sie *sshd* basierend auf der Linux-Betriebssystemversion.

   c. Öffnen oder bearbeiten Sie die Datei *authorized_keys* mithilfe des folgenden Befehls:

      vim authorized_keys

   d. Erstellen oder ändern Sie die Datei *.ssh/autorisierte_schlüssel*.

   e. Fügen Sie den öffentlichen Schlüssel, der auf dem RPS-Server generiert wurde, mithilfe des PuTTY-Schlüsselgenerators zur Datei *.ssh/Authorized_keys* hinzu.

   f. Legen Sie mit dem folgenden Befehl die erforderlichen Mindestberechtigungen für die Datei *.ssh/authorized_keys* fest:

      chmod 400 .ssh/authorized_keys

   Hinweise:

   - Um einen öffentlichen Schlüssel in einem anderen Linux Oracle-Knoten hinzuzufügen, solange RPS der gleiche ist, folgen Sie nur Schritt 2 oben.
   - Befolgen Sie beim Ändern des RPS-Knotens die oben genannten Schritte 1 und 2.

Erstellen eines Sicherungsplans für Oracle-Datenbank (Windows und Linux)

Um Ihre Windows- und Linux-Knoten oder geclusterte Knoten zu schützen, müssen Sie einen Plan erstellen. Der Plan besteht aus einem Sicherungstask. In diesem Sicherungstask können Sie die Knoten, die Sie schützen möchten, das Sicherungsziel und den Ablaufplan für die Sicherung angeben. Beim Sicherungsziel handelt es sich um einen Recovery Point Server, auf dem Sie Ihre Sicherungsdaten speichern möchten. Das Sicherungsziel kann ein lokales Ziel oder ein freigegebener Remote-Ordner sein.

In diesem Abschnitt werden die folgenden Themen behandelt:

Erstellen eines Sicherungsplans mit einem Sicherungstask

Ein Sicherungsplan enthält einen Sicherungstask, der eine Sicherung eines Knotens ausführt und die Daten an einem angegebenen Ziel speichert. Jeder Task besteht aus Parametern, die Quelle, Ziel, Ablaufplan und weitere Sicherungsdetails definieren. Dieser Abschnitt enthält Informationen zum Erstellen eines Sicherungsplans für Oracle-Datenbank.

Gehen Sie wie folgt vor:

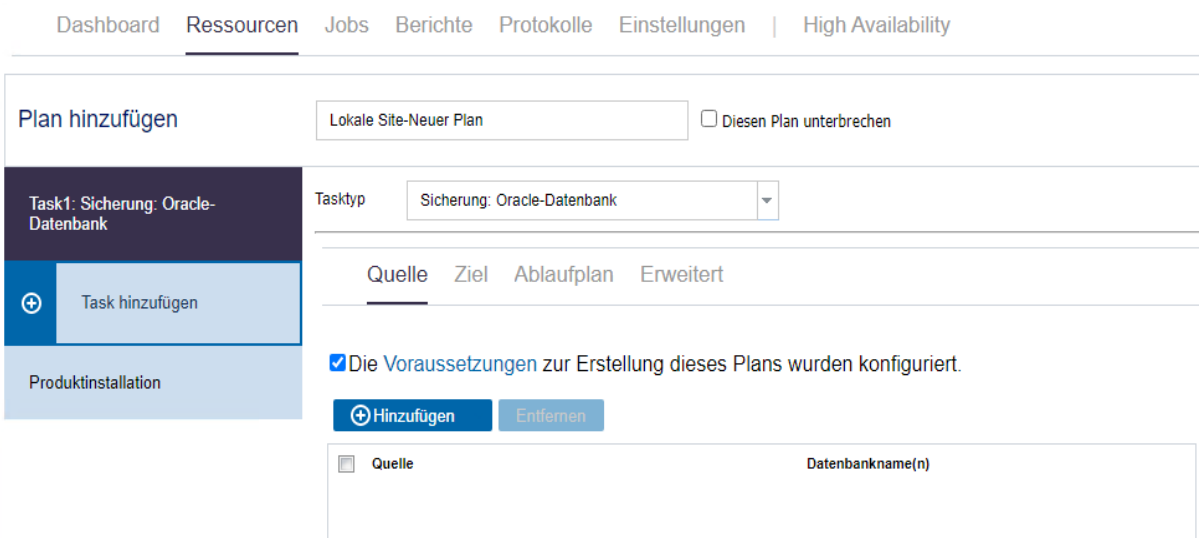
1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Navigieren Sie zu **Ressourcen** > **Plan** > **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

   Die Seite Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.
6. Wählen Sie in der Drop-down-Liste Tasktyp die Option **Sicherung: Oracle-Datenbank** aus.



Geben Sie nun Details unter Quelle, Ziel, Ablaufplan und Erweitert an.

Hinweise:

- Um die physische und logische Blockbeschädigung in den Datendateien auf dem Oracle-Quellrechner zu überprüfen, wird der Befehl "Backup Validate RMAN" verwendet.
- Um dem Sicherungsjob eine Validierung hinzuzufügen, verwenden Sie den folgenden Registrierungsschlüssel:

  \HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\SourceDBValidation

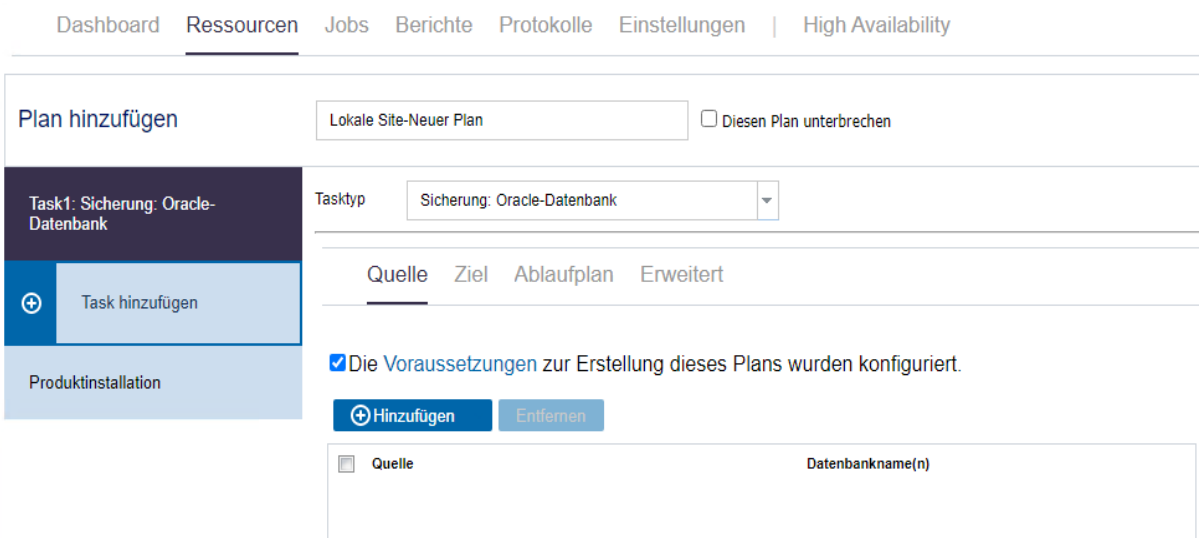
  - Wenn der Schlüssel nicht hinzugefügt wird (Standard), ist die Sicherungsvalidierung nicht aktiviert
  - Wenn der Schlüssel als 1 hinzugefügt wird, ist die Sicherungsvalidierung aktiviert
  - Wenn der Schlüssel mit einem anderen Wert hinzugefügt wurde, ist die Sicherungsvalidierung nicht aktiviert
- Sicherungsvalidierung ist eine zeitintensive Aufgabe. Wenn Sie diese Einstellung aktivieren, wird die Sicherungszeit in Abhängigkeit von der Größe der Datendateien erhöht. Die Validierung wird auch bei einer Zuwachssicherung für die gesamte Quelldatendatei ausgeführt.

Angeben der Quelle

Auf der Seite "Quelle" können Sie die Quellknoten angeben, die Sie schützen möchten. Sie können mehrere Knoten in einem Plan auswählen. Wenn Sie der Konsole keine Knoten hinzugefügt haben, dann können Sie Knoten hinzufügen, wenn Sie einen Plan auf der Quellenseite erstellen oder ändern. Sie können einen Plan auch speichern, ohne Quellknoten hinzuzufügen. Der Plan wird erst bereitgestellt, wenn Sie Quellknoten hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Aktivieren Sie auf der Registerkarte "Quelle" das Kontrollkästchen **Die Voraussetzungen für die Erstellung dieses Plans wurden konfiguriert**, um die Konfiguration der Voraussetzungen zu bestätigen. Weitere Informationen finden Sie unter Überprüfen der Voraussetzungen für Oracle-Datenbank für RMAN (Windows und Linux).



2. Klicken Sie auf **+ Hinzufügen**.
3. Wählen Sie eine der folgenden Optionen:

   Auswählen von zu schützenden Quellen in Arcserve UDP

   Das Dialogfeld "Zu schützende Knoten auswählen" wird geöffnet. Wählen Sie die Knoten in der angezeigten Liste aus. Wählen Sie diese Option aus, wenn Sie die Knoten bereits zu der Konsole hinzugefügt haben.

   Windows-Knoten hinzufügen

   Das Dialogfeld "Windows-Oracle-Knoten hinzufügen" wird geöffnet. Wählen Sie diese Option aus, wenn Sie die Knoten nicht hinzugefügt haben und Sie die zu schützenden Knoten manuell hinzufügen möchten.

Linux-Knoten hinzufügen

Das Dialogfeld "Linux-Oracle-Knoten hinzufügen" wird geöffnet. Wählen Sie diese Option aus, wenn Sie die Knoten nicht hinzugefügt haben und Sie die zu schützenden Knoten manuell hinzufügen möchten.

4. Wenn Sie die Option **Wählen Sie zu sichernde Quellen in Arcserve UDP aus** auswählen, gehen Sie im Dialogfeld "Zu schützende Knoten auswählen" folgendermaßen vor:

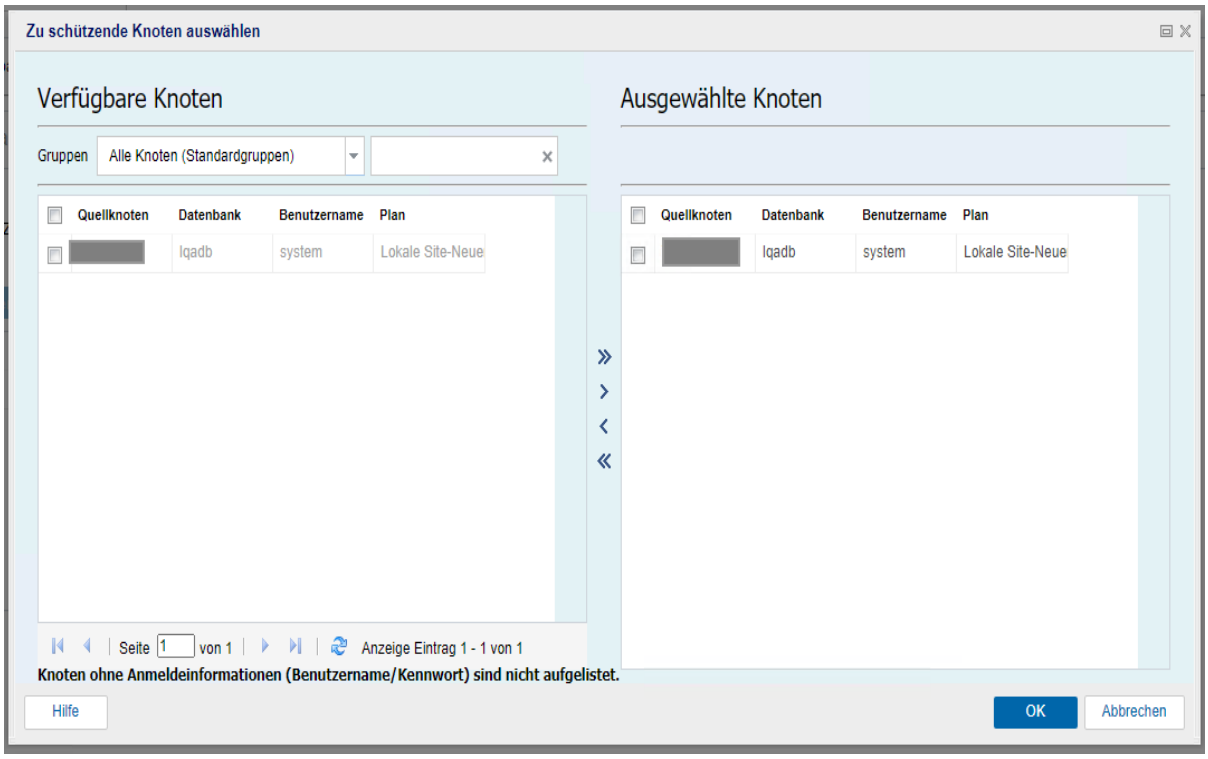
   a. (Optional) Wählen Sie einen Filter aus der Dropdown-Liste "Gruppen" aus, um nach Knoten zu filtern. Sie können Schlüsselwörter eingeben, um den Knotenfilter weiter einzuschränken.

      Die Knoten werden in der Spalte "Verfügbare Knoten" angezeigt.

   b. Wählen Sie die Knoten aus der Spalte "Verfügbare Knoten" aus, und klicken Sie dann auf den einfachen Nach-rechts-Pfeil (>) oder den doppelten Nach-rechts-Pfeil (>>), um die ausgewählten Knoten bzw. alle Knoten in die Spalte "Ausgewählte Knoten" zu verschieben.

      Die Knoten werden in der Spalte "Ausgewählte Knoten" angezeigt.

   c. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.



5. Wenn Sie die Option **Windows-Knoten hinzufügen** auswählen, gehen Sie im Dialogfeld "Windows-Oracle-Knoten hinzufügen" folgendermaßen vor:

a. Geben Sie den Knotennamen oder die IP-Adresse des Oracle-Knotens ein, den Sie hinzufügen möchten.

b. Geben Sie eine Beschreibung für den Knoten ein.

c. Geben Sie die Anmeldeinformationen des Administrators ein.

d. Klicken Sie auf **Hinzufügen**.

   Warten Sie, bis die Validierung von Benutzername und Kennwort abgeschlossen ist.

   Der Knoten wird im mittleren Fensterbereich hinzugefügt.

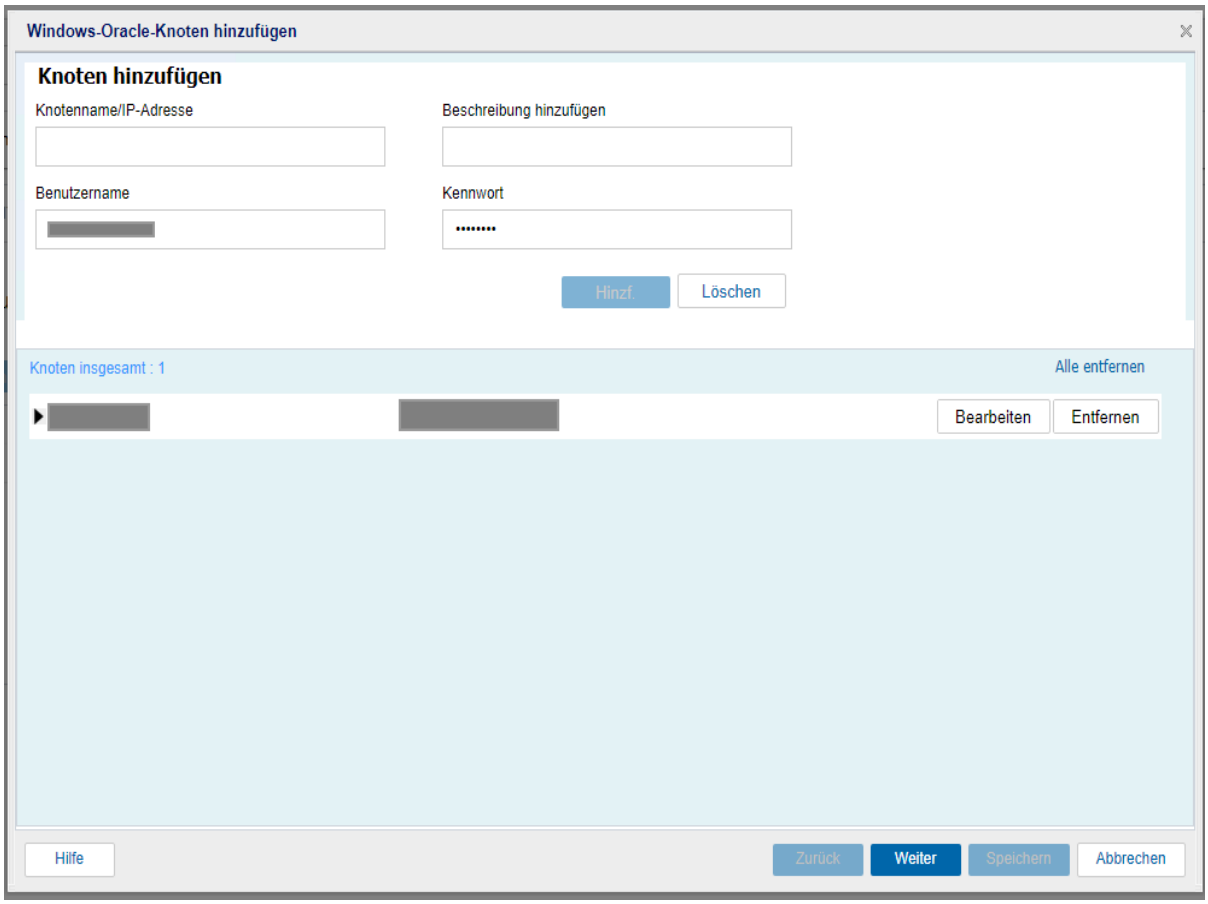
e. Um mehrere Knoten hinzuzufügen, führen Sie die Schritte erneut aus. Alle hinzugefügten Knoten werden im mittleren Fensterbereich aufgeführt.

f. Klicken Sie auf das Erweiterungssymbol neben der IP-Adresse, und überprüfen Sie die hinzugefügten Details.

   Hinweise:

   - Um die hinzugefügten Knoten in der Liste zu bearbeiten, wählen Sie den zu bearbeitenden Knoten aus, und klicken Sie auf **Bearbeiten**.
   - Um die hinzugefügten Knoten aus der Liste zu entfernen, wählen Sie die zu entfernenden Knoten aus, und klicken Sie dann auf **Entfernen**.
   - Um alle hinzugefügten Knoten zu entfernen, klicken Sie auf **Alle entfernen**.

g. Klicken Sie auf **Weiter**.



6. Wenn Sie die Option **Linux-Knoten hinzufügen** auswählen, gehen Sie im Dialogfeld "Linux-Oracle-Knoten hinzufügen" folgendermaßen vor:
   a. Geben Sie den Knotennamen oder die IP-Adresse des Oracle-Knotens ein, den Sie hinzufügen möchten.
   b. Geben Sie eine Beschreibung für den Knoten ein.
   c. Geben Sie den Benutzernamen ein.
   d. Geben Sie für "Oracle Owner" den Benutzernamen ein, der für die Oracle-Installation verwendet wird.
   e. Geben Sie für SSH-Port den Portwert an. Der Standardwert für den Port ist 22.
   f. Klicken Sie auf **Hinzufügen**.

      Warten Sie, bis die Validierung von Benutzername und Kennwort abgeschlossen ist.

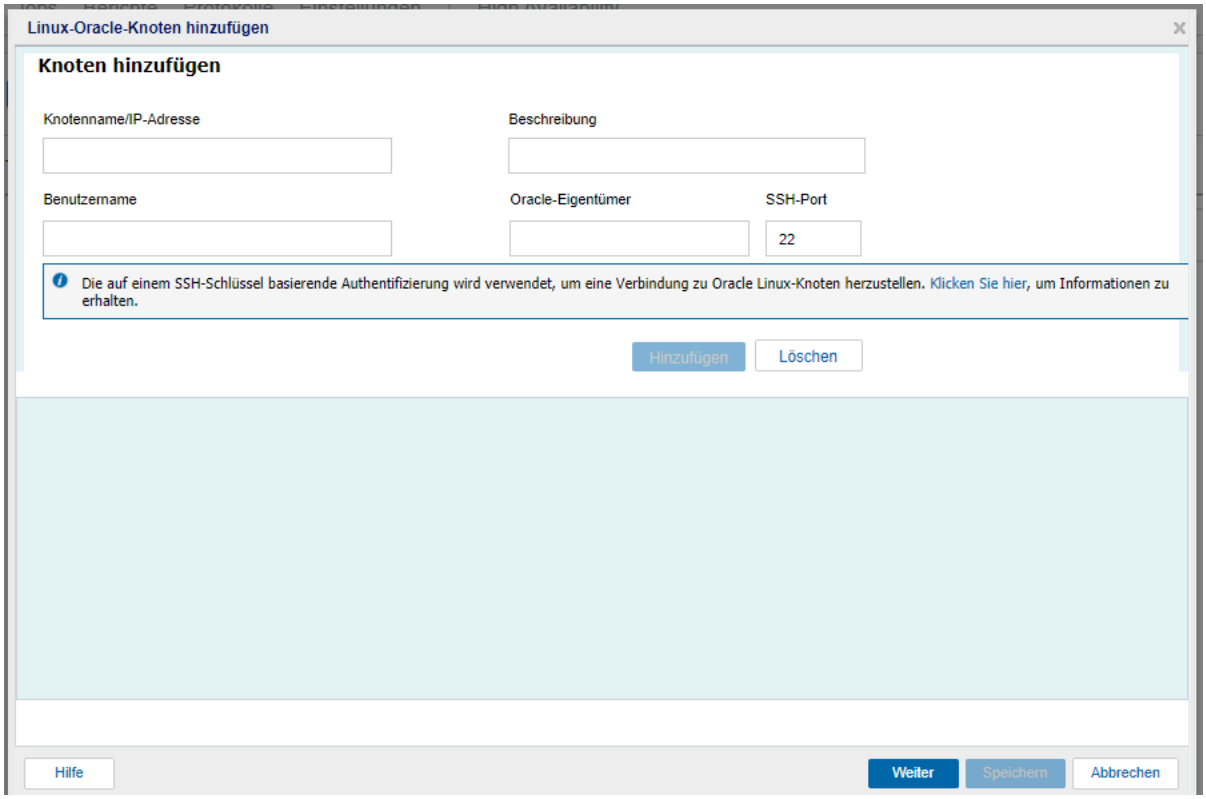
      Der Knoten wird im mittleren Fensterbereich hinzugefügt.
   g. Um mehrere Knoten hinzuzufügen, führen Sie die Schritte erneut aus. Alle hinzugefügten Knoten werden im mittleren Fensterbereich aufgeführt.

h. Klicken Sie auf das Erweiterungssymbol neben der IP-Adresse, und überprüfen Sie die hinzugefügten Details.

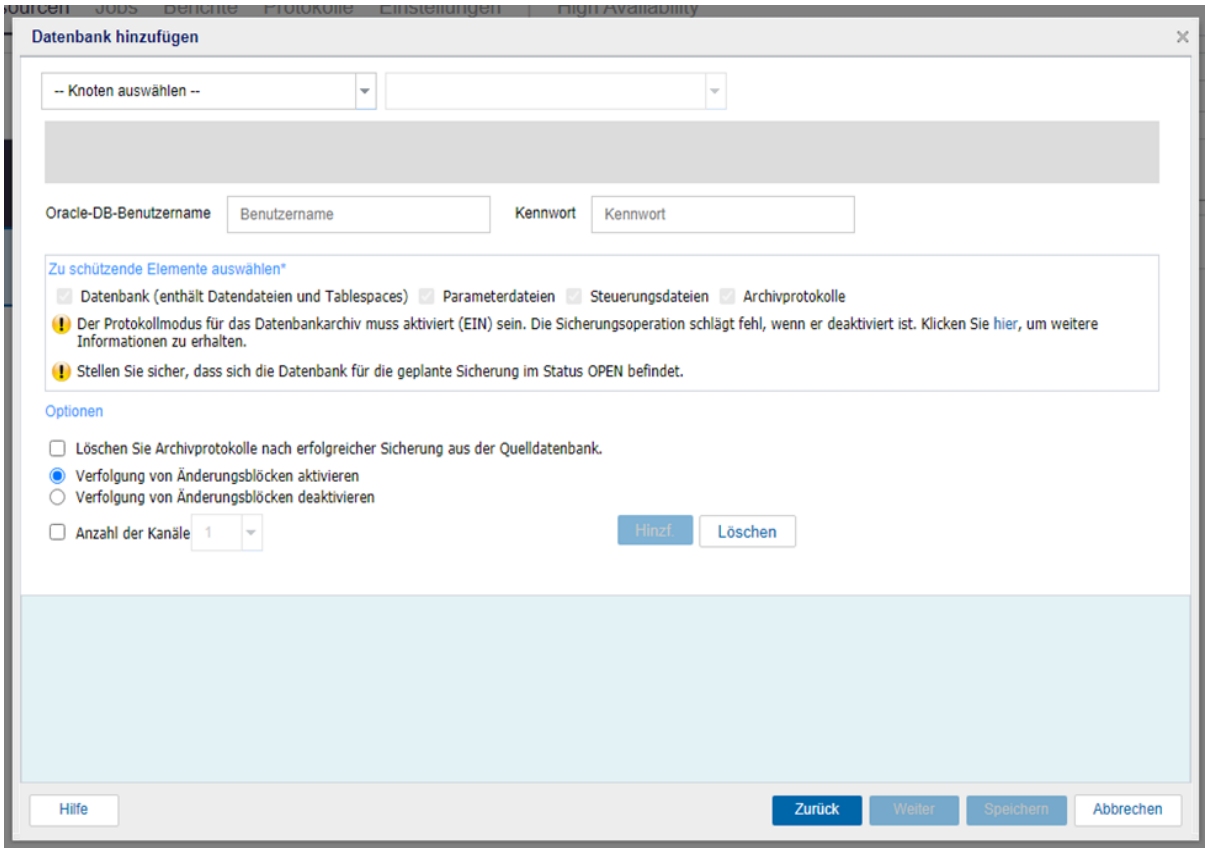
Hinweise:

- Um die hinzugefügten Knoten in der Liste zu bearbeiten, wählen Sie den zu bearbeitenden Knoten aus, und klicken Sie auf **Bearbeiten**.
- Um die hinzugefügten Knoten aus der Liste zu entfernen, wählen Sie die zu entfernenden Knoten aus, und klicken Sie dann auf **Entfernen**.
- Um alle hinzugefügten Knoten zu entfernen, klicken Sie auf **Alle entfernen**.

i. Klicken Sie auf **Weiter**.



7. Führen Sie im Dialogfeld "Datenbank hinzufügen" die folgenden Schritte aus:



a. Wählen Sie den Knoten in der Drop-down-Liste aus.

   Warten Sie, bis die Liste der auf dem ausgewählten Host verfügbaren Datenbanken angezeigt und die Drop-down-Liste aktiviert wird.

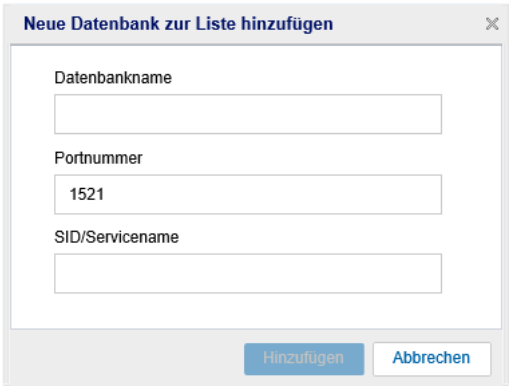
b. Führen Sie in der Drop-down-Liste eine der folgenden Aktionen aus:

   Neue Datenbank hinzufügen

   Gehen Sie wie folgt vor, um eine neue Datenbank hinzuzufügen:

   1. Wählen Sie die Option **Neue Datenbank hinzufügen** aus.
   2. Führen Sie im Dialogfeld "Add New database to List///" die folgenden Aktionen aus, und klicken Sie dann auf **Hinzufügen**:

      - **Datenbankname/SID:** Geben Sie den Datenbanknamen oder SID-Namen ein.
      - **Portnummer**: Geben Sie die Portnummer ein. Der Standardwert für den Port ist 1521.
      - **Dienstname:** Geben Sie den Dienstnamen ein.



Die neue Datenbank wird zur Drop-down-Liste hinzugefügt.

Vorhandene Datenbank auswählen

Wählen Sie die Datenbank in der Drop-down-Liste nach Bedarf aus. Nachdem die Datenbank ausgewählt wurde, wird sie aus der Liste entfernt und im mittleren Fensterbereich angezeigt.

Hinweise:

- Um Mehrfacheingaben für jede Datenbank zu vermeiden, gruppieren Sie die Datenbanken, die Sie mit dem gleichen Benutzernamen und Kennwort konfiguriert haben.
- Um den Datenbanken mit unterschiedlichen Anmeldeinformationen unterschiedliche Dateitypen hinzuzufügen, wählen Sie die einzelnen Datenbanken aus, und führen Sie dann die Hinzufügung durch.
- Gehen Sie folgendermaßen vor, um eine Datenbank aus der Gruppe (im mittleren Fensterbereich) zu entfernen:

  a. Klicken Sie auf den Datenbanknamen.

     Eine Bestätigungsmeldung wird angezeigt.

  b. Klicken Sie auf **Ja**, um zu bestätigen.

  Die Datenbank wurde erfolgreich entfernt und wird wieder zur Drop-down-Liste hinzugefügt.

c. Geben Sie die Anmeldeinformationen des Systembenutzers für Oracle DB ein.

Hinweise:

- Alle zu schützenden Elemente wie Datenbank (einschließlich Datendateien und Tablespaces), Kontrolldateien, Parameterdateien und Archivprotokolle sind standardmäßig aktiviert.

- Stellen Sie sicher, dass der ARCHIVELOG-Modus für die Datenbank aktiviert wurde, bevor der Sicherungsvorgang ausgelöst wird. Informationen darüber, wie Sie die Aktivierung des ARCHIVELOG-Protokollmodus überprüfen, finden Sie unter Überprüfen der Voraussetzungen für Oracle-Datenbanken. Wenn der ARCHIVELOG-Modus nicht aktiviert ist, schlägt der Sicherungsjob fehl.

d. Geben Sie unter "Optionen" Folgendes an:

Archivprotokolle nach erfolgreicher Sicherung aus der Quelldatenbank löschen

Ermöglicht es Ihnen, die Archivprotokolle nach einer erfolgreichen Sicherung aus der Quelldatenbank zu löschen.

Anzahl der Kanäle

Ermöglicht es Ihnen, die Anzahl der Kanäle oder Threads auszuwählen, die für den Sicherungsjob erstellt werden sollen.

Hinweis: Es werden maximal 10 Kanäle unterstützt.

Verfolgung von Änderungsblöcken aktivieren

Ermöglicht es Ihnen, die CBT-Funktion (Change Block Tracking, Verfolgung geänderter Blöcke) zu aktivieren. Verwenden Sie diese Option, um die Leistung von RMAN zu verbessern. Sie hilft dem RMAN-Hilfsprogramm oder der Binärdatei, die Änderungsdaten schneller zu finden und den Sicherungsjob auszuführen.

Verfolgung von Änderungsblöcken deaktivieren

Ermöglicht es Ihnen, die CBT-Funktion zu deaktivieren.

Hinweis: Oracle unterstützt die Funktion zum Verfolgen der Blockänderung deaktivieren nur für die Enterprise Edition (EE).

e. Klicken Sie auf **Hinzufügen**.

Alle hinzugefügten Datenbanken werden aufgelistet.

Hinweis: Nachdem Sie auf die Schaltfläche "Hinzufügen" geklickt haben, werden alle Datenbank-Anmeldeinformationen und die Firewall-Parameter überprüft.

f. Um mehrere Datenbanken hinzuzufügen, führen Sie die Schritte erneut aus. Alle hinzugefügten Datenbanken werden aufgelistet.

g. Klicken Sie auf das Erweiterungssymbol neben der IP-Adresse, und überprüfen Sie die hinzugefügten Details.

Hinweise:

- Um die hinzugefügten Datenbanken in der Liste zu bearbeiten, wählen Sie die zu bearbeitende Datenbank aus, und klicken Sie auf **Bearbeiten**.
- Um die hinzugefügten Datenbanken aus der Liste zu entfernen, wählen Sie die zu entfernenden Datenbanken aus, und klicken Sie dann auf **Entfernen**.

8. Klicken Sie auf **Speichern**.

   Hinweise:

   - Sie können mehrere Knoten und Datenbanken hinzufügen.
   - Um die Quelle zu entfernen, aktivieren Sie das Kontrollkästchen neben der hinzugefügten Quelle, und klicken Sie dann auf **Entfernen**.

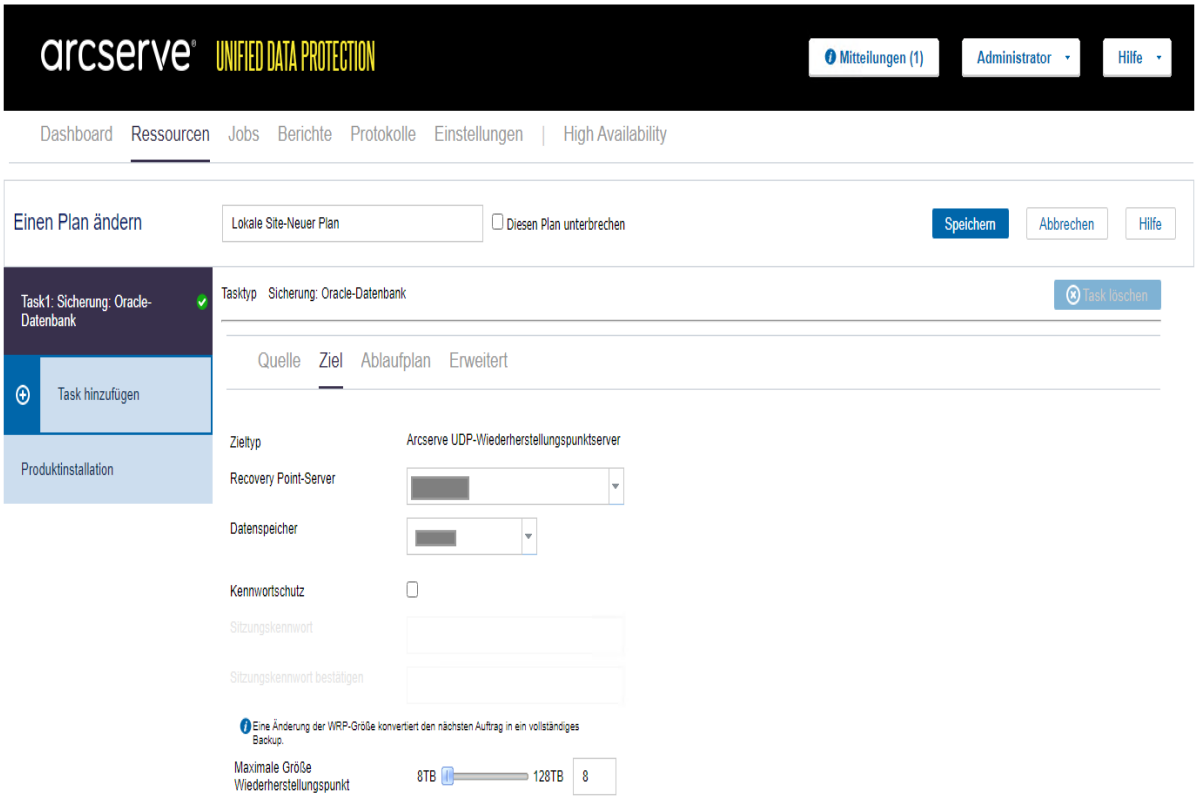
   Die Sicherungsquelle ist nun angegeben.

Angeben des Ziels

Das Ziel ist ein Speicherort, an dem Sie die Sicherungsdaten speichern. Das Ziel ist die grundlegende Angabe, die Sie festlegen müssen, um den Plan zu speichern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ziel**.



2. Gehen Sie folgendermaßen vor:
   - **Recovery Point Server:** Wählen Sie den Ziel-Recovery Point Server (RPS) in der Drop-down-Liste aus.
   - **Datenspeicher:** Wählen Sie den Zieldatenspeicher in der Drop-down-Liste aus.

- **Kennwortschutz:** Aktivieren Sie das Kontrollkästchen **Kennwortschutz**, geben Sie das Sitzungskennwort ein, und geben Sie es zur Bestätigung erneut ein.

  Hinweis: Das Sitzungskennwort ist optional, wenn das Sicherungsziel ein unverschlüsselter RPS-Datenspeicher ist.

- **Maximale Größe Wiederherstellungspunkt:** Gibt die Größe des Recovery Point Servers für die Sicherung an. Legen Sie die Größe des Recovery Point Servers auf der Skala fest.

  Bereich: 8 TB bis 128 TB

Das Ziel ist nun angegeben.

Festlegen des Ablaufplans

Auf der Seite "Ablaufplan" können Sie einen Ablaufplan definieren, damit die Sicherungs-, Zusammenführungs- und Drosselungsfunktion zu festgelegten Intervallen wiederholt wird. Nachdem Sie einen Ablaufplan definiert haben, werden die Jobs automatisch gemäß dem Ablaufplan ausgeführt. Sie können mehrere Ablaufpläne hinzufügen und Einstellungen für die Aufbewahrungszeit angeben.

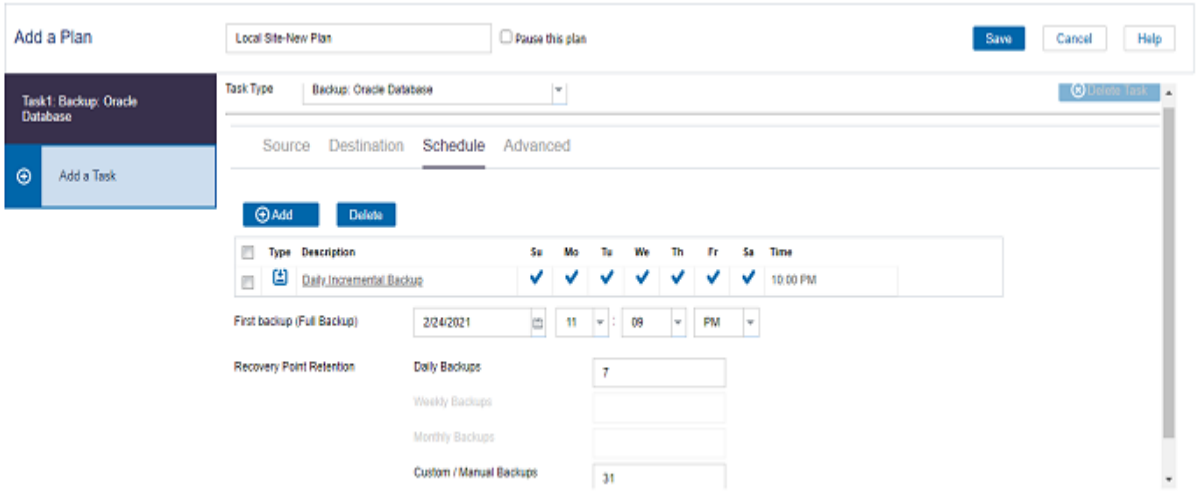
Ein Sicherungsablaufplan ist ein Plan für regelmäßige Ausführungen, die basierend auf der Anzahl der Stunden oder Minuten, die Sie auswählen, mehrmals täglich wiederholt wird. Zusätzlich zum normalen Ablaufplan können in einem Sicherungsablaufplan auch tägliche, wöchentliche und monatliche Sicherungen geplant werden.

Wenn RPS-Server das Sicherungsziel ist, dann ist der Standardwert eine tägliche Zuwachssicherung für alle Dateitypen jeden Abend um 22 Uhr.

Sie können einen Jobplan der Sicherung bearbeiten oder löschen.

Gehen Sie wie folgt vor:

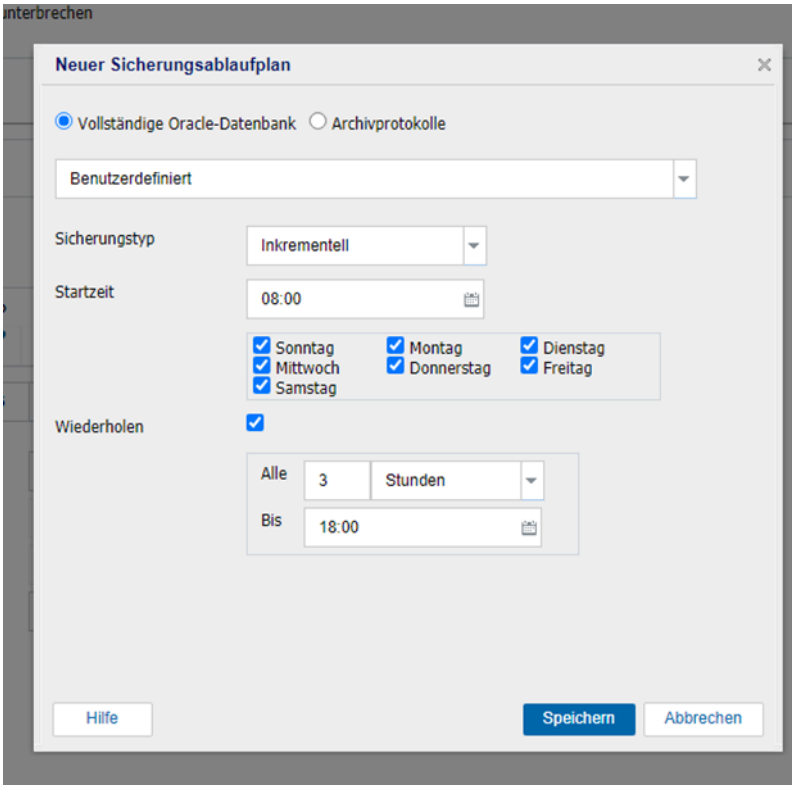
1. Klicken Sie auf die Registerkarte **Ablaufplan**, und fügen Sie dann Ablaufpläne für Sicherung, Zusammenführung und Drosselung für Datenträger-Lesevorgang hinzu.



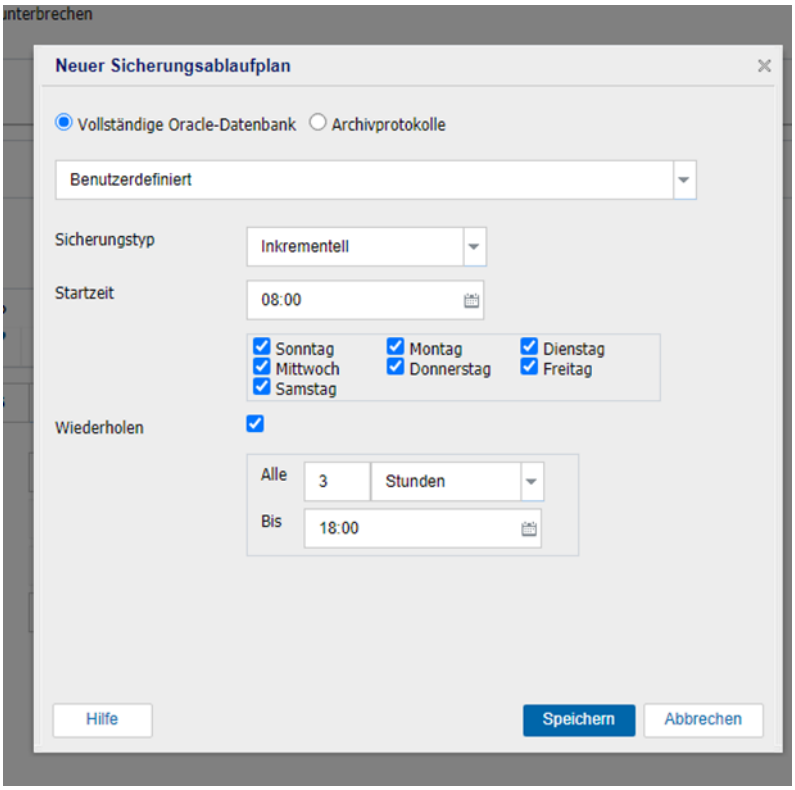
2. Gehen Sie folgendermaßen vor, um einen Sicherungsablaufplan hinzuzufügen:
    a. Klicken Sie auf **Hinzufügen**, und wählen Sie dann die Option **Sicherungsablaufplan hinzufügen** aus.

       Das Dialogfeld Neuer Sicherungsablaufplan wird geöffnet.

b. Wählen Sie im Dialogfeld "Neuer Sicherungsablaufplan" eine der folgenden Optionen aus:



Vollständig Oracle-Datenbank



Gehen Sie folgendermaßen vor:

a. Wählen Sie in der Drop-down-Liste eine der folgenden Optionen aus:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

Stündlich

Gibt an, dass die geplante Sicherung einmal pro Stunde durchgeführt wird.

Minute

Gibt den Ablaufplan für die Sicherung mit einer Mindestdauer von 15 Minuten an.

b. Wählen Sie in der Drop-down-Liste "Sicherungstyp" den Sicherungstyp aus.

Vollständige Sicherung

Legt den Sicherungsablaufplan für vollständige Sicherungen (alle Dateitypen) fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Dateitypen des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Zuwachssicherung

Legt den Ablaufplan für Zuwachssicherungen fest.

Wie geplant sichert Arcserve UDP inkrementell alle Dateitypen seit der letzten erfolgreichen Sicherung. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Diese ist der optimale Weg, um eine Sicherung durchzuführen.

Hinweis: Die Kontrolldatei wird für jeden Sicherungstyp immer vollständig gesichert.

c. Geben Sie die Startzeit für die Sicherung an.

d. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

Hinweis: Stellen Sie sicher, dass die Zeit für die Wiederholung des Ablaufplans nicht weniger als 15 Minuten beträgt.

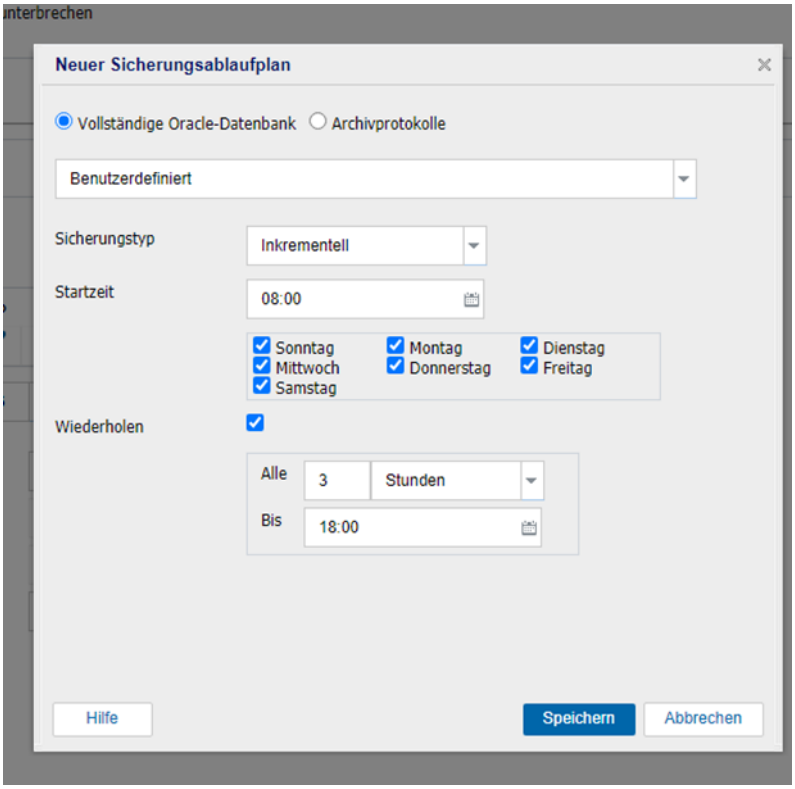
e. Wenn Sie die Option **Stündlich** in der Drop-down-Liste ausgewählt haben, gehen Sie folgendermaßen vor:

1. Wählen Sie den Sicherungstyp in der Drop-down-Liste "Sicherungstyp" aus.
2. Geben Sie die Startzeit für die Sicherung an.
3. Geben Sie die Endzeit für die Sicherung an.
4. Wählen Sie die Wiederholungszeit für die Sicherung in der Drop-down-Liste aus.

Hinweis: Wenn Sie die Wiederholungszeit für die Sicherung anpassen möchten, wählen Sie "Benutzerdefiniert" in der Drop-down-Liste aus, und geben Sie dann die Zeit in Stunden ein.

f. Klicken Sie auf **Speichern**.

Archivprotokolle



Gehen Sie folgendermaßen vor:

a. Wählen Sie in der Drop-down-Liste eine der folgenden Optionen aus:

Benutzerdefiniert

Gibt an, dass die geplante Sicherung mehrmals täglich wiederholt wird.

Täglich

Gibt an, dass die geplante Sicherung einmal täglich durchgeführt wird. Standardmäßig werden alle Wochentage für die tägliche Sicherung ausgewählt. Wenn Sie den Sicherungsjob an einem bestimmten Tag nicht ausführen möchten, dann deaktivieren Sie das Kontrollkästchen für diesen Wochentag.

Wöchentlich

Gibt an, dass die geplante Sicherung einmal in der Woche durchgeführt wird.

Monatlich

Gibt an, dass die geplante Sicherung einmal im Monat durchgeführt wird.

Stündlich

Gibt an, dass die geplante Sicherung einmal pro Stunde durchgeführt wird.

Minute

Gibt den Ablaufplan für die Sicherung mit einer Mindestdauer von 15 Minuten an.

b. Wählen Sie in der Drop-down-Liste "Sicherungstyp" den Sicherungstyp aus.

Vollständige Sicherung

Legt den Ablaufplan für vollständige Sicherungen der Archivprotokolle fest. Arcserve UDP führt wie geplant eine vollständige Sicherung aller verwendeten Archivprotokolle des Quellrechners durch. Eine vollständige Sicherung nimmt abhängig von der Sicherungsgröße üblicherweise etwas Zeit in Anspruch.

Zuwachssicherung

Legt den Ablaufplan für inkrementelle Sicherungen der Archivprotokolle fest.

Als Teil eines Ablaufplans erstellt Arcserve UDP nur Zuwachssicherungen von jenen Archivprotokollen, die seit der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Diese ist der optimale Weg, um eine Sicherung durchzuführen.

c. Geben Sie die Startzeit für die Sicherung an.

d. (Optional) Aktivieren Sie das Kontrollkästchen **Wiederholen**, und geben Sie den Ablaufplan für Wiederholungen an.

Hinweis: Stellen Sie sicher, dass die Zeit für die Wiederholung des Ablaufplans nicht weniger als 15 Minuten beträgt.

e. Wenn Sie die Option **Stündlich** in der Drop-down-Liste ausgewählt haben, gehen Sie folgendermaßen vor:

1. Wählen Sie den Sicherungstyp in der Drop-down-Liste "Sicherungstyp" aus.

2. Geben Sie die Startzeit für die Sicherung an.
3. Geben Sie die Endzeit für die Sicherung an.
4. Wählen Sie die Wiederholungszeit für die Sicherung in der Drop-down-Liste aus.

   Hinweis: Wenn Sie die Wiederholungszeit für die Sicherung anpassen möchten, wählen Sie **Benutzerdefiniert** in der Drop-down-Liste aus, und geben Sie dann die Zeit in Stunden ein.

f. Klicken Sie auf **Speichern**.

Der Sicherungsablaufplan ist nun festgelegt und wird auf der Seite Ablaufplanung angezeigt.

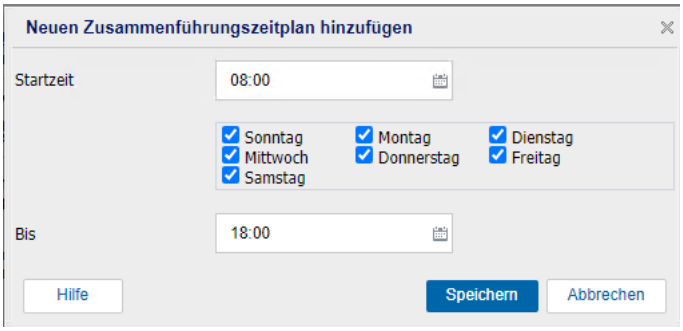
3. Gehen Sie folgendermaßen vor, um einen Ablaufplan für die Zusammenführung hinzuzufügen:

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie dann die Option **Zusammenführungsplan hinzufügen** aus.

      Das Dialogfeld "Neuen Zusammenführungsplan hinzufügen" wird geöffnet.

   b. Gehen Sie im Dialogfeld "Neuen Zusammenführungsplan hinzufügen" folgendermaßen vor:

      - **Startzeit:** Geben Sie die Startzeit an, zu der der Zusammenführungsjob starten soll.
      - **Bis:** Geben Sie die Endzeit des Zusammenführungsjobs an.



   c. Klicken Sie auf **Speichern**.

Der Zusammenführungsplan ist nun festgelegt und wird auf der Seite Ablaufplanung angezeigt.

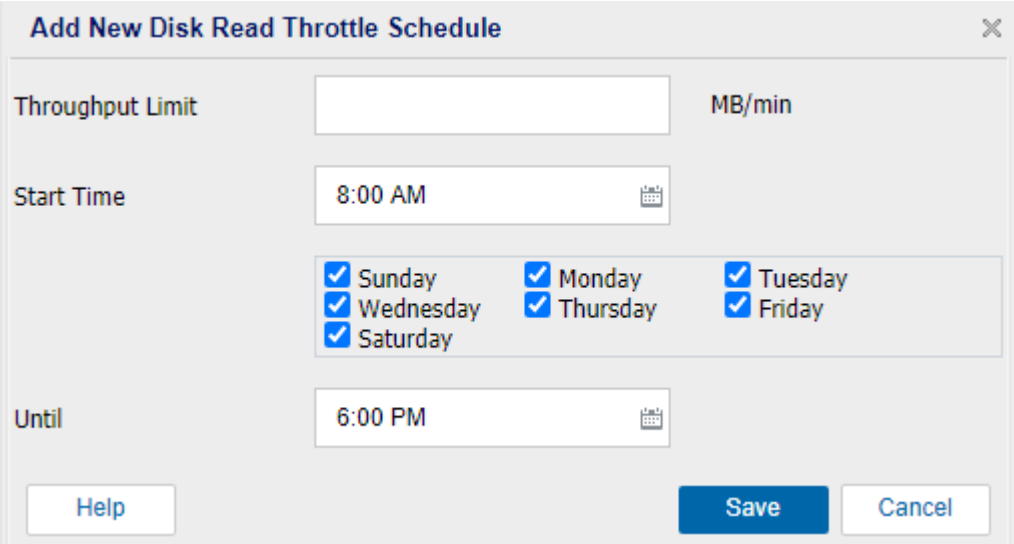
4. Gehen Sie wie folgt vor, um einen Drosselungsplan für Datenträger-Lesevorgänge hinzuzufügen:

   a. Klicken Sie auf **Hinzufügen**, und wählen Sie dann die Option **Drosselungsplan für Datenträger-Lesevorgang hinzufügen** aus.

Das Dialogfeld "Neuen Drosselungsplan für Datenträger-Lesevorgang" hinzufügen wird geöffnet.

b. Gehen Sie im Dialogfeld "Neuen Drosselungsplan für Datenträger-Lesevorgang" folgendermaßen vor:

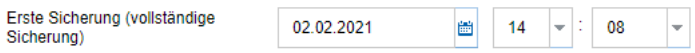
- **Durchsatzbeschränkung:** Geben Sie die Durchsatzbeschränkung in MB pro Minute an.
- **Startzeit:** Geben Sie die Startzeit für den Sicherungsdurchsatzjob an.
- **Bis:** Geben Sie die Endzeit für den Sicherungsdurchsatzjob an.



c. Klicken Sie auf **Speichern**.

Der Drosselungsplan für Datenträger-Lesevorgänge ist nun festgelegt und wird auf der Seite Ablaufplanung angezeigt.

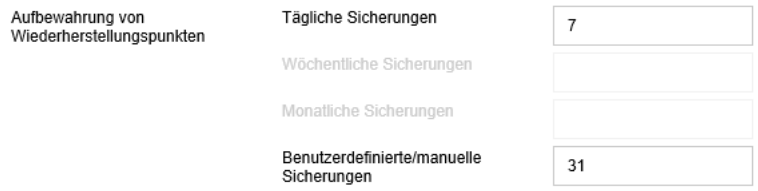
5. Geben Sie die Startzeit für die geplante Sicherung an.



Hinweis: Der obige Screenshot gilt nicht für RMAN-Sicherungen.

6. Geben Sie die Einstellungen für die Aufbewahrung von Wiederherstellungspunkten für benutzerdefinierte, tägliche, wöchentliche und monatliche Wiederholungen an.

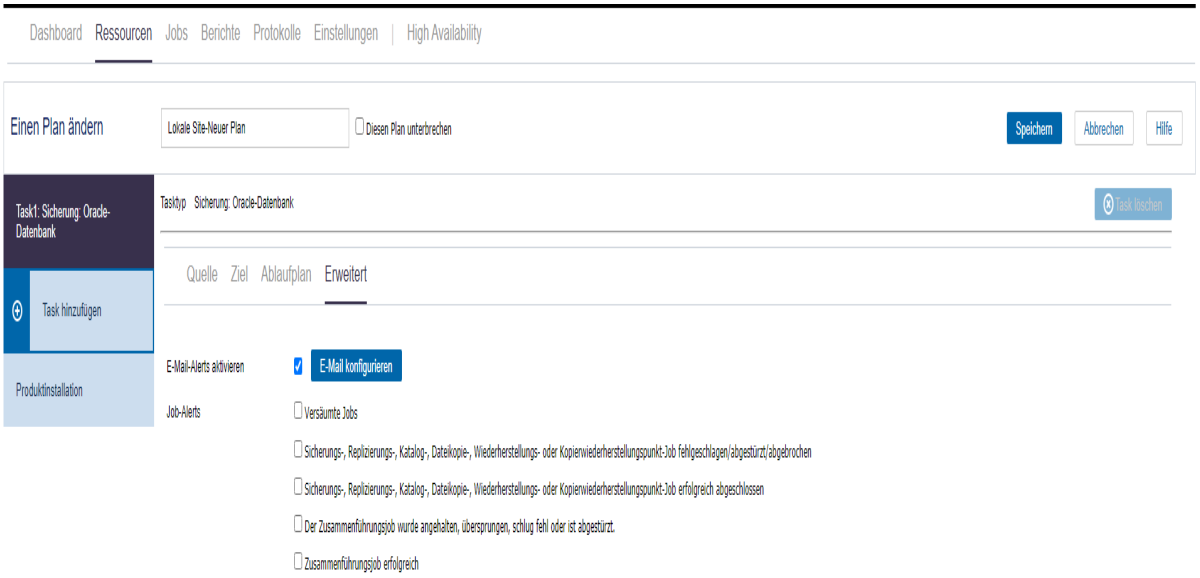
   Diese Optionen sind aktiviert, wenn Sie einen entsprechenden Sicherungsablaufplan hinzugefügt haben. Änderungen an den Aufbewahrungseinstellungen, die Sie auf dieser Seite vornehmen, werden im Dialogfeld "Sicherungsablaufplan" übernommen.



Der Ablaufplan ist nun angegeben.

Festlegen von erweiterten Einstellungen

Auf der Registerkarte Erweitert können Sie eine Reihe von erweiterten Einstellungen für den Sicherungsjob angeben.



Gehen Sie wie folgt vor:

1. Geben Sie die folgenden Details an:

   E-Mail-Alerts aktivieren

   Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Arten der Alerts angeben, die Sie in Form von E-Mails empfangen möchten. Wenn Sie diese Option auswählen, werden folgende Optionen für Ihre Auswahl aktiviert.

   E-Mail konfigurieren

   Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren.

Klicken Sie auf **E-Mail konfigurieren**, um die Details des E-Mail-Servers und des Proxy-Servers zu konfigurieren.

Job-Alerts

Ermöglicht es Ihnen, die Typen der Job-E-Mails anzugeben, die Sie erhalten möchten.

2. Klicken Sie auf **Speichern**.

Die erweiterten Einstellungen sind angegeben.

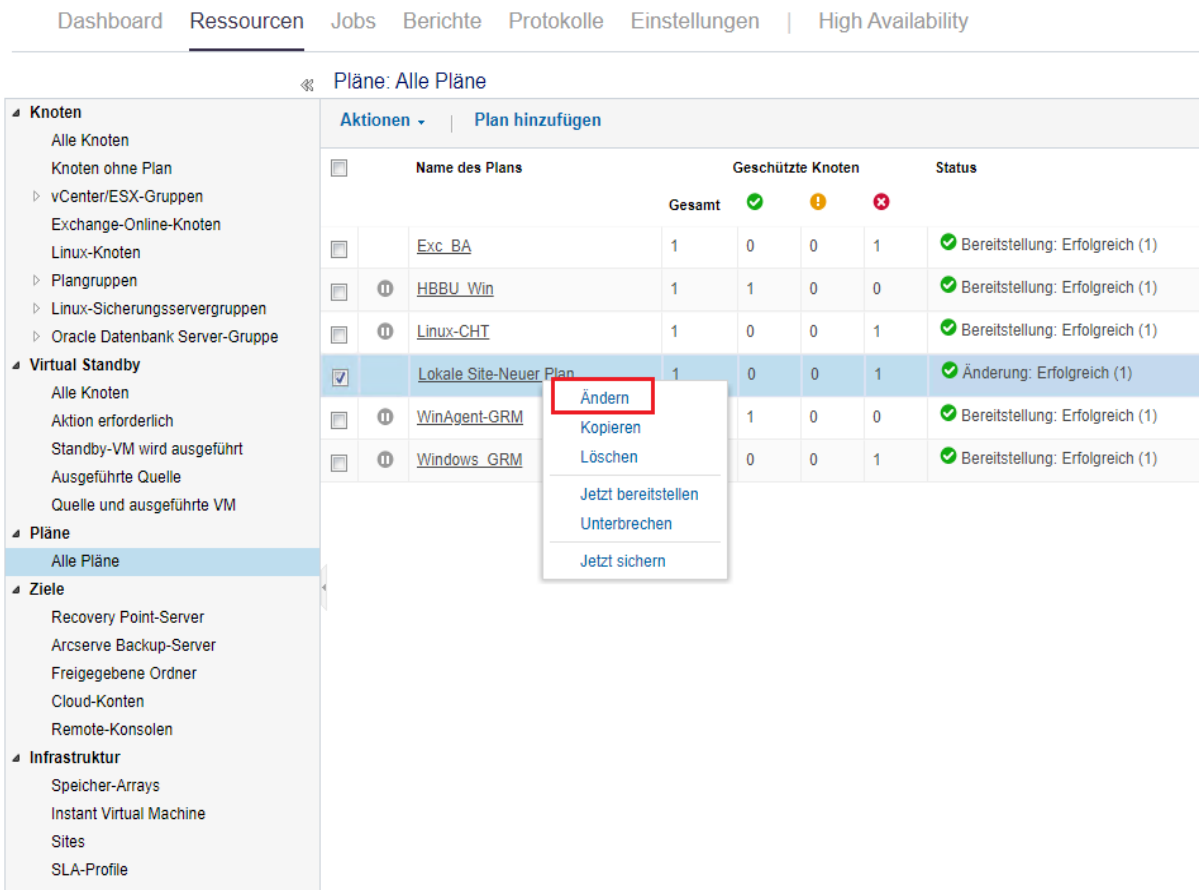
Hinzufügen eines Assured Recovery-Tasks zum Plan

Ein Assured Recovery-Task fügt einen Assured Recovery-Task zu einem vorhandenen Sicherungs-/Replikationsplan hinzu. Jeder Task besteht aus Parametern, die die Quelle, Testeinstellungen, den Ablaufplan und erweiterte Einstellungen definieren. Erstellen Sie einen Assured Recovery-Task auf Basis eines Sicherungs-/Replikationstasks, um zu überprüfen, ob auf die Daten zugegriffen werden kann und sie auf jeden Fall wiederhergestellt werden können, und um die Datenintegritätsprüfung durchzuführen.

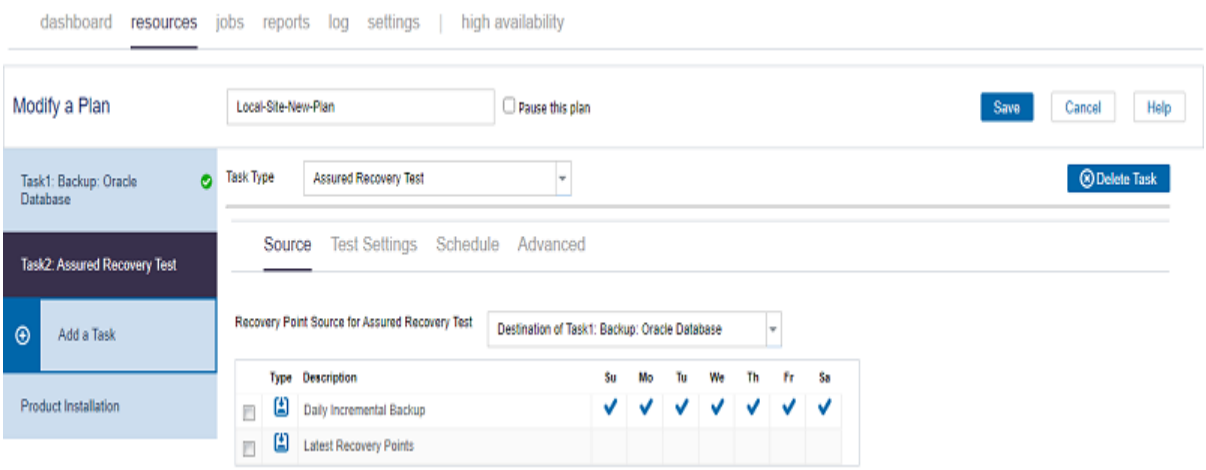
Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie dann auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich mit der rechten Maustaste auf den vorhandenen Sicherungsplan, und klicken Sie dann auf **Ändern**.



4. Klicken Sie auf der Seite "Plan ändern" im linken Fensterbereich auf **Task hinzufügen**.



5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn Sie den Plan unterbrechen, wird der Assured Recovery-Job nicht gestartet. Wenn Sie den Plan wieder aufnehmen, wird der Assured Recovery-Job nicht automatisch fortgesetzt. Sie müssen einen anderen Sicherungsjob manuell ausführen, um den Assured Recovery-Job zu starten.

6. Wählen Sie in der Drop-down-Liste "Tasktyp" die Option **Assured Recovery-Test** aus.

7. Geben Sie nun Details unter Quelle, Testeinstellungen, Ablaufplan und Erweitert an.

8. Klicken Sie auf **Speichern**

   Die Änderungen werden gespeichert, und der Assured Recovery-Task wird automatisch bereitgestellt.

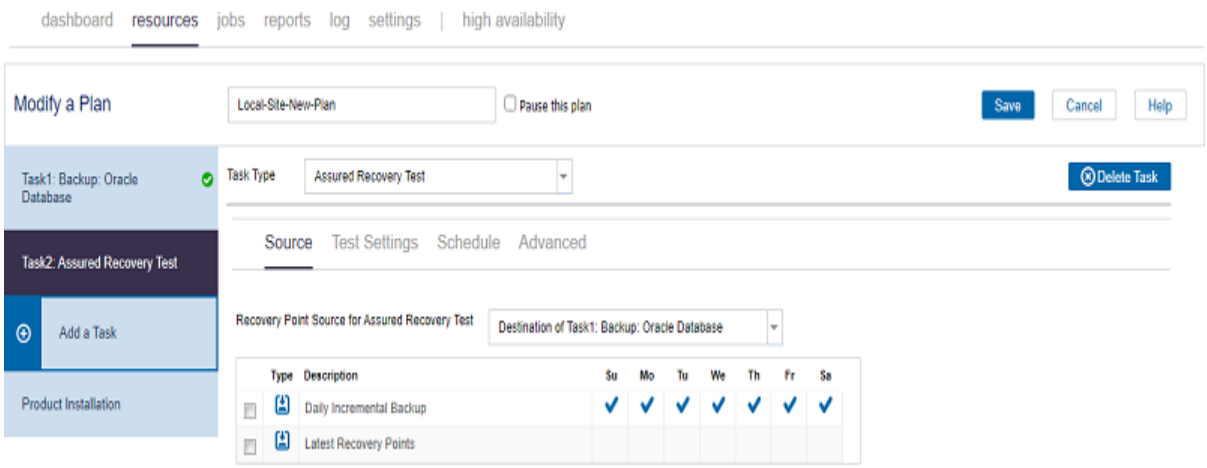
   Hinweis: Um die Integrität von Oracle-Sicherungsdaten wie Kontrolldateien, Datendateien, Archivprotokollen und SP-Dateien zu überprüfen, führt der Assured Recovery-Job den Befehl "RMAN validieren" auf dem Recovery Point Server aus.

Angeben der Quelle

Auf der Registerkarte "Quelle" können Sie den Quellwiederherstellungspunkt angeben, den Sie schützen möchten.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Quelle" in der Drop-down-Liste "Wiederherstellungspunktquelle für Assured Recovery-Test" die gewünschte Option aus.



2. Wählen Sie Typen von Wiederherstellungspunkten für Assured Recovery-Tests aus. Die zwei folgenden Optionen stehen zur Auswahl:

   - Assured Recovery-Test aus ausgewählten Sicherungstypen

     Sie können "Tägliche Sicherungen", "Wöchentliche Sicherungen" oder "Monatliche Sicherungen" auswählen. Die Optionen für tägliche, wöchentliche oder monatliche Sicherungen werden in Abhängigkeit vom Ablaufplan der Quellsicherung aktiviert. Wenn für die Quellsicherung beispielsweise nur eine monatliche Sicherung geplant ist, ist bei der Option "Assured Recovery-Test aus ausgewählten Sicherungstypen" nur "Monatliche Sicherungen" aktiviert.

   - Assured Recovery Test von den letzten Wiederherstellungspunkten

Die Sicherungsquelle ist nun angegeben

Nächste Schritte:

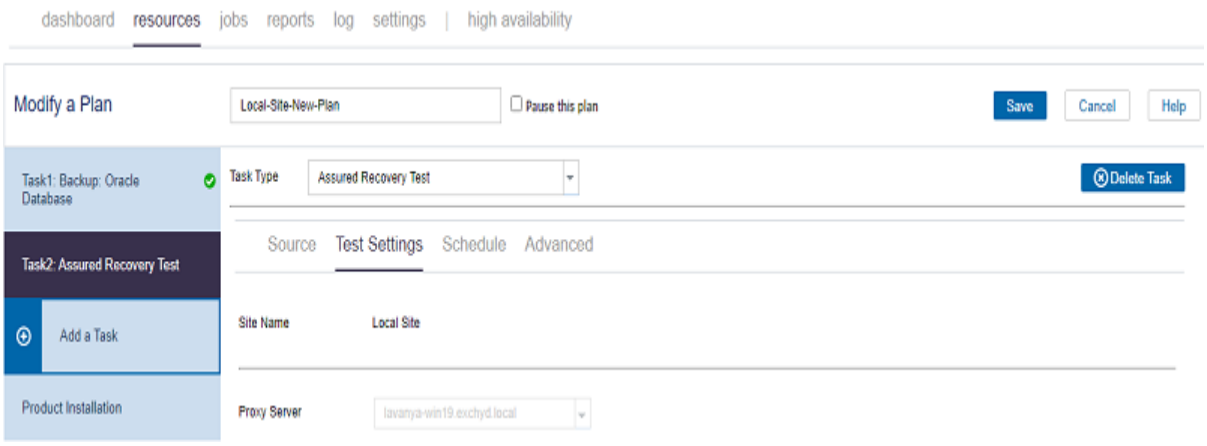
- Angeben der Testeinstellungen
- Angeben eines Ablaufplans für Assured Recovery-Testjobs
- Festlegen von erweiterten Einstellungen

Angeben der Testeinstellungen

Auf der Registerkarte "Testeinstellungen" können Sie den Proxy-Server angeben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Testeinstellungen**.



2. Wählen Sie in der Drop-down-Liste "Proxy-Server" den Proxy-Knoten aus.

   Hinweis: Für Oracle fungiert der Recovery Point Server im Assured Recovery-Test selbst als Proxy-Server.

   Die Testeinstellungen sind angegeben.

Nächste Schritte:

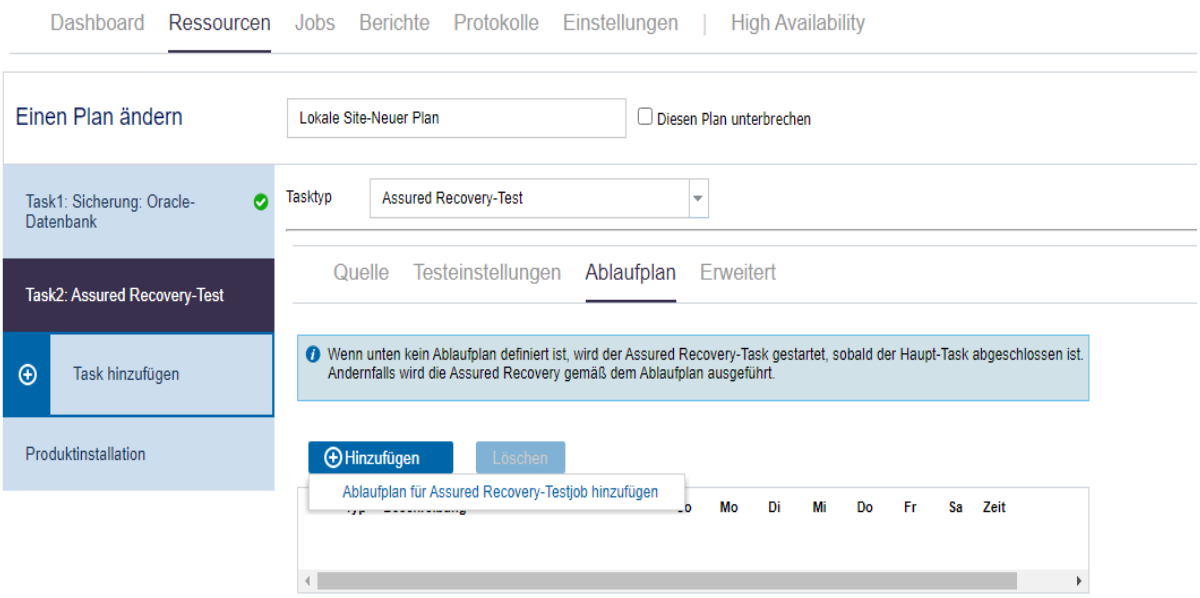
- Angeben eines Ablaufplans für Assured Recovery-Testjobs
- Festlegen von erweiterten Einstellungen

Angeben eines Ablaufplans für Assured Recovery-Testjobs

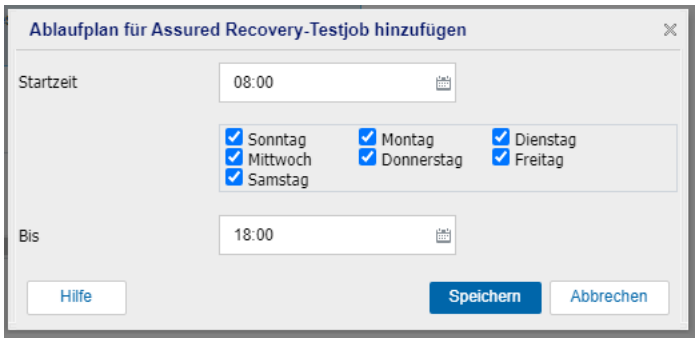
Auf der Registerkarte "Ablaufplan" können Sie den Ablaufplan für Assured Recovery-Testjobs festlegen. Wenn Sie keinen Ablaufplan angeben, wird der Task sofort gestartet, nachdem Sie den primären Task abgeschlossen haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Ablaufplan**.



2. Klicken Sie auf **Hinzufügen**, und wählen Sie dann **Ablaufplan für Assured Recovery-Testjob hinzufügen** aus.
3. Führen Sie im Dialogfeld "Ablaufplan für Assured Recovery-Testjob hinzufügen" die folgenden Schritte aus, und klicken Sie dann auf **Speichern**:
   - **Startzeit:** Geben Sie die Startzeit an, zu der der Assured Recovery-Testjob gestartet werden soll.
   - **Bis:** Geben Sie die Endzeit für den Assured Recovery-Testjob an.



Der Assured Recovery-Testjob wird geplant und auf der Seite "Ablaufplan" angezeigt.

Hinweise:

- Wenn die Assured Recovery-Quelle über den Ablaufplan "Letzte Widerherstellungspunkte + Assured Recovery aktivieren" verfügt, ist der Standardwert 1. Dadurch wird standardmäßig der letzte Widerherstellungspunkt überprüft.

  Bei einem Wert< = 0 werden alle nicht verifizierten Widerherstellungspunkte getestet.

- Wenn die Assured Recovery-Quelle über den Ablaufplan "Täglich/Wöchentlich/Monatlich + Assured Recovery aktivieren" verfügt, ist der Standardwert 9 (7 täglich + 1 wöchentlich + 1 monatlich).

  Bei einem Wert< = 0 werden alle nicht verifizierten Widerherstellungspunkte getestet.

- Wenn Sie nicht den Standardwert verwenden möchten, können Sie einen DWORD-32-Bit-Registrierungsschlüssel an folgendem Ort hinzufügen:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AssuredRecovery\MaxNumberOfRecoveryPoint

Nächster Schritt:

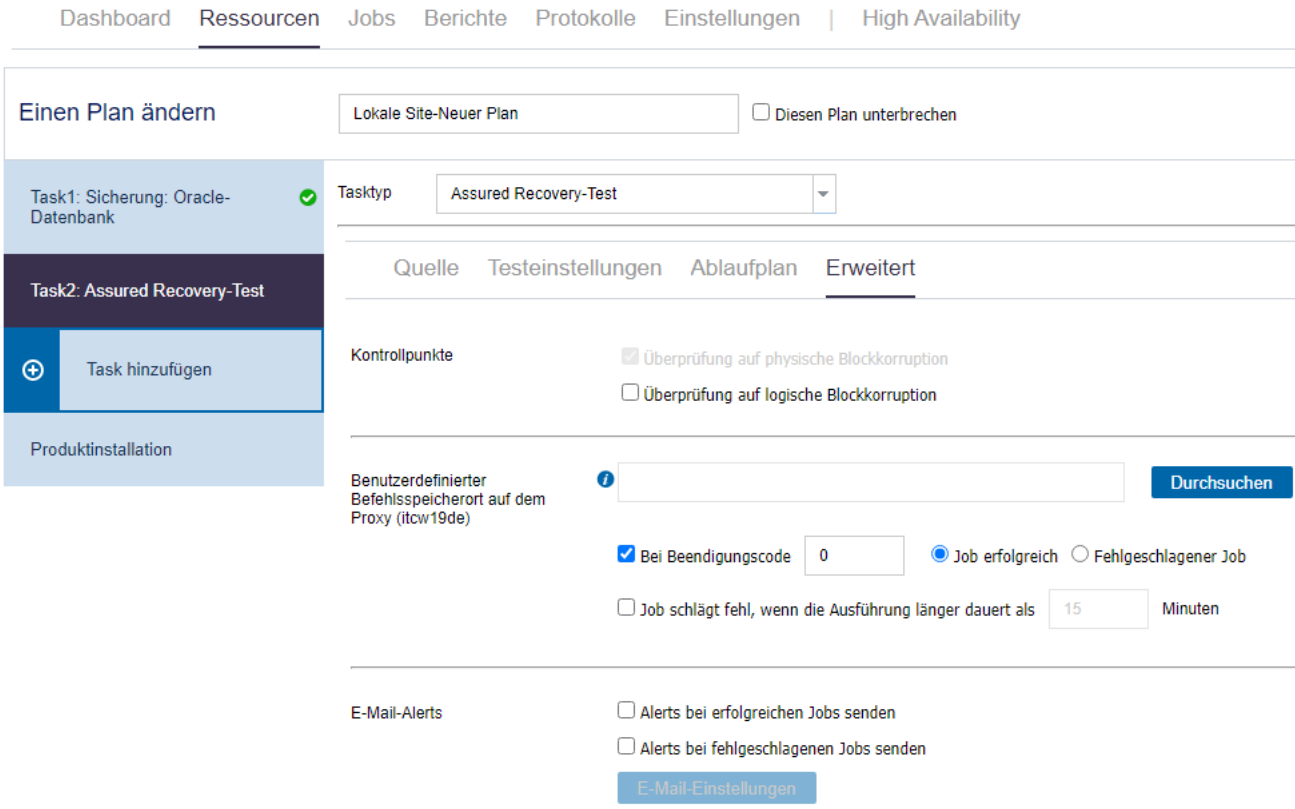
- Festlegen von erweiterten Einstellungen

Festlegen von erweiterten Einstellungen

Auf der Registerkarte "Erweitert" können Sie andere für den Abschluss des Plans erforderliche Einstellungen festlegen. Diese Einstellungen sind optional und müssen nicht vorgenommen werden, wenn Sie keine weiteren Einstellungen hinzufügen müssen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Erweitert**.



2. Gehen Sie folgendermaßen vor:

   Kontrollpunkte

   Überprüfung auf physische Blockkorruption

   RMAN erkennt bei jeder Sicherung nur physisch beschädigte Blöcke und speichert die Informationen zu Beschädigung in der Kontrolldatei und der Datei "alert.log". Standardmäßig ist die Option **Überprüfung auf physische Blockkorruption** aktiviert.

   Überprüfung auf logische Blockkorruption

Standardmäßig werden logisch beschädigte Blöcke von RMAN nicht automatisch erkannt. Aktivieren Sie das Kontrollkästchen **Überprüfung auf logische Blockkorruption**, um die logische Beschädigung zusammen mit der physischen Beschädigung zu erkennen. Wenn eine logische Beschädigung gefunden wird, speichert RMAN die Informationen zur Beschädigung in der Datei "alert.log".

Benutzerdefinierter Befehlsspeicherort auf dem Proxy

Hinweis: Diese Option wird nicht angezeigt, wenn Sie Agent-basierte Linux-Sicherung/-Replikation als Wiederherstellungspunktquelle des Assured Recovery-Tests ausgewählt haben.

Gibt das benutzerdefinierte Skript an, das auf dem Proxy-Server gespeichert ist. Sie können die Volume-Informationen des Proxy-Servers durchsuchen. Wenn IVM als Assured Recovery-Typ ausgewählt ist, wird das Skript in die VM kopiert und ausgeführt, wenn die VM gestartet wird. Wenn IVHD als Assured Recovery-Typ ausgewählt ist, wird das Skript auf dem Proxy-Server ausgeführt.

Hinweis: Der Assured Recovery-Job unterstützt nur das ausführbare Windows-BAT-Skript oder die ausführbare Binärdatei. Diese Einschränkung schränkt jedoch Ihre Nutzung des Assured Recovery-Jobs nicht ein. Sie können ein zum Starten Ihres PowerShell-Skripts geschriebenes Windows-Batch-Skript verwenden, mit dem Namen "test.bat" und dem folgenden Inhalt:

Powershell.exe -NoProfile -ExecutionPolicy ByPass -Command "& '%ScriptPath%\AR-check.ps1'"

Darüber hinaus werden die folgenden Argumente gemäß Ihren Anforderungen an das Skript übergeben.

- set PlanName=%1%

- set NodeName=%2%

- set ProxyServer=%3%

- set RecoveryPointName=%3%

- set MountPointRootPathName=%5% (gilt nur für Instant Virtual Disk-Testtyp)

Dadurch wird das BAT-Skript aufgerufen und wie folgt ausgeführt:

Für den Testtyp Instant Virtual Machine:

"%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName

Für den Testtyp Instant Virtual Disk:

%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName MountPointRootPathName

Bei Beendigungscode

Gibt den Beendigungscode für "Job erfolgreich durchführen" oder "Job fehlschlagen" an.

Job erfolgreich

Gibt an, dass der Assured Recovery-Job erfolgreich durchgeführt wird, wenn das Skript den Beendigungscode zurückgibt.

Job fehlschlagen

Gibt an, dass der Assured Recovery-Job fehlschlagen wird, wenn das Skript den Beendigungscode zurückgibt.

Job schlägt fehl, wenn er länger ausgeführt wird als

Gibt an, ob das Skript über die festgelegte Zeit hinaus ausgeführt wird.

Standardwert: 15 Minuten.

E-Mail-Alerts

Ermöglicht es Ihnen, E-Mail-Alerts zu aktivieren. Sie können E-Mail-Einstellungen konfigurieren und die Typen der Alerts angeben, die Sie in einer E-Mail erhalten möchten.

- Wenn Sie E-Mail-Alerts für erfolgreiche Assured Recovery-Jobs erhalten möchten, aktivieren Sie das Kontrollkästchen **Alerts bei erfolgreichen Jobs senden**.
- Wenn Sie E-Mail-Alerts für fehlgeschlagene Assured Recovery-Jobs erhalten möchten, aktivieren Sie das Kontrollkästchen **Alerts bei fehlgeschlagenen Jobs senden**.

  Hinweis: Für Jobs mit Linux-Sicherungsserver nicht verfügbar.

  E-Mail-Einstellungen

  Ermöglicht es Ihnen, die E-Mail-Einstellungen zu konfigurieren.

  Klicken Sie auf **E-Mail-Einstellungen**, um die Details des E-Mail-Servers und des Proxy-Servers zu konfigurieren. Weitere Informationen zur Konfiguration von E-Mail-E-Mail-Einstellungen finden Sie unter Konfigurieren von E-Mails und Alerts.

Die erweiterten Einstellungen sind angegeben.

(Optional) Ausführen einer manuellen Sicherung

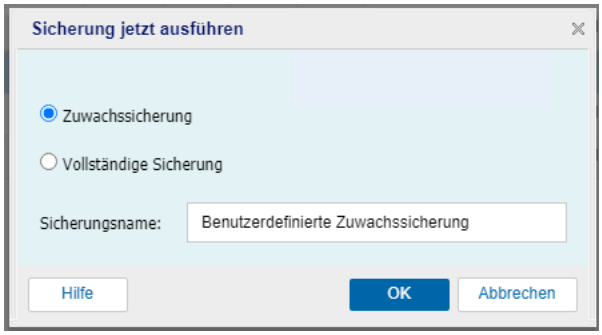
Normalerweise werden Ihre Sicherungen automatisch durchgeführt und von den Ablaufplan-Einstellungen gesteuert. Als Ergänzung zu geplanten Sicherungen können Sie Ihre Knoten durch manuelle Sicherungen bedarfsgerecht sichern. Wenn Sie z. B. einen Wiederholungsplan für vollständige Sicherungen und Zuwachssicherungen festgelegt haben und größere Veränderungen an Ihrem Rechner vornehmen möchten, müssen Sie sofort eine manuelle Sicherung durchführen, ohne auf die nächste geplante Sicherung zu warten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Navigieren Sie zu **Ressourcen** > **Plan** > **Alle Pläne**.

   Die Liste aller Pläne wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Plan, und wählen Sie dann **Jetzt sichern** aus.

   Das Dialogfeld Sicherung jetzt ausführen wird geöffnet.
4. Wählen Sie im Dialogfeld "Sicherung jetzt ausführen" den gewünschten Sicherungstyp aus, und geben Sie dann gegebenenfalls den Sicherungsnamen an.



Es sind folgende Optionen verfügbar:

Zuwachssicherung

Startet eine Zuwachssicherung Ihres Rechners. Eine Zuwachssicherung sichert nur jene Blöcke, die seit der vorherigen Sicherung geändert wurden.

Hinweis: Wenn Sie eine Sicherung zum ersten Mal ausführen, wird automatisch die vollständige Sicherung initiiert, auch wenn Sie die Option "Zuwachssicherung" ausgewählt haben.

Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

Vollständige Sicherung

Startet eine vollständige Sicherung Ihres gesamten Rechners oder der ausgewählten Volumes.

Hinweise:

- Sie können die Sicherung auch manuell über die Seite "Knoten" ausführen.
- Wenn Sie keinen Sicherungsnamen angeben, wird automatisch der Name "Benutzerdefinierte vollständige Sicherung" oder "Benutzerdefinierte Zuwachssicherung" vergeben.

5. Klicken Sie auf **OK**.

   Das Dialogfeld "Fortschrittinformationen" wird angezeigt.

6. Warten Sie, bis der Sicherungsjob abgeschlossen ist, und klicken Sie dann auf **OK**.

7. Um die Sicherungsjobs zu überwachen, navigieren Sie zu **Jobs** > **Jobs in Bearbeitung**.

   Warten Sie, bis der Sicherungsjob abgeschlossen ist.

   Hinweis: Nur ein Job kann gleichzeitig ausgeführt werden. Wenn Sie versuchen, einen Sicherungsjob manuell zu starten, während gerade ein anderer Job ausgeführt wird, werden Sie in einer Warnmeldung darüber informiert, dass ein anderer Job ausgeführt wird, und aufgefordert, es später erneut zu versuchen.

   Die manuelle Sicherung wird erfolgreich ausgeführt.

Wiederherstellen einer Oracle-Datenbank mit RMAN

Sie können die gesamte Oracle-Datenbank wiederherstellen oder eine spezifische Wiederherstellung von Tablespaces und Tabellen durchführen. Sie können die Datenbank auch vom Wiederherstellungspunkt am Oracle-Basisspeicherort oder an einem alternativen Speicherort oder Knoten wiederherstellen.

Führen Sie zum Wiederherstellen einer Oracle-Datenbank die folgenden Schritte aus:

1. Auswählen der wiederherzustellenden Oracle-Datenbankelemente
2. Definieren der Wiederherstellungsoptionen

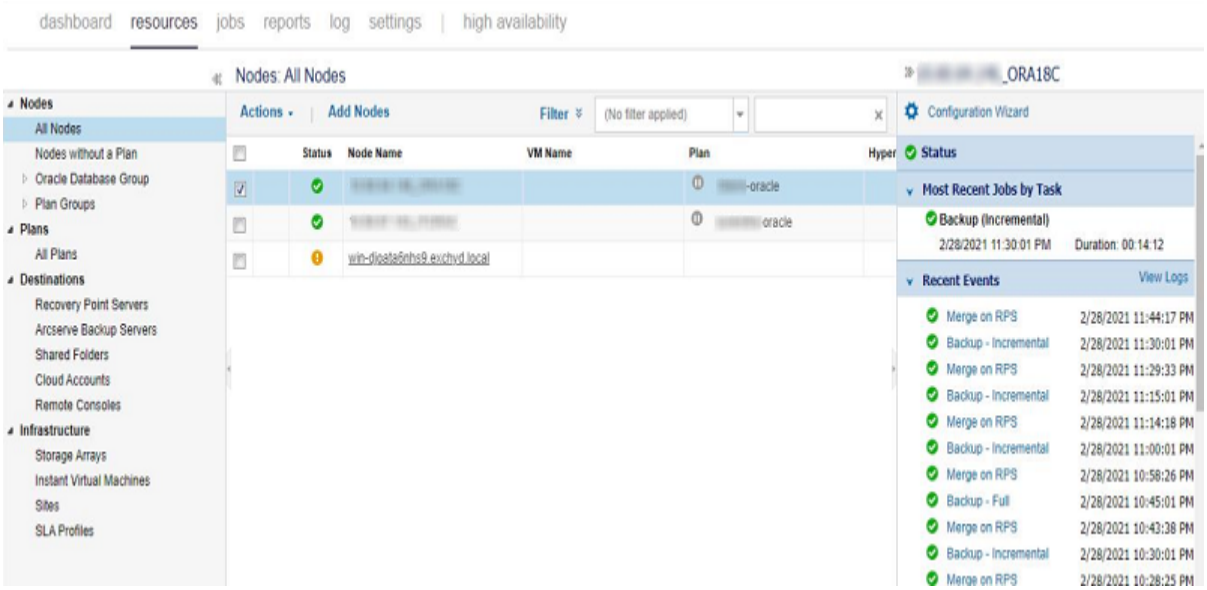
Auswählen der wiederherzustellenden Oracle-Datenbankelemente

Dieser Abschnitt enthält Informationen zum Suchen nach und Auswählen von wiederherzustellenden Oracle-Datenbankelementen.

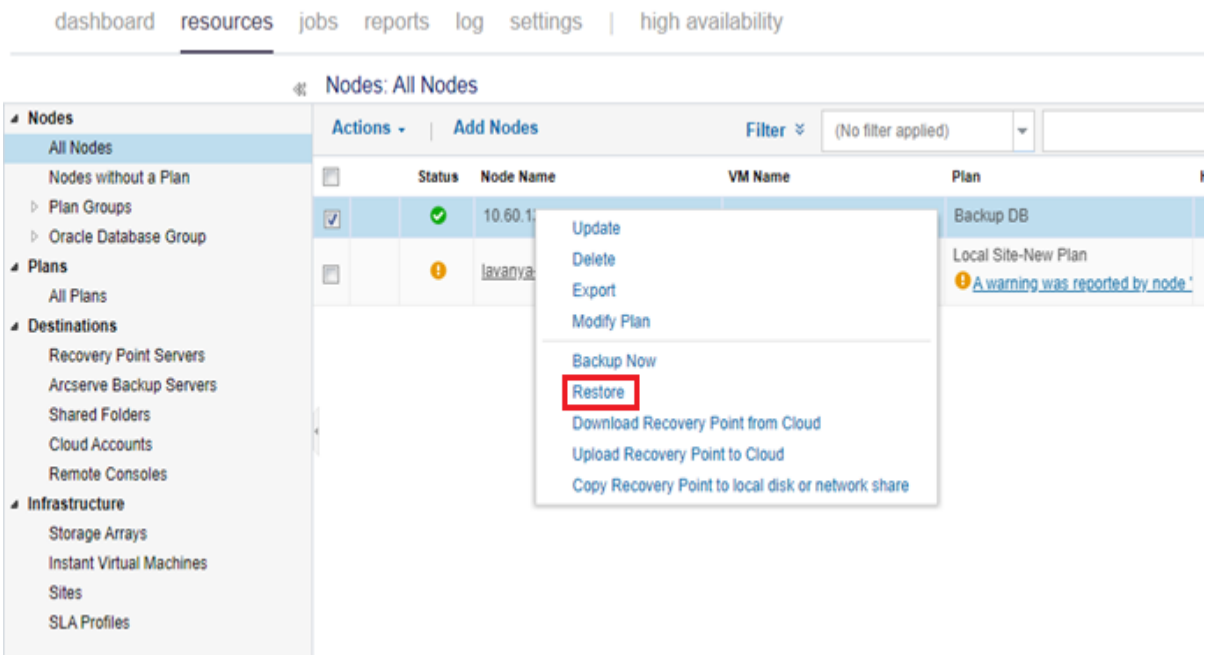
Gehen Sie wie folgt vor:

1. Melden Sie sich beim UDP-Konsolenkonto an.
2. Klicken Sie auf der Seite der UDP-Konsole auf die Registerkarte **Ressourcen**.
3. Navigieren Sie im linken Fensterbereich zu **Knoten** > **Alle Knoten**.

   Die Liste der vorhandenen Knoten wird im mittleren Fensterbereich angezeigt.



4. Klicken Sie mit der rechten Maustaste auf den Oracle-Knoten, und wählen Sie dann die Option **Wiederherstellen** aus.

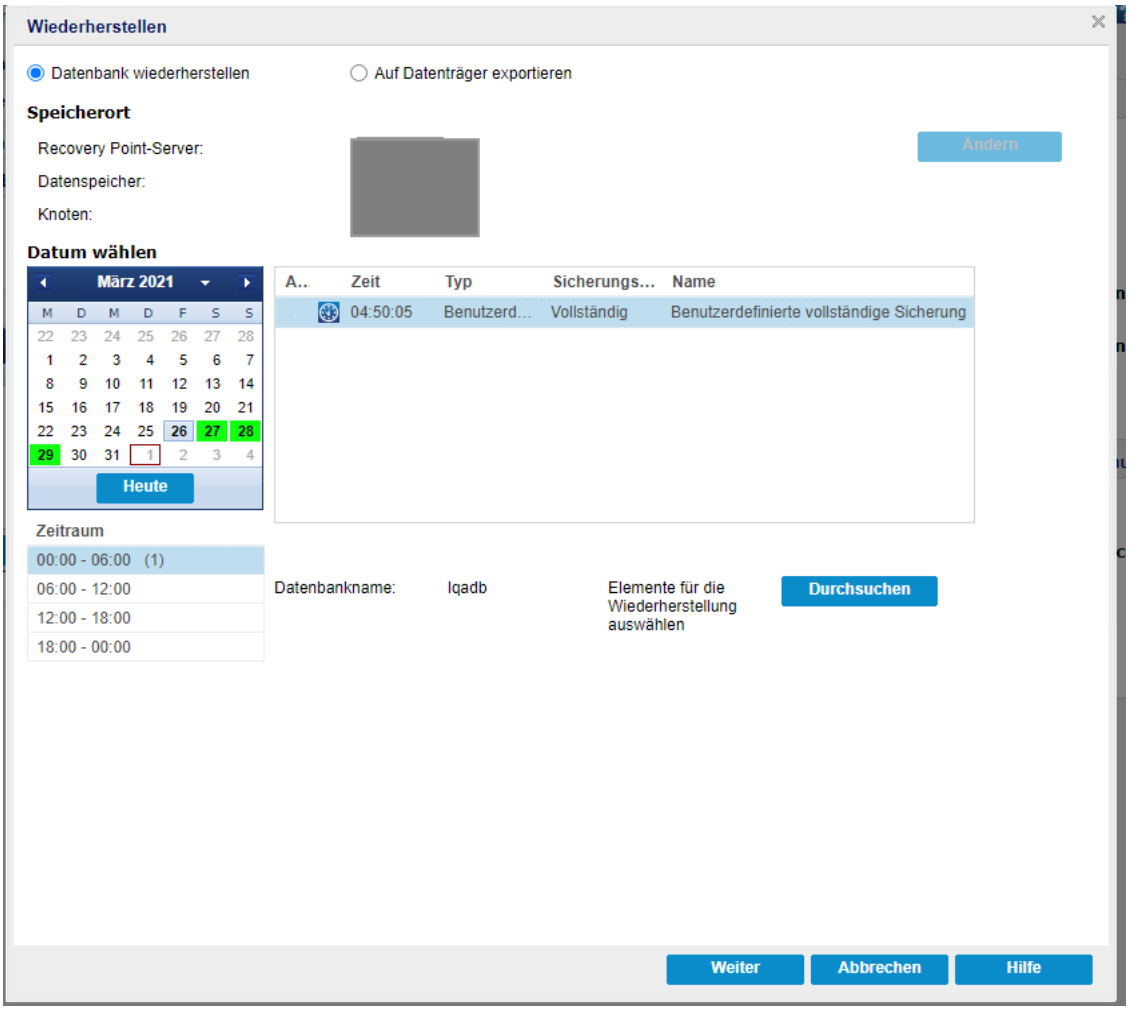


Sie werden automatisch beim Agentenknoten angemeldet, und der Wiederherstellungsassistent wird angezeigt.

5. Wählen Sie im Wiederherstellungsassistenten eine der folgenden Optionen aus:

   Datenbank wiederherstellen

   Die Option "Datenbank wiederherstellen" umfasst Schritte für die vollständige Datenbankwiederherstellung und für die spezifische Wiederherstellung.



Gehen Sie wie folgt vor, um die Oracle-Datenbankelemente auszuwählen:

a. (Optional) Klicken Sie auf **Ändern**, um die Details des Speicherorts für die Sicherung zu ändern.

   Hinweis: Diese Option ist nur gültig, wenn die Option "Sicherung auf Datenträger exportieren" ausgewählt ist.

b. Wählen Sie im Abschnitt "Datum wählen" ein Datum aus.

   Basierend auf der Auswahl wird die Liste der Wiederherstellungspunkte mit dem Zeitpunkt der Sicherung, dem Typ der durchgeführten Sicherung (vollständige Sicherung oder Zuwachssicherung) und dem Namen der Sicherung angezeigt.

c. Wählen Sie in der Liste der Sicherungs-Wiederherstellungspunkte einen Sicherungs-Wiederherstellungspunkt aus, den Sie wiederherstellen möchten.

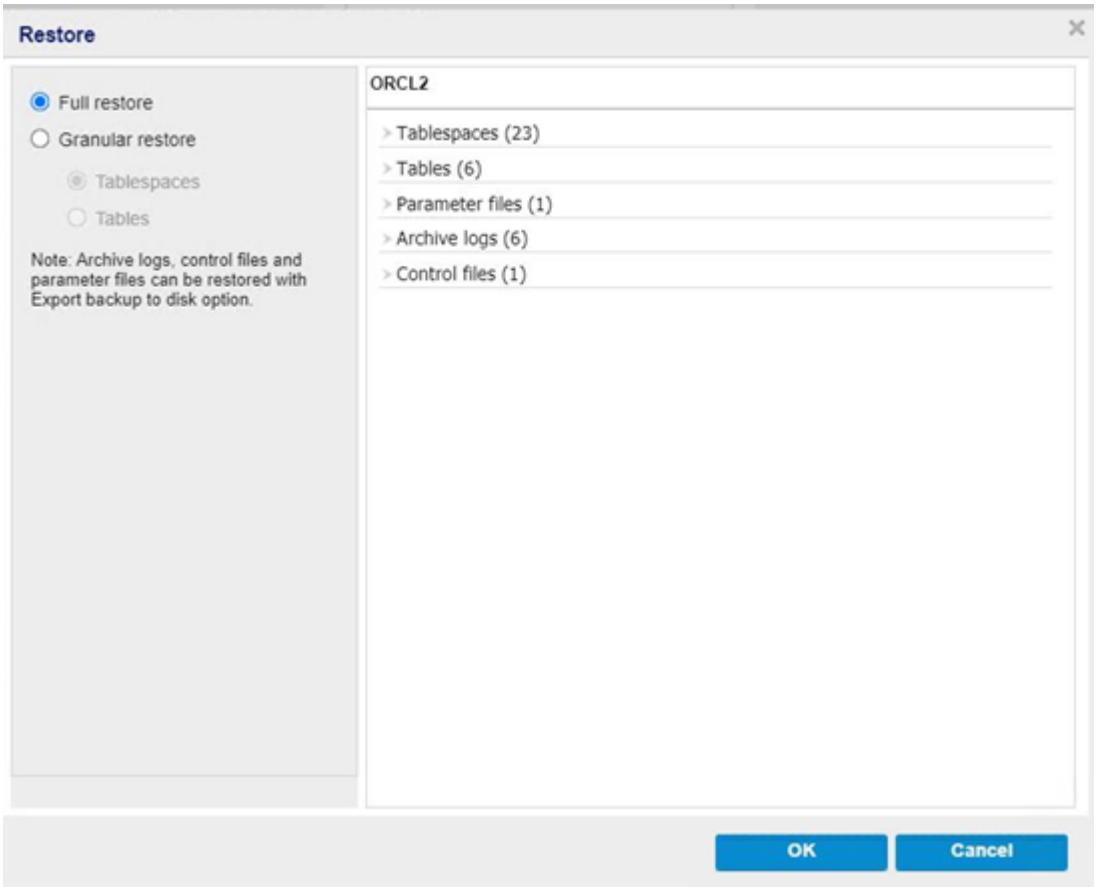
Hinweis: Standardmäßig ist der letzte Sicherungs-Wiederherstellungspunkt ausgewählt.

d. Gehen Sie wie folgt vor, um die Datenbankelemente auszuwählen:

   - Klicken Sie auf die Schaltfläche **Durchsuchen**.

     Das Dialogfeld "Wiederherstellen" wird angezeigt.

   - Führen Sie im Dialogfeld "Wiederherstellen" die folgenden Schritte aus:



     - Führen Sie im linken Fensterbereich die folgenden Aktionen aus:

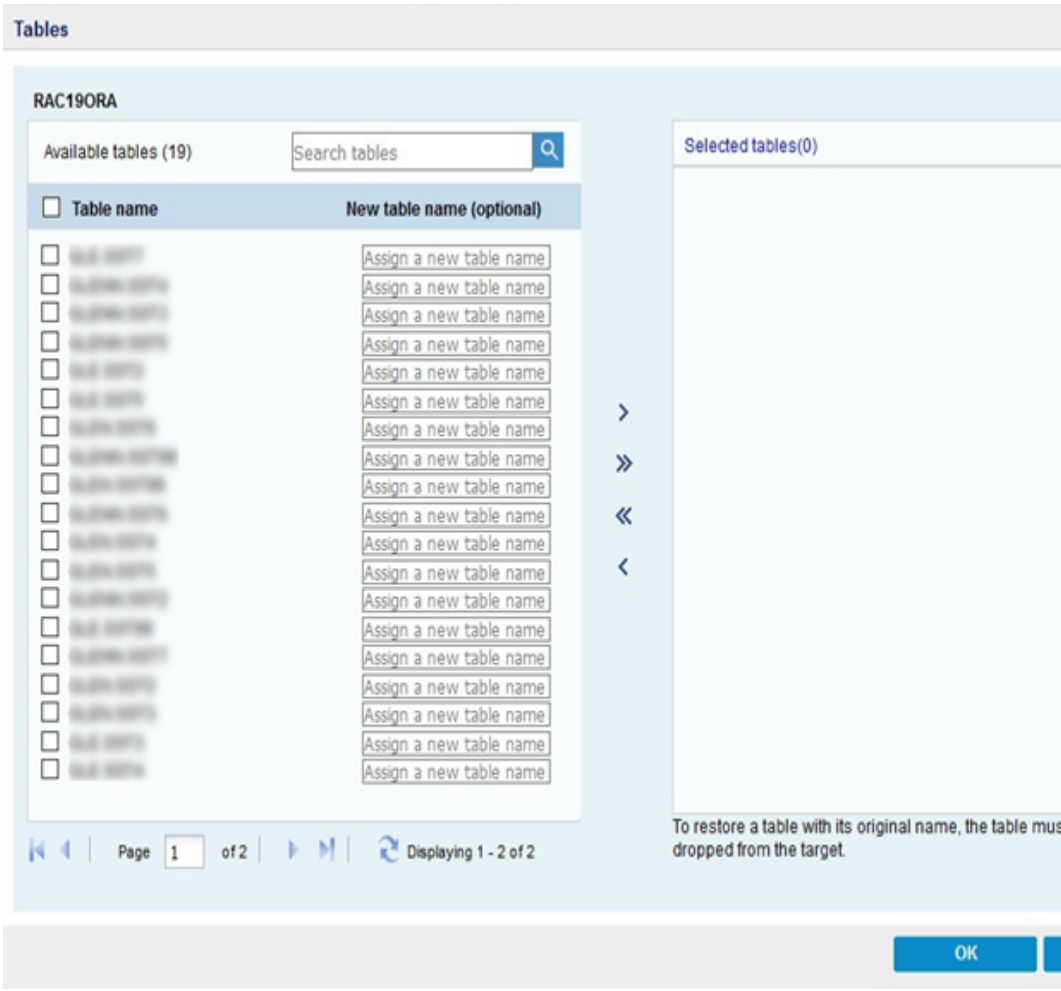
       - Um eine vollständige Wiederherstellung aller Datenbankelemente durchzuführen, wählen Sie **Vollständige Wiederherstellung** aus.
       - Um Tablespaces und Tabellen wiederherzustellen, wählen Sie **Spezifische Wiederherstellung** aus.

Hinweis: Die Oracle-Datenbankelemente wie Archivprotokolle, Kontrolldateien und Parameterdateien sind bei Anzeige des Dialogfelds "Wiederherstellen" standardmäßig ausgewählt. Zusätzlich werden diese Elemente bei Bedarf wiederhergestellt.

- Klicken Sie im rechten Fensterbereich auf die einzelnen Dateien, um sie zu erweitern, und sehen Sie sich die Details an.
- (Optional) Um die spezifischen Tabellen auszuwählen, klicken Sie im rechten Fensterbereich auf die Option **Tabellen**.

  Ein Dialogfeld zur Tabellenauswahl wird angezeigt.

  Führen Sie im Dialogfeld zur Tabellenauswahl die folgenden Schritte aus, und klicken Sie dann auf **OK**:



- Führen Sie im linken Fensterbereich die folgenden Aktionen aus:
  - Um die verfügbaren Tabellen zu durchsuchen, wählen Sie im Suchfeld den Namen der Tabelle aus, und klicken Sie dann auf das Such-symbol.
  - Wählen Sie die Tabellen aus, die Sie wiederherstellen möchten.
  - (Optional) Geben Sie den neuen Namen für eine Tabelle ein, die Sie wiederherstellen möchten.

  Klicken Sie nach Auswahl der Tabellen auf den Nach-rechts-Pfeil (>), um die Tabellen in die Liste der ausgewählten Tabellen zu verschieben.
- Deaktivieren Sie im rechten Fensterbereich die Tabellen, die Sie nicht wiederherstellen möchten, und klicken Sie dann auf den Nach-links-Pfeil (<), um sie in die Liste der verfügbaren Tabellen zu verschieben.

– Klicken Sie auf **OK**.

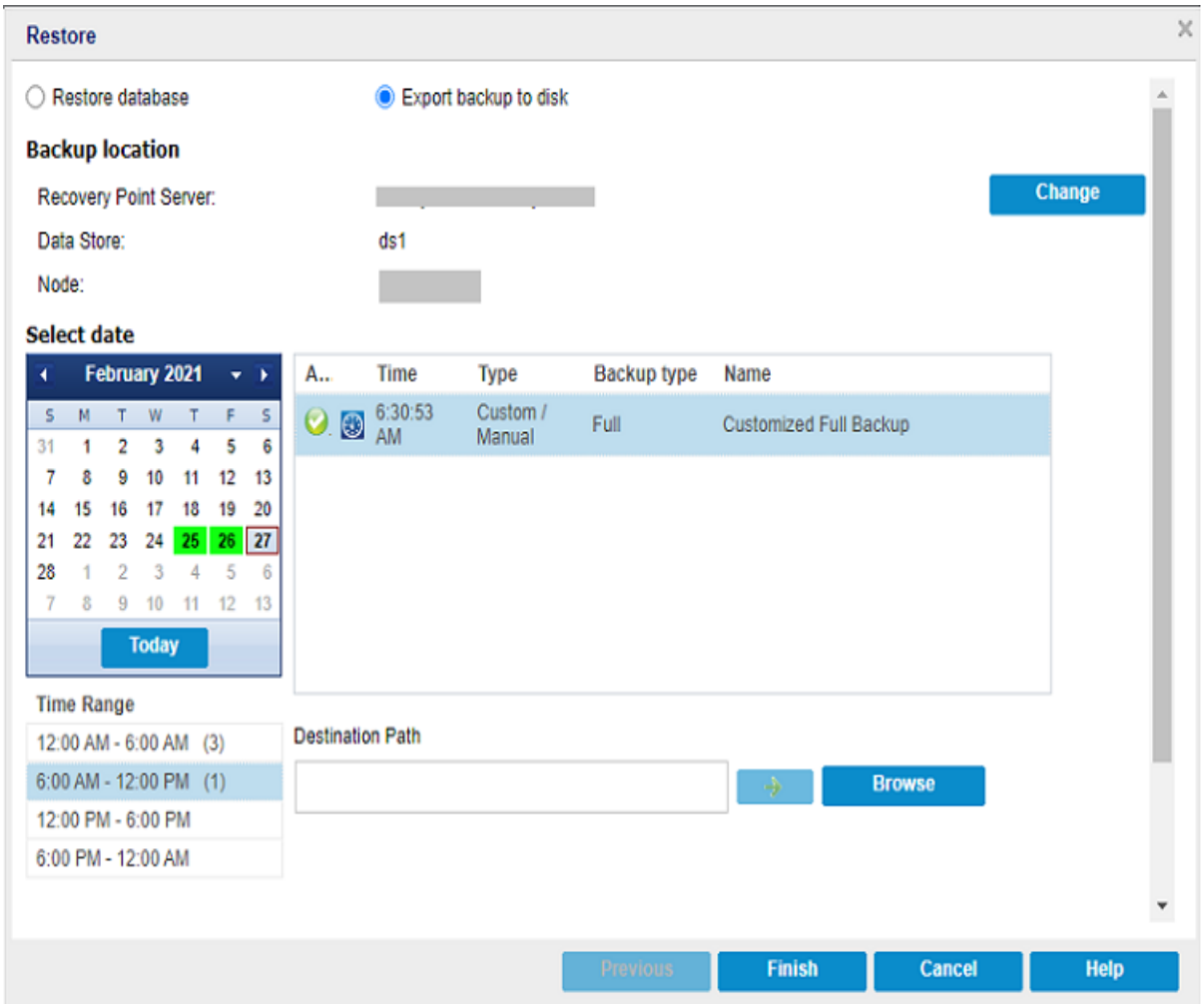
e. Klicken Sie auf **Weiter**.

Das Dialogfeld "Wiederherstellungsoptionen" wird angezeigt.

Die wiederherzustellenden Oracle-Datenbankelemente sind ausgewählt. Nun können Sie die Wiederherstellungsoptionen definieren.

Auf Datenträger exportieren

Stellt die Oracle-Datenbankelemente im Ordner oder Freigabeordner auf dem Datenträger wieder her.



Gehen Sie zum Exportieren auf Datenträger wie folgt vor:

a. (Optional) Klicken Sie auf **Ändern**, um die Details des Speicherorts für die Sicherung zu ändern.

b. Wählen Sie im Abschnitt "Datum wählen" ein Datum aus.

   Basierend auf der Auswahl wird die Liste der Wiederherstellungspunkte mit dem Zeitpunkt der Sicherung, dem Typ der durchgeführten Sicherung (vollständige Sicherung oder Zuwachssicherung) und dem Namen der Sicherung angezeigt.

c. Wählen Sie in der Liste der Sicherungs-Wiederherstellungspunkte einen Sicherungs-Wiederherstellungspunkt aus, den Sie wiederherstellen möchten.

   Hinweis: Standardmäßig ist der letzte Sicherungs-Wiederherstellungspunkt ausgewählt.

d. Geben Sie im Feld "Zielpfad" den vollständigen Pfad der Remote-Netzwerkfreigabe ein.

e. Um die Verbindung zu überprüfen, klicken Sie auf das grüne Pfeilsymbol neben dem Feld "Zielpfad", geben Sie den Benutzernamen und das Kennwort nach Bedarf ein, und klicken Sie dann auf **OK**.

f. Wenn die Verbindung zur Remote-Netzwerkfreigabe erfolgreich hergestellt wurde, klicken Sie auf die Schaltfläche **Durchsuchen**.

   Das Dialogfeld "Speicherort für die Sicherung auswählen" wird angezeigt.

g. Wählen Sie im Dialogfeld "Speicherort für die Sicherung auswählen" einen wiederherzustellenden Ordner aus, und klicken Sie auf **OK**.

h. Klicken Sie auf **Fertig stellen**.

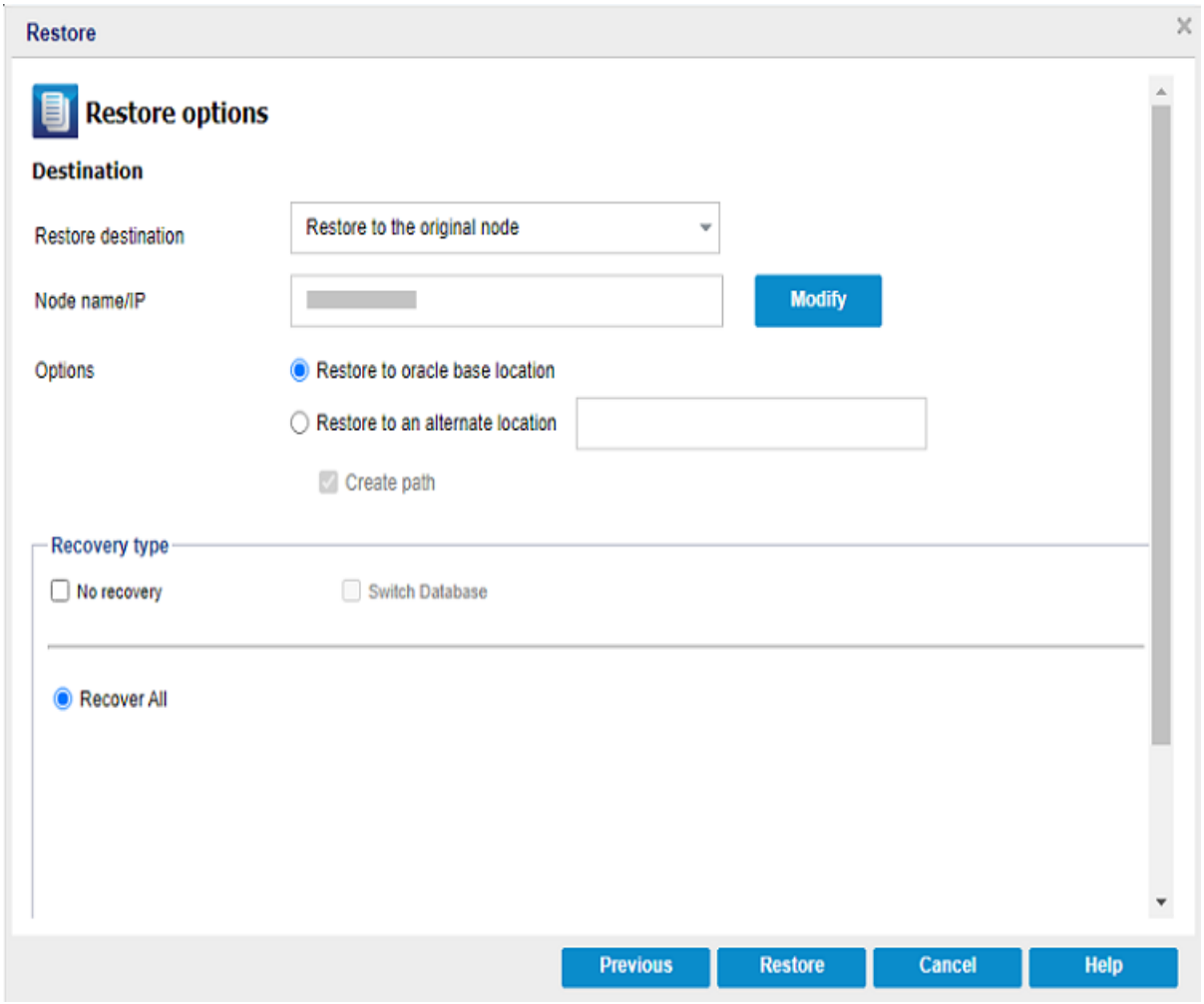
   Die Oracle-Datenbankelemente werden auf den Datenträger exportiert.

Definieren der Wiederherstellungsoptionen

Dieser Abschnitt enthält Informationen zum Definieren von Wiederherstellungsoptionen für die ausgewählten Oracle-Datenbankelemente.

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld Wiederherstellungsoptionen das Wiederherstellungsziel aus.



Hinweise:

- Während der Wiederherstellung ist für jeden Wiederherstellungspunkt der vollständigen Sicherung nur die Option "Alle wiederherstellen" verfügbar.
- Für Wiederherstellungspunkte, die Zuwachssicherungen zugeordnet sind, sind alle Optionen für die Wiederherstellung verfügbar, wie "Alle

wiederherstellen", "Zeitpunkt", "Bis SCN" und "Bis Protokollfolgenummer".

Es sind folgende Zieloptionen verfügbar:

Auf dem ursprünglichen Knoten wiederherstellen

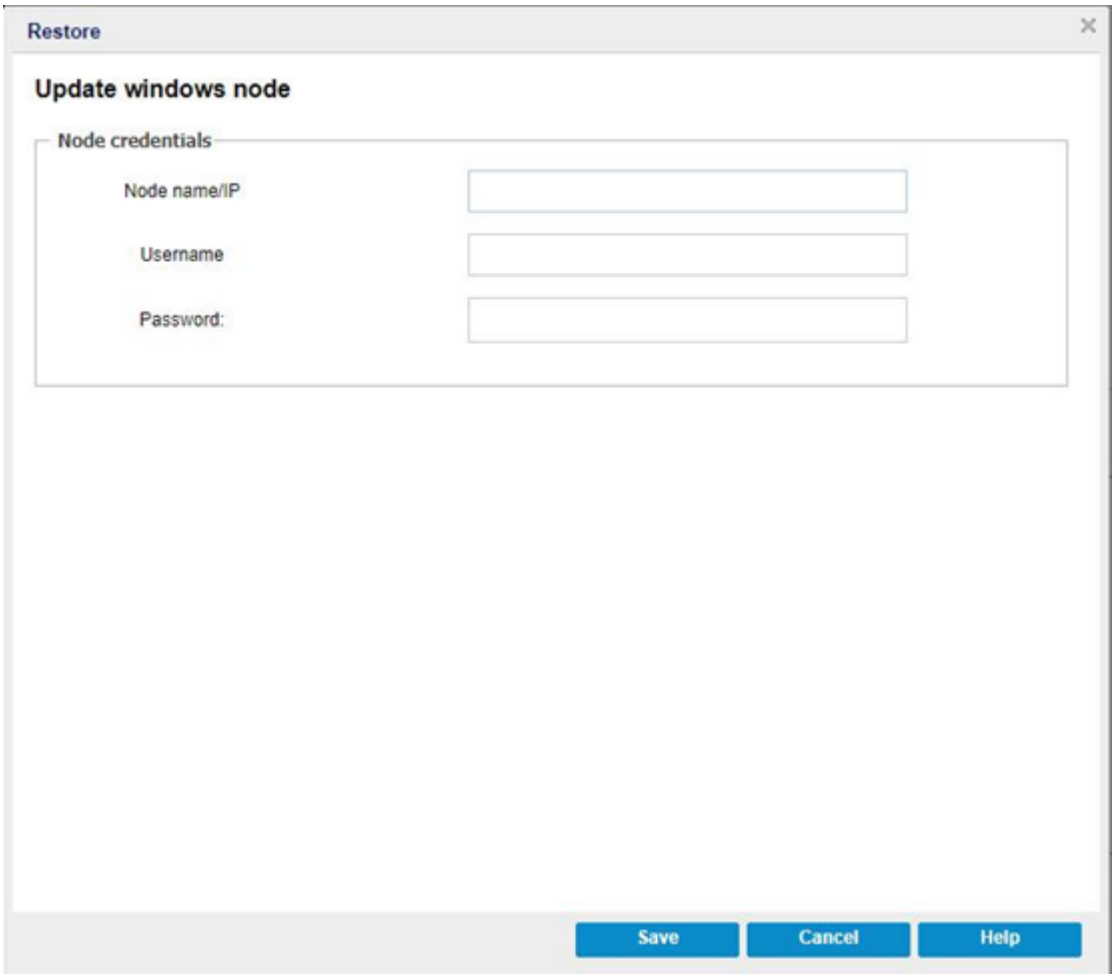
Gehen Sie zum Wiederherstellen auf dem ursprünglichen Knoten wie folgt vor:

- Die vorhandenen Details zu Knotenname/IP werden automatisch angezeigt. Wenn die Angaben zu Knotenname/IP geändert werden müssen, klicken Sie auf **Ändern**.

  Je nach Knotentyp wird das Dialogfeld "Windows-Knoten aktualisieren" oder "Linux-Knoten aktualisieren" angezeigt.

  Windows-Knoten aktualisieren

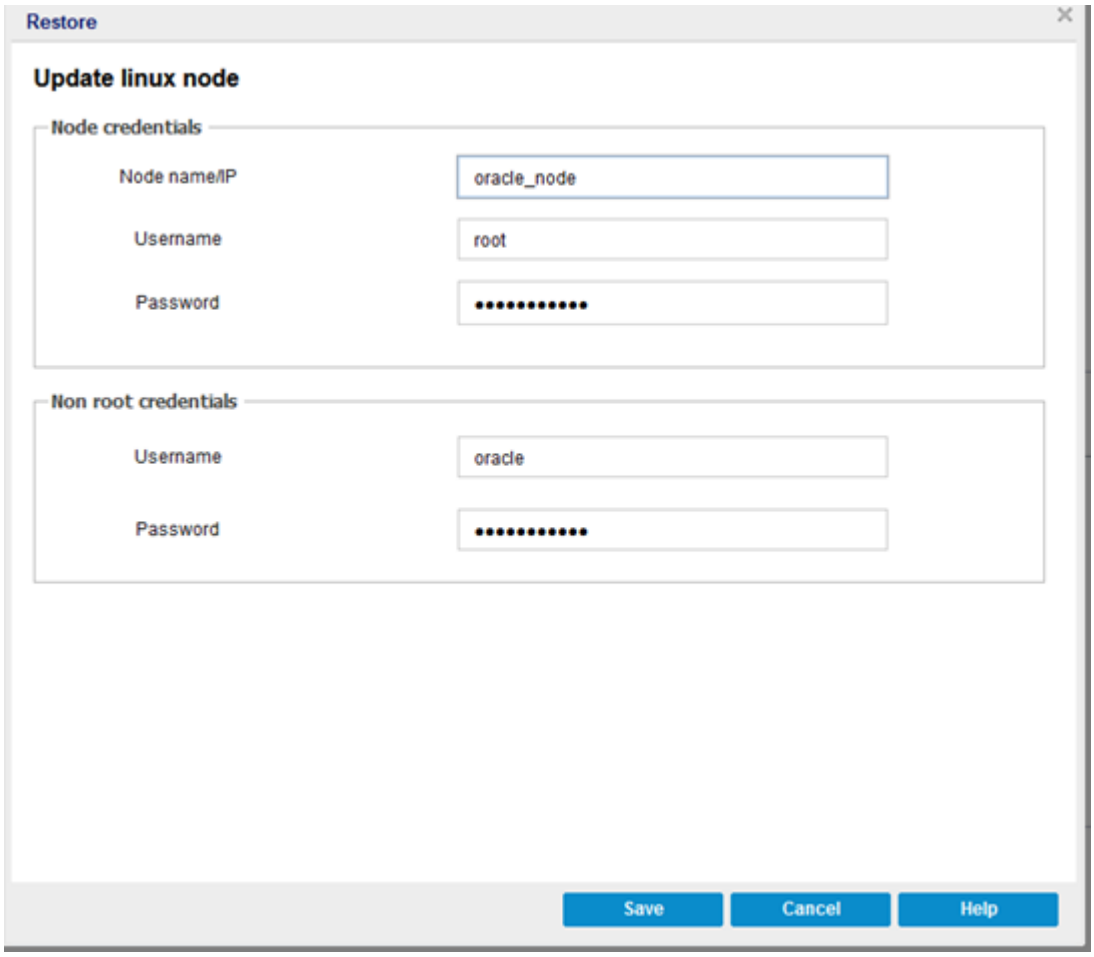
  Geben Sie im Dialogfeld "Windows-Knoten aktualisieren" nach Bedarf den Knotennamen/die IP-Adresse, den Benutzernamen und das Kennwort ein, und klicken Sie dann auf **Speichern**.



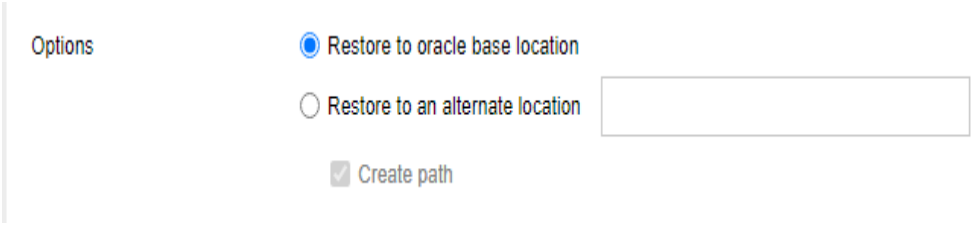
Linux-Knoten aktualisieren

Aktualisieren Sie im Dialogfeld "Linux-Knoten aktualisieren" die folgenden Details, und klicken Sie dann auf **Speichern**:

- Geben Sie für "Knoten-Anmeldeinformationen" den Knotennamen/die IP, den Benutzername und das Kennwort nach Bedarf ein.
- Geben Sie für "Nicht-Root-Anmeldeinformationen" den Benutzernamen und das Kennwort nach Bedarf ein.



- Wählen Sie unter "Optionen" eine der folgenden Optionen aus:



Es sind folgende Optionen verfügbar:

Am Oracle-Basisspeicherort wiederherstellen

Stellt die ausgewählten Datenbankelemente an dem Oracle-Basisspeicherort wieder her, von dem aus Sie eine Sicherung erstellt haben.

Am alternativen Speicherort wiederherstellen

Stellt die Daten an einem alternativen Speicherort wieder her. Bei Auswahl dieser Option müssen Sie einen Pfad für den alternativen Speicherort angeben.

Hinweis: Das Kontrollkästchen **Pfad erstellen** wird automatisch aktiviert, wenn Sie die Option **An einem alternativen Speicherort wiederherstellen** auswählen.

Auf dem alternativen Knoten wiederherstellen

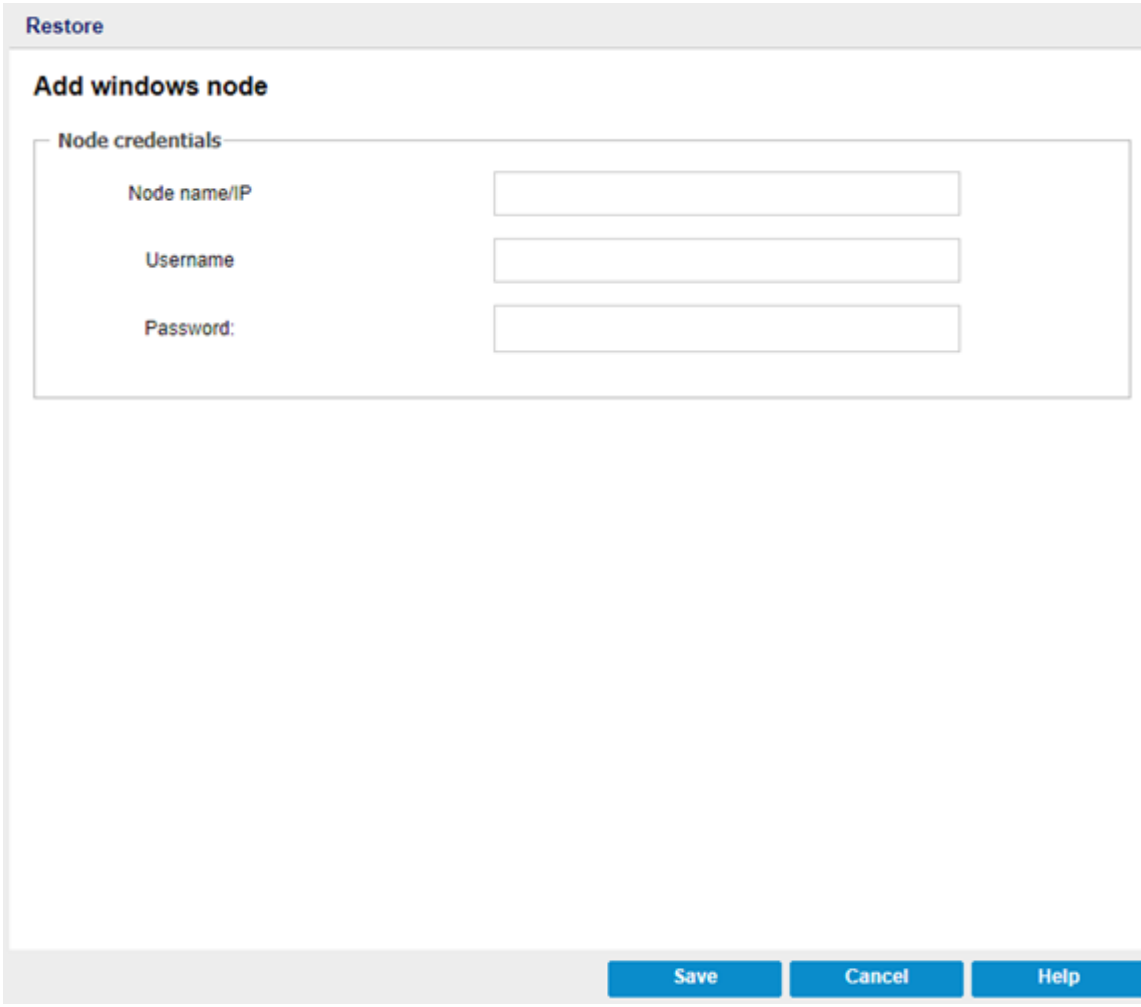
Gehen Sie zum Wiederherstellen auf dem alternativen Knoten wie folgt vor:

- Klicken Sie auf die Schaltfläche **Hinzufügen**, um einen neuen Knoten/eine neue IP hinzuzufügen.

  Je nach Knotentyp wird das Dialogfeld "Windows-Knoten hinzufügen" oder "Linux-Knoten hinzufügen" angezeigt.

  Windows-Knoten hinzufügen

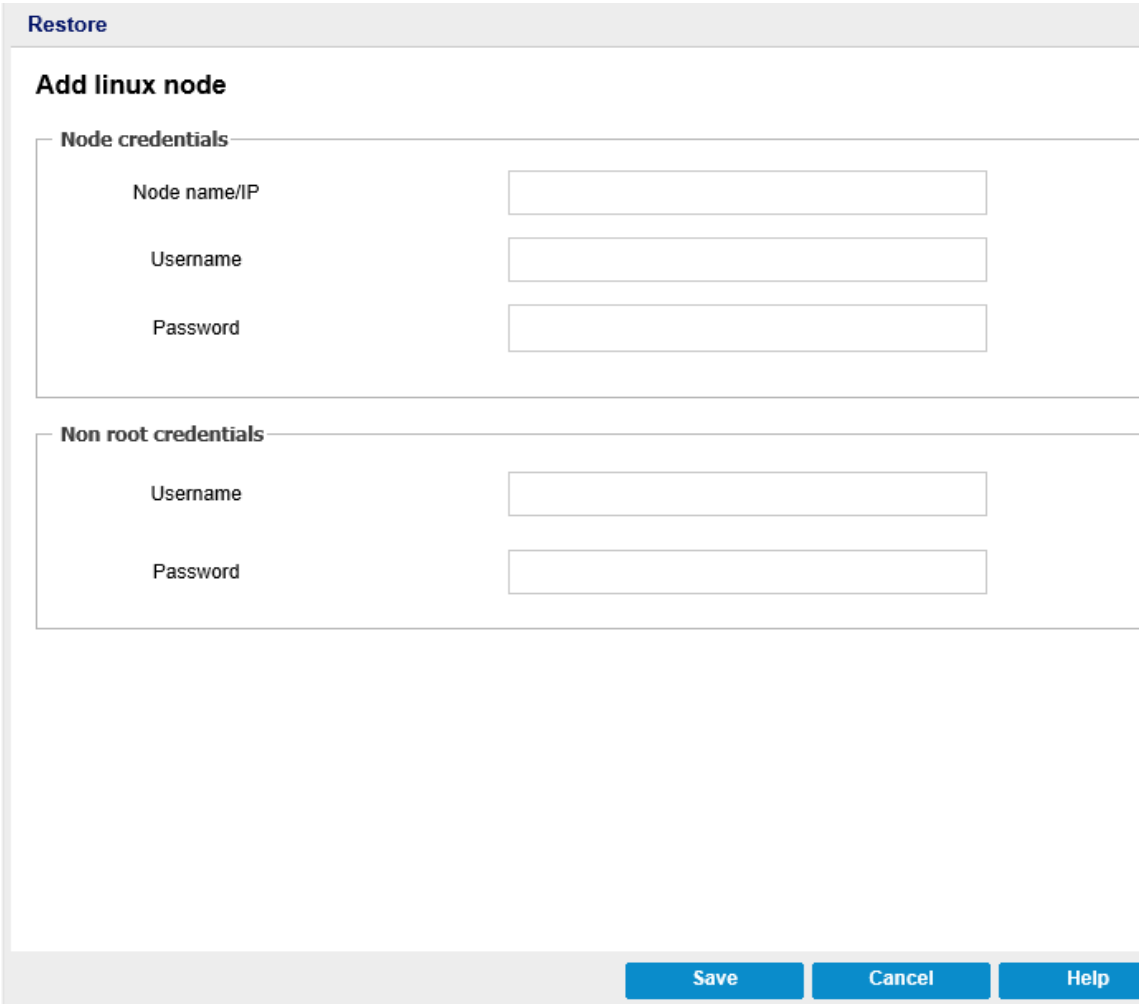
  Geben Sie im Dialogfeld "Windows-Knoten hinzufügen" nach Bedarf den Knotennamen / die IP-Adresse, den Benutzernamen und das Kennwort ein, und klicken Sie dann auf **Speichern**.



Linux-Knoten hinzufügen

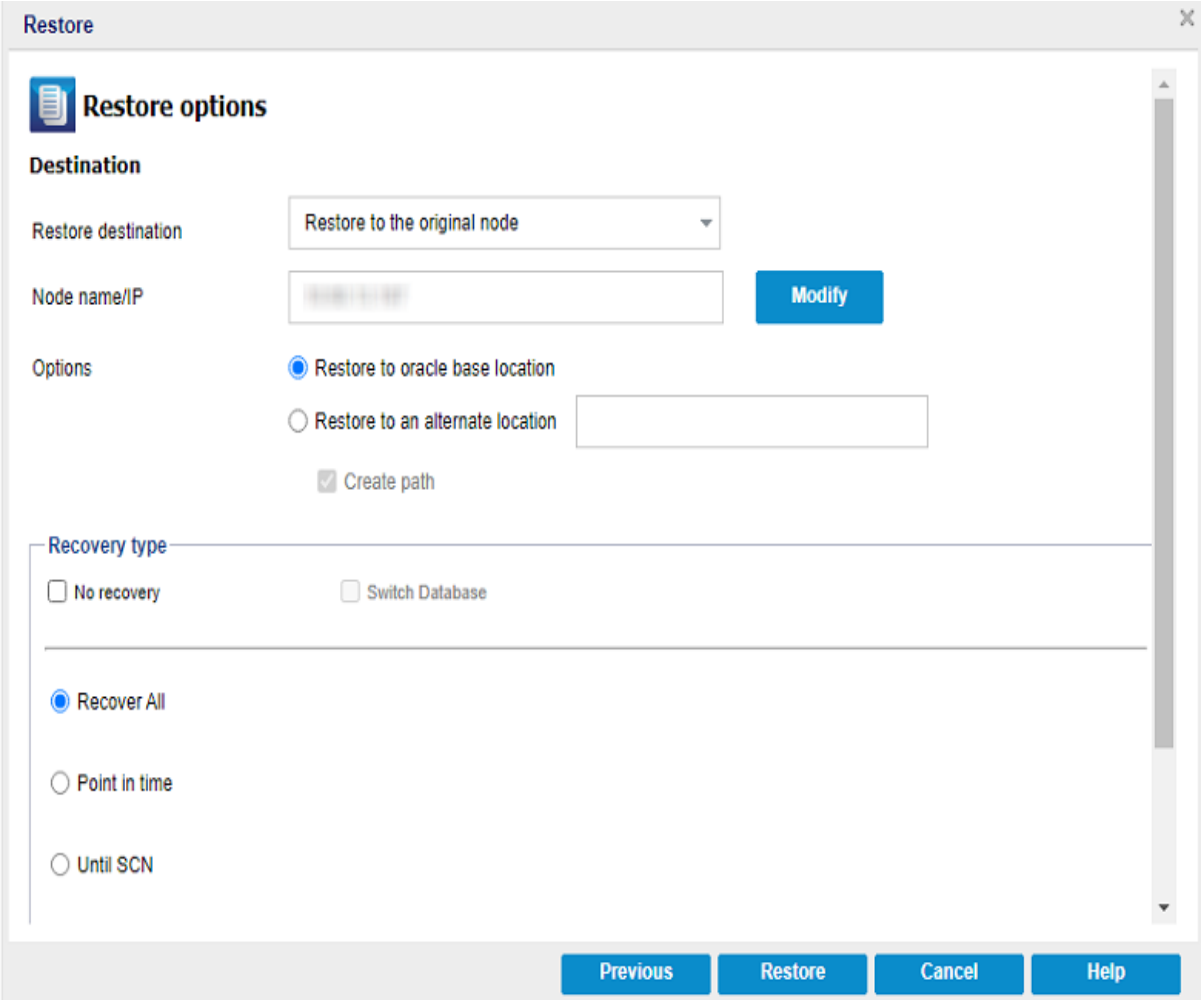
Fügen Sie im Dialogfeld "Linux-Knoten hinzufügen" die folgenden Details hinzu, und klicken Sie dann auf **Speichern**:

- Geben Sie für "Knoten-Anmeldeinformationen" den neuen Knotennamen/die neue IP, den Benutzername und das Kennwort nach Bedarf ein.
- Geben Sie für "Nicht-Root-Anmeldeinformationen" den neuen Benutzernamen und das Kennwort nach Bedarf ein.



- Unter "Optionen" ist die Option **An einem alternativen Speicherort wiederherstellen** standardmäßig aktiviert. Geben Sie einen Pfad für den alternativen Speicherort ein.

2. Gehen Sie im Abschnitt "Wiederherstellungstyp" wie folgt vor:



- Wenn Sie die Wiederherstellung nicht ausführen möchten, aktivieren Sie das Kontrollkästchen **Keine Wiederherstellung**. Basierend auf der Auswahl wird die folgende Option aktiviert:

  Datenbank wechseln

  Wenn Sie die Datenbankelemente an den neuen Speicherort verschieben möchten, aktivieren Sie das Kontrollkästchen **Datenbank wechseln**.

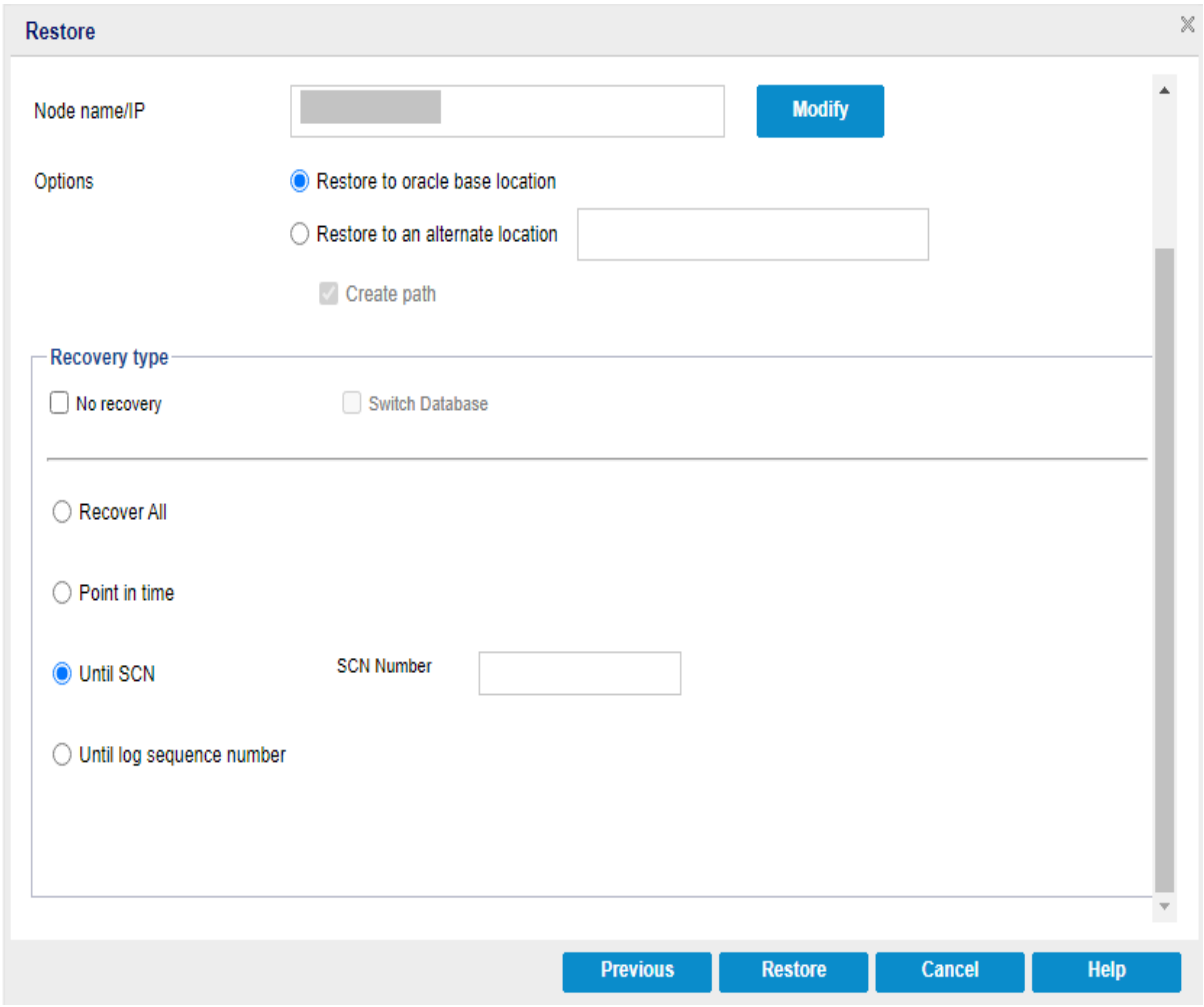
  Hinweis: Die Option "Datenbank wechseln" wird nur unterstützt, wenn die Wiederherstellung an einem alternativen Speicherort oder alternativen Knoten durchgeführt wird.

- Wenn Sie die Wiederherstellung auf einen bestimmten Zeitpunkt durchführen möchten, wählen Sie **Zeitpunkt** aus, und geben Sie dann Folgendes an:

- Wählen Sie ein Datum zur Durchführung der Wiederherstellung auf einen bestimmten Zeitpunkt aus.
- Wählen Sie die Startzeit nach Bedarf aus.

Hinweis: Das Datum und die Startzeit für die Wiederherstellung auf einen bestimmten Zeitpunkt müssen kleiner als der ausgewählte Wiederherstellungspunkt der Sicherung und größer als der vorherige Wiederherstellungspunkt sein.

- Wenn Sie alle Datenbankelemente bis zum angegebenen SCN-Zeitstempel (System Change Number) wiederherstellen möchten, wählen Sie **Bis SCN** aus, und geben Sie dann den Wert für "SCN-Nummer" nach Bedarf ein.



- Wenn Sie alle Datenbankelemente bis zur angegebenen Protokollfolgenummer wiederherstellen möchten, wählen Sie **Bis Protokollfolgenummer** aus, und geben Sie die Werte für "Protokollfolgenummer" und "Thread-Nummer" nach Bedarf ein.

3. Klicken Sie auf **Wiederherstellen**.

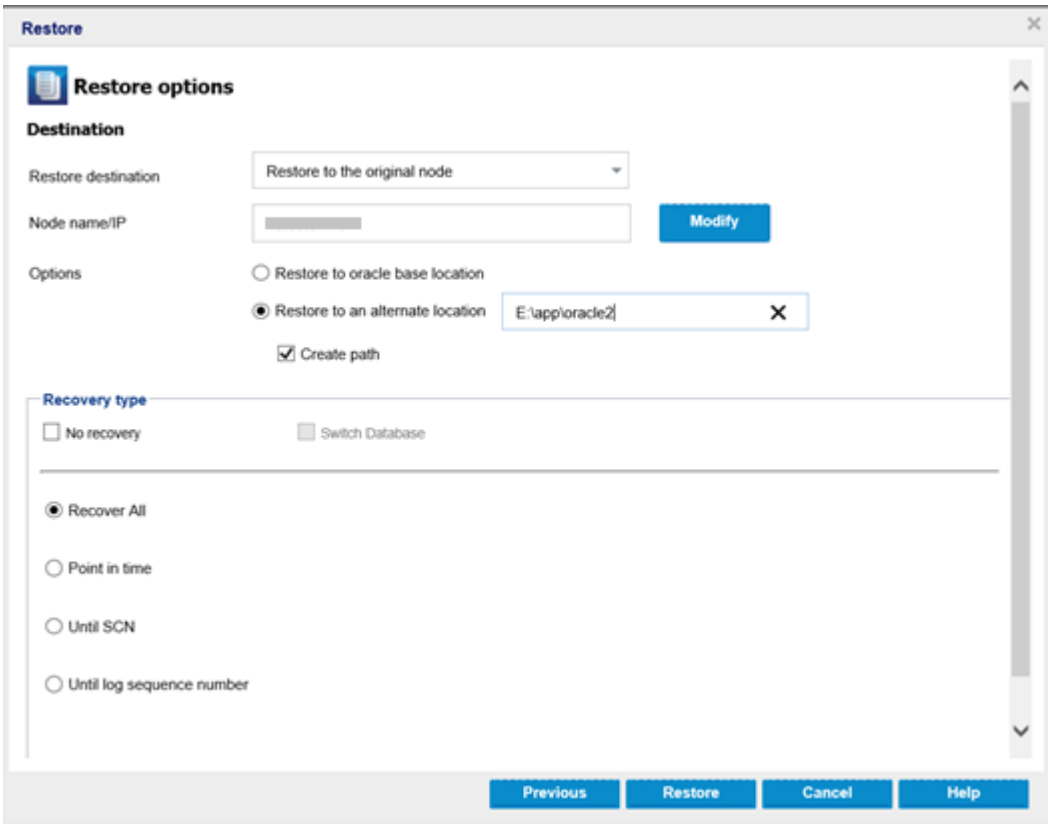
Die Oracle-Datenbankelemente werden wiederhergestellt.

Wiederherstellen einer Datenbank an einem alternativen Speicherort unter Windows

Dieser Abschnitt enthält Informationen zum Wiederherstellen der Datenbank an einem alternativen Speicherort unter Windows.

Gehen Sie wie folgt vor:

1. Wählen Sie in der UDP-Konsole den Wiederherstellungspunkt aus, von dem aus Sie die Wiederherstellung durchführen müssen. Weitere Informationen finden Sie unter Definieren der Wiederherstellungsoptionen.
2. Wählen Sie im Dialogfeld "Wiederherstellungsoptionen" im Drop-down-Menü "Ziel wiederherstellen" die Option **Auf dem ursprünglichen Knoten wiederherstellen** aus.



3. Geben Sie für "Knotenname/IP" den Knotennamen oder die IP-Adresse ein.
4. Wählen Sie unter "Optionen" die Option **An einem alternativen Speicherort wiederherstellen** aus, und fügen Sie dann einen Pfad des alternativen Speicherorts hinzu.

   Hinweise:

- Stellen Sie sicher, dass der hinzugefügte Pfad keine Sonderzeichen oder Leerzeichen enthält.
- Das Kontrollkästchen **Pfad erstellen** wird automatisch aktiviert, wenn Sie die Option **An einem alternativen Speicherort wiederherstellen** auswählen.
- Wenn die Datenbank noch nicht heruntergefahren wurde, wird eine Benachrichtigung angezeigt, in der Sie aufgefordert werden, die Datenbank herunterzufahren. Klicken Sie zur Bestätigung auf **OK**.

5. Bestätigen Sie über die UDP-Konsole, dass der Wiederherstellungsjob erfolgreich war.
6. Stellen Sie eine Verbindung zu **sqlplus** her, und bestätigen Sie, dass die Datenbank aktiv ist und ausgeführt wird.

   Die wiederhergestellte Datenbank ist am angegebenen alternativen Speicherort betriebsbereit. Allerdings kann es nach dem Neustart der Datenbank passieren, dass die Datenbank auf die vorherige Kopie zurückgesetzt oder aufgrund eines bekannten Problems nicht ordnungsgemäß wiederhergestellt wird. Um nach der Wiederherstellung an einem alternativen Speicherort weitere Probleme zu vermeiden, wird die Ausführung der folgenden Schritte empfohlen. Diese Schritte helfen beim Erstellen oder Platzieren der richtigen Kopie von "spfile/pfile".

   a. Gehe Sie zu **%ORACLE_HOME%\database**, und benennen Sie "spfile<SID>.ora" um.
   b. Stellen Sie eine Verbindung zu **sqlplus** her.
   c. Wechseln Sie zur SQL-Eingabeaufforderung, und führen Sie den folgenden Befehl aus:

      sqlplus > create pfile from spfile.

   d. Gehen Sie zu **%ORACLE_HOME%\database**, öffnen Sie **init<SID>.ora** in einem beliebigen Editor, und gehen Sie dann wie folgt vor:

      1. Aktualisieren Sie den Wert für "db_create_file_dest" mit dem Pfad, der für den alternativen wiederhergestellten Speicherort angegeben wurde.
      2. Entfernen Sie den zusätzlichen "\" am Ende des Pfads unter dem Parameter *diagnostic_dest*.

         Ändern Sie Folgendes:

         Von *diagnostic_dest='E:\app\oracle2\ORA19C280220211833\'*

Zu *diagnostic_dest='E:\app\oracle2\ORA19C280220211833'*

3. Speichern Sie die Datei.

e. Wechseln Sie zur SQL-Eingabeaufforderung, und führen Sie die folgenden Befehle aus:

Sqlplus > shutdown immediate

sqlplus > startup

sqlplus > create spfile from pfile

Hinweis: Wenn die DB nicht aus *spfile* gestartet wird, sind Wiederherstellungen aus den entsprechenden Sicherungen auf den ursprünglichen Knoten beschränkt. Um dies zu vermeiden, starten Sie die Datenbank nach der Erstellung von *spfile* neu. Führen Sie zum Neustarten die folgenden Befehle aus:

sqlplus > shutdown immediate

sqlplus > startup

Wiederherstellen einer Datenbank auf einem alternativen Knoten unter Windows

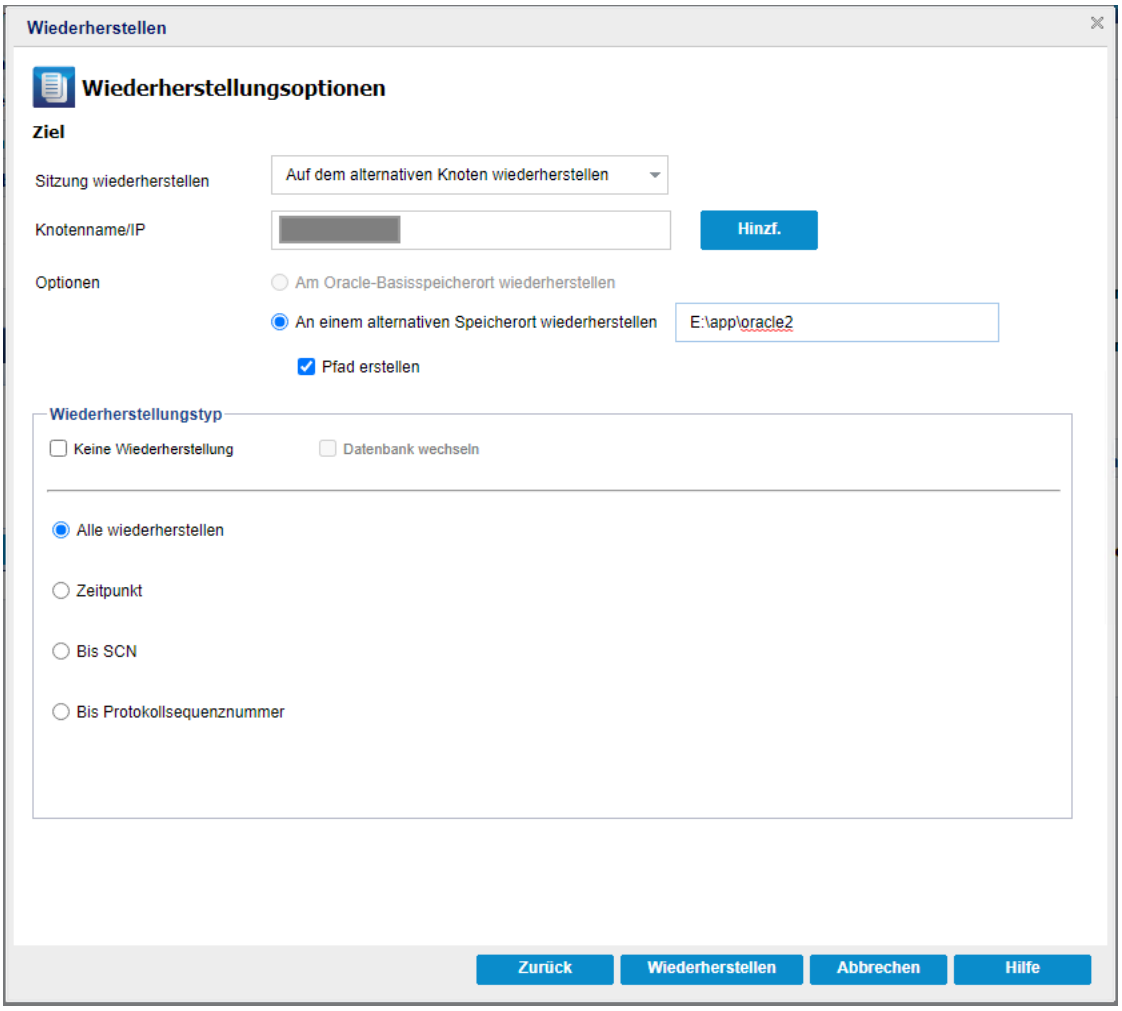
Dieser Abschnitt enthält Informationen zum Wiederherstellen der Datenbank auf einem alternativen Knoten unter Windows.

Hinweise:

- Wenn die **Verfolgung geänderter Blöcke** (Change Block Tracking, CBT) deaktiviert ist und eine Wiederherstellung auf einem alternativen Knoten durchgeführt wird, schlägt die Wiederherstellung möglicherweise fehl. Wählen Sie daher die Option "Nur wiederherstellen" aus, wenn Sie über die erforderlichen Protokolle verfügen und die Datenbank nach der Wiederherstellung manuell wiederherstellen können. Um dieses Problem zu umgehen, aktivieren Sie die **Verfolgung geänderter Blöcke**, bevor Sie eine Wiederherstellung vom Typ "auf einem alternativen Knoten" auf dem Quellknoten durchführen.
- Stellen Sie sicher, dass Sie auf dem alternativen Knoten, auf dem Sie die Wiederherstellung durchführen möchten, die gleiche Version der Oracle-Software installieren und eine Datenbank mit der derselben SID erstellen wie auf dem ursprünglichen Knoten (Quellknoten). Wenn beispielsweise der Quellknoten die SID "orcl" aufweist, erstellen Sie "orcl" auf einem alternativen Knoten, bevor Sie die Wiederherstellung starten. Dies ist erforderlich, wenn Oracle-Software mit einem Domänenkonto installiert wird. Bei Verwendung eines virtuellen Kontos ist dies nicht erforderlich.

Gehen Sie wie folgt vor:

1. Wählen Sie in der UDP-Konsole den Wiederherstellungspunkt aus, von dem aus Sie die Wiederherstellung durchführen müssen. Weitere Informationen finden Sie unter Definieren der Wiederherstellungsoptionen.
2. Wählen Sie im Dialogfeld "Wiederherstellungsoptionen" im Drop-down-Menü "Ziel wiederherstellen" die Option **Auf dem alternativen Knoten wiederherstellen** aus.



3. Geben Sie für "Knotenname/IP" den Knotennamen oder die IP-Adresse ein.
4. Wählen Sie unter "Optionen" die Option **An einem alternativen Speicherort wiederherstellen** aus, und fügen Sie dann einen Pfad des alternativen Speicherorts hinzu.

   Hinweise:

   - Stellen Sie sicher, dass der hinzugefügte Pfad keine Sonderzeichen oder Leerzeichen enthält.
   - Das Kontrollkästchen **Pfad erstellen** wird automatisch aktiviert, wenn Sie die Option **An einem alternativen Speicherort wiederherstellen** auswählen.
   - Wenn die Datenbank noch nicht heruntergefahren wurde, wird eine Benachrichtigung angezeigt, in der Sie aufgefordert werden, die Datenbank herunterzufahren. Klicken Sie zur Bestätigung auf **OK**.

5. Bestätigen Sie über die UDP-Konsole, dass der Wiederherstellungsjob erfolgreich war.
6. Stellen Sie eine Verbindung zu **sqlplus** auf dem alternativen Knoten her, und bestätigen Sie, dass die Datenbank aktiv ist und ausgeführt wird.

   Die wiederhergestellte Datenbank ist am angegebenen alternativen Speicherort betriebsbereit. Allerdings kann es nach dem Neustart der Datenbank passieren, dass die Datenbank auf die vorherige Kopie zurückgesetzt oder aufgrund eines bekannten Problems nicht ordnungsgemäß wiederhergestellt wird. Um nach der Wiederherstellung an einem alternativen Speicherort weitere Probleme zu vermeiden, wird die Ausführung der folgenden Schritte empfohlen. Diese Schritte helfen beim Erstellen oder Platzieren der richtigen Kopie von "spfile/pfile".

   a. Gehe Sie zu **%ORACLE_HOME%\database**, und benennen Sie "spfile<SID>.ora" um.

   b. Stellen Sie eine Verbindung zu **sqlplus** her.

   c. Wechseln Sie zur SQL-Eingabeaufforderung, und führen Sie den folgenden Befehl aus:

      sqlplus > create pfile from spfile.

   d. Gehen Sie zu **%ORACLE_HOME%\database**, öffnen Sie **init<SID>.ora** in einem beliebigen Editor, und gehen Sie dann wie folgt vor:

      1. Aktualisieren Sie den Wert für "db_create_file_dest" mit dem Pfad, der für den alternativen wiederhergestellten Speicherort angegeben wurde.

         Beispiel: **.db_create_file_dest-='E:\app\oracle2\ORA19C280220211833'*

      2. Entfernen Sie den zusätzlichen "\" am Ende des Pfads unter dem Parameter *diagnostic_dest*.

         Ändern Sie Folgendes:

         Von *diagnostic_dest='E:\app\oracle2\ORA19C280220211833\'*

         Zu *diagnostic_dest='E:\app\oracle2\ORA19C280220211833'*

      3. Speichern Sie die Datei.

   e. Wechseln Sie zur SQL-Eingabeaufforderung, und führen Sie die folgenden Befehle aus:

      sqlplus > shutdown immediate

      sqlplus > startup

sqlplus > create spfile from pfile

Hinweis: Wenn die DB nicht aus *spfile* gestartet wird, sind Wiederherstellungen aus den entsprechenden Sicherungen auf den ursprünglichen Knoten beschränkt. Um dies zu vermeiden, starten Sie die Datenbank nach der Erstellung von *spfile* neu. Führen Sie zum Neustarten die folgenden Befehle aus:

sqlplus > shutdown immediate

sqlplus > startup

Einschränkungen

Folgende Einschränkungen sind in der aktuellen Version bekannt:

- Wenn der RPS-Server geändert wird, ist die nachfolgende Sicherung eine vollständige Sicherung.
- Die Wiederherstellung auf einem alternativen Knoten wird nicht unterstützt, wenn sich Quelle und Ziel auf zwei verschiedenen Oracle-Versionen befinden.
- Nach dem Upgrade auf 8.1 werden die Wiederherstellungspunkte, die vor dem Upgrade auf 8.0 erstellt wurden, ungültig, wenn der Job "An einem alternativen Speicherort oder an einem alternativen Knoten wiederherstellen" ausgeführt wird. Die Wiederherstellungspunkte werden ungültig, da sie nicht die Details der DataFile-Zuordnung in der Flash-Datenbank enthalten.
- Bei der Wiederherstellung von Archivprotokollen an einen alternativen Speicherort oder alternativen Knoten in 8.1 muss zuerst die Zuwachssicherung (Alle Datentypen) ausgeführt werden. Anschließend können die Ablaufpläne der Archivprotokollprotokolle für Wiederherstellungen verwendet werden.
- Wenn der Oracle-Listener an einem nicht standardmäßigen Speicherort konfiguriert ist, wird die Oracle-Datenbank nicht automatisch in der Knotenliste angezeigt und muss während der Planerstellung manuell hinzugefügt werden.
- Die Option "Unterbrechen/Wiederaufnehmen" ist im Menü "Knoten" für Oracle-Knoten nicht verfügbar.
- Oracle unterstützt Tablespace nicht, wenn der Tablespace-Name Dollarzeichen ($) in Oracle 19c enthält.
- Die spezifische Wiederherstellung wird nicht unterstützt, wenn die Oracle-Datenbank mithilfe eines virtuellen Kontos installiert wird.

- UDP 8.1 unterstützt keine Sicherung von Datenbanken verschiedener Oracle-Versionen, die auf demselben Server installiert sind.
- Tabellenwiederherstellung gemäß Oracle-Einschränkungen:
  - Aus den Tablespaces SYSTEM und SYSAUX erstellte Tabellen können nicht wiederhergestellt werden.
  - Vom System oder Systembenutzer erstellte Tabellen können nicht wiederhergestellt werden.
- RPS fungiert als Sicherungs-, Wiederherstellungs- und Assured Recovery-Agent.
- Für die Standard Edition wird nur die vollständige DB-Wiederherstellung mit der Option "Alle wiederherstellen" und "Point-in-Time (PIT)" vom letzten Wiederherstellungspunkt und zwischenzeitlichen Wiederherstellungspunkten unterstützt.
- Für die Standard Edition wird die Tablespace-Wiederherstellung mit "recover all" vom letzten Wiederherstellungspunkt unterstützt, und die UNTIL-Klausel wird im RMAN-Skript nicht unterstützt.
- Für die Standard Edition unterstützt Oracle keine Wiederherstellungen auf Tabellenebene.
- Nach einer vollständigen DB-Wiederherstellung wird die nächste Zuwachssicherung automatisch in eine vollständige Sicherung konvertiert.
- Wenn sich die WRP-Größe ändert, ist die nächste Sicherung eine vollständige Sicherung.
- Es werden maximal 10 Kanäle unterstützt.

Kapitel 5: Schützen von Microsoft SharePoint-Umgebungen

In diesem Abschnitt werden die folgenden Themen behandelt:

Installationshinweise für Microsoft SharePoint-Umgebungen

Dieses Thema enthält die Informationen, die Sie benötigen, um den Arcserve UDP Agent für Microsoft SharePoint-Umgebungen installieren und konfigurieren zu können. Es wird vorausgesetzt, dass Sie mit den Eigenschaften und Anforderungen Ihrer Microsoft SharePoint-Serverfarm vertraut sind.

Besondere Aspekte der Umgebung

SharePoint-Umgebungen können komplex und auf viele Rechnern verteilt sein. Die Konfiguration der Serverfarm muss von Microsoft unterstützt werden. Eine verteilte SharePoint-Umgebung kann beispielsweise folgende Komponenten enthalten:

- Ein oder mehr Web-Front-End-Server.
- Ein oder mehr von SharePoint Server Farm verwendete Datenbankserver.
- In den meisten Fällen wird der SharePoint in einer Domänenumgebung installiert. Es gibt einen oder mehrere Domänencontroller und DNS-Server.

Installationshinweise

Berücksichtigen Sie bei der Installation der Agenten Folgendes:

- SharePoint-ist eine verteilte Umgebung. Es wird empfohlen, UDP Agent auf jedem Server in der SharePoint-Farm einschließlich Web-Front-End-Server und Datenbankserver zu installieren.
- Wir empfehlen außerdem, die gesamte Domänenumgebung einschließlich Domänencontroller und DNS-Server zu schützen. Sie werden benötigt, um die Farm, die Konfiguration der Farm und die Web-Anwendung wiederherzustellen.

Schützen von Microsoft SharePoint-Servern

Mit Arcserve UDP können Sie Microsoft SharePoint-Server sichern. Um sicherzustellen, dass die Wiederherstellung wie erwartet funktioniert, wird empfohlen, den gesamten Rechner und nicht nur ausgewählte Volumes auf allen SharePoint-Servern zu schützen.

Bei Domänencontrollern und DNS-Servern können Sie die ausgewählten Volumes sichern, solange der Domänendienst und der DNS-Dienst ordnungsgemäß funktionieren, nachdem sie von der Instanz-VM gestartet wurden.

- Beachten der Hinweise
- Durchführen einer Sicherung des SharePoint-Servers

Beachten der Hinweise

Es wird empfohlen, alle Server, einschließlich der Web-Front-End-Server, Datenbankserver, Domänencontroller und DNS-Server, zu einem Plan mit dem gleichen Ablaufplan hinzuzufügen. Auf diese Weise werden alle Server fast gleichzeitig gesichert. Dies ist für eine verteilte Umgebung sehr wichtig. Während der Wiederherstellung können Sie dasselbe über die Wiederherstellungspunkten erreichen, die gleichzeitig für alle Server gesichert werden.

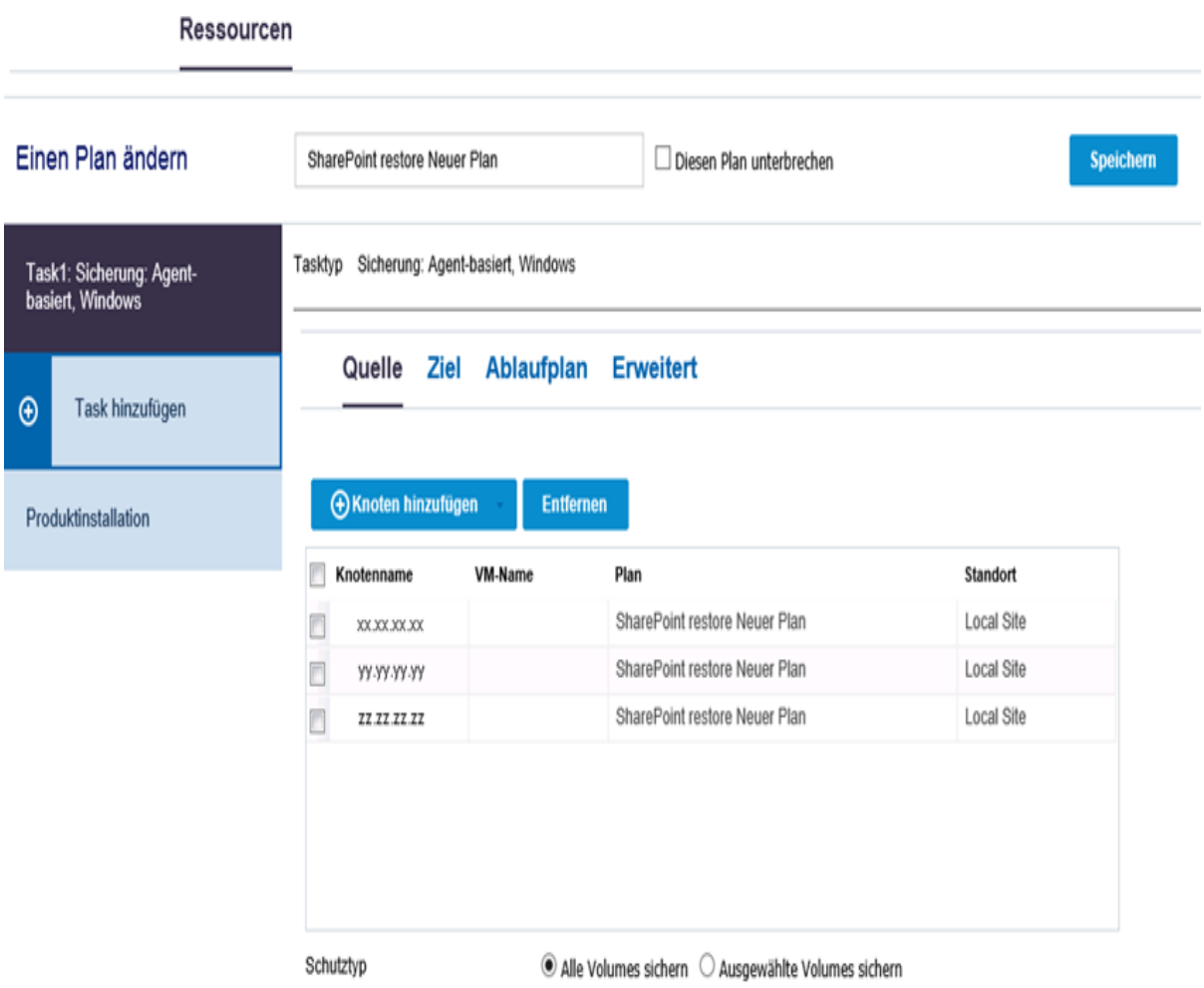
Hinweis: Wenn die Topologie der SharePoint-Farm geändert wird, werden neue Server hinzugefügt, um einen besseren Lastausgleich für SharePoint zu realisieren. Sie müssen die neuen Server sofort zum gleichen Plan hinzufügen.

Durchführen einer Sicherung des SharePoint-Servers

Verwenden Sie die Arcserve UDP-Konsole, um Sicherungen der SharePoint-Umgebung auf Datenbankebene durchzuführen.

Gehen Sie wie folgt vor:

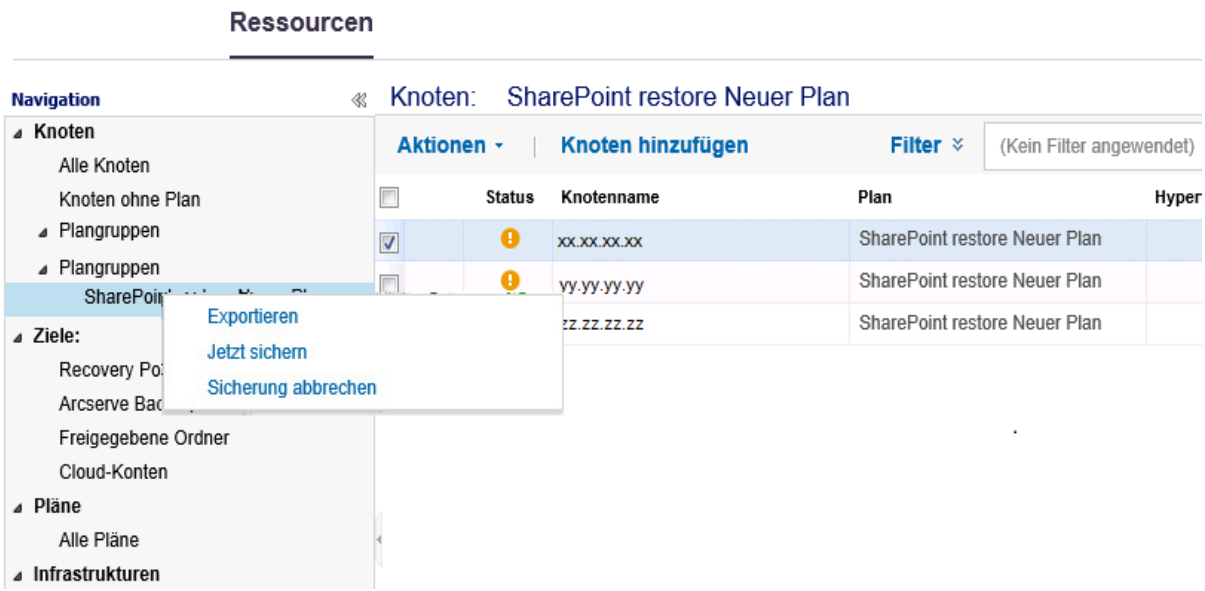
1. Melden Sie sich bei der Konsole an.
2. Klicken Sie auf **Ressourcen** und navigieren Sie zu **Knoten** in linken **Navigationsbereich**.
3. Klicken Sie auf **Alle Knoten**.
4. Fügen Sie alle Knoten in der SharePoint-Farm-Umgebung hinzu.
5. (optional) Erstellen Sie einen Datenspeicher.
6. Erweitern Sie **Pläne** im Fensterbereich **Navigation** und klicken Sie auf **Alle Pläne**.
7. Klicken Sie auf **Hinzufügen**, um einen neuen Plan zu erstellen.
8. Fügen Sie auf der Registerkarte **Quelle** alle Knoten hinzu, die in der SharePoint-Farm-Umgebung enthalten sind.



9. Konfigurieren Sie weitere Einstellungen, und speichern Sie den Plan.

   Der Plan wird für die SharePoint-Farm-Umgebung erstellt. Die Einstellungen des Plans werden für alle Knoten bereitgestellt. Der Sicherungsjob startet zum geplanten Zeitpunkt.

   Sie können den Sicherungsjob manuell starten, indem Sie auf "Jetzt sichern" klicken. Der Sicherungsjob für alle Knoten der SharePoint-Farm beginnt. Die Daten werden im selben Datenspeicher gespeichert.


Ressourcen
Navigation
Knoten
Alle Knoten
Knoten ohne Plan
Plangruppen
Plangruppen
Ziele:
Recovery Po
Arcserve Bac
Freigegebene Ordner
Cloud-Konten
Pläne
Alle Pläne
Infrastrukturen
Exportieren
Jetzt sichern
Sicherung abbrechen
Knoten: SharePoint restore Neuer Plan
Aktionen
Knoten hinzufügen
Filter
(Kein Filter angewendet)
Status
Knotenname
Plan
Hyper
xx.xx.xx.xx
SharePoint restore Neuer Plan
yy.yy.yy.yy
SharePoint restore Neuer Plan
SharePoint restore Neuer Plan

Wiederherstellen einer SharePoint-Umgebung

Die folgende spezifische Wiederherstellungen werden unterstützt:

- Farm
- Farm nur mit Konfiguration
- SharePoint-Dienste
- Web-Anwendungen
- Inhaltsdatenbanken
- Standorterfassungen
- Sites
- Listen
- Listenelemente (einschließlich Dokumente)

Mit anderen Lösungen können weitere spezifische Wiederherstellungen durchgeführt werden:

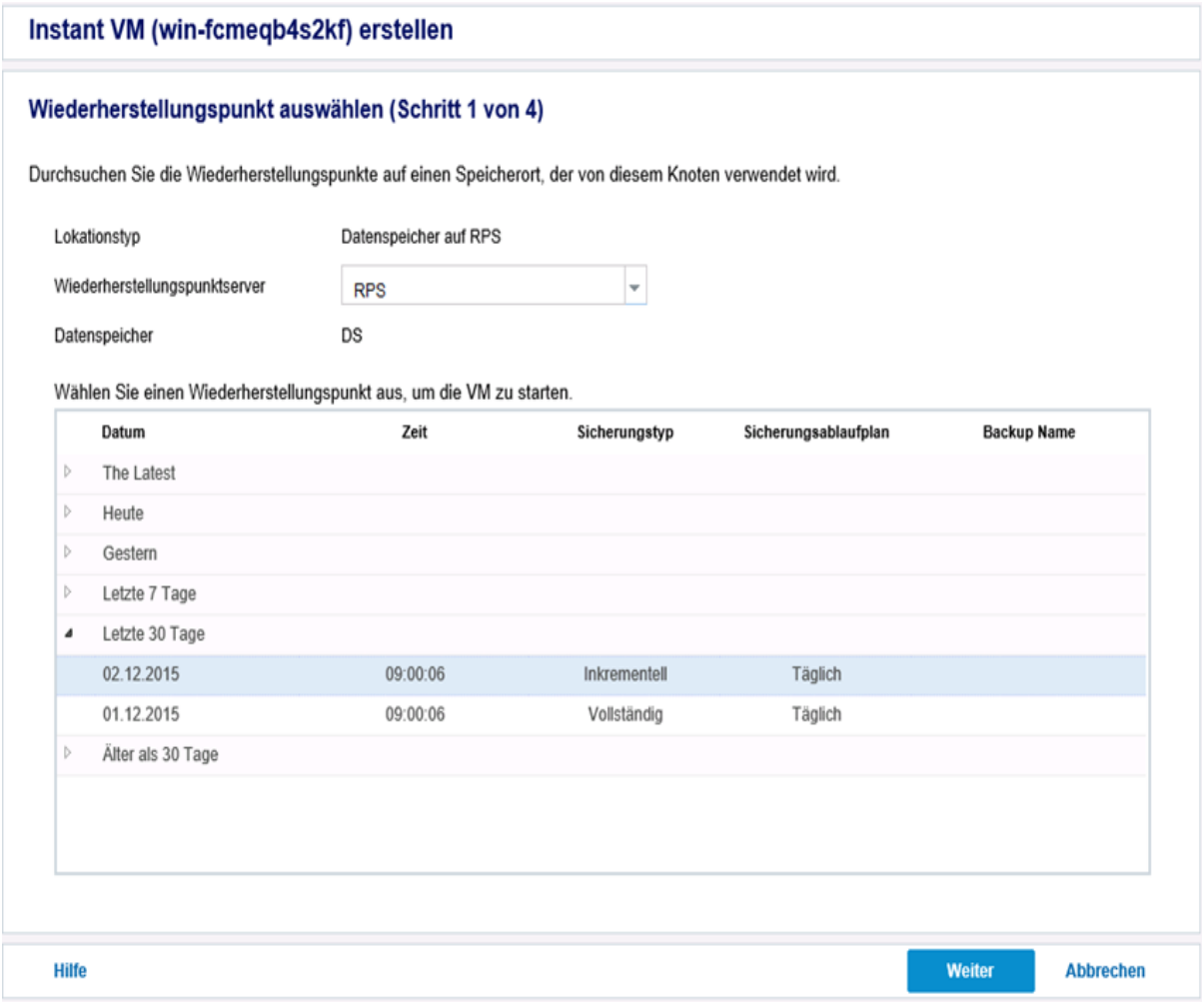
- Wiederherstellen mit der Instant VM:Diese Lösung unterstützt Farm, Farm nur mit Konfiguration, SharePoint-Dienste und Webanwendungen.
- Wiederherstellen über die Benutzeroberfläche von Arcserve UDP Agent: Diese Lösung unterstützt Inhaltsdatenbanken.
- Wiederherstellen durch Laden einer Datenbank mithilfe eines Wiederherstellungspunkts: Diese Lösung unterstützt Standortsammlungen, Standorte, Listen und Listenelemente.

Wiederherstellen mit der Instant VM

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Konsole an.
2. Klicken Sie auf **Ressourcen**, **Knoten**.
3. Klicken Sie mit der rechten Maustaste auf den Knoten, der sich im Plan für die SharePoint-Umgebung befindet.
4. Klicken Sie auf die Option zum **Erstellen einer Instant VM**, um sofortige virtuelle Rechner für den Rechner der SharePoint-Umgebung zu erstellen.

   Der Assistent zum **Erstellen einer Instant VM** wird geöffnet.
5. Suchen Sie nach Wiederherstellungspunkten von einem Speicherort, und wählen Sie einen Wiederherstellungspunkt aus, um die Instant VM zu starten.

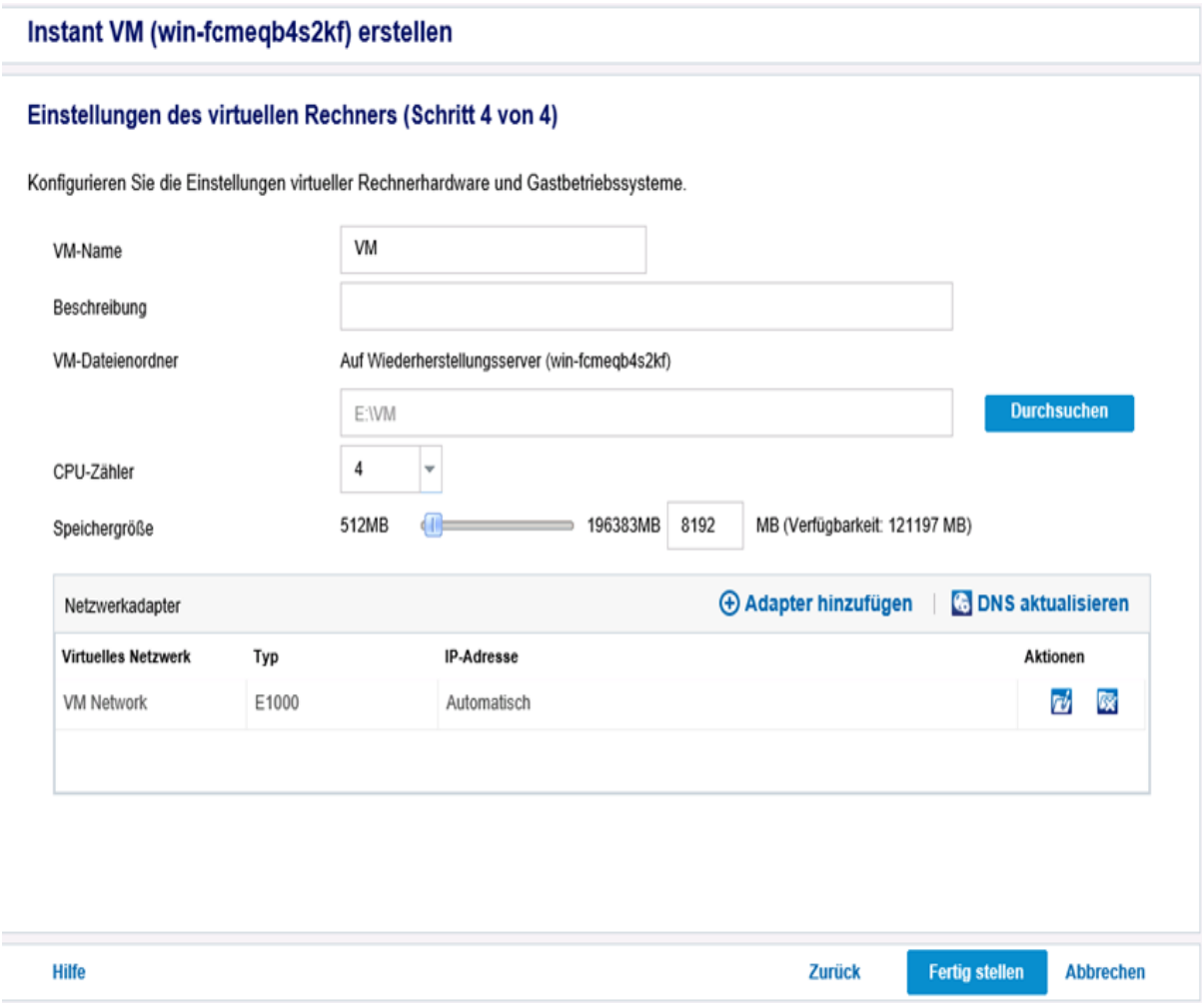


6. Klicken Sie auf **Weiter**.

7. Geben Sie einen Speicherort auf VMware vSphere oder Microsoft Hyper-V an, um die Instant VM zu hosten. Beispiel: Der Hypervisor-Typ ist VMware vSphere.
8. Klicken Sie auf **Weiter**.
9. Geben Sie einen Rechner an, um die Instant VM auszuführen.

   Beispiel: Verwenden Sie den aktuellen RPS.
10. Klicken Sie auf **Weiter**.
11. Konfigurieren Sie die Hardware und die Systemeinstellungen der Instant VM.
12. Erstellen Sie ein neues virtuelles Netzwerk als isolierte Netzwerkumgebung für die SharePoint-Wiederherstellung. Weitere Informationen zum Erstellen einer Isolierung finden Sie im Abschnitt zum Erstellen eines isolierten Netzwerks für die SharePoint-Wiederherstellung.
13. Klicken Sie auf das Pluszeichen, um einen Netzwerkadapter hinzuzufügen.
14. Wählen Sie das richtige virtuelle Netzwerk, das eine isolierte Netzwerkumgebung für SharePoint-Wiederherstellung ist, und verwenden Sie die Standardkonfiguration der TCP/IP-Einstellungen "Source:XXX.XXX.XXX.XXX".

    Wichtig! Beim Erstellen einer Instant VM für einen Rechner, der Web-Front-End-Server für die SharePoint-Umgebung ist, fügen Sie einen weiteren Netzwerkadapter zum Übertragen der Sicherungsdatendatei hinzu. Die IP-Adresse des neuen Adapters muss sich im selben virtuellen Netzwerk wie die ursprünglichen Web-Front-End-Server für SharePoint und im selben IP-Segment befinden. Dann kann die ursprüngliche SharePoint-Umgebung den Netzwerkadapter für den Zugriff auf alle freigegebenen Ordner der Instant VM verwenden.



15. Klicken Sie auf **Fertig stellen**.

    Das Dialogfeld "VM starten" wird geöffnet.

16. Klicken Sie auf **Später starten**.

    Eine neue Instant VM wird erstellt, die in **Infrastrukturen** unter den **Instant VMs** auf der Konsole angezeigt wird.

17. Erstellen Sie Instant VMs für alle Knoten in der Umgebung der SharePoint-Farm.

18. Nachdem die Instant VMs für alle Knoten erstellt wurden, starten Sie sie nacheinander.

    - Starten Sie den Domänen-Controller zuerst, dann den DNS-Server.
    - Starten Sie dann den Datenbankserver und zuletzt die Web-Front-End-Server.

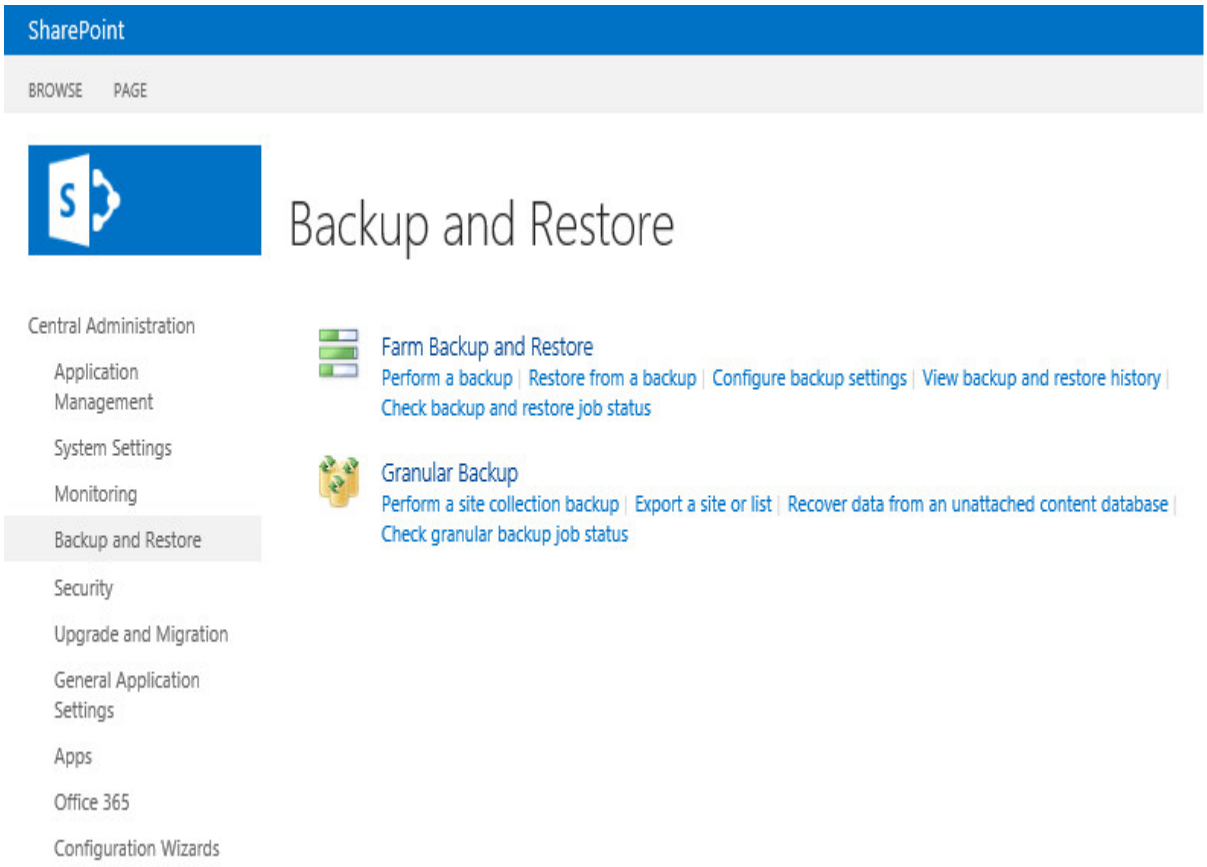
19. Klicken Sie mit der rechten Maustaste auf die zu startende Instant VM, und wählen Sie **Starten**, um die Instant VM zu starten.

20. Warten Sie, bis diese Instant VMs für die Rechner der SharePoint-Umgebung gestartet sind.

Die temporäre SharePoint-Umgebung wurde eingerichtet.

21. Melden Sie sich bei der Instant VM an, bei der der Rechner Web-Front-End-Server für die SharePoint-Umgebung ist. Öffnen Sie die Zentraladministration, klicken Sie auf die Überschrift "Sicherung und Wiederherstellung", und wählen Sie die Verknüpfung "Sicherung durchführen".

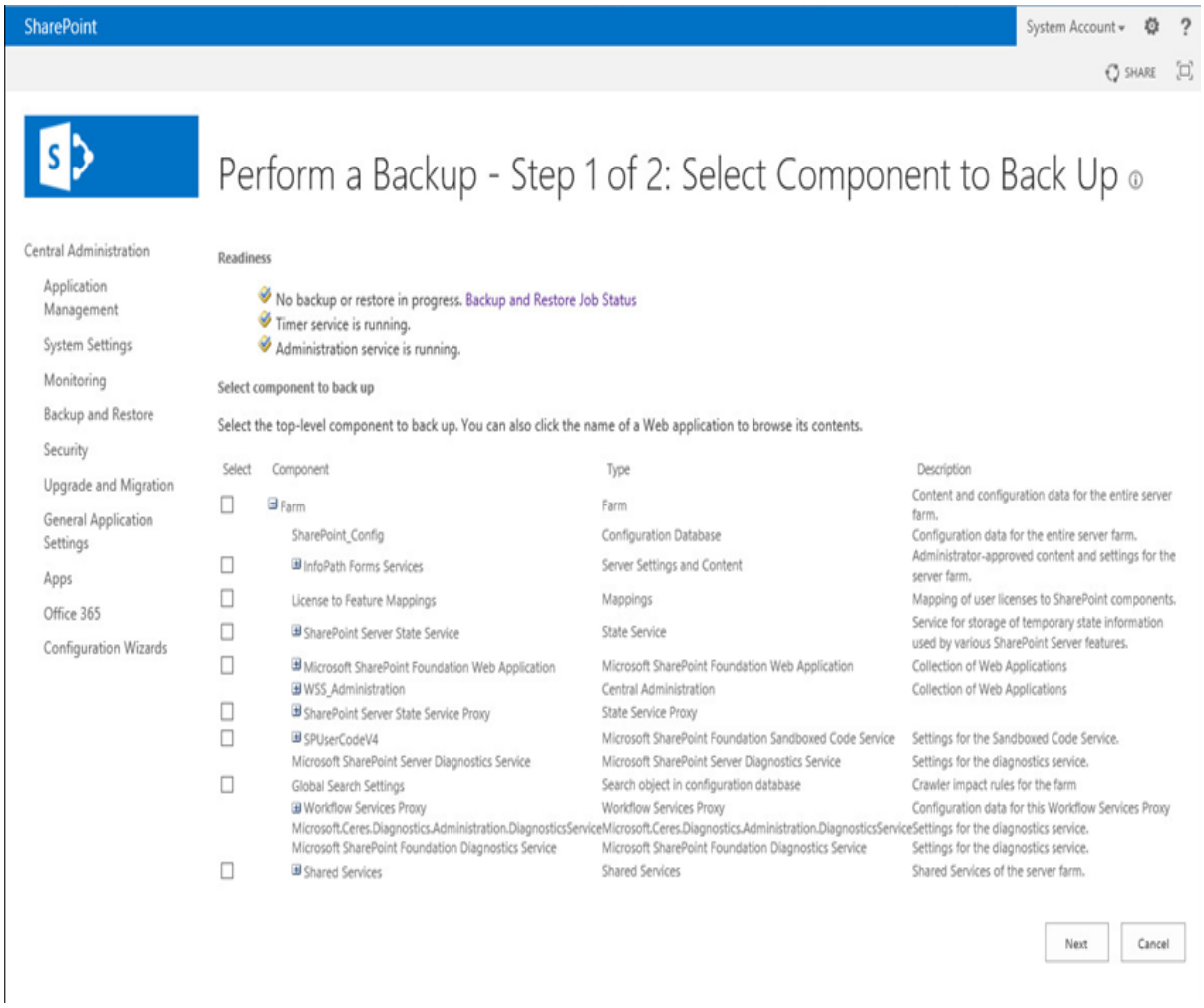
    Hinweis: Wenn Sie eine HTTP 404-Fehlermeldung erhalten, nachdem Sie eine Webanwendung wie "Sharepoint – 80" geöffnet haben, deaktivieren Sie IPv6, und deaktivieren Sie das Kontrollkästchen **Internetprotokoll, Version 6 (TCP/IP)** im Fenster der LAN-Eigenschaften.



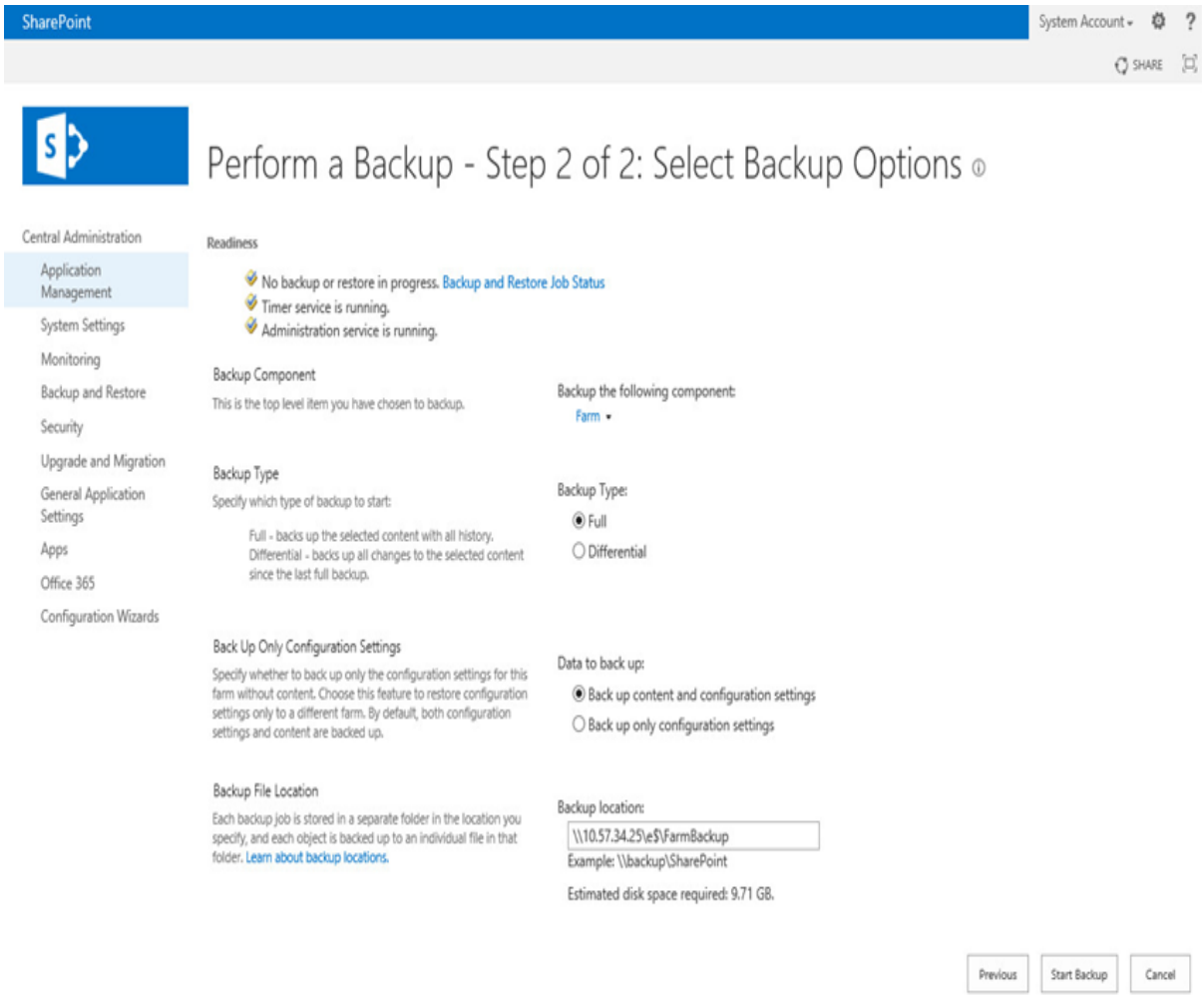
22. Wählen Sie die Komponente aus, die Sie für die Farm wiederherstellen möchten, und klicken Sie auf **Weiter**.

    Sichern Sie beispielsweise die Webanwendungen "SharePoint – 80". Erweitern Sie den Knoten "Microsoft SharePoint Foundation-Webanwendung", und wählen Sie die Komponenten "SharePoint – 80".

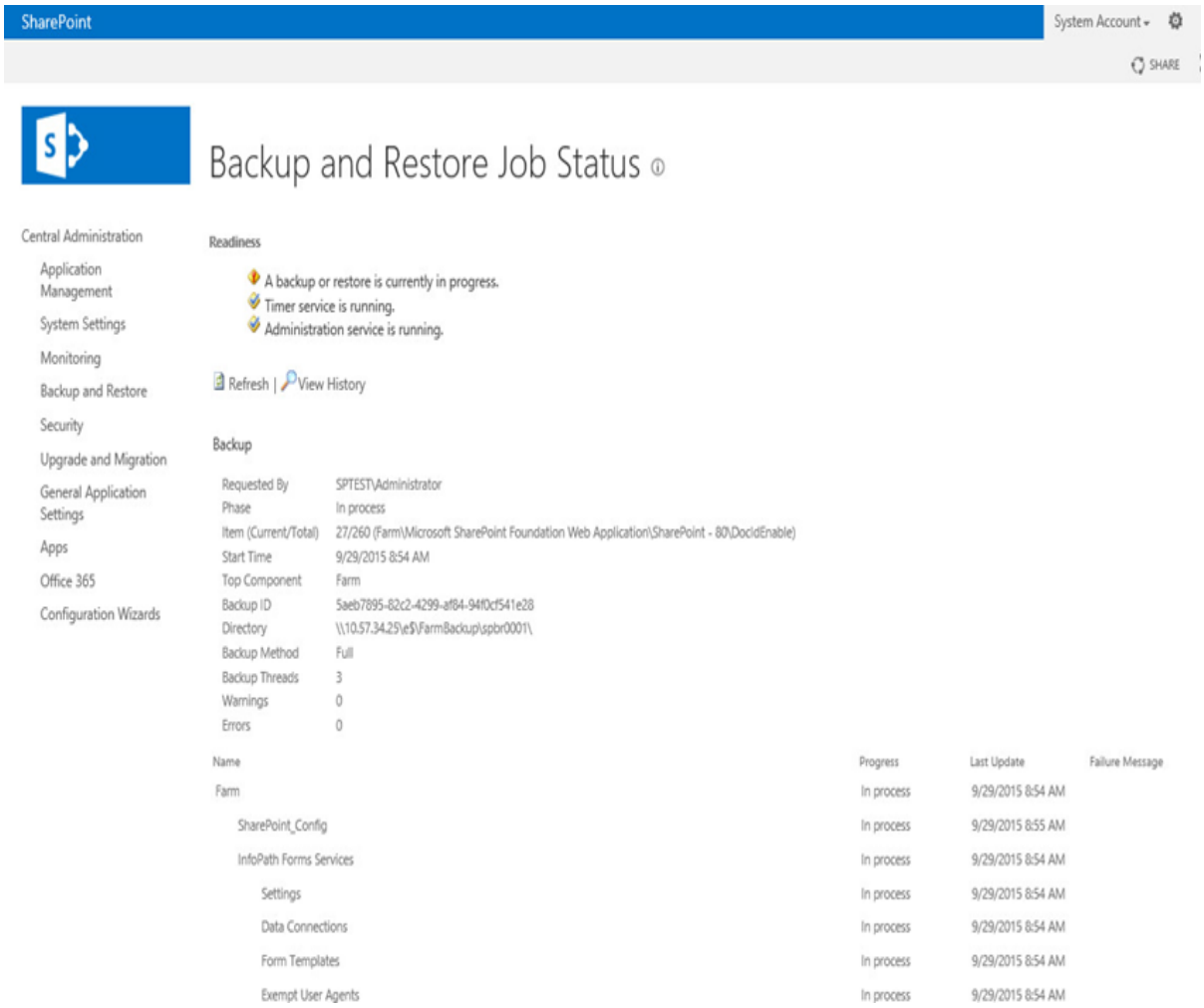
    Sichern Sie Access Services. Erweitern Sie den Knoten "Gemeinsame Dienstanwendungen" unter "Gemeinsame Dienste", und wählen Sie die Komponente "Access Services 2010" aus.



23. Geben Sie als Sicherungstyp "Vollständig" an.
24. Erstellen Sie einen freigegebenen Ordner für die Instant VM, auf der der Rechner Web-Front-End-Server für SharePoint-Umgebung ist.
25. Gewähren Sie Vollzugriff für alle Benutzer auf den freigegebenen Ordner.
26. Geben Sie den Pfad des freigegebenen Ordners unter "Speicherort der Sicherungsdatei" an, um die Sicherungsdatei zu speichern, und klicken Sie dann auf **Sicherung starten**.

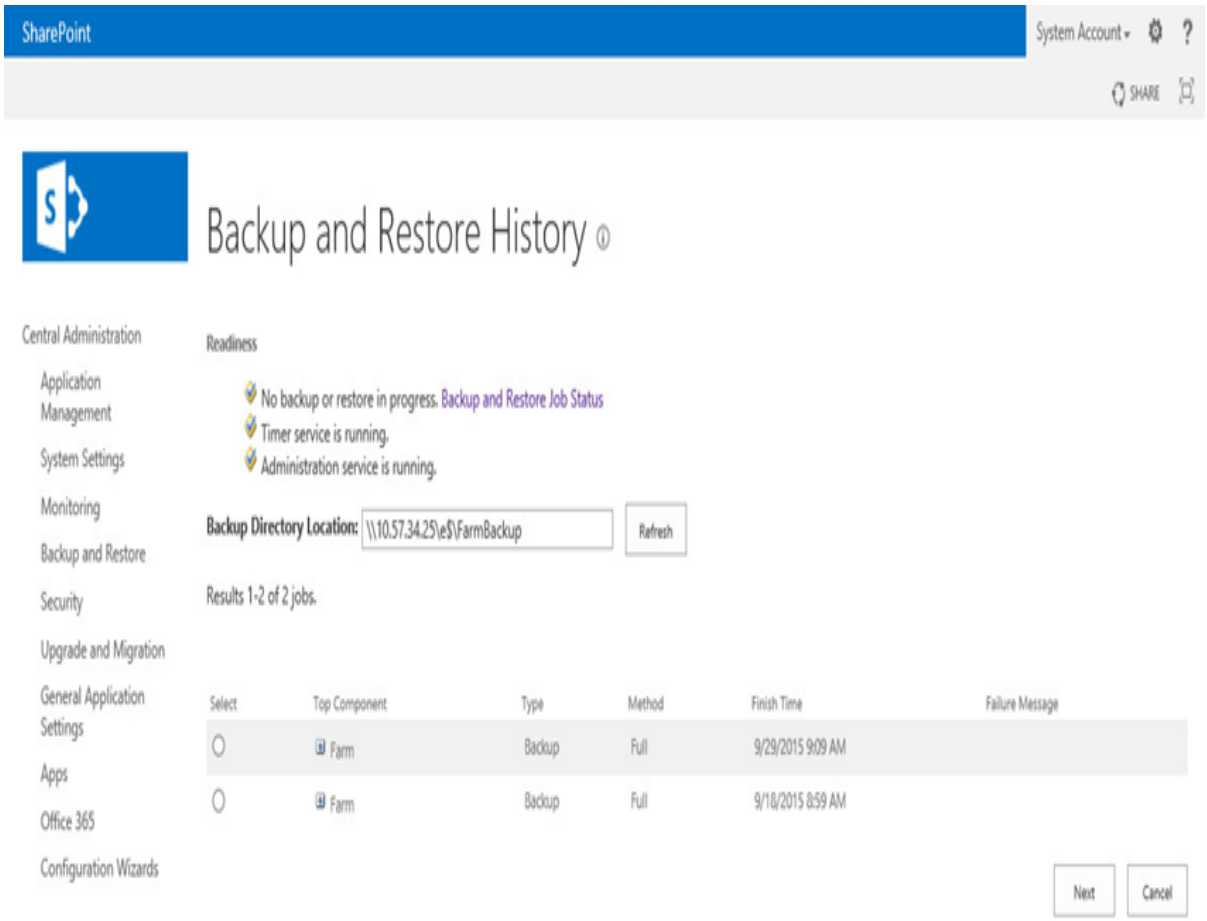


27. Warten Sie, bis der Sicherungsjob abgeschlossen ist.



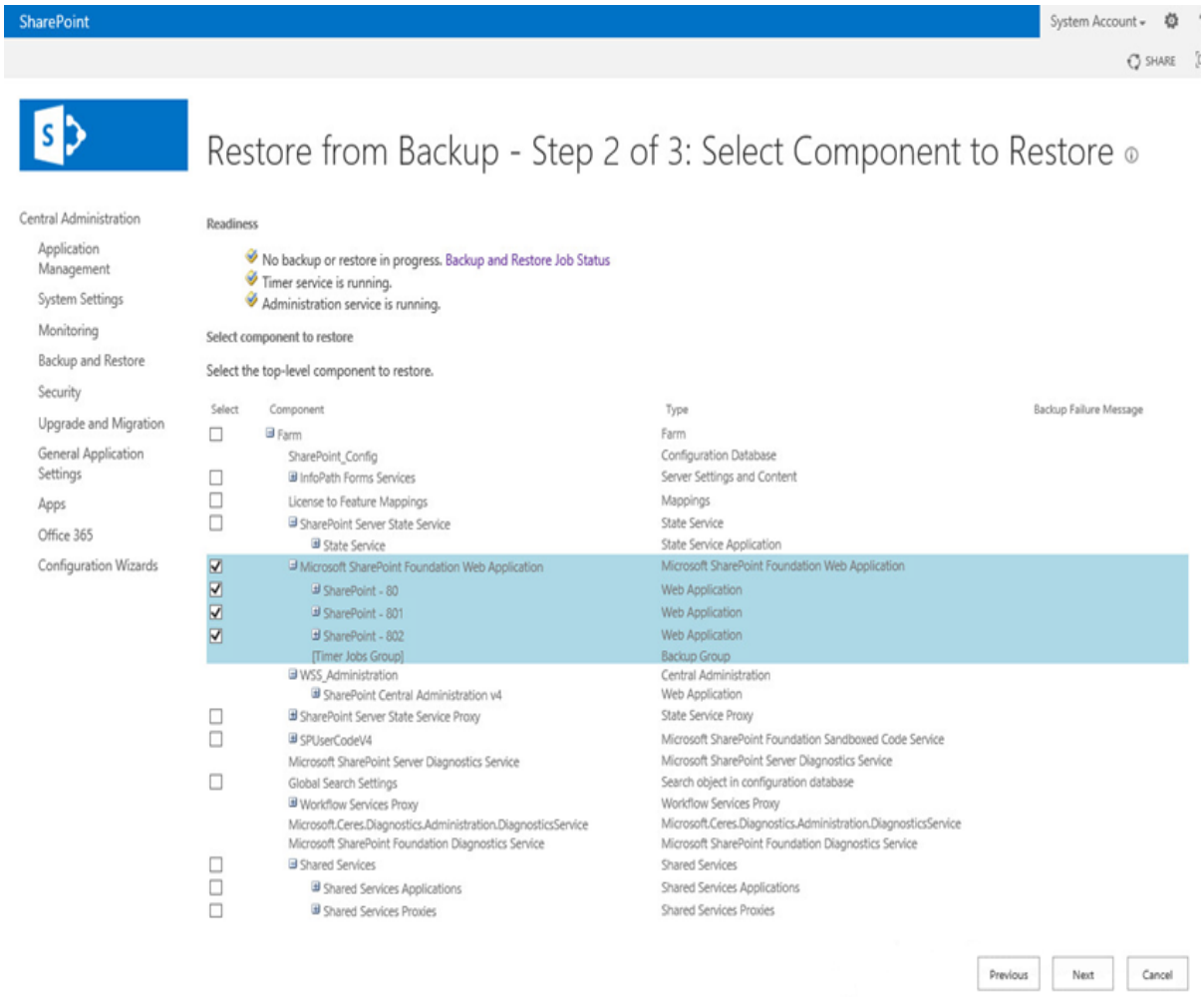
28. Nachdem der Sicherungsjob für die Farm abgeschlossen ist, melden Sie sich bei dem Rechner an, der Web-Front-End-Server für die ursprüngliche SharePoint-Umgebung ist.
29. Öffnen Sie die Zentraladministration, klicken Sie auf "Sicherung und Wiederherstellung", und wählen Sie die Verknüpfung "Farm aus Sicherung wiederherstellen".
30. Geben Sie den freigegebenen Ordner im Feld "Speicherort des Sicherungsverzeichnisses" ein, und klicken Sie auf **Aktualisieren**.

    Hinweis: Der freigegebene Ordner wurde bereits in einem der vorherigen Schritte erstellt.
31. Wählen Sie die Sicherungsinstanz aus der Übersichtsliste, und klicken Sie auf **Weiter**.



32. Wählen Sie die Konfiguration und den Inhalt in der wiederherzustellenden Farm, und klicken Sie dann auf **Weiter**.

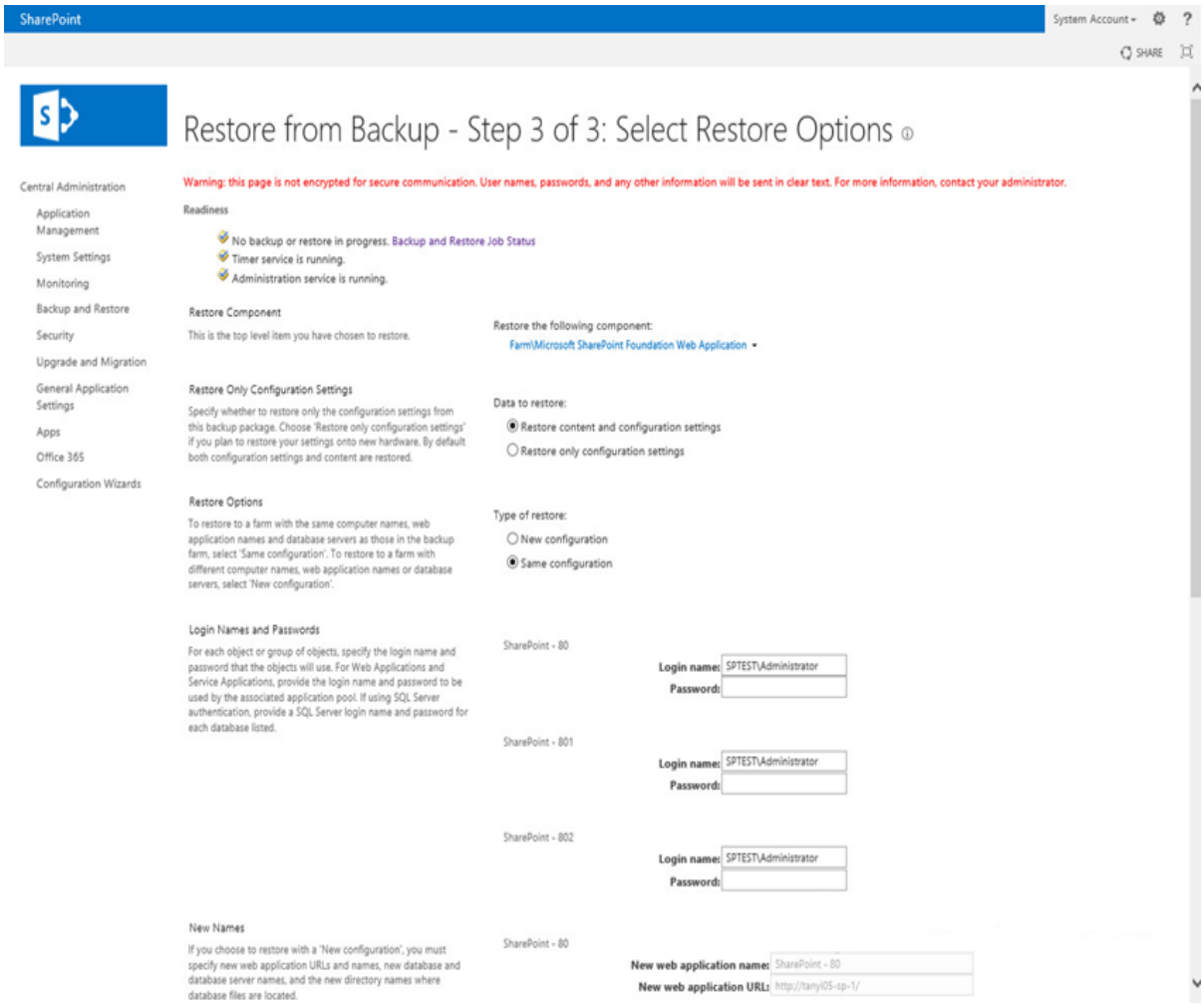
    Wählen Sie beispielsweise alle Farmkomponenten, die SharePoint Services-Komponente oder die Webanwendungen-Komponente.



Die Seite zeigt verschiedene Optionen für die ausgewählte Dienst- und Inhaltskonfiguration an.

33. Wählen Sie, ob Sie Folgendes tun möchten:

    - Inhalt und Konfigurationseinstellungen wiederherstellen oder nur Konfigurationseinstellungen wiederherstellen
    - Konfiguration überschreiben oder in den Wiederherstellungsoptionen neu erstellen



34. Klicken Sie auf die Schaltfläche **Wiederherstellung starten**, um den Wiederherstellungsvorgang zu starten.

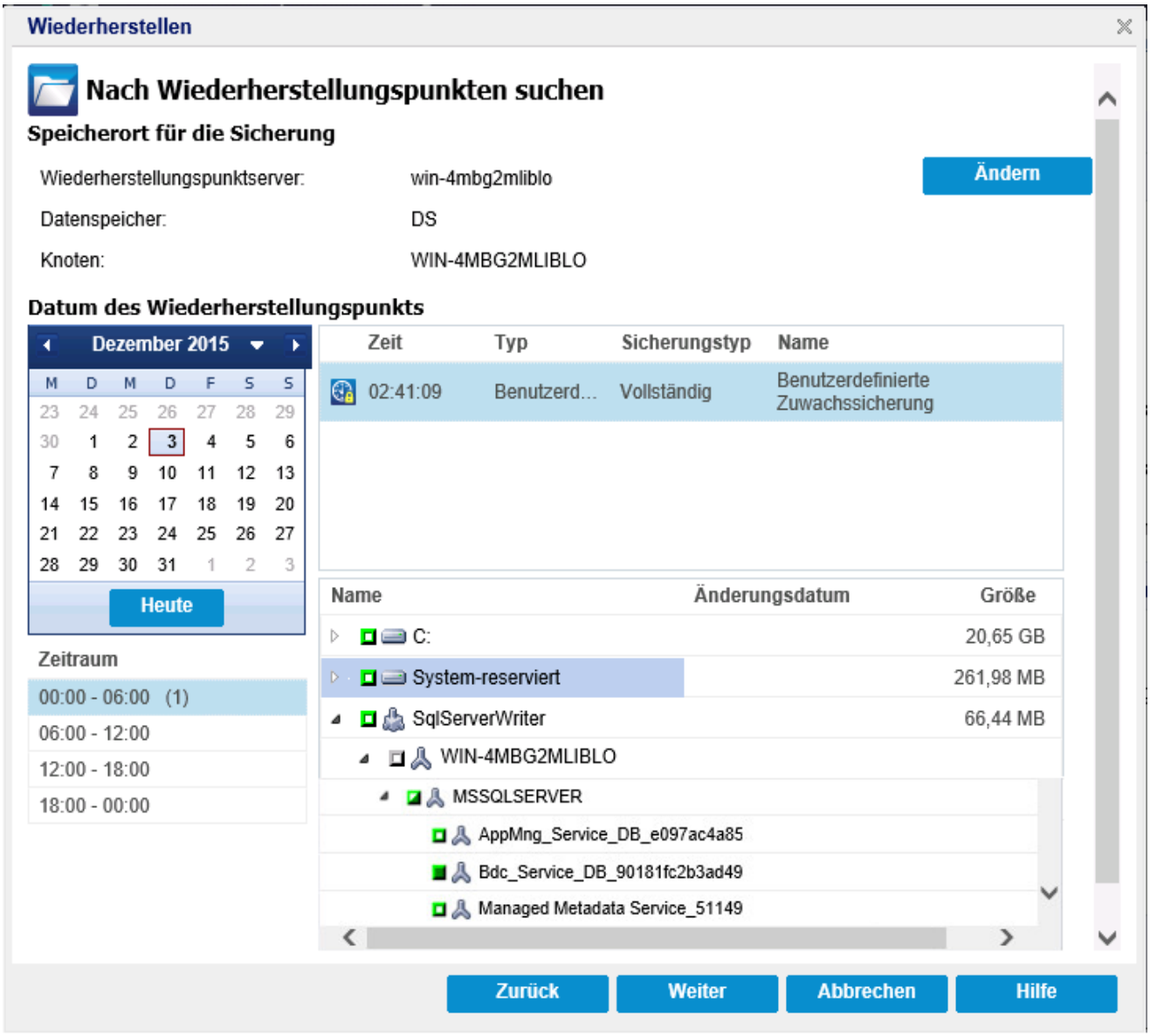
    Nachdem der Wiederherstellungsjob abgeschlossen ist, sind die ausgewählten Komponenten in der Farm wiederhergestellt.

Wiederherstellen über die Benutzeroberfläche von Arcserve UDP Agent

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Konsole an.
2. Klicken Sie mit der rechten Maustaste auf den Knoten, der dem vom SharePoint verwendeten Datenbankserver entspricht.
3. Klicken Sie auf "Wiederherstellen".

   Die Benutzeroberfläche des Arcserve UDP-Agenten wird geöffnet, der auf dem Datenbankserver gehostet wird.
4. Klicken Sie auf "Wiederherstellungspunkte durchsuchen".
5. Klicken Sie auf den Wiederherstellungspunkt, der die Datenbank enthält, die wiederhergestellt werden soll.
6. Wählen Sie unter SqlServerWriter/{SqlServerName}/{SqlServerInstantsName} die Datenbank aus, die wiederhergestellt werden soll.
7. Klicken Sie auf "Weiter".



8. Wählen Sie das Wiederherstellungsziel aus, und klicken Sie auf "Weiter".

   Wenn Sie "Am ursprünglichen Speicherort wiederherstellen" auswählen, wird die Datenbank am ursprünglichen Speicherort wiederhergestellt. Wenn Sie "An einem alternativen Speicherort wiederherstellen" auswählen, wird die Datenbank am angegebenen Speicherort wiederhergestellt. In beiden Fällen wird die wiederhergestellte Datenbank automatisch in SQL Server integriert. Wenn Sie "Nur Speicherauszugsdatei" auswählen, werden die Datendatei für die Datenbank und die Protokolldatei am angegebenen Speicherort gespeichert.

9. Klicken Sie auf "Fertig stellen", und warten Sie, bis der Wiederherstellungsjob beendet ist.

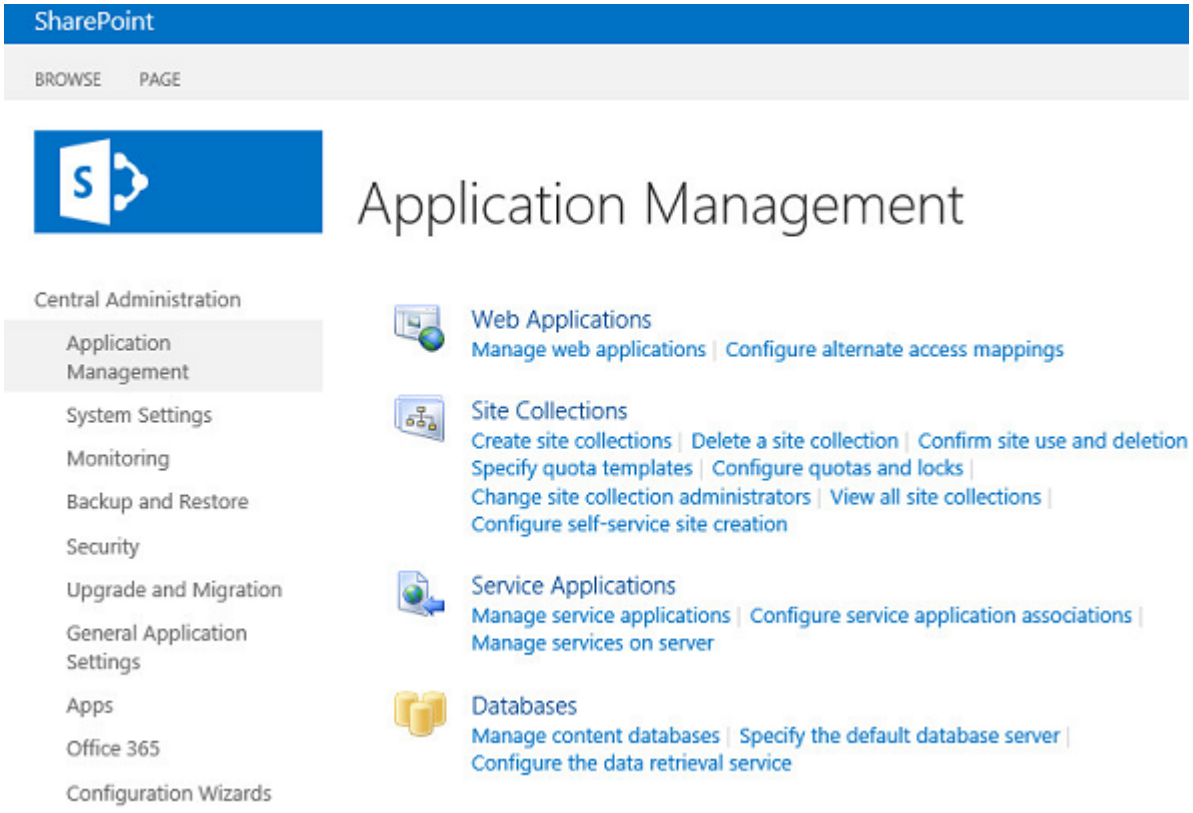
   Hinweis: Wenn Sie "Nur Speicherauszugsdatei" ausgewählt haben, fügen Sie zunächst die Datenbank hinzu. Führen Sie die Schritte in Wiederherstellen aus

einem Wiederherstellungspunkt mithilfe der Datenbankoption 'Laden' durch, und überprüfen Sie, ob die neue Inhaltsdatenbank der ursprünglichen zugehörigen Webanwendung zugeordnet ist. Gehen Sie andernfalls vor wie unter Hinzufügen der wiederhergestellten Inhaltsdatenbank zur ursprünglichen Webanwendung beschrieben.

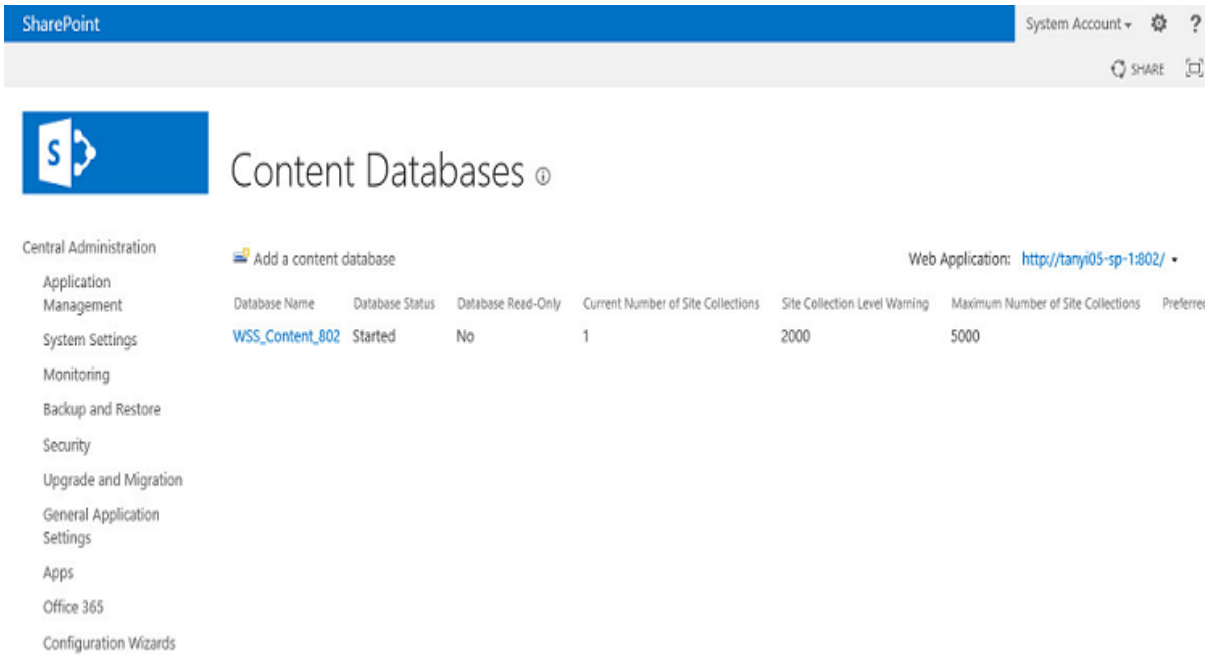
Hinzufügen der wiederhergestellten Inhaltsdatenbank zur ursprünglichen Webanwendung

Gehen Sie wie folgt vor:

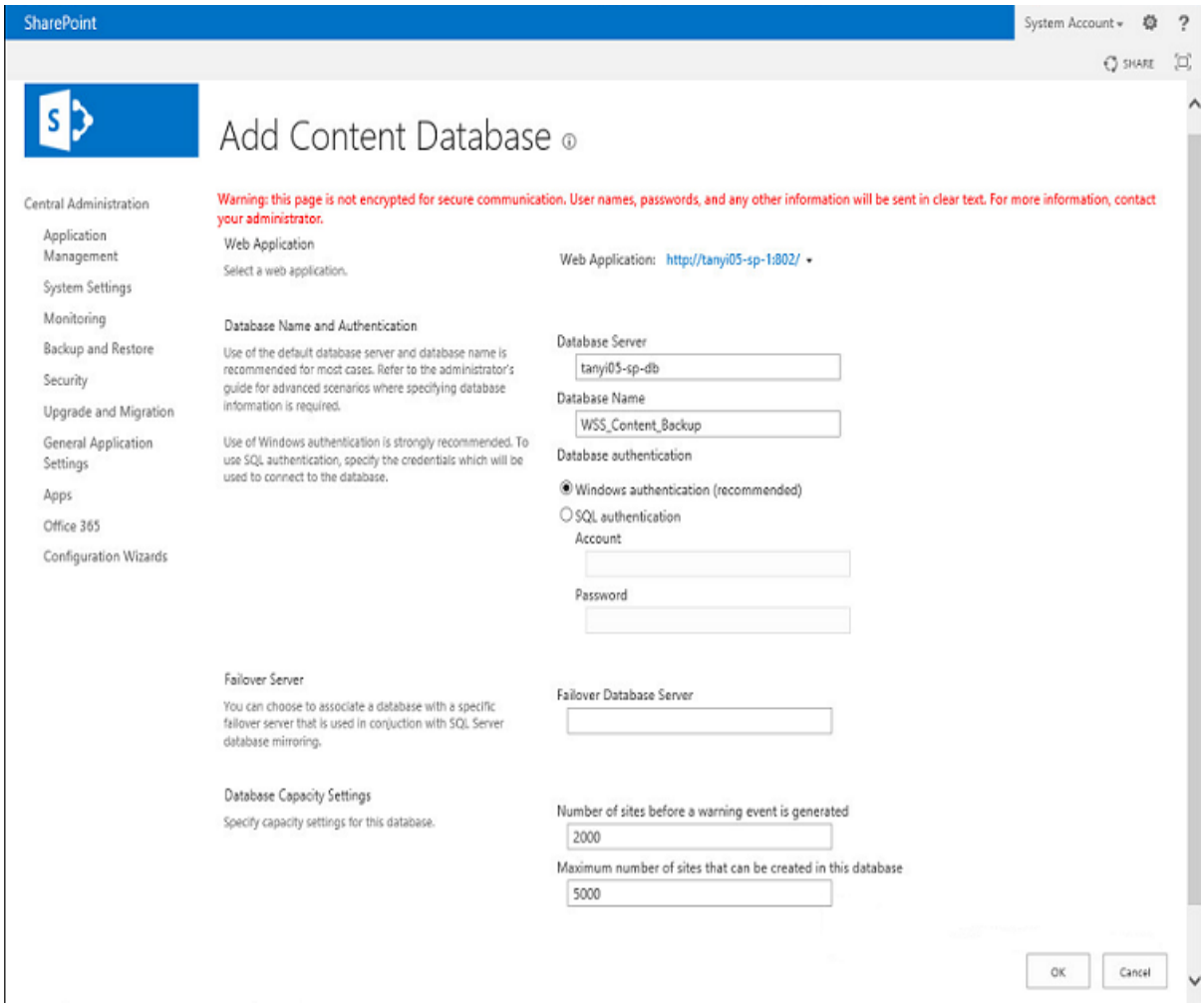
1. Öffnen Sie die SharePoint-Zentraladministration, und wählen Sie "Anwendungsverwaltung" aus.



2. Wählen Sie "Inhaltsdatenbanken verwalten" aus.



3. Wählen Sie die Webanwendung aus, und klicken Sie auf "Inhaltsdatenbank hinzufügen".
4. Geben Sie den Datenbankserver und den Datenbanknamen (z. B. WSS_Content_Backup) ein, und klicken Sie dann auf "OK".

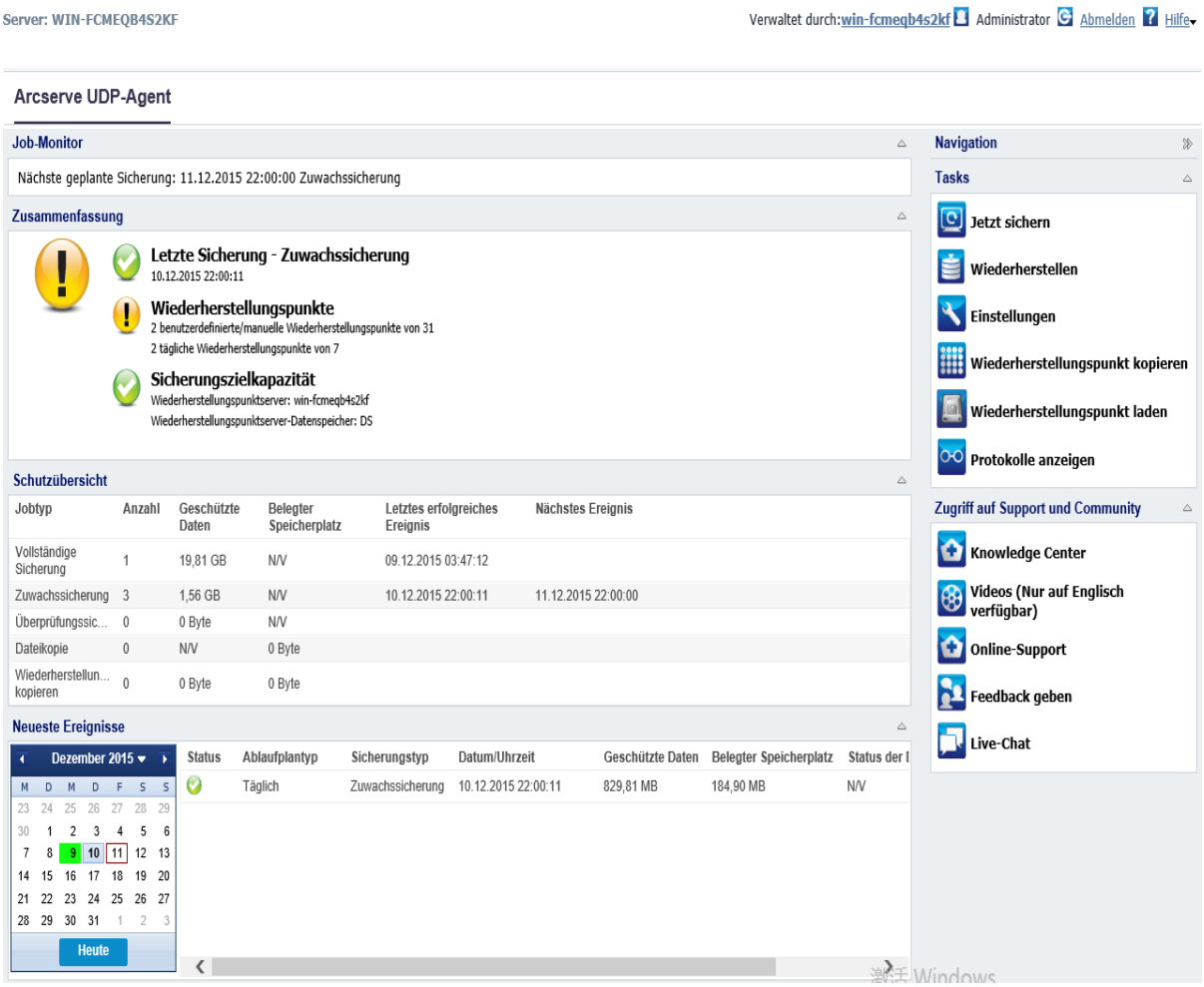


Die Inhaltsdatenbank ist jetzt der ursprünglichen zugehörigen Webanwendung zugeordnet.

Wiederherstellen durch Laden einer Datenbank mithilfe eines Wiederherstellungspunkts

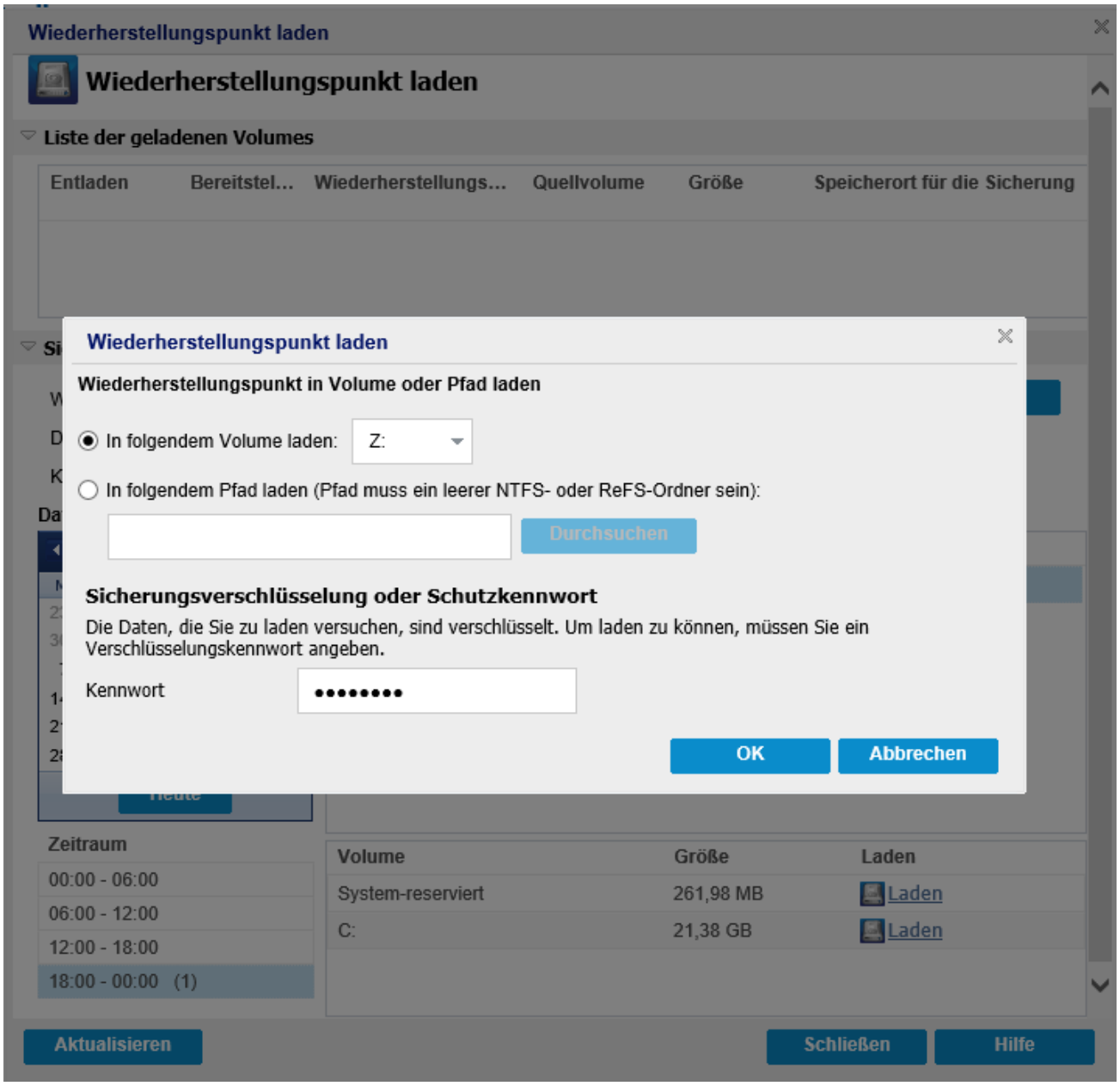
Gehen Sie wie folgt vor:

1. Öffnen Sie die Benutzeroberfläche des Arcserve UDP-Agenten, der auf dem Datenbankserver gehostet wird.

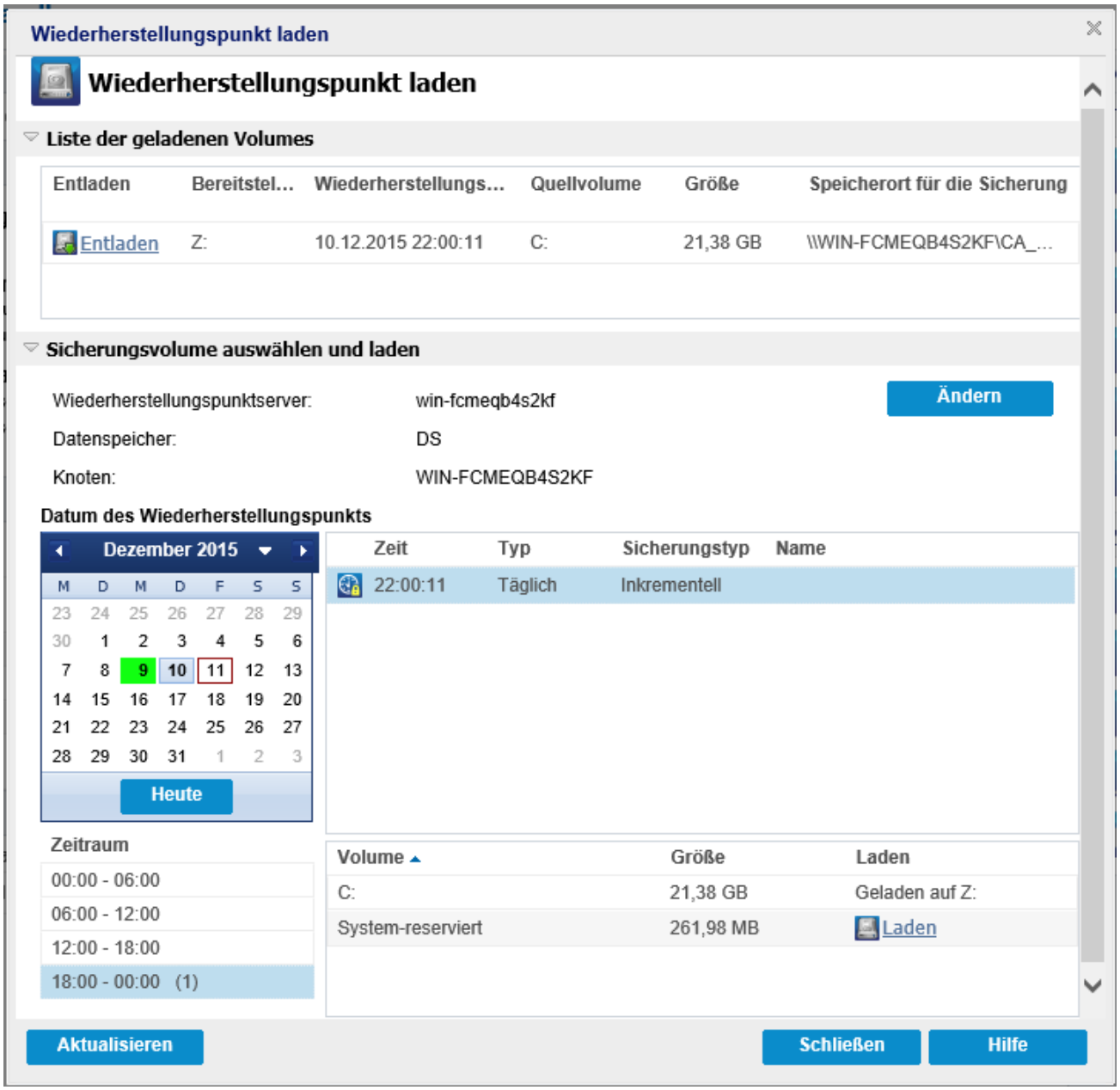


2. Klicken Sie in der Taskliste auf **Wiederherstellungspunkt laden**.
3. Wählen Sie das Volume, das die SQL Server-Datenbank für SharePoint enthält.

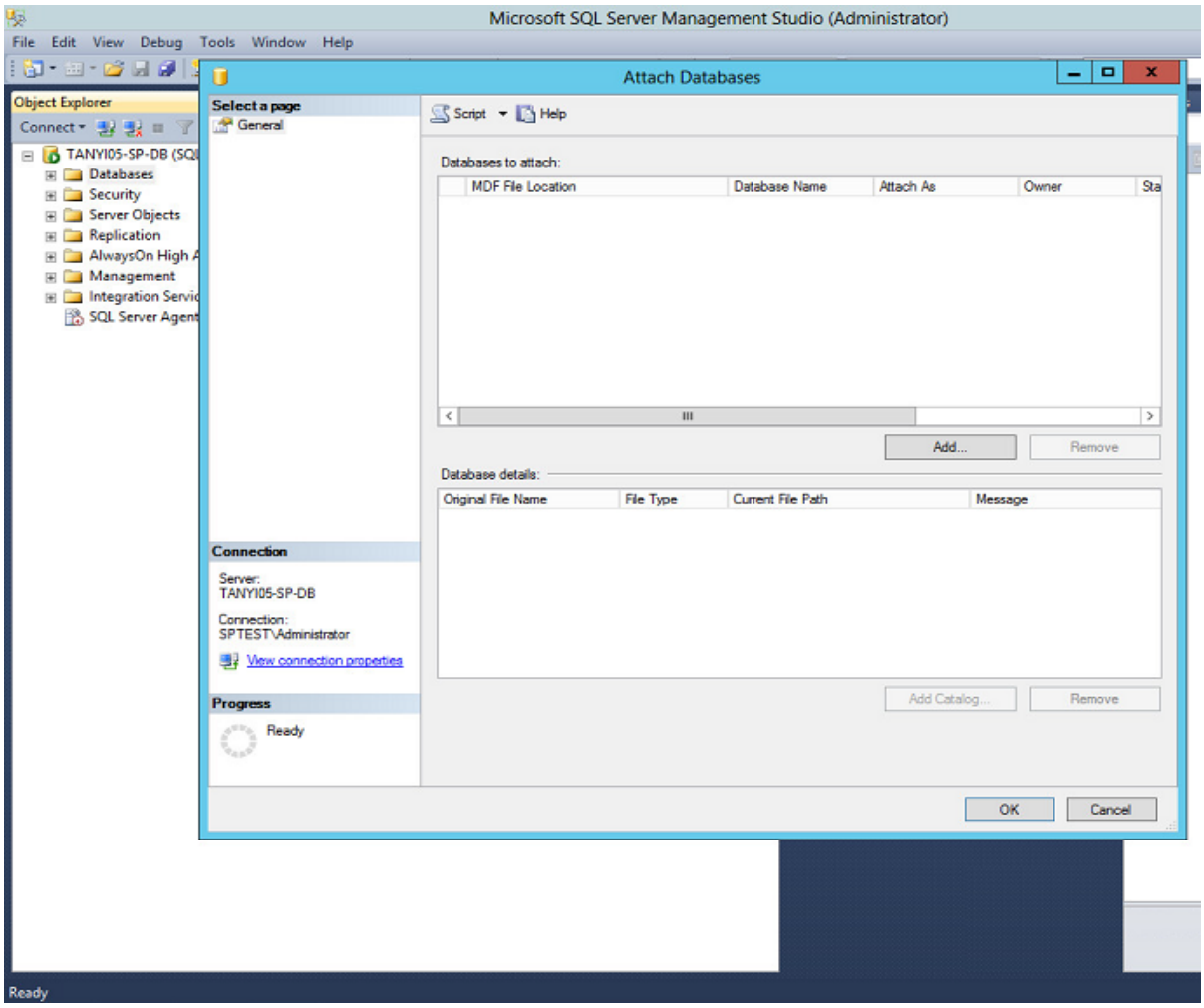
   Standardmäßig wird die Datenbankdatei beispielsweise unter "C:\Programme\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA" gespeichert, sodass Sie dann Volume C wählen müssen.
4. Wählen Sie im folgenden Dialogfenster den Namen des neuen Volumes aus, das geladen werden soll, und klicken Sie auf **OK**.



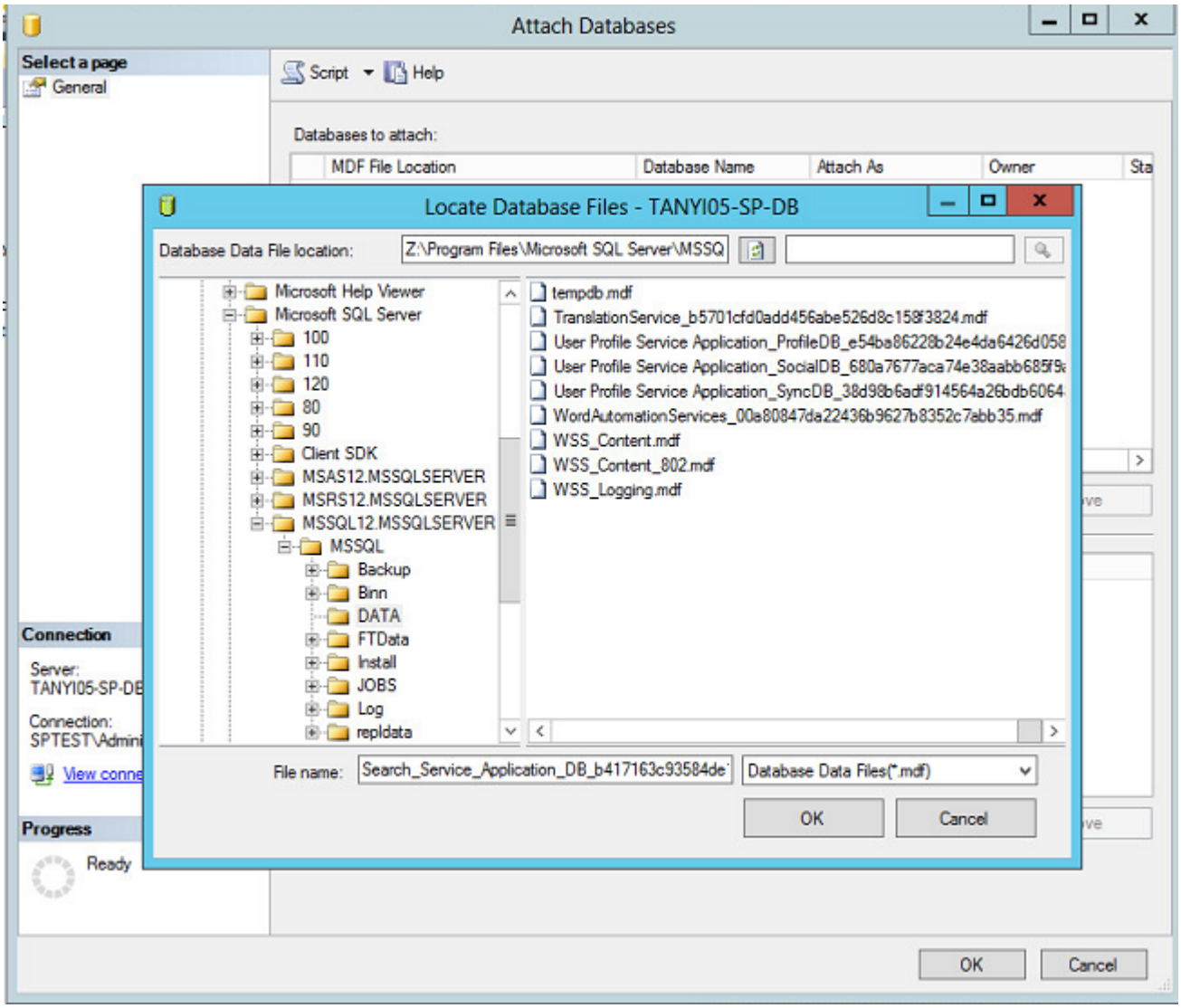
Das neue Volume wird auf der Benutzeroberfläche unter "Geladene Volumes" aufgeführt.



5. Öffnen Sie SQL Server Management Studio, um die Sicherungsdatenbank anzufügen.
6. Klicken Sie mit der rechten Maustaste auf den Ordner "Datenbanken", und wählen Sie "Anfügen" aus.



7. Klicken Sie auf "Hinzufügen", um die Datenbankdatei auszuwählen, die angefügt werden soll.



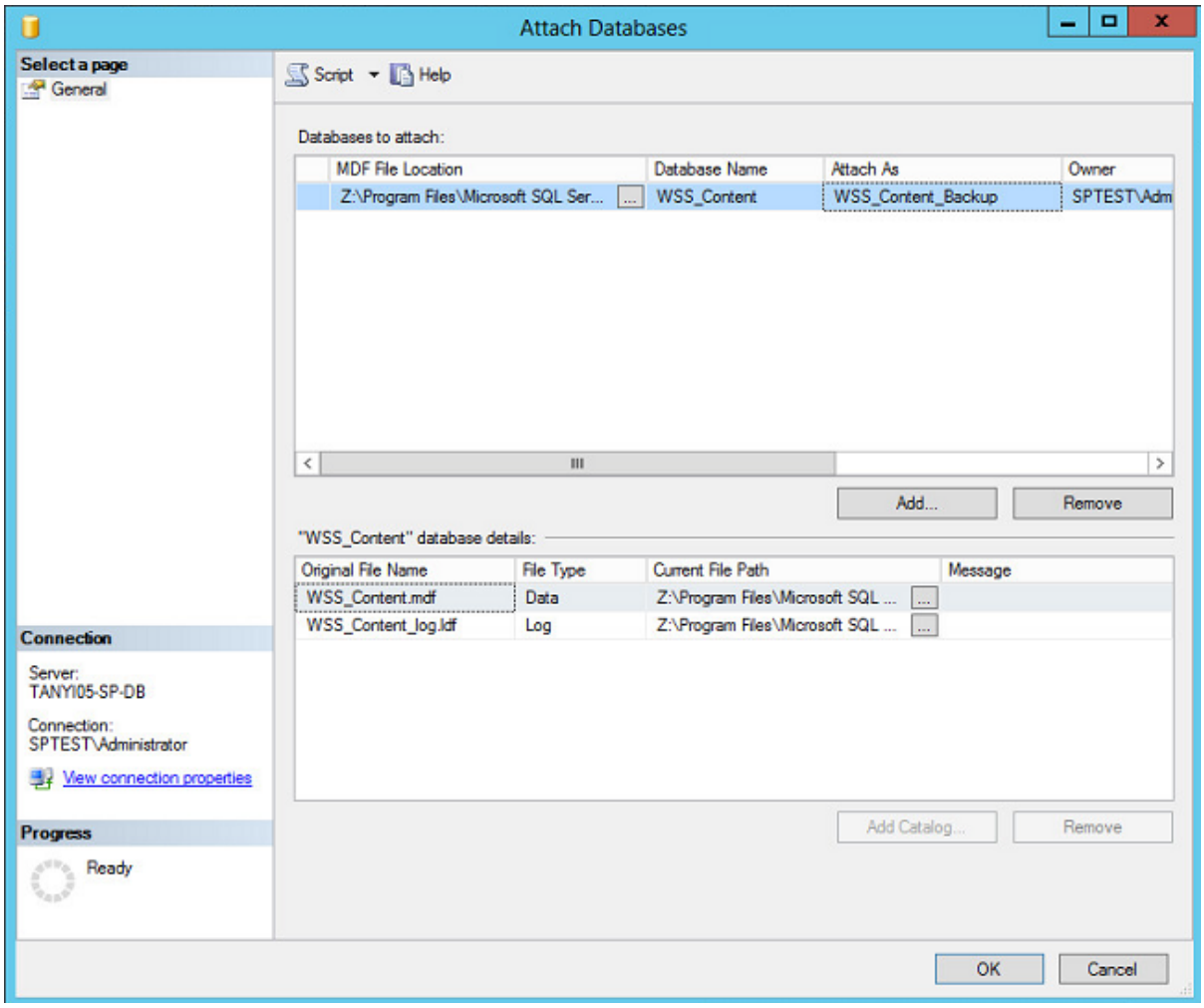
8. Wenn das geladene Volume Z ist, wählen Sie als Speicherort der Datendatei der Datenbank "Z:\Programme\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA".

9. Wählen Sie die Datei mit dem Namen "WSS_Content.mdf", und klicken Sie auf "OK".

   Hinweis: "WSS_Content.mdf" ist der Standard-Datendateiname der Datenbank für die SharePoint-Webanwendung. Wenn Sie eine andere Datenbank wiederherstellen möchten, die von einer neuen Webanwendung erstellt wird, müssen Sie den entsprechenden Datendateinamen der Datenbank verwenden.

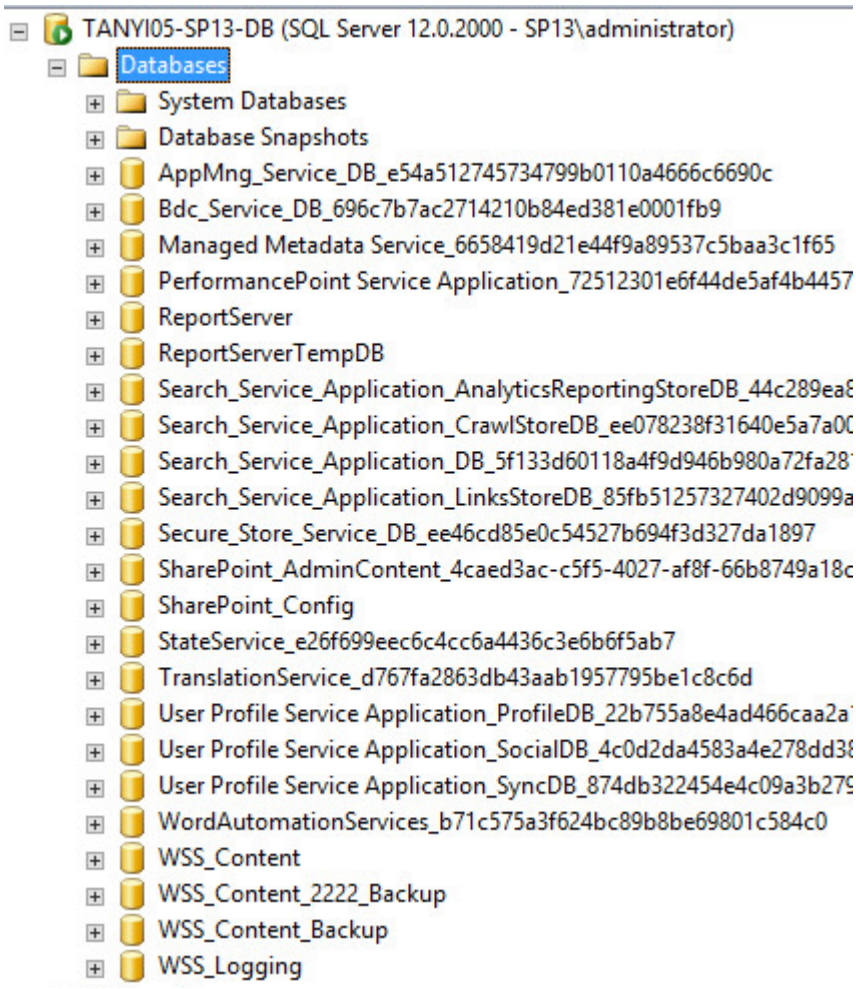
10. Klicken Sie auf die Spalte "Anfügen als", um den Datenbanknamen einzugeben, (z. B. "WSS_Content_Backup"), und klicken Sie auf "OK".

    Hinweis: Bevor Sie eine Inhaltsdatenbank wiederherstellen, stellen Sie sicher, dass der Name der Datenbank nicht in einer anderen Webanwendung vorhanden ist.

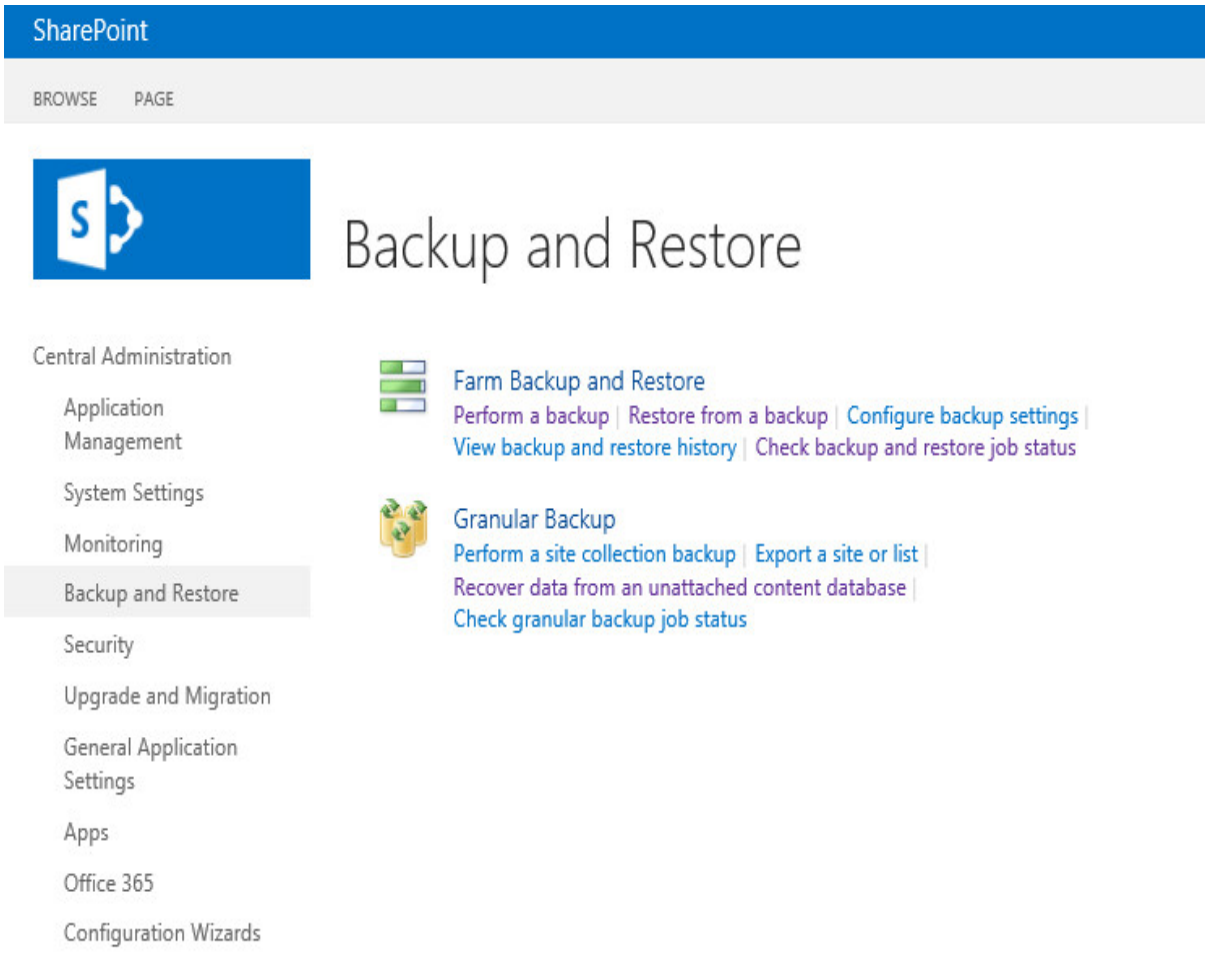


Die neue Datenbank wird im Ordner "Datenbanken" angefügt.

Hinweis: Die neue Datenbank ist keiner Webanwendung zugeordnet.

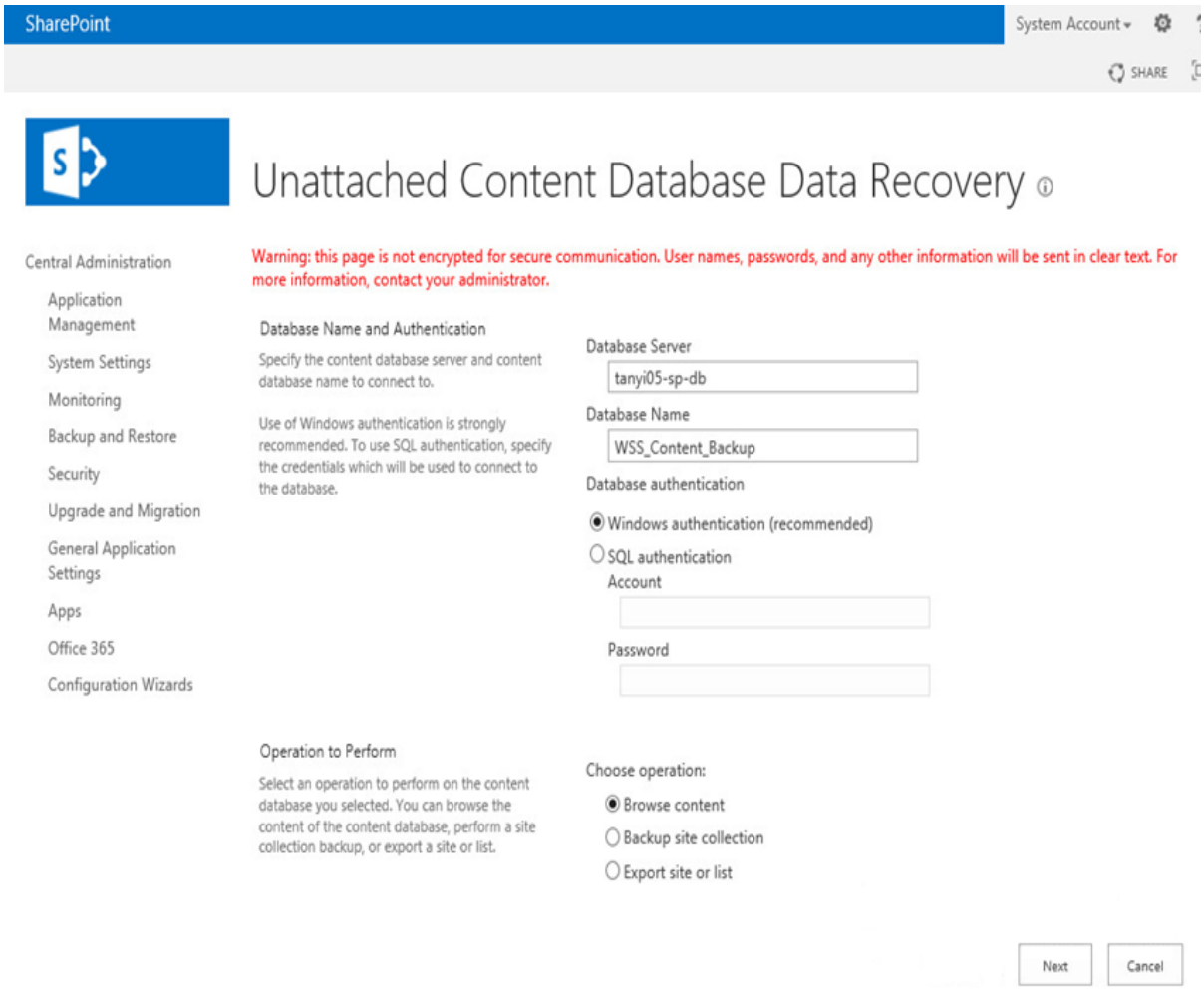


11. Melden Sie sich auf dem Rechner an, der der Web-Front-End-Server in der SharePoint Server-Farm ist.
12. Öffnen Sie die zentrale Verwaltung, und klicken Sie auf "Sichern und Wiederherstellen".



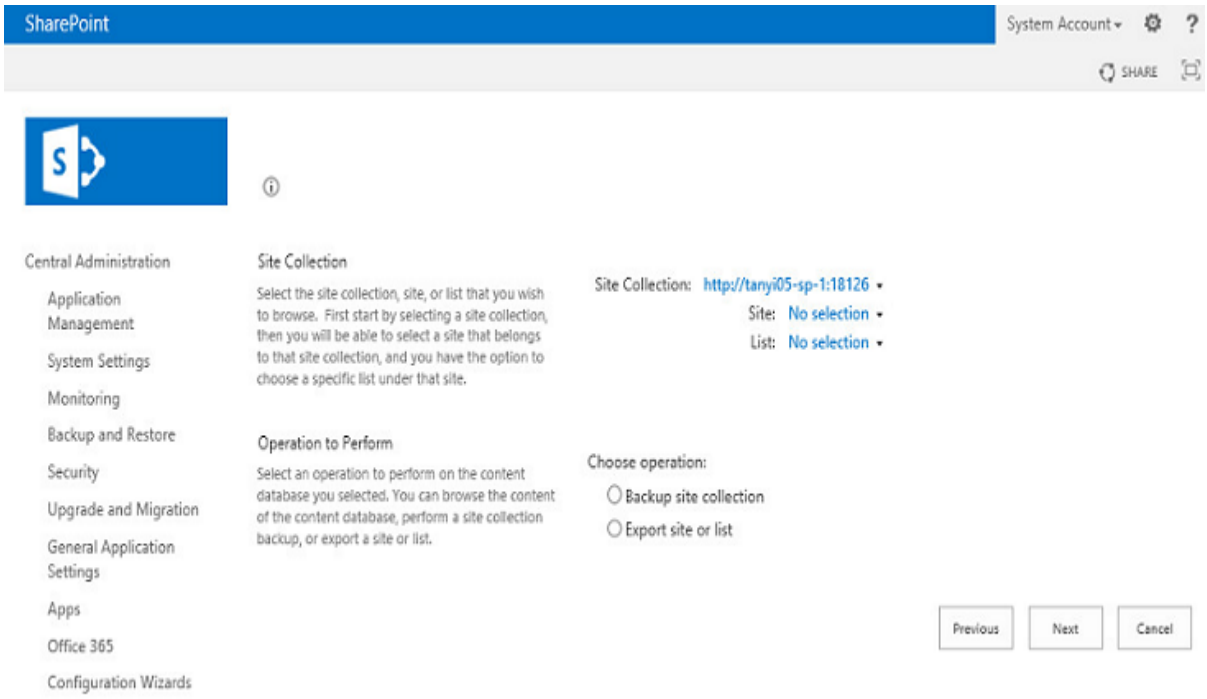
13. Klicken Sie auf den Link "Recover Data from an Unattached Content Database", geben Sie den SQL Server-Namen und den Datenbanknamen für die nicht angefügte Datenbank an, und verwenden Sie die Windows-Authentifizierung.
14. Wählen Sie die Option zum Durchsuchen von Inhalten, und klicken Sie auf **Weiter**.

    Hinweis: Der SQL Server-Name ist der Name des von der SharePoint Server-Farm verwendeten Datenbankservers; Datenbankname ist der Name der neu angefügten Datenbank.



15. Wählen Sie, ob Sie die Websitesammlung sichern oder die ausgewählte Site und Liste exportieren möchten.

    Hinweis: Wenn die Datenbank eine nicht angefügte Inhaltsdatenbank ist, enthält die Websitesammlungs-URL standardmäßig die Webanwendungs-Portnummer für die zentrale Verwaltung.



Sie haben eine Wiederherstellung durch Laden einer Datenbank mithilfe eines Wiederherstellungspunkts durchgeführt.

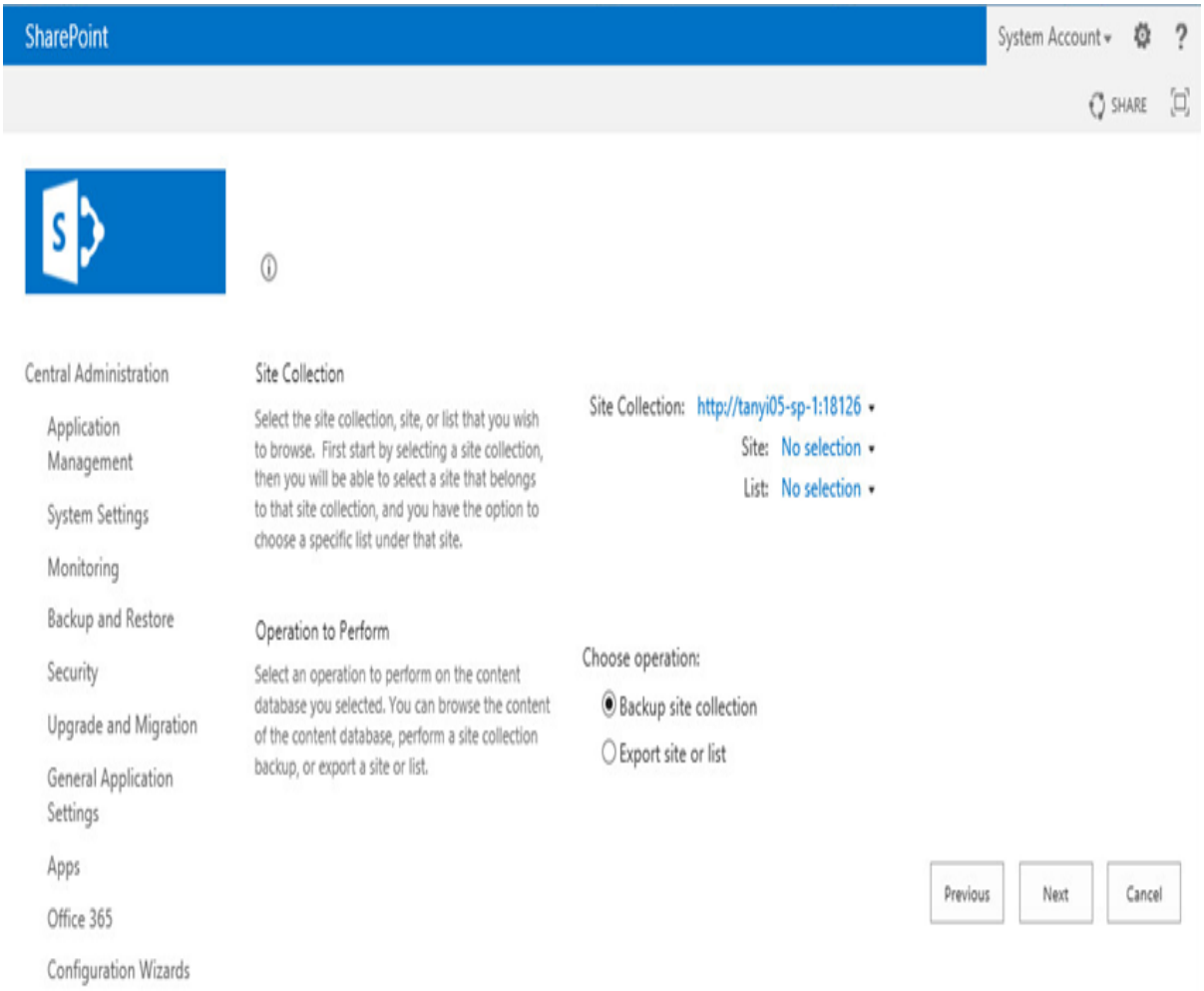
Wiederherstellen einer Websitesammlung

Gehen Sie wie folgt vor:

1. Stellen Sie die Websitesammlungsinhalte aus einer nicht angefügten Inhaltsdatenbank wieder her.

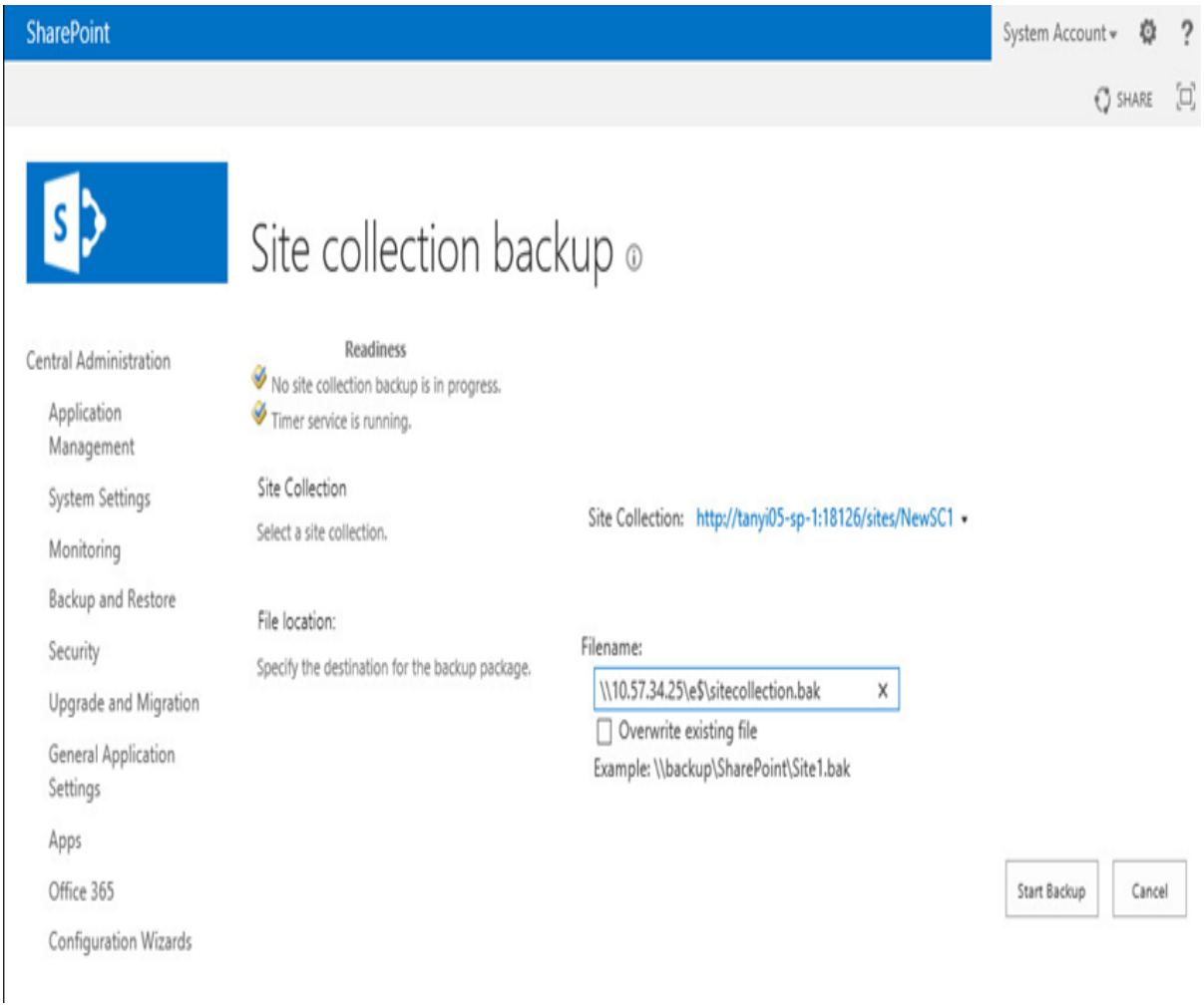
   Über die zentrale Verwaltung

   a. Wählen Sie für Websitesammlung die Option "Sicherung", und klicken Sie auf "Weiter".



   b. Wählen Sie die Websitesammlung, und geben Sie den Dateispeicherort für das Sicherungspaket an.

   c. Wählen Sie "Vorhandene Datei überschreiben" aus.



d. Klicken Sie zum Starten der Sicherung auf die Schaltfläche "Sicherung starten".

   Die Websitesammlung wird in einer Datei gesichert.

Mithilfe von PowerShell-Befehlen

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

   ConnectAsUnattachedDatabase: Gibt an, dass nur nicht angefügte Datenbanken in der Farm zurückgegeben werden.

   DatabaseName: Gibt den Namen der Inhaltsdatenbank an.

   DatabaseServer: Gibt den Namen des Host-Servers für die Inhaltsdatenbank an, die unter dem Parameter "DatabaseName" angegeben ist.

   Weitere Informationen finden Sie im Microsoft-Artikel.

b. Backup-SPSite -Identity xxxx -Path xxxx

Identity: Gibt die URL oder die GUID der Websitesammlung an, die gesichert werden soll.

Path: Gibt den vollständigen Pfad der Sicherungsdatei (z. B. C:\-backup\sitecollection.bak) an.

Weitere Informationen finden Sie im Microsoft-Artikel.

2. Klicken Sie zum Öffnen der Konsole auf die SharePoint-Verwaltungsshell.
3. Verwenden Sie PowerShell-Befehle, um die Websitesammlung wiederherzustellen.

```
Restore-SPSite -Identity xxxx -Path xxxx
```

Identity: Gibt die URL an, unter der die Websitesammlung wiederhergestellt wird. (z. B. http://www.contoso.com)

Path: Gibt einen gültigen Pfad des Speicherorts für die Sicherung an.(Beispiel: C:\-backup\sitecollection.bak)

Weitere Informationen finden Sie im Microsoft-Artikel.

Hinweis: Die Wiederherstellung einer Websitesammlung an dem ursprünglichen Speicherort führt zu einem Fehler. Sie können die folgenden Schritte ausführen:

a. New-SPContentDatabase -Name xxxx -DatabaseServer xxxx -WebApplication xxxx

Name: Gibt die neue Inhaltsdatenbank an, die in der Farm erstellt werden soll.

DatabaseServer: Gibt den Namen des Host-Servers für die Inhaltsdatenbank an, die unter dem Parameter "Name" angegeben ist.

WebApplication: Fügt die Inhaltsdatenbank an die angegebene SharePoint-Webanwendung an.

b. Restore-SPSite -Identity xxxx -Path xxxx -GradualDelete -DatabaseServer xxxx -DatabaseName xxxx

Identity: Gibt die URL an, unter der die Websitesammlung wiederhergestellt wird. (z. B. http://www.contoso.com)

Path: Gibt einen gültigen Pfad des Speicherorts für die Sicherung an.(Beispiel: C:\backup\sitecollection.bak)

GradualDelete: Gibt an, dass die mit dem Parameter "Force" überschriebene Websitesammlung mit einem Zeitgeberjob schrittweise gelöscht wird, statt direkt vollständig gelöscht zu werden. Auf diese Weise werden die Auswirkungen auf die SharePoint 2010-Produkte und die SQL Server-Leistung reduziert.

DatabaseName: Gibt die SQL Server-Inhaltsdatenbank an, in der die Websitesammlungsdaten gespeichert werden.

DatabaseServer: Gibt den Namen des SQL Servers an, auf dem die mit dem Parameter "DatabaseName" angegebene Inhaltsdatenbank vorhanden ist.

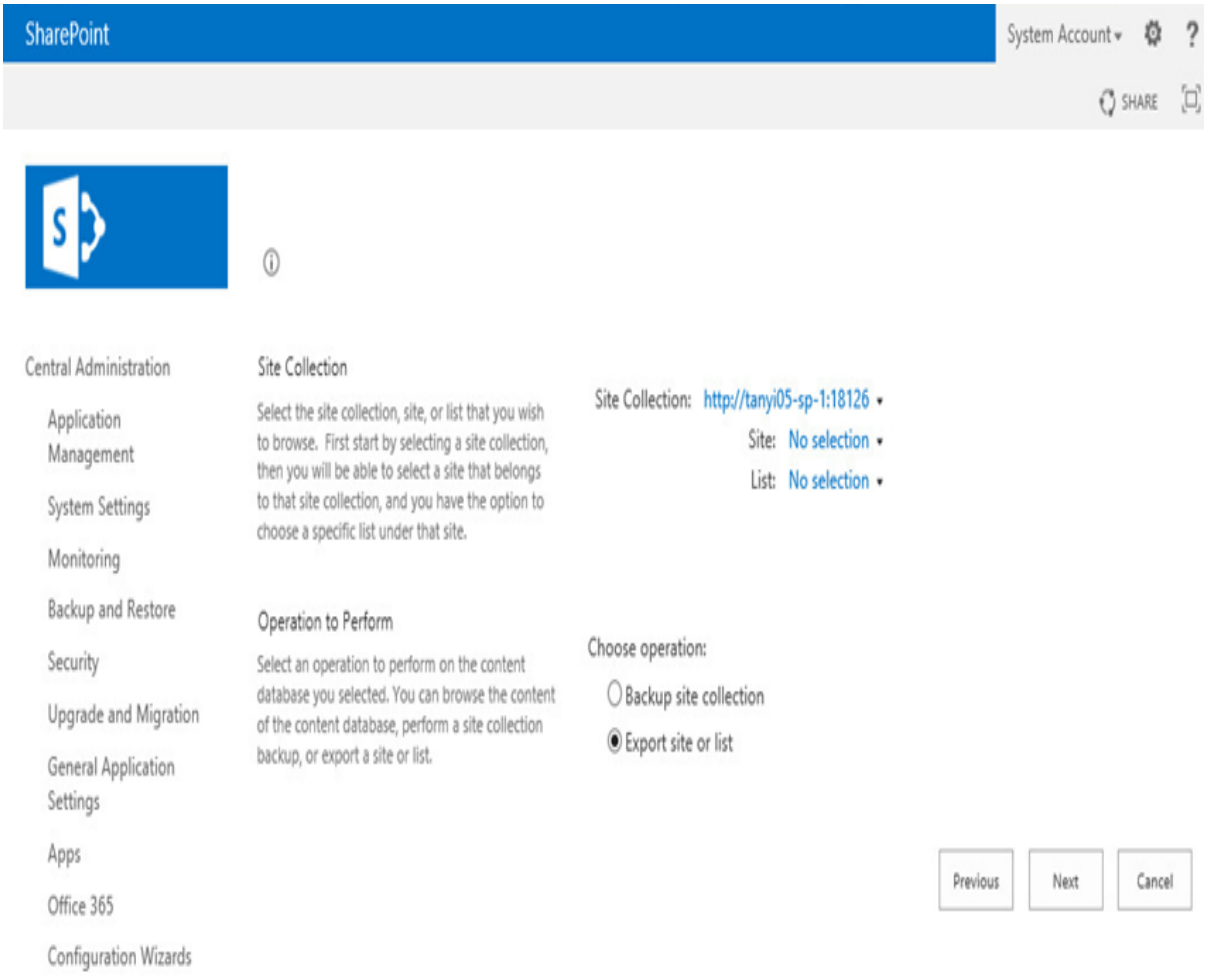
Wiederherstellen einer Site

Gehen Sie wie folgt vor:

1. Stellen Sie Siteinhalte aus einer nicht angefügten Inhaltsdatenbank wieder her.

   Über die zentrale Verwaltung

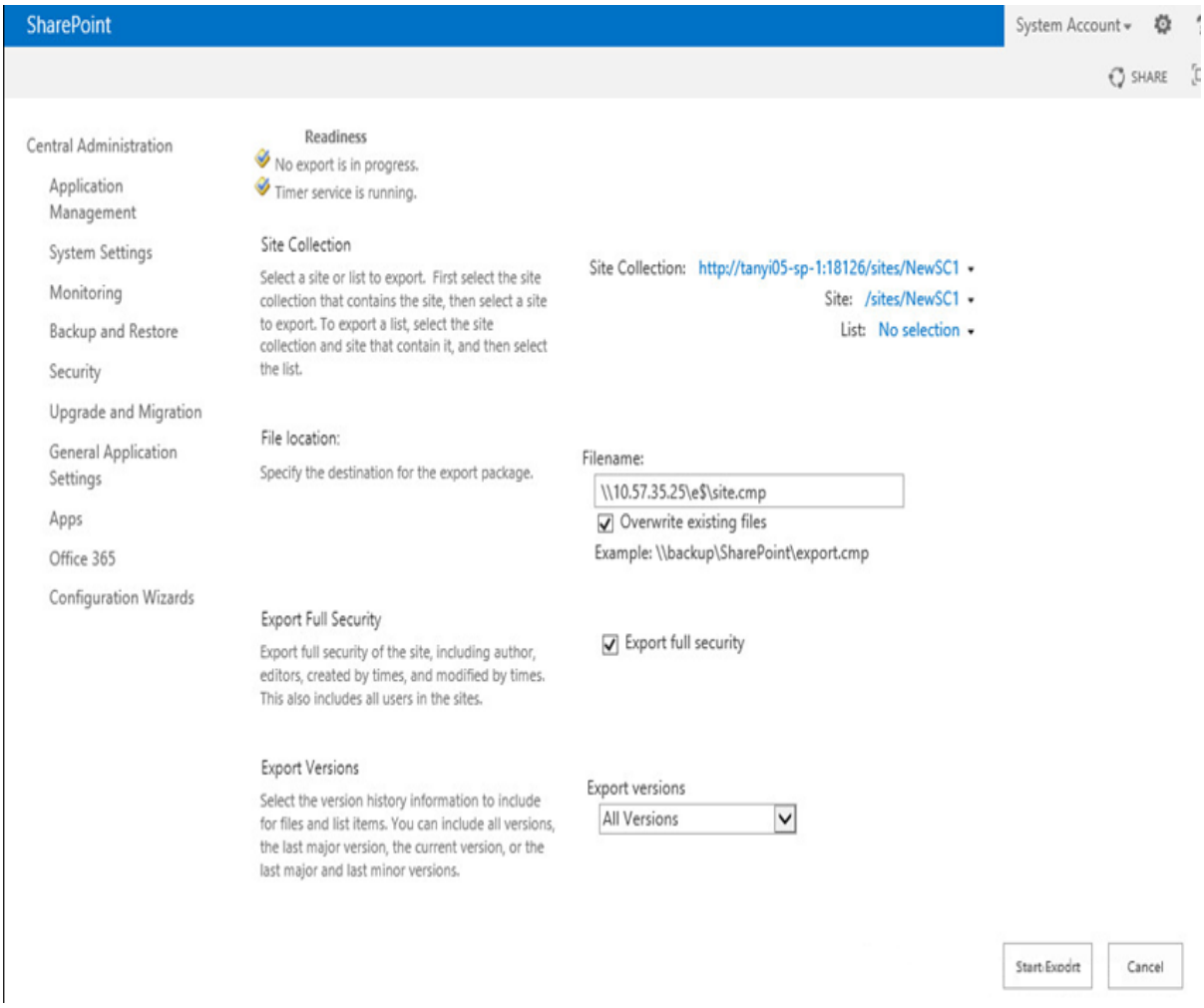
   a. Wählen Sie die Option "Website oder Liste exportieren", und klicken Sie auf "Weiter".



   b. Wählen Sie die Site, und geben Sie den Dateispeicherort für das Exportpaket an.

      Beispiel: Der Name der Site, die wiederhergestellt werden soll, ist "TestSite1" und die URL ist "/TestSite1/".

   c. Wählen Sie die Optionen für Sicherheit und Versionen (standardmäßig sind alle Versionen ausgewählt).



d. Klicken Sie auf die Schaltfläche "Export starten", um den Export zu starten. Die Site wird dann in eine Datei exportiert.

Mithilfe von PowerShell-Befehlen

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

ConnectAsUnattachedDatabase: Gibt an, dass nur nicht angefügte Datenbanken in der Farm zurückgegeben werden.

DatabaseName: Gibt den Namen der Inhaltsdatenbank an.

DatabaseServer: Gibt den Namen des Host-Servers für die Inhaltsdatenbank an, die unter dem Parameter "DatabaseName" angegeben ist.

Weitere Einzelheiten finden Sie im Microsoft-Artikel.

b. Festlegen des zu exportierenden Objekts

$ExportObject = New-Object Microsoft.SharePoint.Deployment.SPExportObject

$ExportObject.Type = [Microsoft.SharePoint.Deployment.SPDeploymentObjectType]::Web

$ExportObject.Url = $SiteUrl

$SiteUrl: Gibt die URL an, unter der die Site gesichert wird.

c. Konfigurieren der Exporteinstellungen

$ExportSettings = New-Object Microsoft.SharePoint.Deployment.SPExportSettings

$ExportSettings.UnattachedContentDatabase = $database

$ExportSettings.SiteUrl = $CAUrl

$CAUrl: Gibt die URL der zentralen Verwaltungssite an.

$ExportSettings.FileLocation = $ExportPath

$ExportSettings.LogFilePath = $ExportPath

$ExportPath: Gibt den Pfad zum Speichern der Sicherungsdatei an (z. B. C:\backup).

$ExportSettings.BaseFileName = $ExportFile

$ExportFile: Gibt den Dateinamen der Sicherungsdatei an (z. B. site.cmp).

$ExportSettings.IncludeVersions = [Microsoft.SharePoint.Deployment.SPIncludeVersions]::All

$ExportSettings.ExportMethod = [Microsoft.SharePoint.Deployment.SPExportMethodType]::ExportAll

$ExportSettings.IncludeVersions = [Microsoft.SharePoint.Deployment.SPIncludeVersions]::All

$ExportSettings.ExportObjects.Add($ExportObject)

$ExportSettings.Validate()

$ExportJob = New-Object Microsoft.SharePoint.Deployment.SPExport($ExportSettings)

Sichern der Site in einer Datei

$ExportJob.Run()

Weitere Einzelheiten finden Sie im Microsoft-Artikel.

2. Klicken Sie zum Öffnen der Konsole auf die SharePoint-Verwaltungsshell.
3. Verwenden Sie PowerShell-Befehle, um die Site am ursprünglichen Ort oder an einem neuen Ort wiederherzustellen.

```
Import-SPWeb -Identity xxxx -Path xxxx -Inclu-
deUserSecurity:$true -UpdateVersions:xxxx
```

Identity: Gibt die URL oder die Web-GUID an, in die importiert werden soll. Beispiel: http://www.contoso.com.

Path: Gibt den Namen der Importdatei an. Beispiel: C:\backup\site.cmp'

IncludeUserSecurity: Erhält die Benutzersicherheitseinstellungen außer für SP-Listen mit unterbrochener Vererbung und festgelegten Berechtigungen auf Elementebene.

UpdateVersions: Gibt das Verhalten für Situationen an, wenn die in eine Site zu importierende Dateiversion bereits in der Site vorhanden ist. Sie können eine der folgenden Optionen auswählen:

Add: Fügt die Datei als neue Version hinzu.

Overwrite: Überschreibt die aktuelle Datei sowie alle ihre Versionen (löschen, dann einfügen).

Ignore: Ignoriert die Datei, wenn diese auf dem Ziel existiert. Die neue Datei wird nicht hinzugefügt.

Der Standardwert ist "Add".

Weitere Einzelheiten finden Sie im Microsoft-Artikel.

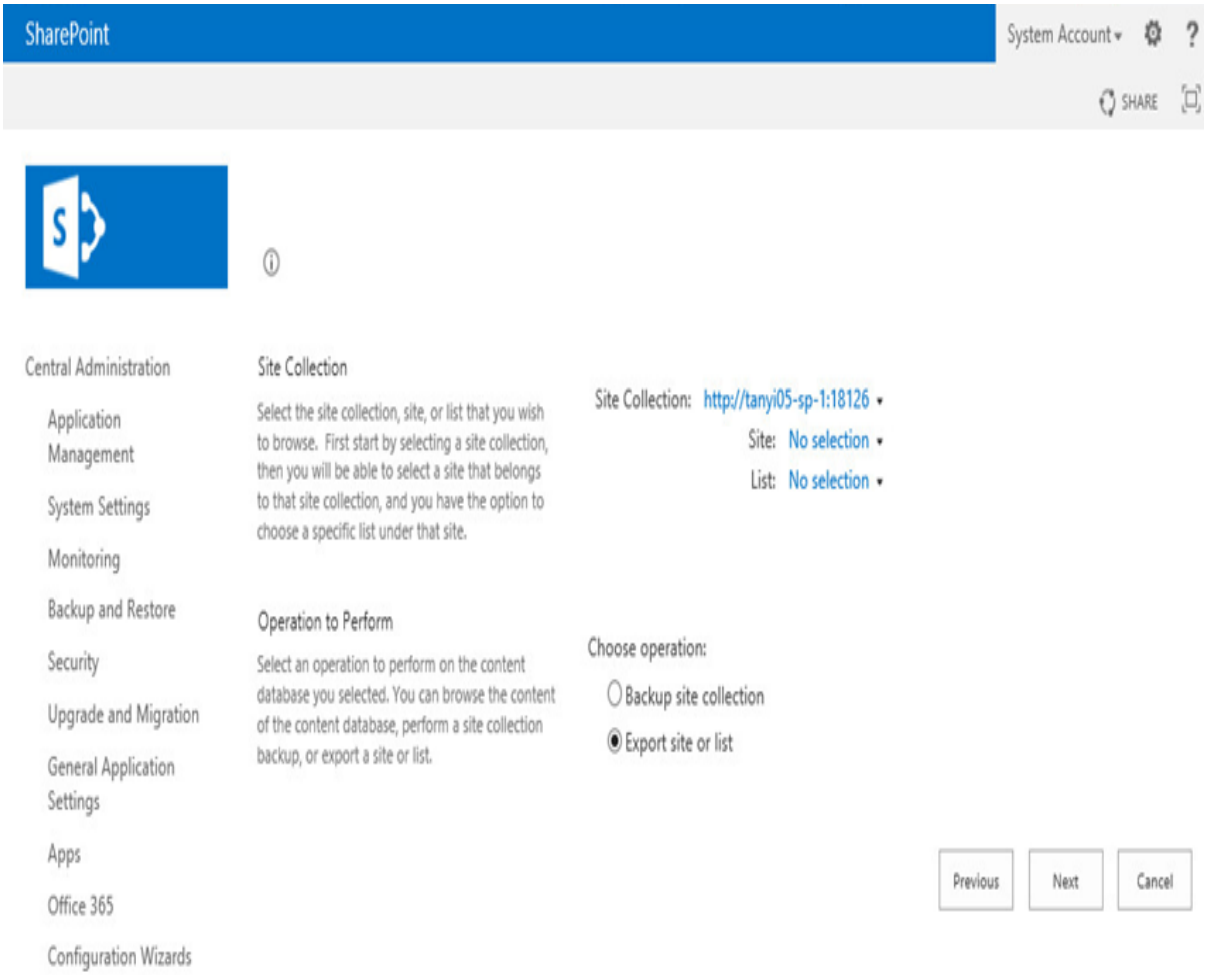
Wiederherstellen einer Liste oder Bibliothek

Gehen Sie wie folgt vor:

1. Stellen Sie die Listen- oder Bibliotheksinhalte aus einer nicht angefügten Inhaltsdatenbank wieder her.

   Über die zentrale Verwaltung

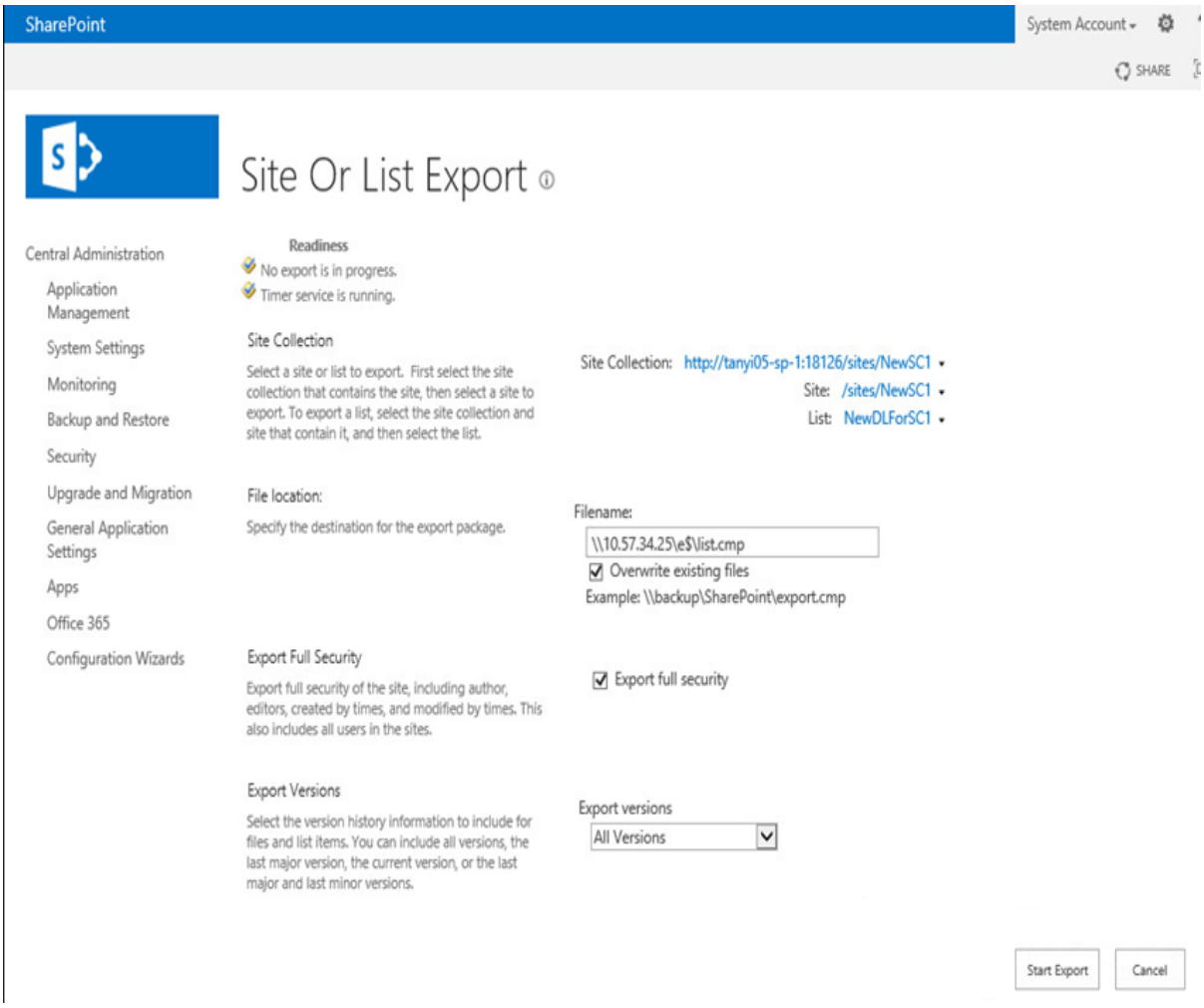
   a. Wählen Sie die Option "Website oder Liste exportieren", und klicken Sie auf **Weiter**.



   b. Wählen Sie die Site und die Liste, und geben Sie den Dateispeicherort für das Exportpaket an.

      Beispiel: Der Name der Liste/Bibliothek, die wiederhergestellt werden soll, ist "NewList1" und die URL ist "/TestSite1/NewList1".

   c. Wählen Sie die Optionen für Sicherheit und Versionen (standardmäßig sind alle Versionen ausgewählt).



d. Klicken Sie auf **Export starten**, um den Export zu starten.

   Die Liste oder Bibliothek wird in eine Datei exportiert.

Mithilfe von PowerShell-Befehlen

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

   ConnectAsUnattachedDatabase: Gibt an, dass nur nicht angefügte Datenbanken in der Farm zurückgegeben werden.

   DatabaseName: Gibt den Namen der Inhaltsdatenbank an.

   DatabaseServer: Gibt den Namen des Host-Servers für die Inhaltsdatenbank an, die unter dem Parameter "DatabaseName" angegeben ist.

   Weitere Einzelheiten finden Sie im Microsoft-Artikel.

b. Festlegen des zu exportierenden Objekts

   $ExportObject = New-Object Microsoft.SharePoint.Deployment.SPExportObject

$ExportObject.Type = [Microsoft.SharePoint.Deployment.SPDeploymentObjectType]::List

$ExportObject.Url = $ListUrl

$ListUrl: Gibt die URL an, unter der die Liste oder Bibliothek gesichert wird. Wenn es sich um eine Liste handelt, verwenden Sie den Parameter "/Lists/{ListName}". Wenn es sich um eine Bibliothek handelt, verwenden Sie den Parameter "/{LibraryName}".

c. Konfigurieren der Exporteinstellungen

$ExportSettings = New-Object Microsoft.SharePoint.Deployment.SPExportSettings

$ExportSettings.UnattachedContentDatabase = $database

$ExportSettings.SiteUrl = $CAUrl

$CAUrl: Gibt die URL der zentralen Verwaltungssite an.

$ExportSettings.FileLocation = $ExportPath

$ExportSettings.LogFilePath = $ExportPath

$ExportPath: Gibt den Pfad zum Speichern der Sicherungsdatei an (z. B. C:\backup).

$ExportSettings.BaseFileName = $ExportFile

$ExportFile: Gibt den Dateinamen der Sicherungsdatei an (z. B. site.cmp).

$ExportSettings.IncludeVersions = [Microsoft.SharePoint.Deployment.SPIncludeVersions]::All

$ExportSettings.ExportMethod = [Microsoft.SharePoint.Deployment.SPExportMethodType]::ExportAll

$ExportSettings.IncludeVersions = [Microsoft.SharePoint.Deployment.SPIncludeVersions]::All

$ExportSettings.ExportObjects.Add($ExportObject)

$ExportSettings.Validate()

$ExportJob = New-Object Microsoft.SharePoint.Deployment.SPExport($ExportSettings)

d. Sichern der Liste oder Bibliothek in einer Datei

$ExportJob.Run()

Weitere Einzelheiten finden Sie im Microsoft-Artikel.

2. Klicken Sie zum Öffnen der Konsole auf die SharePoint-Verwaltungsshell.

3. Verwenden Sie PowerShell-Befehle, um die Liste oder Bibliothek am ursprünglichen Ort oder an einem neuen Ort wiederherzustellen.

```
Import-SPWeb -Identity xxxx -Path xxxx -Inclu-
deUserSecurity:$true -UpdateVersions:xxxx
```

Identity: Gibt die URL oder die Web-GUID an, in die importiert werden soll. Beispiel: http://www.contoso.com

Path: Gibt den Namen der Importdatei an. Beispiel: C:\backup\list.cmp'

IncludeUserSecurity: Erhält die Benutzersicherheitseinstellungen außer für SP-Listen mit unterbrochener Vererbung und festgelegten Berechtigungen auf Elementebene.

UpdateVersions: Gibt das Verhalten für Situationen an, wenn die in eine Site zu importierende Dateiversion bereits in der Site vorhanden ist. Sie können eine der folgenden Optionen auswählen:

Add: Fügt die Datei als neue Version hinzu.

Overwrite: Überschreibt die aktuelle Datei sowie alle ihre Versionen (löschen, dann einfügen)

Ignore: Ignoriert die Datei, wenn diese auf dem Ziel existiert. Die neue Datei wird nicht hinzugefügt.

Der Standardwert ist "Add".

Weitere Einzelheiten finden Sie im Microsoft-Artikel.

Wiederherstellen einer Datei

Gehen Sie wie folgt vor:

1. Stellen Sie die Liste oder die Bibliothek an einem neuen Speicherort wieder her. Weitere Informationen finden Sie unter Wiederherstellen einer Liste oder Bibliothek.

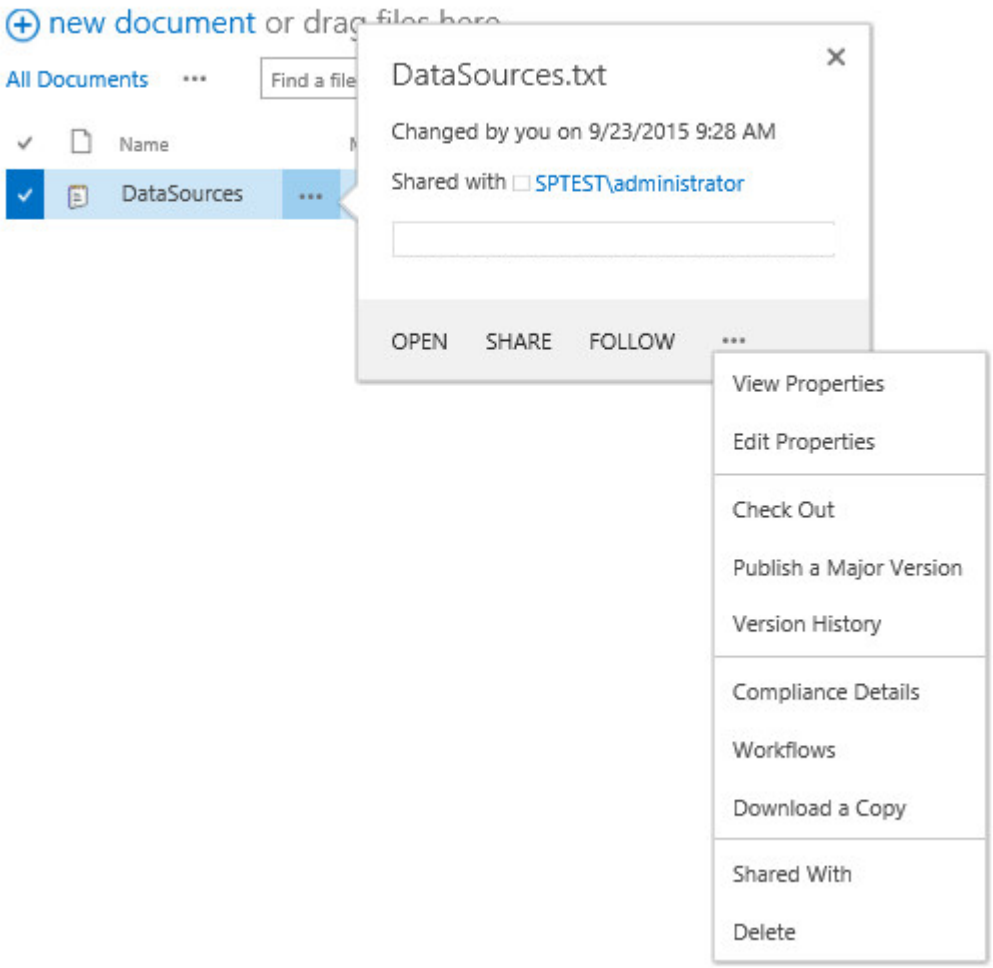
   Beispiel: Die ursprüngliche Liste trägt den Namen NewList1 und die URL lautet http://contoso.com/TestSite1/NewList1.

   - Mithilfe von PowerShell-Befehlen wird die Liste oder Bibliothek am neuen Speicherort wiederhergestellt. Beispiel: http://contoso.com/TestSite2

     Import-SPWeb -Identity http://contoso.com/TestSite2 -Path C:\-backup\list.cmp -IncludeUserSecurity:$true -UpdateVersions:Overwrite

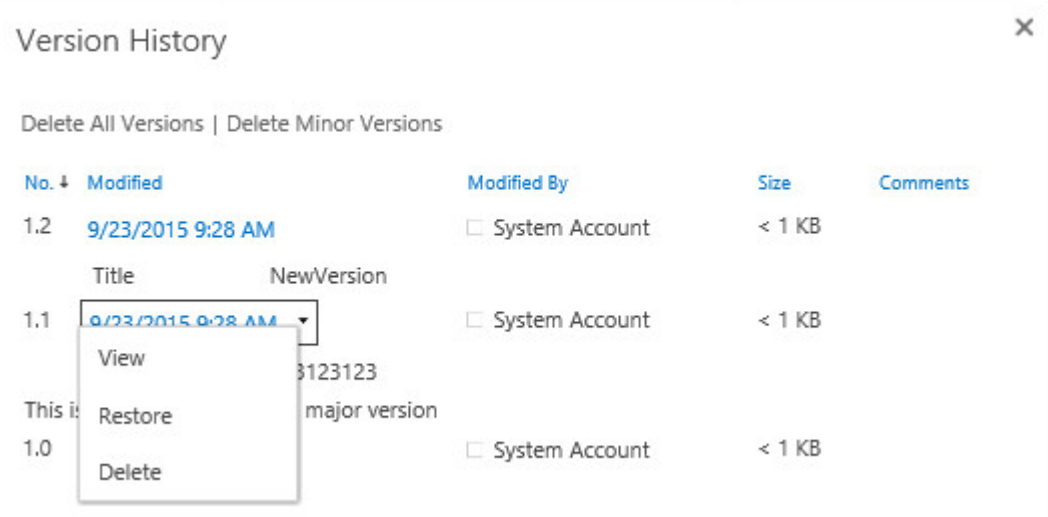
   - Navigieren Sie zur neuen URL der Liste oder Bibliothek. Alle Elemente werden in http://contoso.com/TestSite2/NewList1 wiederhergestellt.

2. Navigieren Sie zur URL des neuen Speicherorts der Liste oder Bibliothek.
3. Überprüfen Sie die Dateiversionsübersicht in der Liste oder Bibliothek.



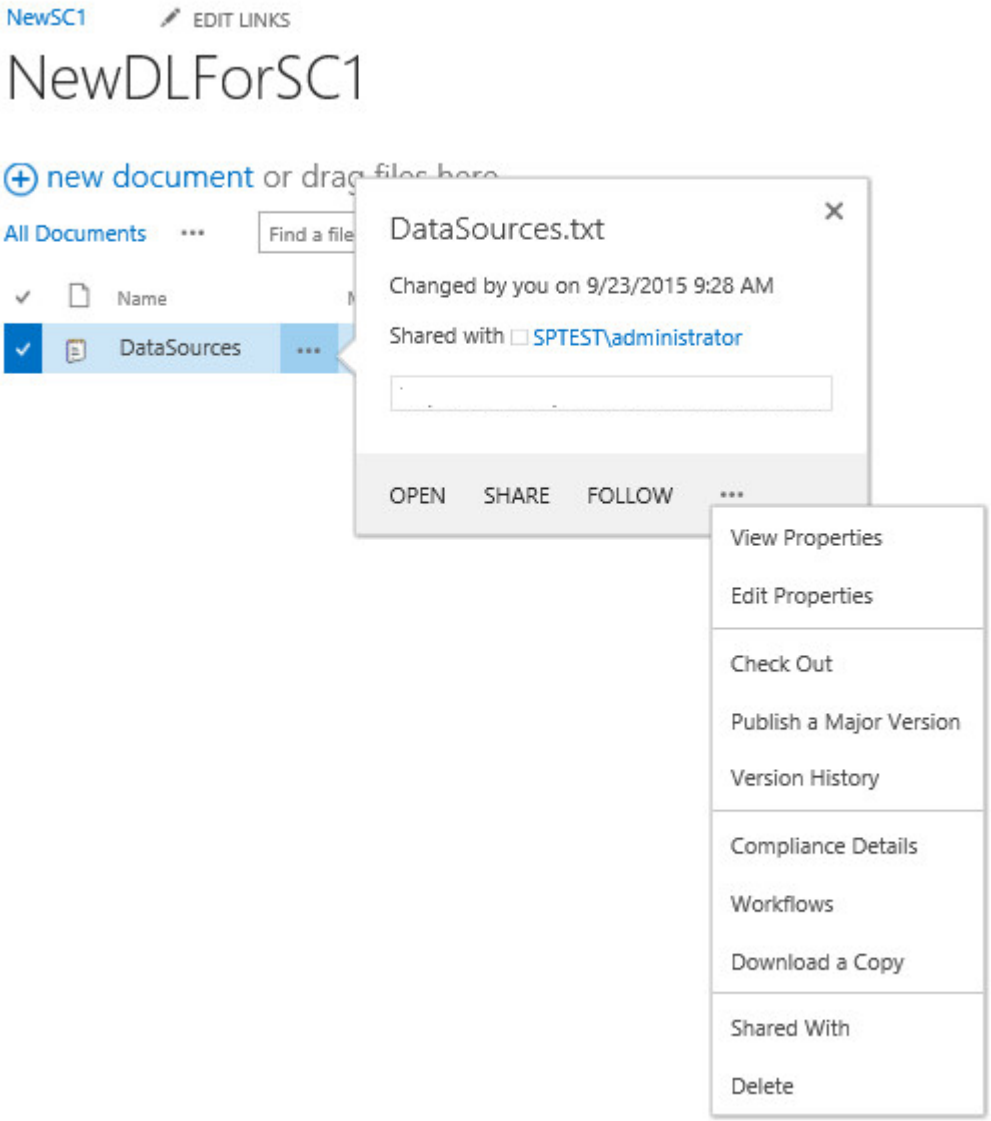
4. Wählen Sie die gewünschte Version für die Datei aus und auf "Wiederherstellen".

   Beispiel: Wiederherstellen der Version 1.1 für die Datei.



   Die Datei wird in der Version 1.1 wiederhergestellt.

5. Klicken Sie auf "Kopie herunterladen", um die Datei in der gewünschten Version 1.1 an einem Speicherort zu speichern.



Die gespeicherte Datei wird am ursprünglichen Speicherort der Liste oder Bibliothek wiederhergestellt.

Erstellen eines isolierten Netzwerks für die SharePoint-Wiederherstellung

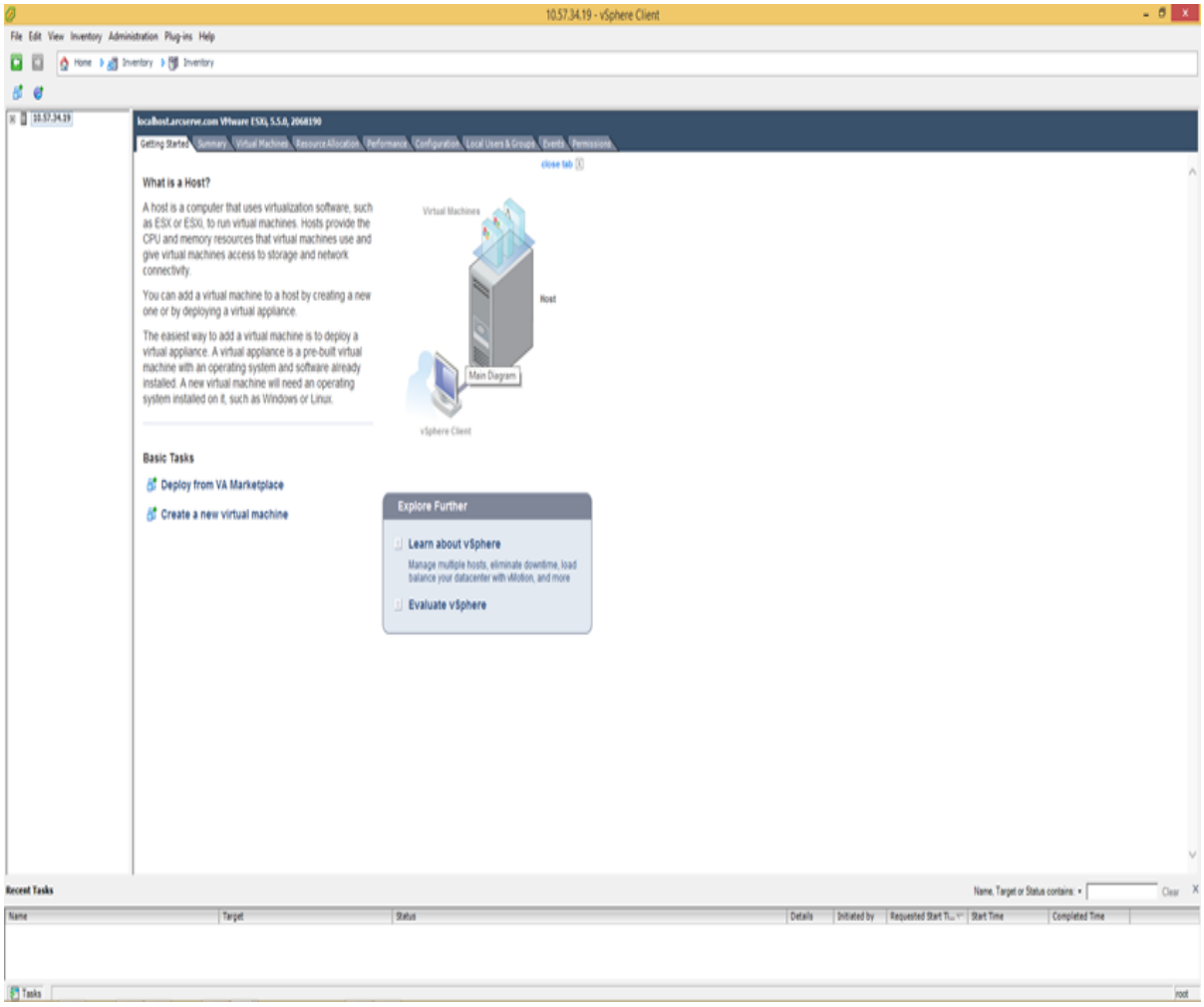
Sie können ein isoliertes Netzwerk erstellen, um SharePoint auf Hyper-V- und VMware-Rechnern wiederherzustellen.

- Erstellen eines isolierten Netzwerks für die SharePoint-Wiederherstellung bei VMware-VMs
- Erstellen eines isolierten Netzwerks für die SharePoint-Wiederherstellung bei Hyper-V-VMs

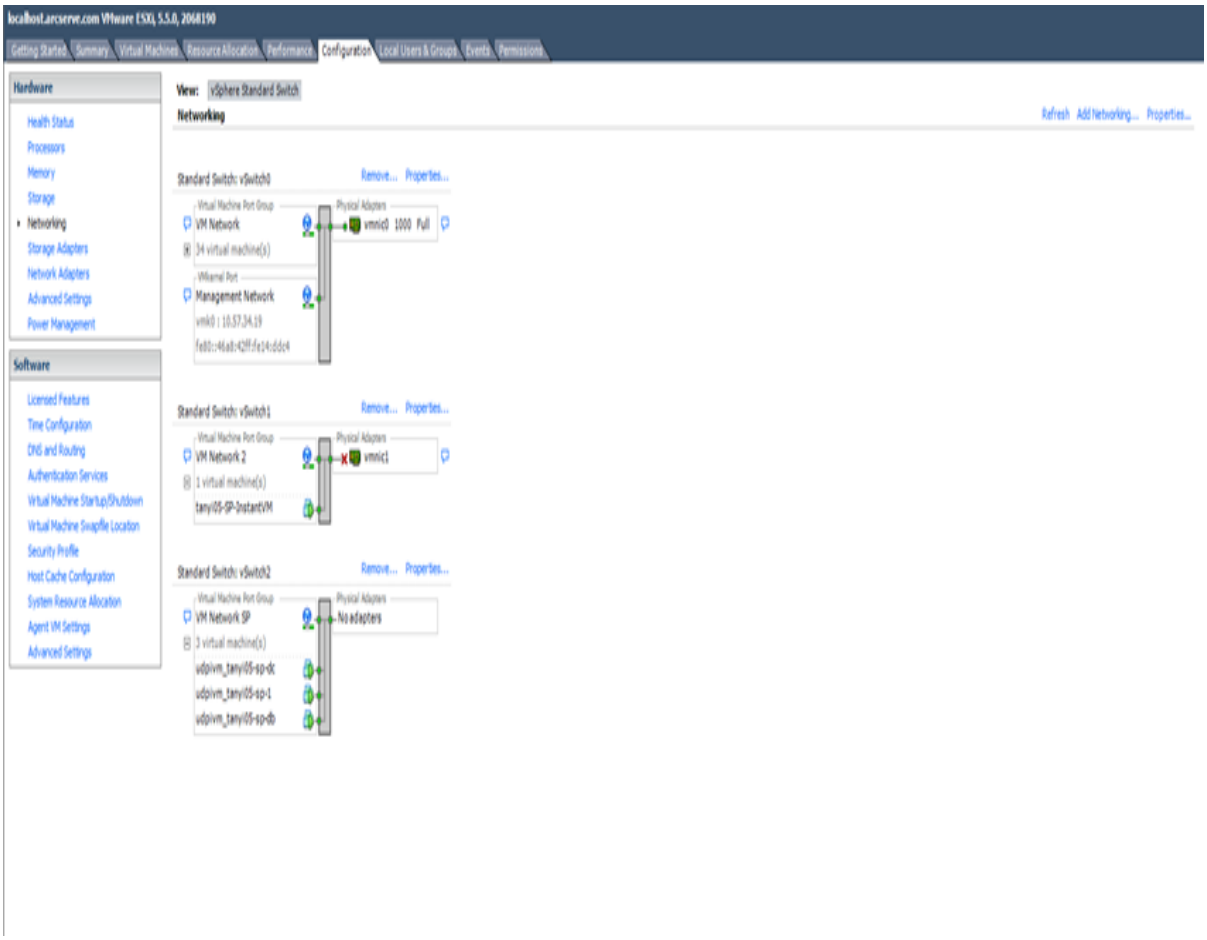
Erstellen eines isolierten Netzwerks für die SharePoint-Wiederherstellung bei VMware-VMs

Gehen Sie wie folgt vor:

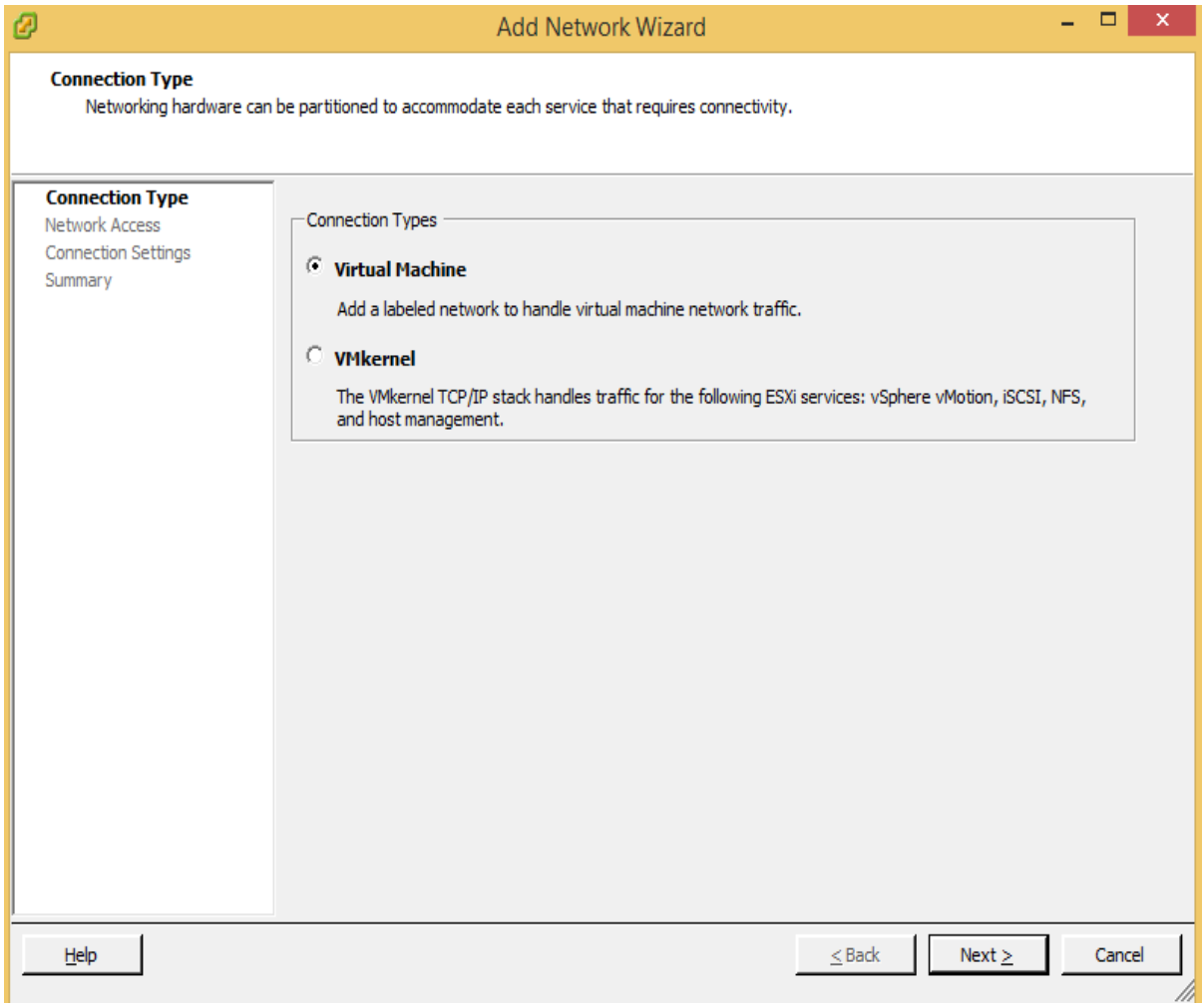
1. Melden Sie sich mithilfe des vSphere-Clients beim VMware ESXi-Server an.



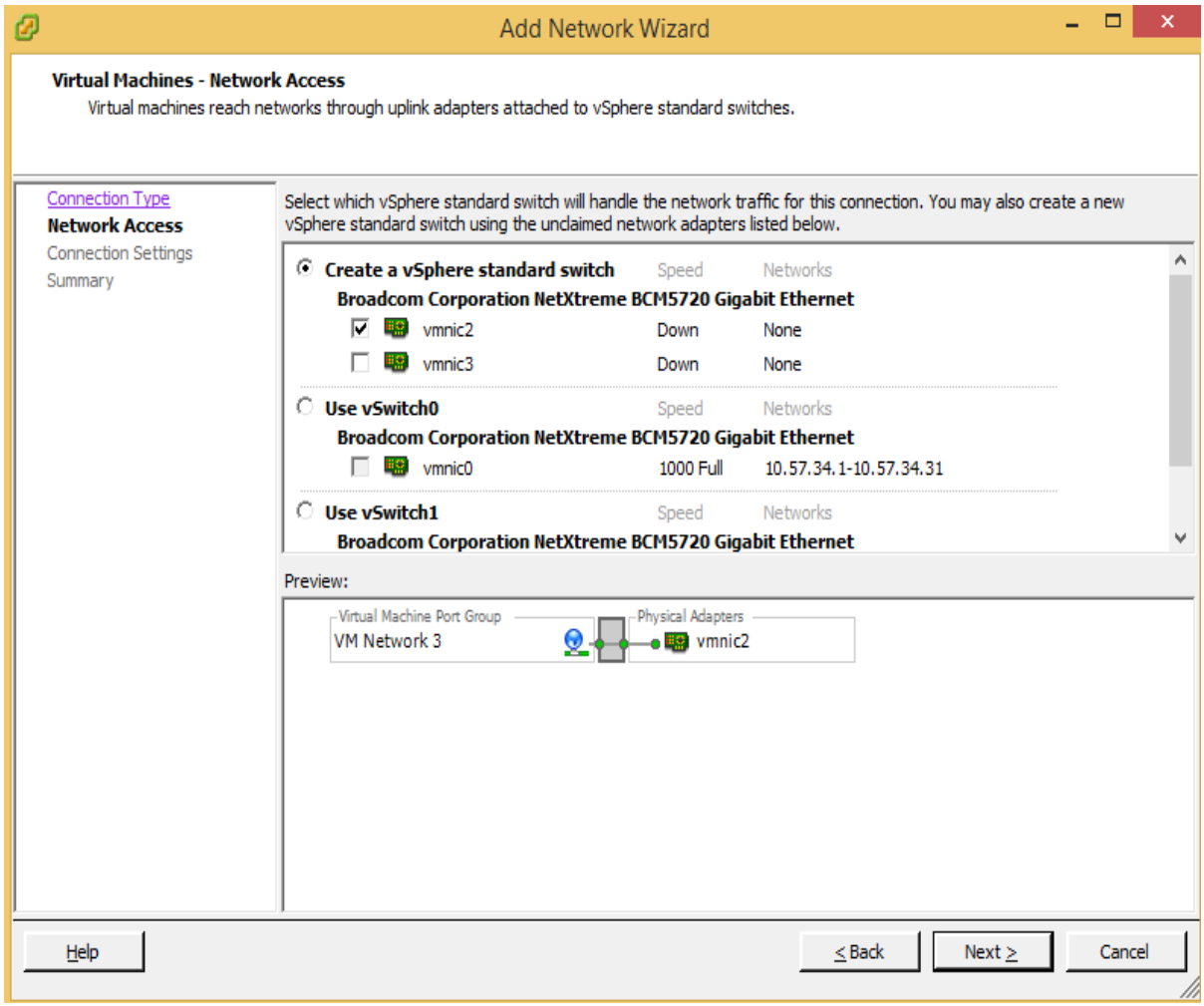
2. Klicken Sie auf die Registerkarte "Konfiguration".
3. Wählen Sie "Netzwerke" im Hardware-Fensterbereich aus, und klicken Sie auf "Netzwerk hinzufügen".



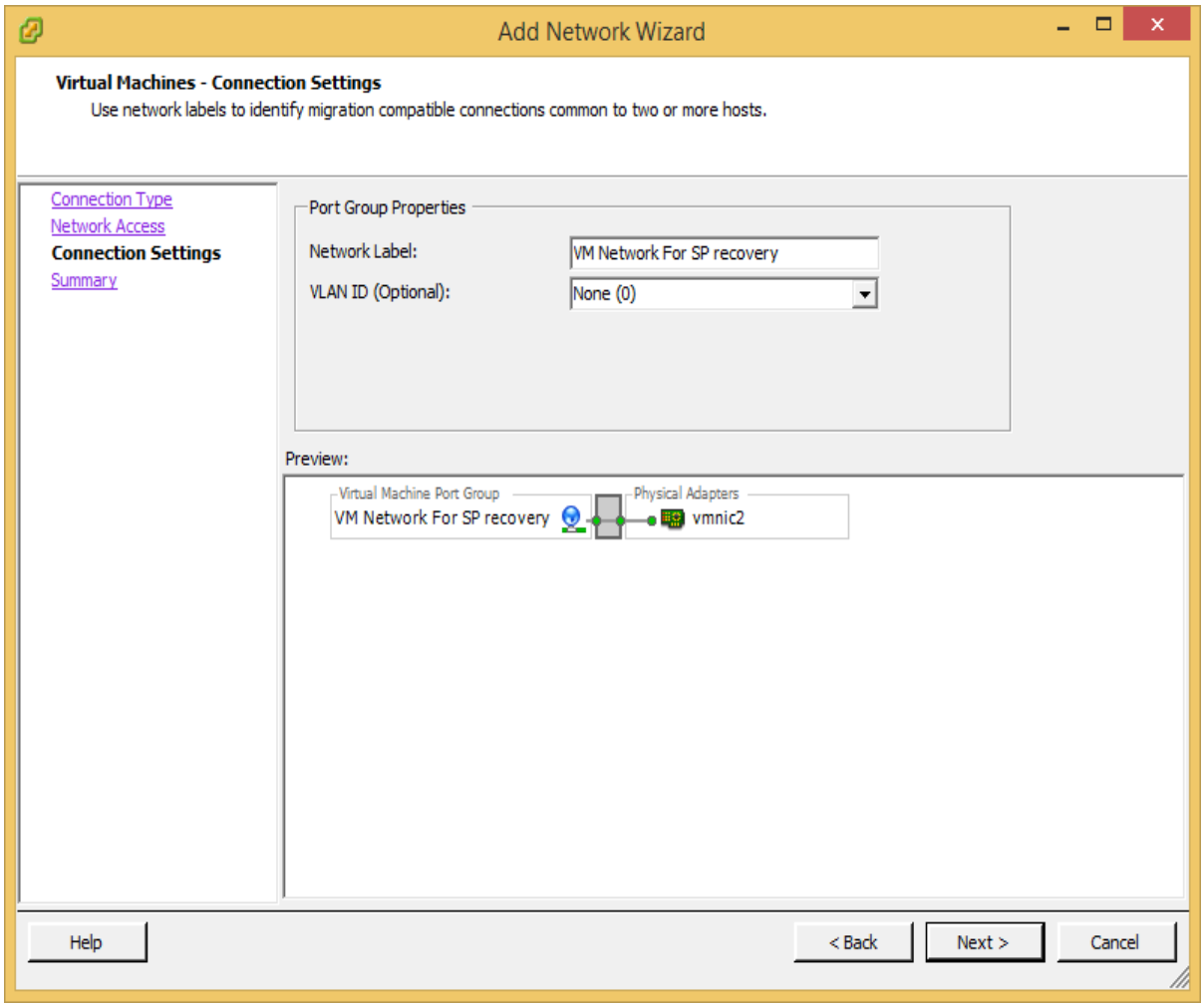
4. Stellen Sie sicher, dass das Optionsfeld "Virtueller Rechner" aktiviert ist, und klicken Sie auf "Weiter".



5. Wählen Sie die physische NIC, die Sie verwenden müssen, um den virtuellen Switch mit anderen physischen Ressourcen im Netzwerk zu verbinden, und klicken Sie auf "Weiter".

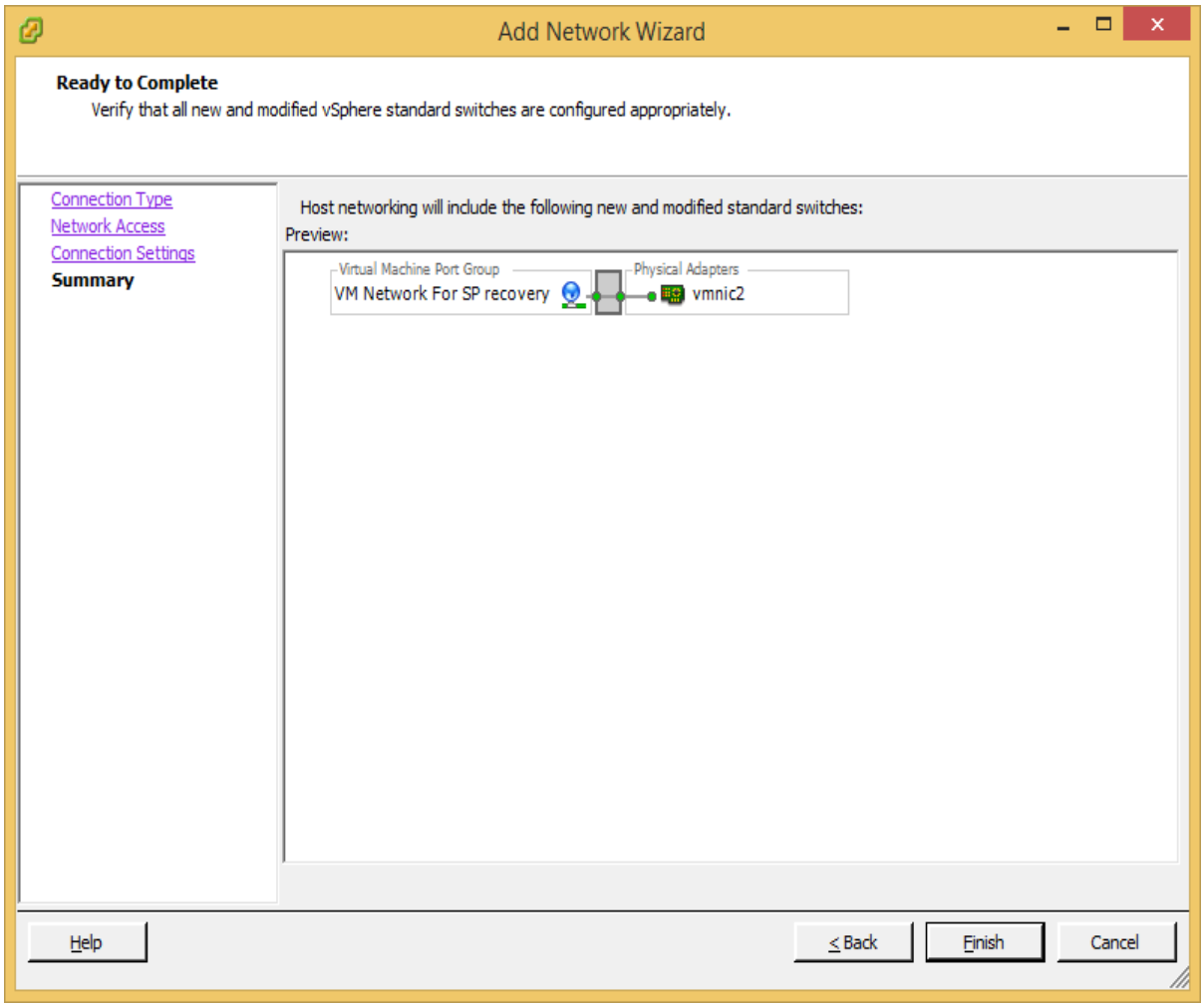


6. Weisen Sie dem virtuellen Switch eine Netzwerkbezeichnung und gegebenenfalls eine VLAN-ID zu, und klicken Sie auf **Weiter**.



7. Stellen Sie sicher, dass Ihre Einstellungen für den virtuellen Switch richtig sind, und klicken Sie auf **Fertig stellen**.

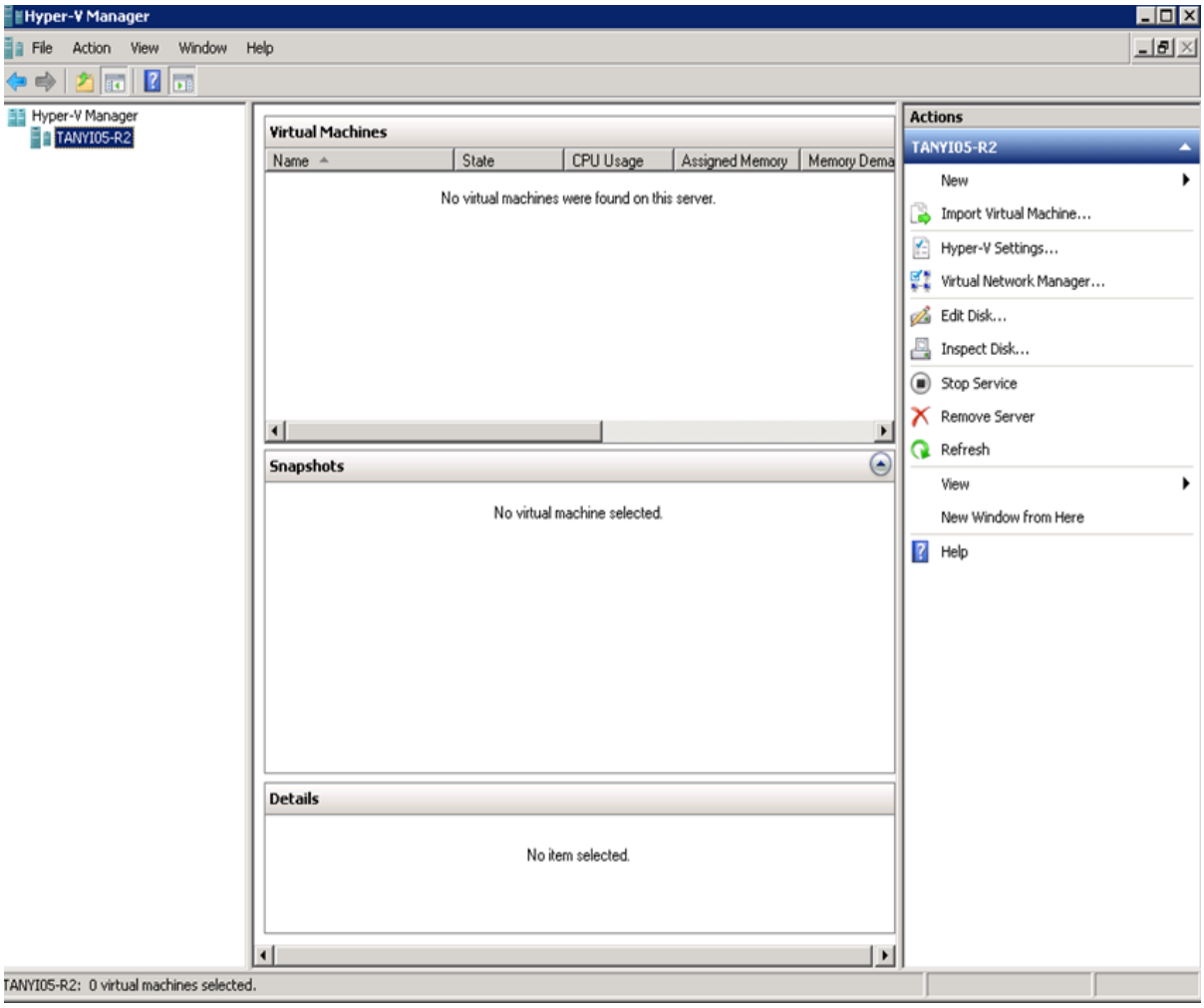
   Wenn Sie auf die Registerkarte "Netzwerkkonfiguration" zurückkehren, können Sie feststellen, dass der neue virtuelle Switch hinzugefügt wurde.


Add Network Wizard
Ready to Complete
Verify that all new and modified vSphere standard switches are configured appropriately.
Connection Type
Network Access
Connection Settings
Summary
Host networking will include the following new and modified standard switches:
Preview:
Virtual Machine Port Group
VM Network For SP recovery
Physical Adapters
vmnic2
Help
< Back
Finish
Cancel

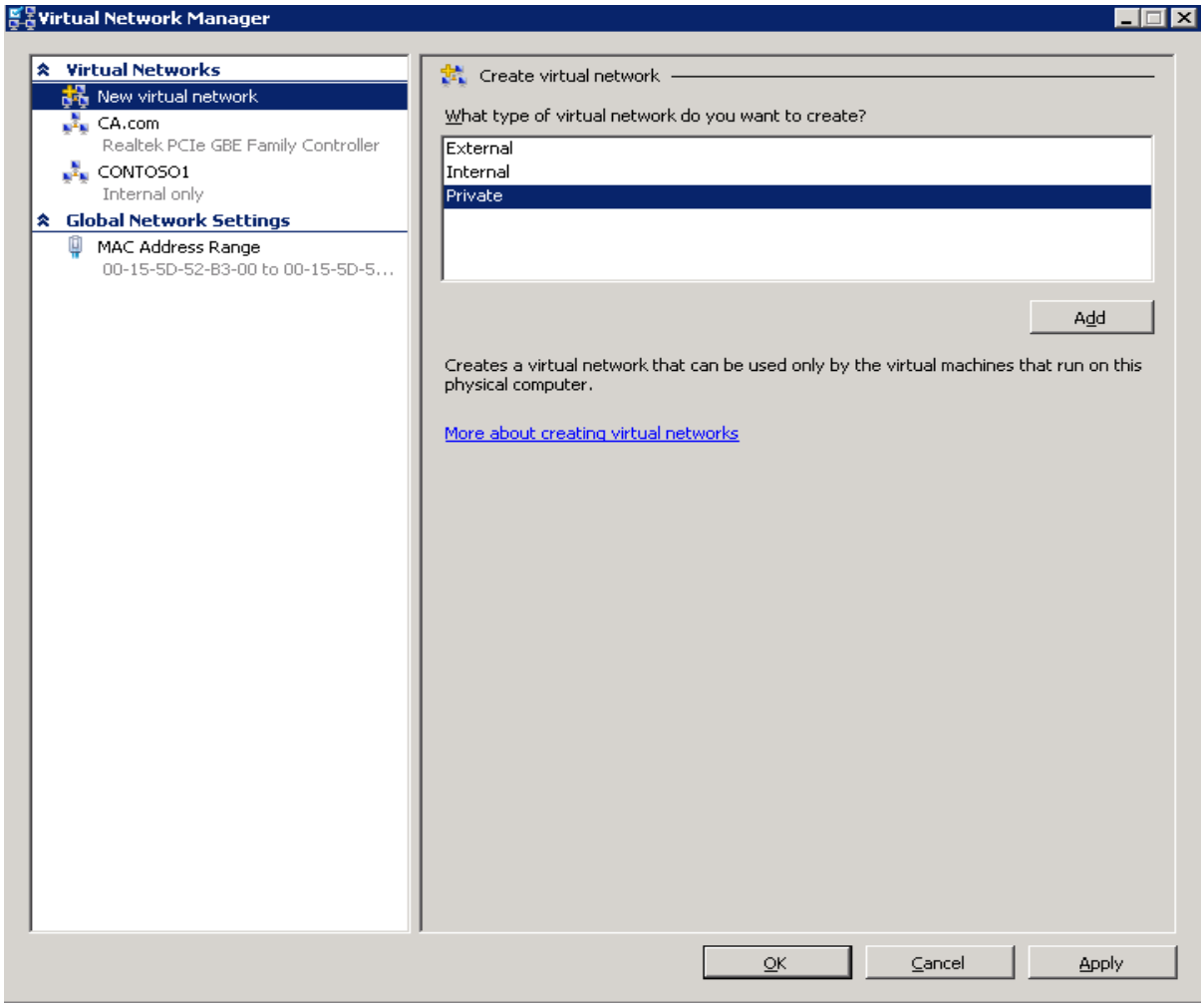
Erstellen eines isolierten Netzwerks für die SharePoint-Wiederherstellung bei Hyper-V-VMs

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Hyper-V-Manager an.
2. Klicken Sie auf "Virtueller Netzwerk-Manager".

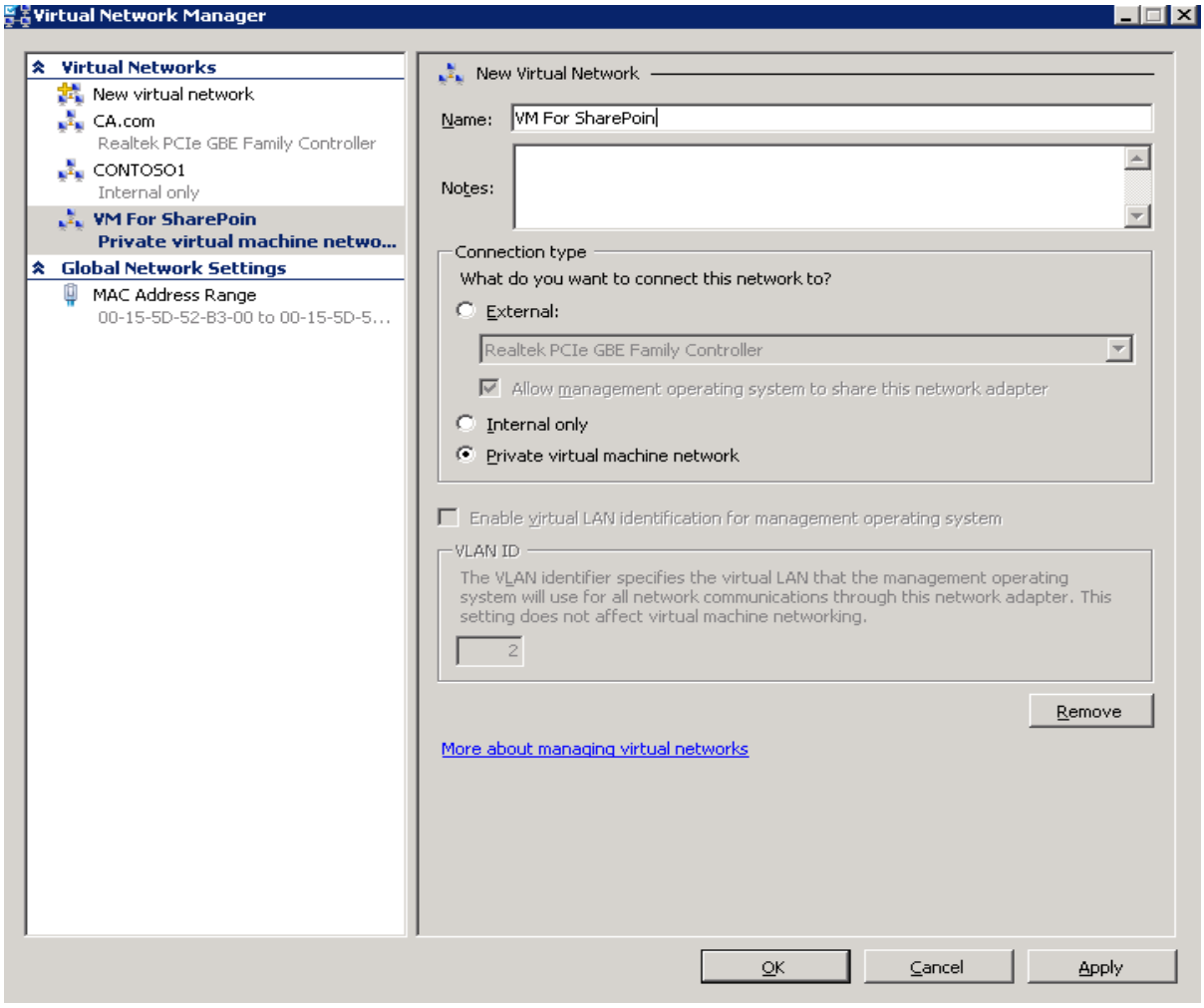


3. Klicken Sie auf "Neues virtuelles Netzwerk", wählen Sie den Typ "Privat" und klicken Sie dann auf **Hinzufügen**.



4. Geben Sie einen Namen für das private virtuelle Netzwerk ein, und klicken Sie auf "OK".

   Das neue virtuelle Netzwerk wird hinzugefügt.


Virtual Network Manager
Virtual Networks
New virtual network
CA.com
Realtek PCIe GBE Family Controller
CONTOSO1
Internal only
VM For SharePoin
Private virtual machine netwo...
Global Network Settings
MAC Address Range
00-15-5D-52-B3-00 to 00-15-5D-5...
New Virtual Network
Name:
VM For SharePoin
Notes:
Connection type
What do you want to connect this network to?
External:
Realtek PCIe GBE Family Controller
Allow management operating system to share this network adapter
Internal only
Private virtual machine network
Enable virtual LAN identification for management operating system
VLAN ID
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
2
Remove
More about managing virtual networks
OK
Cancel
Apply

Kapitel 6: Generieren von Arcserve UDP-Berichten

In diesem Abschnitt werden die folgenden Themen behandelt:

Kennenlernen von Arcserve UDP-Berichten

Die Registerkarte **Berichte** bietet Zugriff auf verschiedene Arten von Berichten, beispielsweise zu Alerts, Datentrends, Sicherungsstatus, Datenverteilung und SLA. Der linke Fensterbereich enthält eine Liste von Berichten, die Sie generieren können. Im mittleren Fensterbereich werden die Details des ausgewählten Berichts angezeigt. Hier können Sie eine Reihe von Berichtseinstellungen konfigurieren. Der Bericht wird für eine Gruppe von Knoten oder Servern generiert. Sie können den Bericht auch filtern, um detaillierte Informationen für einen individuellen Knoten anzuzeigen.

Weitere Informationen zu Berichten finden Sie unter Arcserve UDP-Berichte.

Dieser Bericht mit Drill-down-Funktion enthält die folgenden Elemente:

Auftrag - Knoten

Zeigt den Knotennamen an, wo Jobs von Arcserve UDP Agents, Host-Based VM oder Virtual Standby ausgeführt werden.

Geschützte Knoten

Zeigt den Namen des Agentenknotens und Knotens an, der durch Arcserve Unified Data Protection-Agent, hostbasierte VM-Backups, Virtual Standby oder Arcserve Backup geschützt ist.

Produkt

Zeigt das Produkt an, das auf dem Knoten installiert ist. Der Produktname könnte Arcserve Unified Data Protection-Agent Arcserve Unified Data Protection Recovery Point Server, hostbasierte VM oder Arcserve Backup lauten.

Filter/Aktionen

Zeigt die globalen und lokalen Optionen für Filter und Aktionen für Berichte an. Weitere Informationen finden Sie unter Verwenden von Filtern und Aktionen.

Arcserve UDP-Berichte

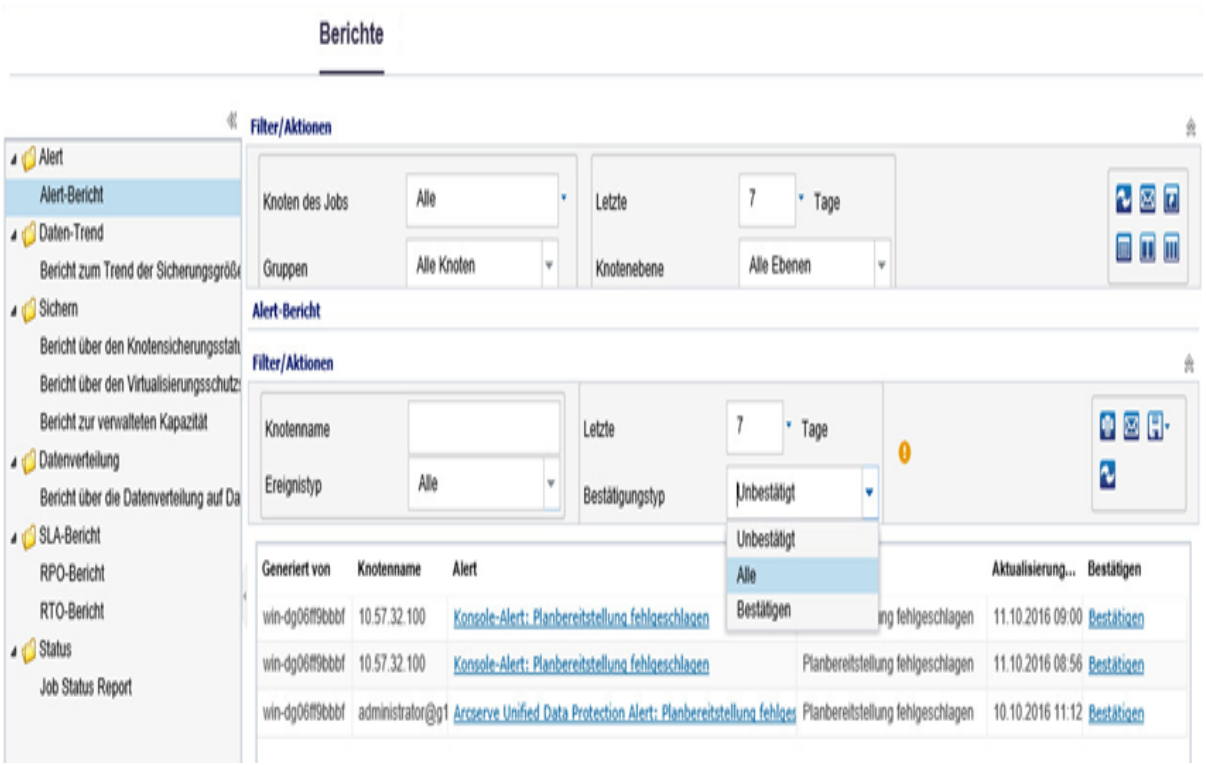
Arcserve UDP bietet die folgenden Arten von Berichten:

- Alert-Bericht
- Bericht zum Trend der Sicherungsgröße
- **Sicherungsbezogene Berichte:** Arcserve UDP bietet drei Arten von sicherungsbezogenen Berichten:
  - Bericht zum Knotensicherungsstatus
  - Bericht über den Virtualisierungsschutzstatus
  - Bericht zur verwalteten Kapazität
- Bericht über die Datenverteilung auf Datenträgern
- **SLA-Bericht:** Der SLA-Bericht (Service Level Agreement) zeigt Compliance-Berichte im Zusammenhang mit Recovery Point Objective (RPO) und Recovery Time Objective (RTO) an.
  - RPO-Bericht
  - RTO-Bericht
- **Jobstatusbericht:** Arcserve UDP hilft Ihnen dabei, Jobstatusberichte zu erstellen, um Details zu allen in einem festgelegten Zeitraum durchgeführten Jobs abzurufen.

Alert-Berichte

Arcserve UDP zeigt die Alert-Informationen für Knoten an. Neben den gängigen Filtern und Aktionen bietet der Alert-Bericht die Möglichkeit, Ihr Alert-Dashboard zu bereinigen, indem Sie Alerts bestätigen. Ihr Alert-Berichts-Dashboard zeigt standardmäßig nur unbestätigte Alerts an. Sie können bei jedem Alert auf den entsprechenden **Bestätigungslink** klicken, um diesen aus der Dashboardansicht zu entfernen. Wenn Sie den bestätigten Bericht anzeigen möchten, wählen Sie in der Option **Bestätigungstyp** des lokalen Filters die Option **Bestätigen** aus.

Alert-Bericht

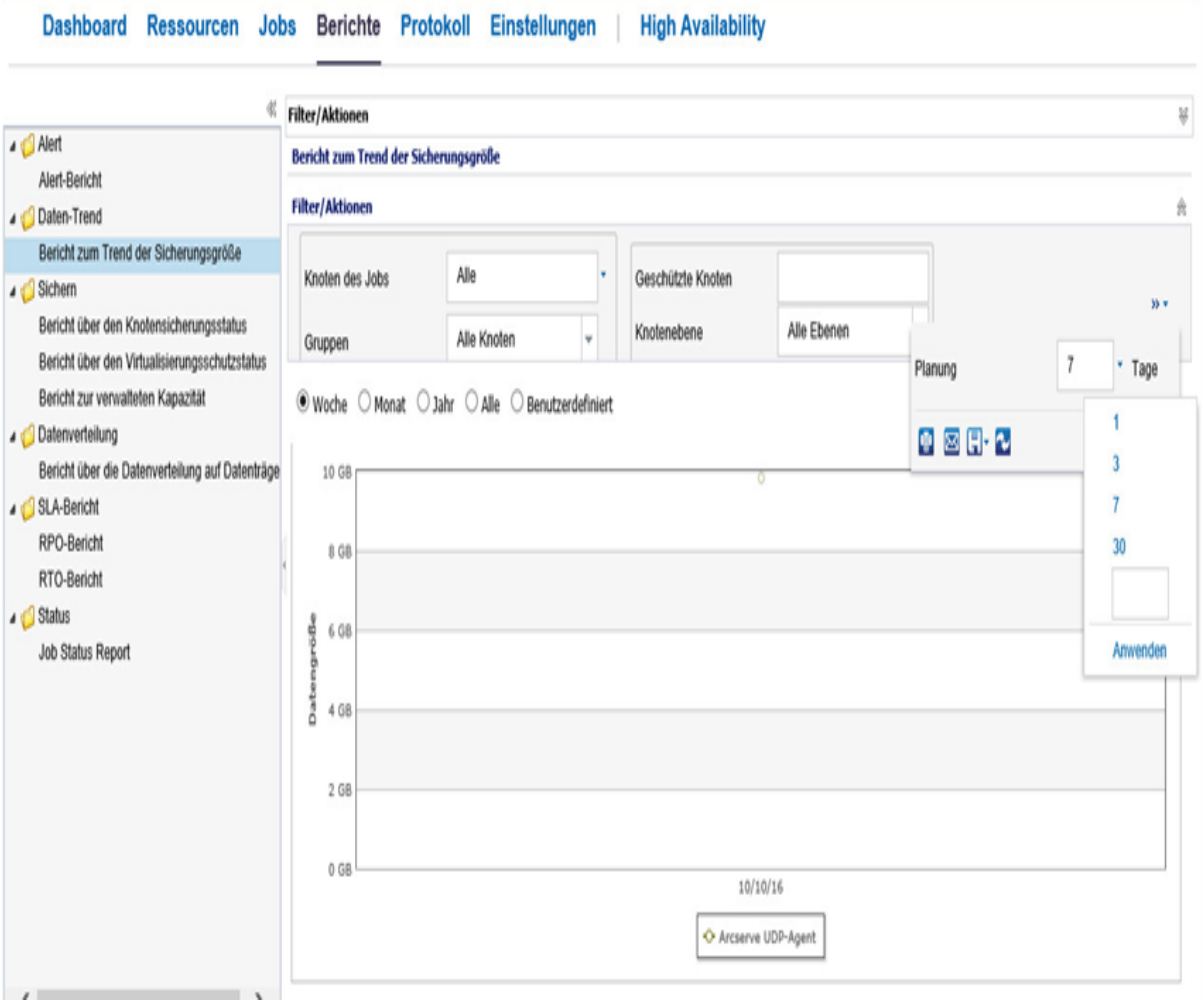


Berichte zum Trend der Sicherungsgröße

Der Arcserve UDP Bericht zum Trend der Sicherungsgröße zeigt die Größe der Sicherungsdaten von Arcserve Backup und Arcserve Unified Data Protection Agent in einer Verlaufsansicht an, und projiziert den Wachstumstrend, sodass Sie Vorbereitungen für zukünftige Speicherplatzanforderungen treffen können. Dieser Bericht enthält Informationen zu Knoten, die auf unterstützten Windows- und Linux-Betriebssystemen ausgeführt werden, und ermöglicht es Ihnen, detailliertere Informationen zu einzelnen Knoten aufzuschlüsseln.

Neben den gängigen Filtern und Aktionen bietet der Bericht zum Trend der Sicherungsgröße die Möglichkeit, Ergebnisse basierend auf der Anzahl von **Tagen** anzuzeigen. Standardmäßig ist der Filter für die **Letzten** Tage nicht anwendbar. Verwenden Sie stattdessen **Ansicht** Modus-Filter (Woche/Monat/Jahr/benutzerdefiniert).

Bericht zum Trend der Sicherungsgröße



Berichte zum Knotensicherungsstatus

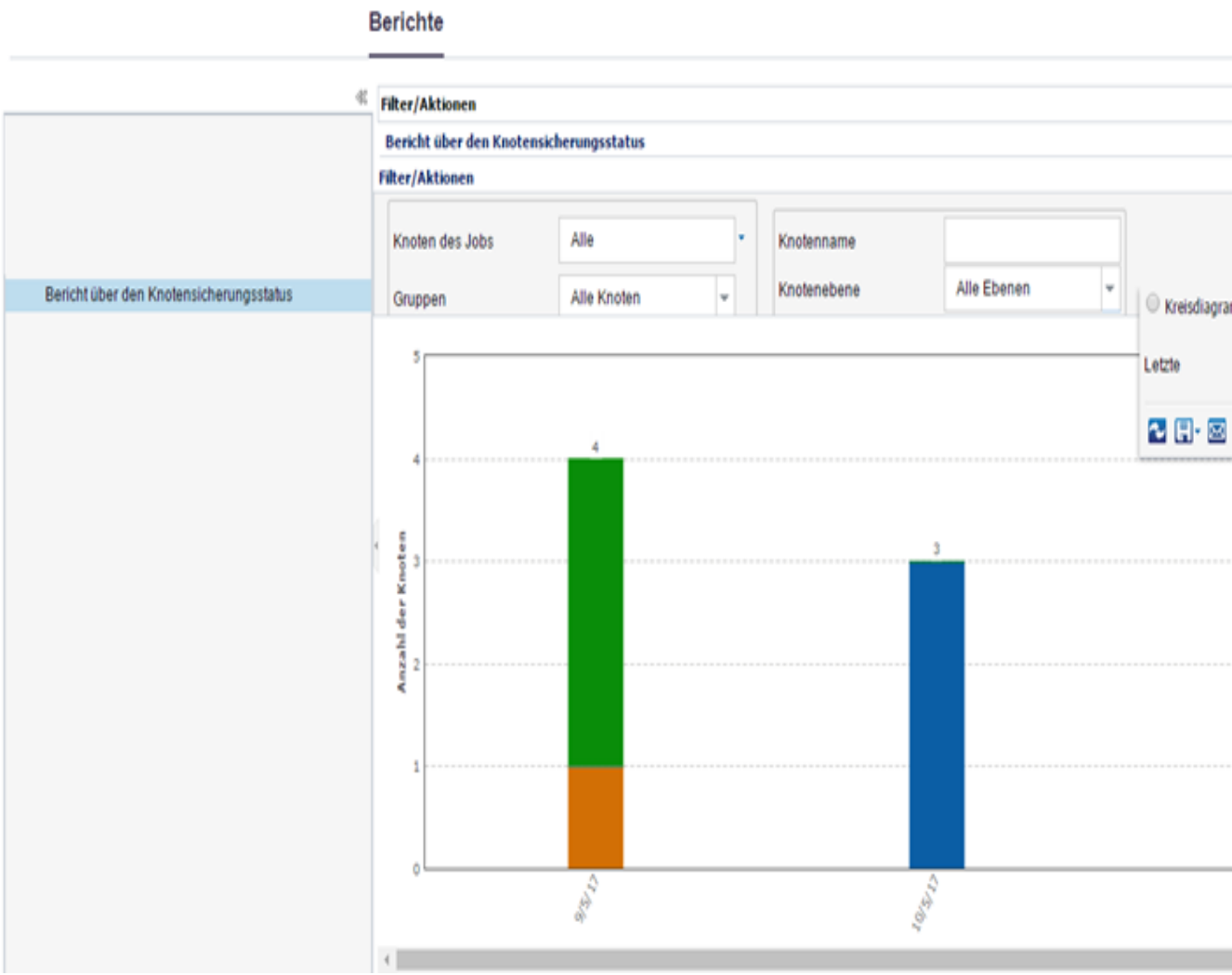
Arcserve UDP zeigt den aktuellen Sicherungsstatus aller Knoten für den angegebenen Zeitraum an. Dieser Bericht enthält ausführliche Informationen zu Knoten basierend auf Kategorien, wie z. B. den ausgewählten Typ der Gruppen und Knotenebene.

Neben den gängigen Filtern und Aktionen bietet der Bericht zum Knotensicherungsstatus die Möglichkeit, Ergebnisse basierend auf der Anzahl von **Tagen** anzuzeigen. Im Balkendiagramm wird über jedem Balken die Knotenanzahl angezeigt.

Der Bericht zeigt folgenden Jobstatus an:

- **Erfolgreich:** Gibt eine Liste der Jobs an, die erfolgreich abgeschlossen wurden.
- **Fehlgeschlagen:** Gibt eine Liste der fehlgeschlagenen Jobs an.
- **Unvollständig:** Gibt eine Liste der Jobs an, die mit dem Status "Unvollständig" beendet wurden.
- **Abgebrochen:** Gibt eine Liste der Jobs an, die abgebrochen wurden.
- **Entgangen:** Gibt eine Liste der Jobs an, die nicht abgerufen wurden.
- **Keine Sicherungen:** Bietet eine Liste der Knoten ohne zugewiesenen Plan oder der Knoten mit zugewiesenem Plan, für die die Sicherungen noch ausstehen.

Bericht zum Knotensicherungsstatus:

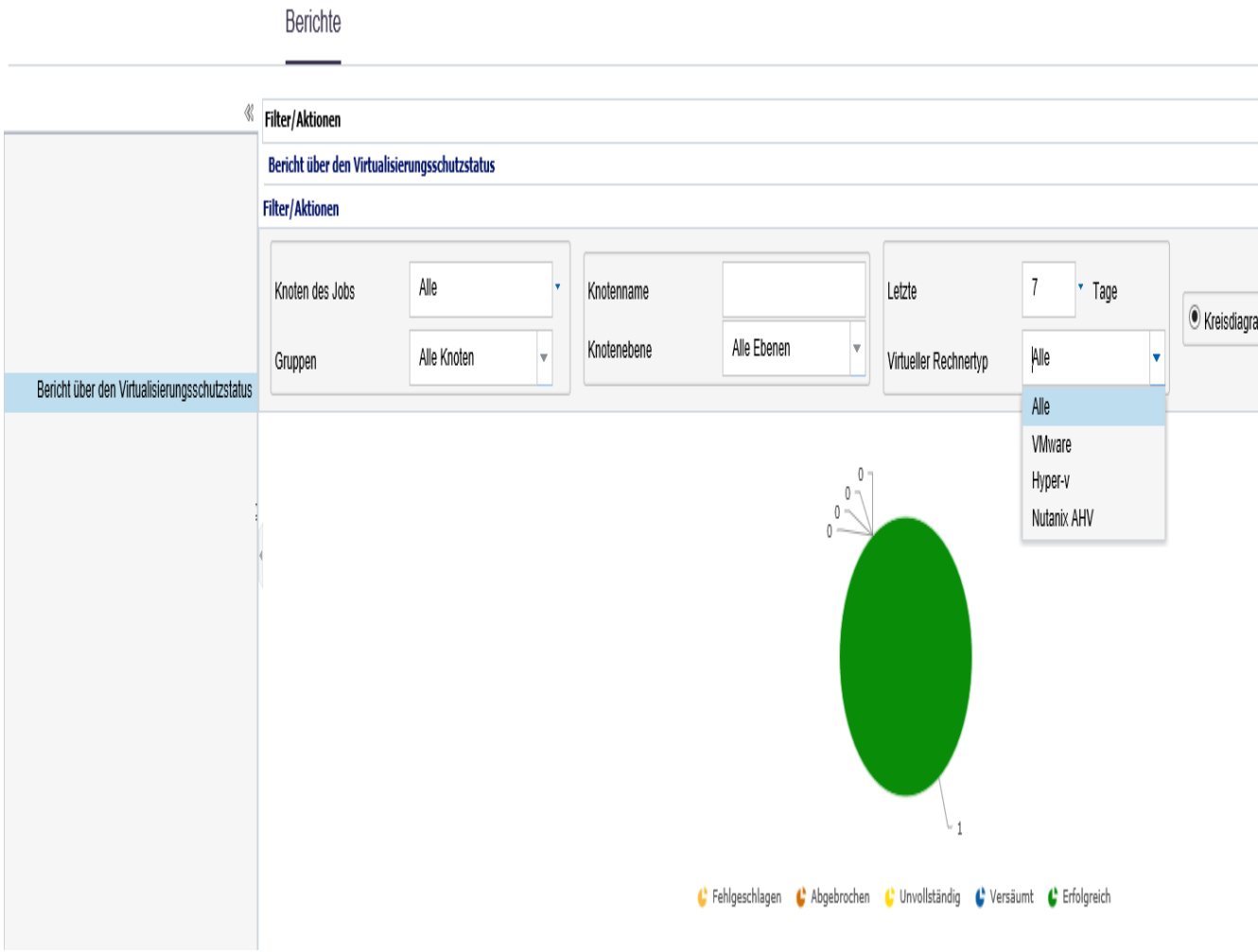

Berichte
Filter/Aktionen
Bericht über den Knotensicherungsstatus
Filter/Aktionen
Bericht über den Knotensicherungsstatus
Knoten des Jobs
Alle
Gruppen
Alle Knoten
Knotenname
Knotenebene
Alle Ebenen
Letzte
Anzahl der Knoten
0
1
2
3
4
5
4
3
9/5/17
10/5/17

Berichte über den Virtualisierungsschutzstatus

Zeigt den aktuellsten Sicherungsstatus der virtuellen Rechner an, die von Host-Based VM Backup, Virtual Standby oder Arcserve Backup geschützt werden. Dieser Bericht enthält Informationen für einen angegebenen Zeitraum und kann detailliertere Informationen zu einzelnen ausgewählten Kategorien aufschlüsseln.

Neben den gängigen Filtern und Aktionen bietet der Bericht über den Virtualisierungsschutzstatus die Möglichkeit, Ergebnisse basierend auf der Anzahl der **Tage** anzuzeigen und Berichte als Kreisdiagramm oder Tabelle anzuzeigen.

Bericht über den Virtualisierungsschutzstatus



Berichte zur verwalteten Kapazität

Zeigt die Rohdatengröße der letzten erfolgreichen vollständigen Sicherung für alle Knoten an, die von Arcserve Backup, Arcserve Unified Data Protection Agent und Host-based VM Backup geschützt werden.

Weitere Informationen zu Filtern und Aktionen finden Sie in den gängigen Filtern und Aktionen.

Hinweise:

- Die Eingabe eines Werts in den Filter **Letzte Tage** wirkt sich nicht auf das Ergebnis für den globalen Filter aus. Unabhängig von der Anzahl der Tage, die Sie angeben, werden bei Anwendung des Filter die neuesten Werte angezeigt.
- Die Daten in Verbindung mit der Knotensicherung im gelöschten Datenspeicher können angezeigt werden, da der Bericht zur verwalteten Kapazität nicht aktualisiert wird, solange die Sicherung nicht auf dem neuesten Sicherungsziel ausgeführt wird. Wenn Sie beispielsweise den Plan geändert haben, sodass Sicherungen auf Datenspeicher DS2 ausgeführt werden, und den Datenspeicher DS1 gelöscht haben, werden die gelöschten Daten von DS1 unter Umständen weiterhin im Bericht angezeigt, solange Sie keine Sicherung auf DS2 durchführen.
- Im Rasterbereich des Berichts sind die folgenden drei Spalten nur auf VM-Knoten anwendbar, die per hostbasierter agentenloser Sicherung geschützt werden:

  Verwendeter Speicherplatz für Volumes (VM)

  Zeigt die Summe des belegten Speicherplatzes aller Volumes auf dem Gast-BS der VM an.

  Für Windows: Bezieht sich auf die Summe des belegten Speicherplatzes aller NTFS-Volumes

  Für Linux VM: Bezieht sich auf die Summe des belegten Speicherplatzes aller Volumes.

  Für Linux-VMs werden nur VMware-VMs in dieser Spalte unterstützt. In diesem Fall müssen Sie den VM-Knoten mit Root-Anmeldeinformationen aktualisieren. Diese Spalte ist leer, unabhängig davon, ob es sich um eine VMware-Linux-VM oder eine Hyper-V-Linux-VM handelt.

  Bei der Unterstützung von Linux-VMs gelten für VMware-Red-Hat- oder CentOS-Rechner bestimmte Einschränkungen. Weitere Informationen finden Sie in den Hinweisen zu bekannten Problemen für Arcserve UDP v6 Update 1.

  Synthetische Lesegröße

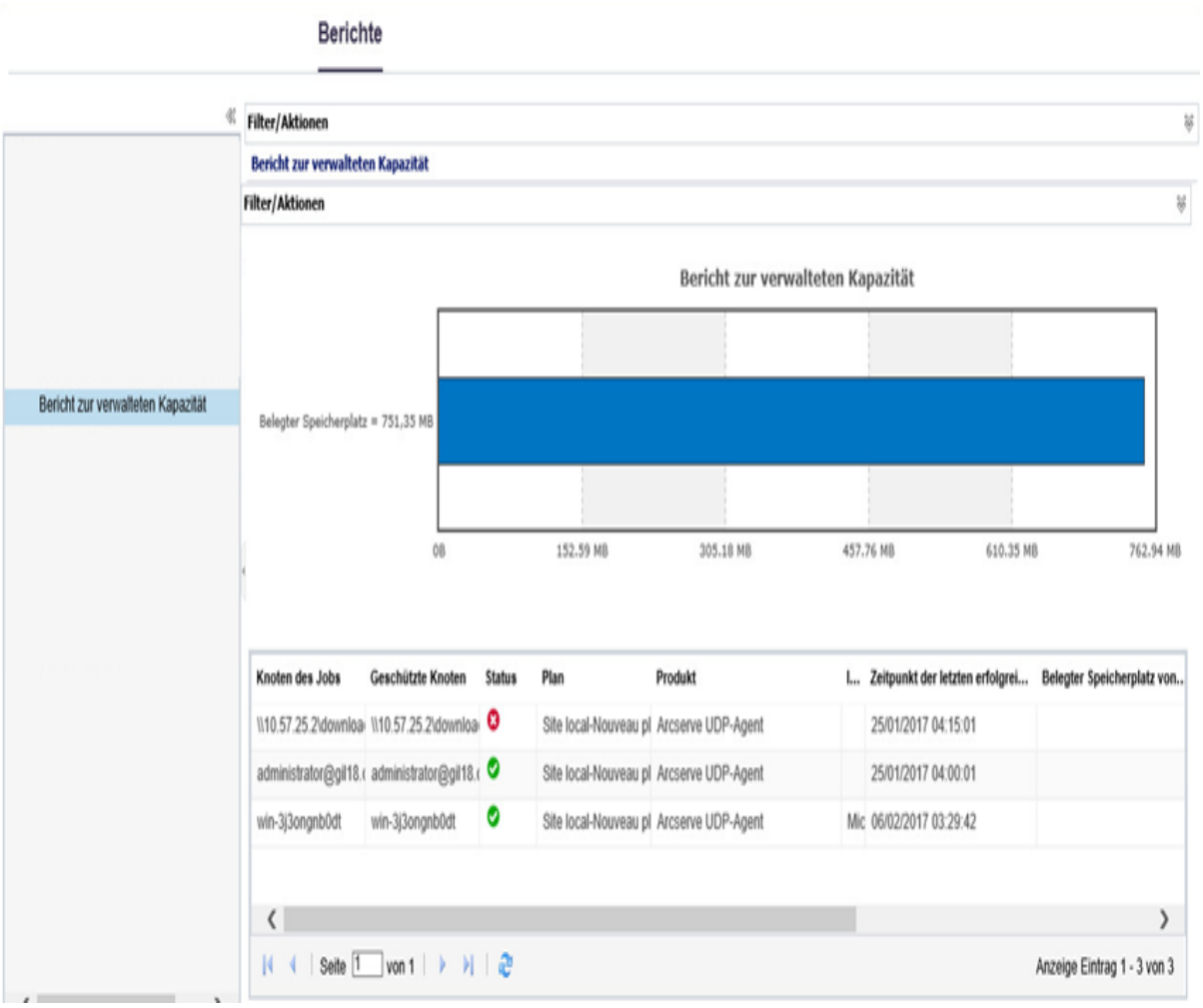
Gibt die Gesamtgröße der während der Sicherung gelesenen Daten an.

Bereitstellungsgröße des virtuellen Datenträgers

Zeigt die Summe der Bereitstellungsgröße aller virtueller Datenträger der VM an.

- Normalerweise ist die Rohdatengröße die Größe der in das Sicherungsziel geschriebenen Daten. Die hostbasierte agentenlose Sicherung entspricht nicht unbedingt der synthetischen Lesegröße, da Arcserve UDP keine reinen Null-datenblöcke in das Sicherungsziel schreibt. Es werden also alle Nulldatenblöcke bei der Sicherung übersprungen. Darüber hinaus können Sie die angezeigten Daten für die Rohdatengröße durch Konfigurieren einiger Registrierungswerte für VM-Knoten anpassen, die durch hostbasierte agentenlose Sicherung geschützt werden. Weitere Informationen zum Konfigurieren der Regis-trierungswerte und zugehöriger Verhalten finden Sie unter Grundlegendes zur Rohdatengröße im Bericht zur verwalteten Kapazität für hostbasierte agen-tenlose Sicherungen von VMs.

  Bericht zur verwalteten Kapazität

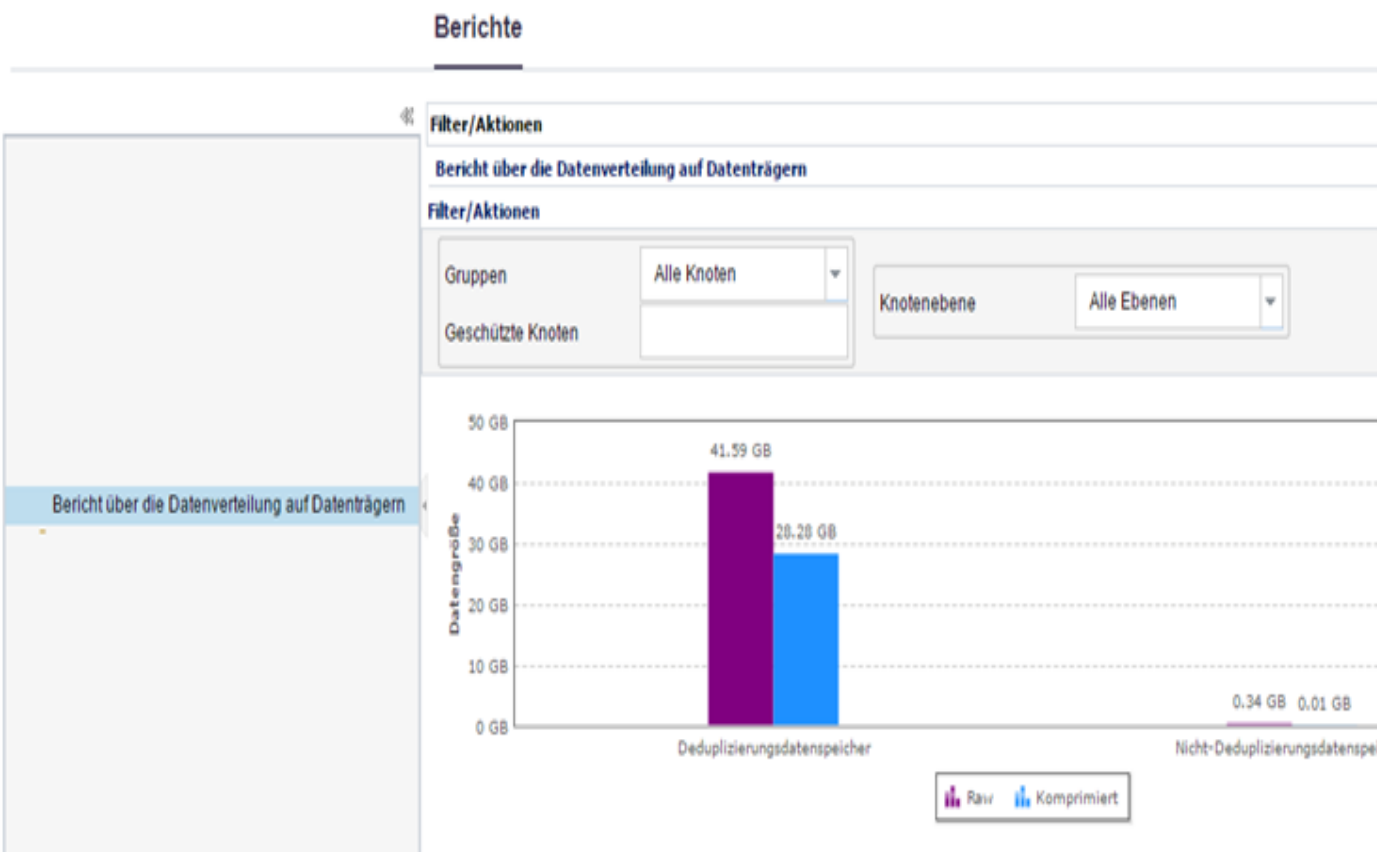

Berichte
Filter/Aktionen
Bericht zur verwalteten Kapazität
Filter/Aktionen
Bericht zur verwalteten Kapazität
Bericht zur verwalteten Kapazität
Belegter Speicherplatz = 751,35 MB
0B
152.59 MB
305.18 MB
457.76 MB
610.35 MB
762.94 MB
Knoten des Jobs
Geschützte Knoten
Status
Plan
Produkt
I...
Zeitpunkt der letzten erfolgrei...
Belegter Speicherplatz von...
\\10.57.25.2\downloa
\\10.57.25.2\downloa
Site local-Nouveau pl
Arcserve UDP-Agent
25/01/2017 04:15:01
administrator@gil18.
administrator@gil18.
Site local-Nouveau pl
Arcserve UDP-Agent
25/01/2017 04:00:01
win-3j3ongnb0dt
win-3j3ongnb0dt
Site local-Nouveau pl
Arcserve UDP-Agent
Mic
06/02/2017 03:29:42
Seite 1 von 1
Anzeige Eintrag 1 - 3 von 3

Berichte über die Datenverteilung auf Datenträgern

Zeigt die komprimierte und aktuelle Backupdatenmenge (unformatiert) für andere Zieltypen (mit und ohne Deduplizierung und lokale Ziele) an. DieserBericht ermöglicht Ihnen alle Knoten, einschließlich Knoten von Arcserve Backup und Arcserve UDP Agent anzuzeigen. Um Arcserve Backup Dateninformationen anzuzeigen, aktivieren Sie den **Ablaufplan der Arcserve Backup-Datensynchronisation** in der Registerkarte **Einstellung**. Für neueste Informationen klicken Sie in den Einstellungen auf **Jetzt ausführen**.

Weitere Informationen zu Filtern und Aktionen finden Sie in den gängigen Filtern und Aktionen.

Bericht über die Datenverteilung auf Datenträgern –



Hinweis: Der Bericht über die Datenverteilung auf Datenträgern richtet sich nach den am Sicherungsziel verfügbaren Wiederherstellungspunktdaten. Mit der Option **Aktualisieren** können Sie bei Bedarf eine Synchronisierung initiieren und erhalten den aktuellen Status in den Berichten.

RPO-Berichte

Der Recovery Point Objective (RPO)-Bericht ist der Compliance-Bericht, der angezeigt, wie die Wiederherstellungspunkte in der Sicherungsumgebung verteilt sind. Der Bericht ist hilfreich, um bei einem Notfall zu ermitteln, welches der älteste und der aktuellste Point-in-Time ist, zu dem der Knoten zurückgesetzt werden kann. Da der RPO-Bericht für das Sicherungsziel ist, wird er mit Daten ausgefüllt, wenn Sicherungsdaten bereitstehen. Der Bericht wird entweder über eine Aktualisierung nach Bedarf oder gemäß Zeitplan gefüllt.

Hinweis: Der Bericht wird auch direkt über das Arcserve UDP-Dashboard befüllt. Wenn Sie im Dashboard im RPO-Balkendiagramm auf einen Monat klicken, wird der RPO-Berichtsbildschirm für diesen Monat auf der RPO-Seite angezeigt.

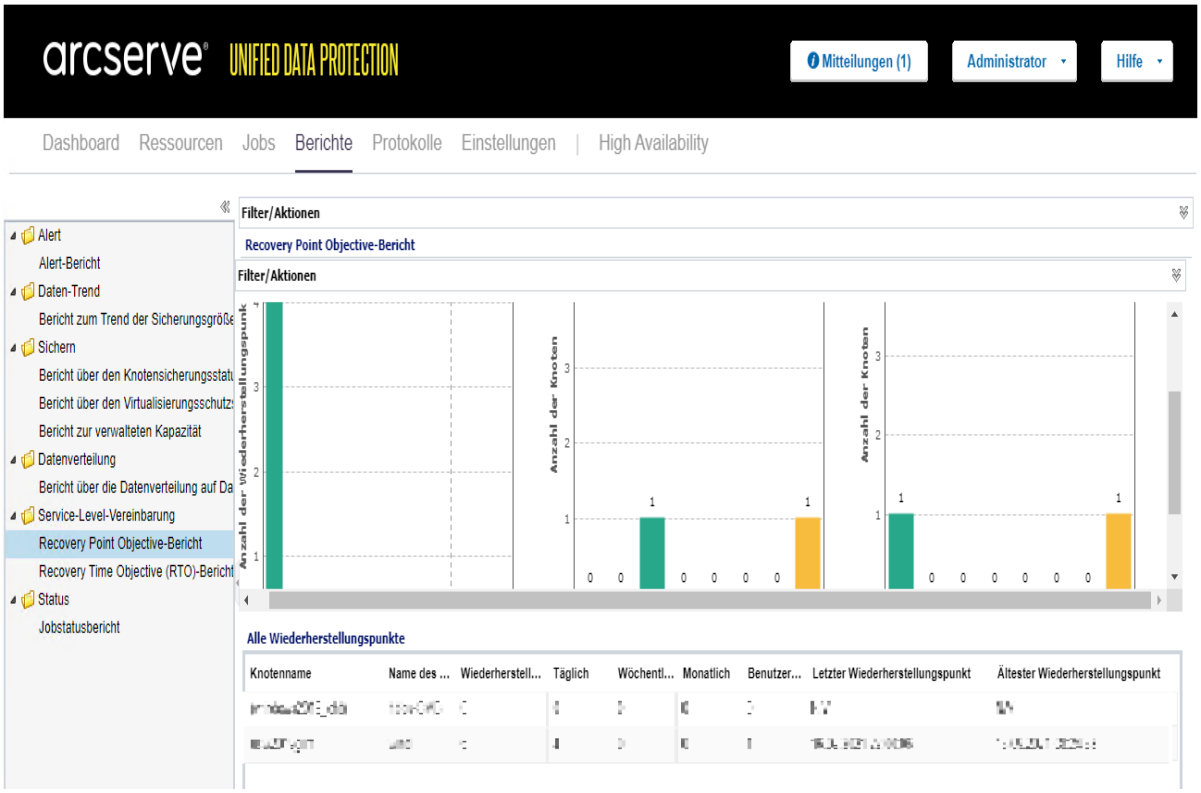
Das RPO bar-Diagramm enthält folgende Informationen:

- Monatliche Verteilung von Wiederherstellungspunkten im Sicherungsziel.
- Alter des neuesten Wiederherstellungspunkts, der für jeden Knoten verfügbar ist.
- Alter des ältesten Wiederherstellungspunkts, der für jeden Knoten verfügbar ist.
- Zahlen über jedem Balken
- *Zieltyp* ermöglicht Ihnen das Ziel auszuwählen. Zum Beispiel:in einer Cloud, auf einem Recovery Point Server und für lokale Freigabe.
- Unter *Zielname* können Sie ein Ziel aus der Liste von Zielen auswählen, die nach der Auswahl des gewünschten Zieltyps angezeigt wird.
- Es werden jeweils die betreffenden Ergebnisse angezeigt, wenn Sie in einem der folgenden drei Diagramme auf einen Balken klicken: *Anzahl von Wiederherstellungspunkten* für jeden Monat, *Alter des neuesten Wiederherstellungspunkts* und *Alter des ältesten Wiederherstellungspunkts*.

Unter dem RPO-Balkendiagramm werden im Abschnitt Alle Wiederherstellungspunkte Informationen wie Knotenname, Planname, Wiederherstellungspunkte, Täglich, Wöchentlich, Monatlich, Benutzerdefiniert, Letzter Wiederherstellungspunkt und Alter Wiederherstellungspunkt angezeigt.

Neben den gängigen Filtern und Aktionen stellen RPO-Berichte die einzigartige Option **Aktualisieren** im lokalen Filter bereit.

RPO-Bericht



Hinweis: Der Bericht hängt von den Wiederherstellungspunktdaten ab, die auf dem Sicherungsziel verfügbar sind. Mit der Option **Aktualisieren** können Sie bei Bedarf eine Synchronisierung initiieren und erhalten den aktuellen Status in den Berichten.

RTO-Berichte

Der Recovery Time Objective (RTO)-Bericht ist der Compliance-Bericht, der anzeigt, ob das festgelegte Recovery Time Objective für alle ausgeführten Wiederherstellungsjobs eingehalten wurde. Der RTO-Bericht zeigt die folgenden Statustypen an:

- **RTO erfüllt:** Der Recovery-Job hat das festgelegte Ziel erreicht.
- **RTO nicht erfüllt:** Der Recovery-Job hat das festgelegte Ziel nicht erreicht.
- **RTO nicht definiert**: Kein Ziel für den Recovery-Job definiert.
- **RTO nicht getestet:** Es ist ein Recovery Time Objective festgelegt, der Job wurde aber noch nicht getestet.

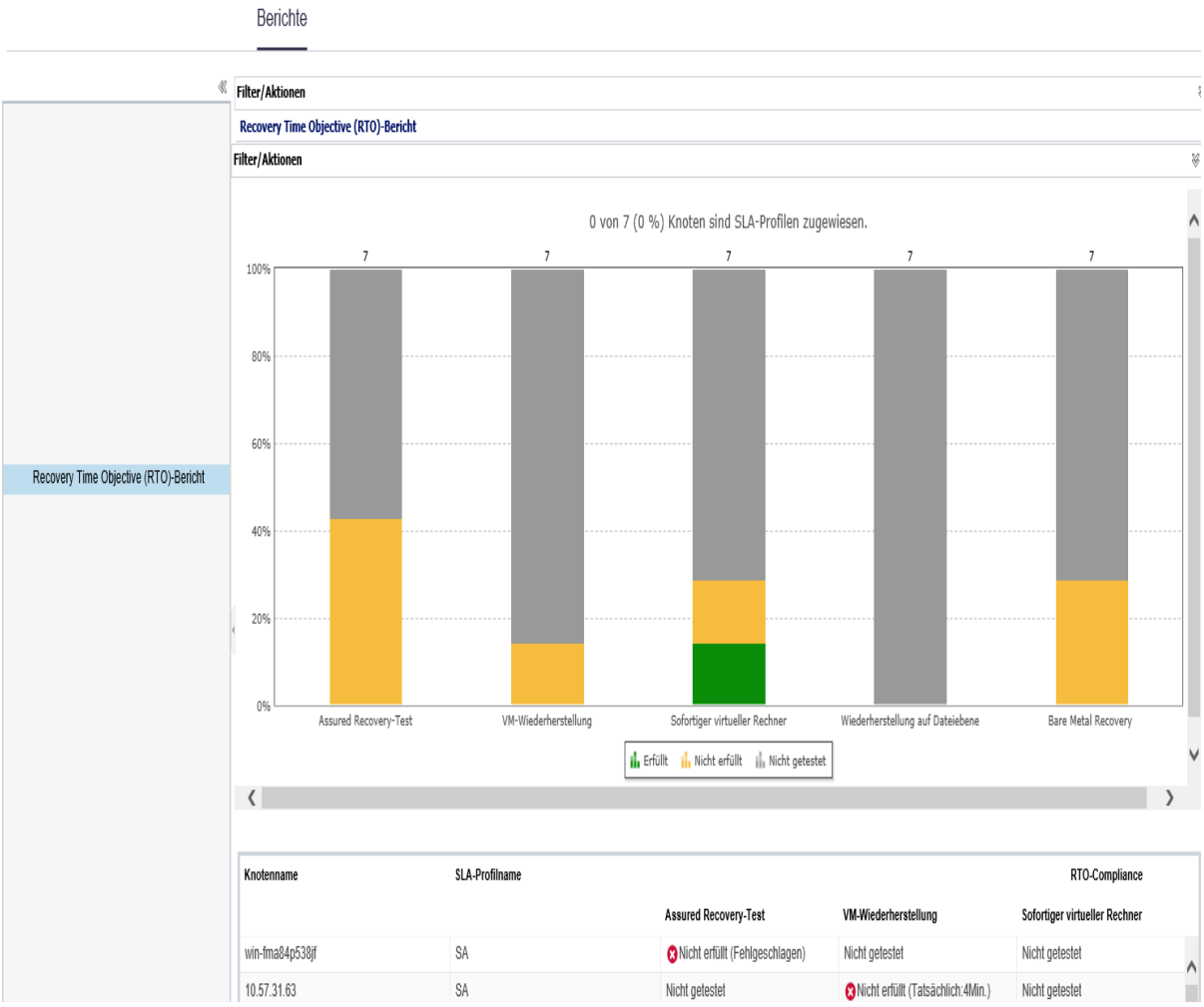
Sie können Recovery Time Objectives für alle Wiederherstellungsjobs definieren. Weitere Informationen finden Sie unter Erstellen des SLA-Profils.

Neben den allgemeine Filtern und Aktionen, bieten RTO Berichte die einzigartigen Menüoptionen **SLA Profile** und RTO Status im lokalen Filter.

Hinweis: Der RTO-Bericht wird für Bare-Metal-Wiederherstellungsjobs, die für auf dem lokalen Ziel definierte Sicherungsjobs ausgeführt werden, nicht unterstützt.

RTO-Bericht – Dashboard

RTO Bericht – Aspekte	Beschreibung
Für die Erzeugung des RTO-Diagramms berücksichtigten Parameter	• Erfüllt • Nicht erfüllt • Nicht getestet
Formel zur Bestimmung des RTO-Status in Prozent (%)	Dem SLA-Profil zugewiesene Knoten/Gesamtknoten * 100
Im Diagramm genutzte Farbcodierung	• Erfüllt = Grün • Nicht erfüllt = Rot • Nicht getestet = Grau

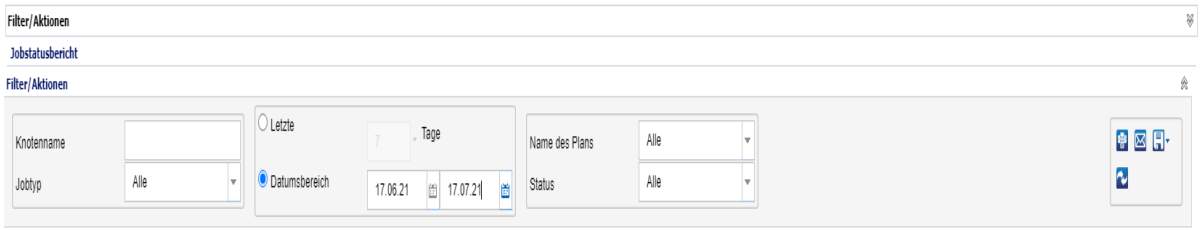

Berichte
Filter/Aktionen
Recovery Time Objective (RTO)-Bericht
Filter/Aktionen
Recovery Time Objective (RTO)-Bericht
0 von 7 (0 %) Knoten sind SLA-Profilen zugewiesen.
7
7
7
7
7
100%
80%
60%
40%
20%
0%
Assured Recovery-Test
VM-Wiederherstellung
Sofortiger virtueller Rechner
Wiederherstellung auf Dateiebene
Bare Metal Recovery
Erfüllt
Nicht erfüllt
Nicht getestet
Knotenname
SLA-Profilname
RTO-Compliance
Assured Recovery-Test
VM-Wiederherstellung
Sofortiger virtueller Rechner
win-fma84p538jf
SA
Nicht erfüllt (Fehlgeschlagen)
Nicht getestet
Nicht getestet
10.57.31.63
SA
Nicht getestet
Nicht erfüllt (Tatsächlich:4Min.)
Nicht getestet

Jobstatus-Berichte

Der Jobstatus-Bericht hilft dabei, sich einen Überblick über den allgemeinen Status aller Jobtypen zu verschaffen, die in der Konsole ausgeführt werden. Dieser Bericht kann hilfreich sein, wenn es darum geht, Audit-Anforderungen zu erfüllen. Neben den gängigen Filtern und Aktionen bietet Ihnen der Jobstatus-Bericht auch die Möglichkeit, Ergebnisse basierend auf dem Jobtyp, der Job-ID, dem Jobstatus und dem Plannamen (sowohl aktiven als auch gelöschten) anzuzeigen. Die Zeitmessung lässt sich in Stunden: Minuten: Sekunden anzeigen.

Sie können den Jobstatusbericht mithilfe der lokalen Filter anzeigen. Die Option "Filter/Aktionen" enthält Folgendes:

- **Knotenname:** Filtert den Jobstatusbericht nach Knotennamen.
- **Jobtyp:** Filtert den Jobstatusbericht nach Jobtyp.
- **Zuletzt:** Zeigt den Jobstatusbericht für die letzte Anzahl von Tagen an.
- **Datumsbereich:** Zeigt den Jobstatusbericht innerhalb des angegebenen Datumsbereichs an.



Hinweis: Sie können je nach Bedarf zwischen dem Filter "Letzter Zeitraum" und "Datumsbereich" wählen. Standardmäßig ist der Filter "Letzte" ausgewählt, und der Jobberichtsstatus der letzten 7 Tage wird angezeigt.

Im Protokoll können Sie auf die Job-ID klicken, um Details anzuzeigen. Ebenso können Sie den Jobstatus jedes Jobs sehen.

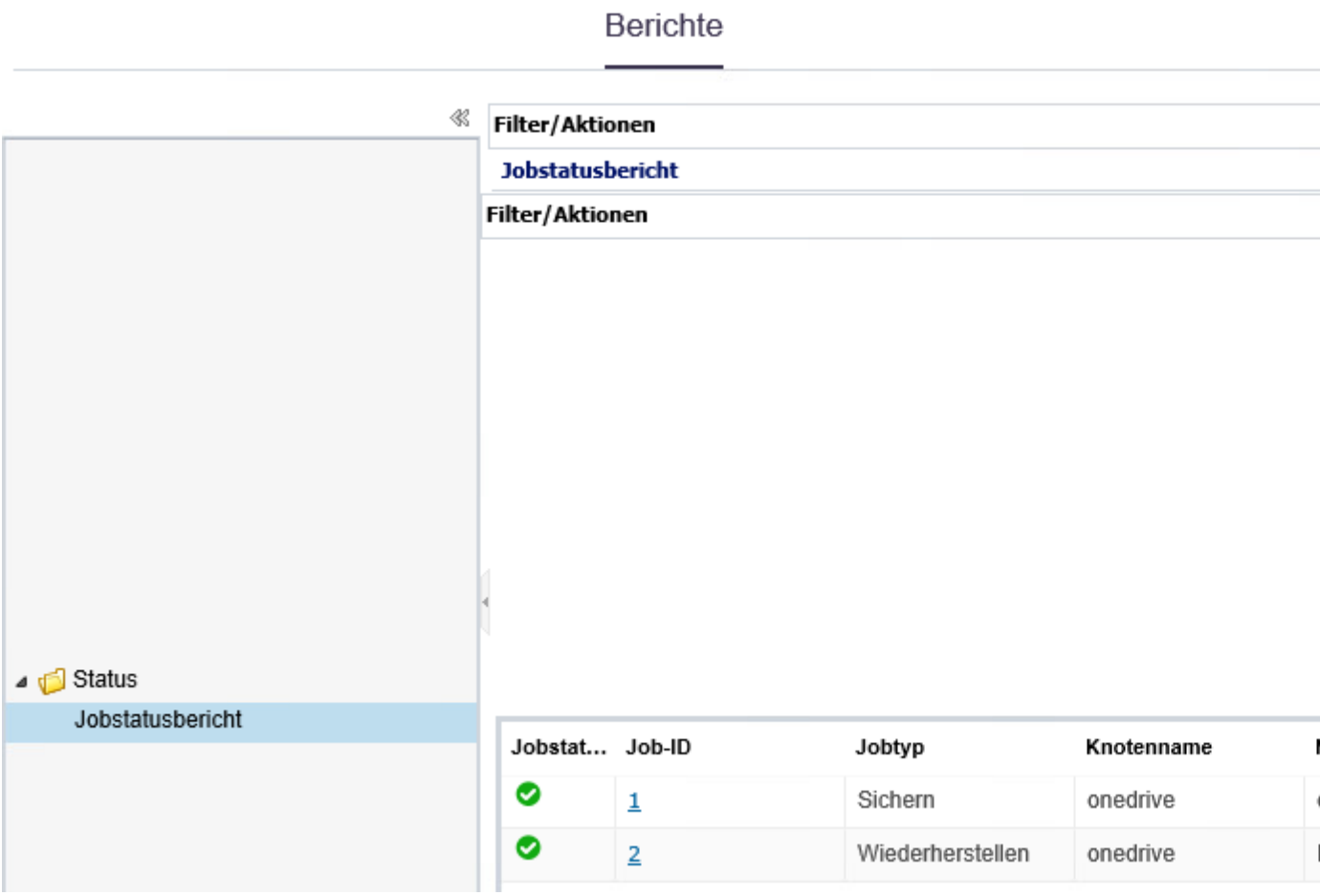
Sie können die tatsächlichen Werte an Quelle und Ziel für Jobtypen anzeigen. Der Bericht zeigt folgenden Jobstatus an:

- **Erfolgreich:** Gibt eine Liste der Jobs an, die erfolgreich abgeschlossen wurden.
- **Fehlgeschlagen:** Gibt eine Liste der fehlgeschlagenen Jobs an.
- **Unvollständig:** Gibt eine Liste der Jobs an, die mit dem Status "Unvollständig" beendet wurden.

- **Abgebrochen:** Gibt eine Liste der Jobs an, die abgebrochen wurden.
- **Entgangen:** Gibt eine Liste der Jobs an, die nicht abgerufen wurden.

Hinweis: Die Standard-Aufbewahrungszeit für das Abrufen des Jobstatus ist 180 Tage. Sie können die Konfiguration ändern, um die Standard-Aufbewahrungszeit bis zur Bereinigung anzupassen.

Bericht über den Jobstatus



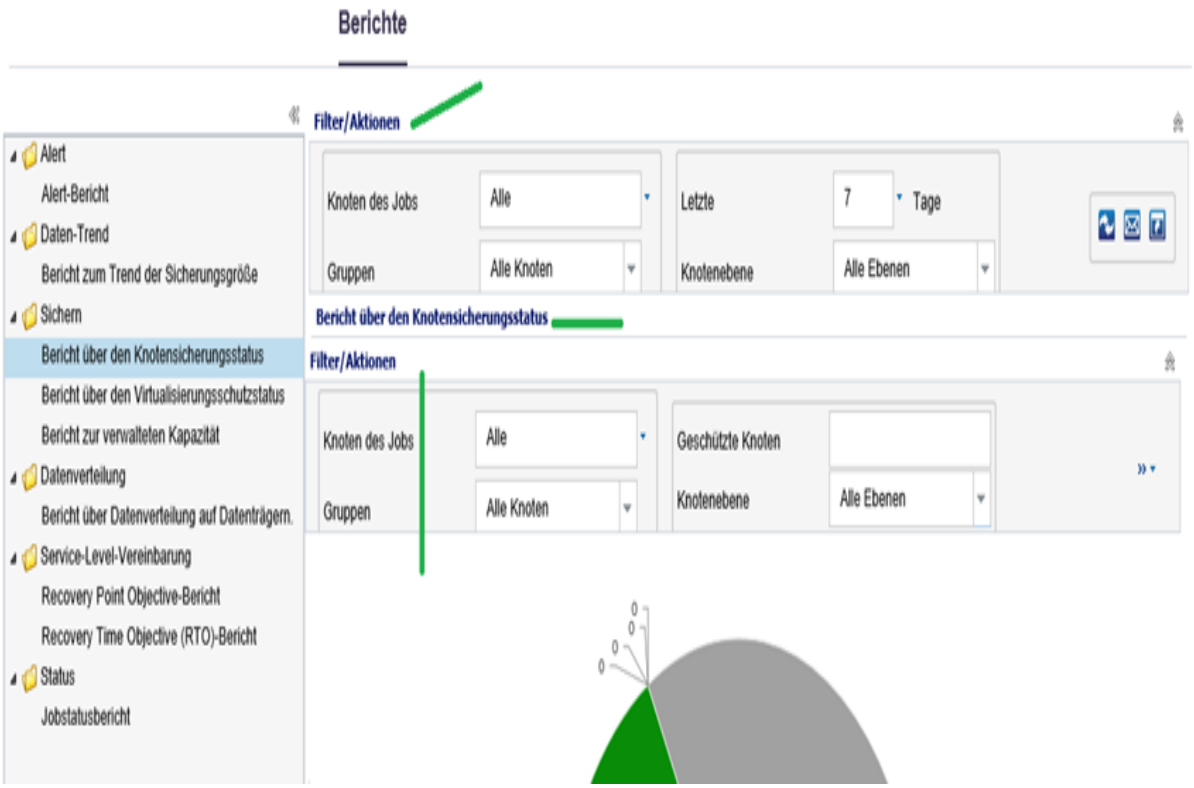
Hinweis: Wenn mehrere Aufträge ausgeführt werden, wird der Statusbericht "Job" generiert. Wenn Sie jedoch auf das Kreisdiagramm klicken, sind die angezeigten Drill-down-Daten möglicherweise inkonsistent. Aktualisieren Sie den Bericht, um diese Inkonsistenz zu beheben.

Verwenden von Filtern und Aktionen

Jede Berichtsseite enthält zwei Optionen für Filter/Aktionen. Die erste Option ist die globale Option. Sie wird auf der Berichtsseite angezeigt. Die andere Option ist die lokale Option. Sie wird unter dem Namen des Berichts auf der Berichtsseite angezeigt und gibt Lösungen zu einem spezifischen Bericht an.

Voraussetzung ist, dass Sie Microsoft.NET Framework (Version 3.5) auf dem Computer installieren, auf dem Sie die Konsole für den Export von Report Chart installiert haben, um Bilder in einen Bericht erfolgreich zu exportieren.

Hinweis: Adobe Flash wird nicht mehr benötigt, und die Installation von .NET Framework als Voraussetzung ermöglicht Ihnen das Anzeigen der Diagramme.



Filter

Sowohl die globale als auch die lokale Option enthält Filter, in die Sie Daten eingeben können, um Optionen für die Berichtsanzeige festzulegen. Die verfügbaren Optionen für globale Filter sind für alle Berichte ähnlich. Die verfügbaren Optionen für lokale Filter fallen für die verschiedenen Berichte unterschiedlich aus.

Aktionen

Für Berichte mit globaler Option:

- **Aktualisieren**: Damit können Sie Informationen mit Bezug zur Seite aktualisieren.
- **Planen, dass Berichte per E-Mail gesendet werden**: Damit können Sie einen Ablaufplan für das Versenden von Berichten per E-Mail erstellen. Weitere Informationen finden Sie unter E-Mails planen.

  Hinweis: Mit einer geplanten E-Mail können maximal 5.000 Datensätze exportiert werden.
- **Zurücksetzen**: Damit können Sie alle Filterparameter in die Standardwerte umändern.
- **Die Berichtsansicht zeigt nur einen Bericht an**: Damit können Sie einen Bericht in einem eigenen Fensterbereich anzeigen.
- **Die Berichtsansicht zeigt mehrere Berichte in zwei Spalten an**: Damit können Sie den Bereich für die Berichtsanzeige in zwei Spalten aufteilen, um mehrere Berichte anzuzeigen.
- **Die Berichtsansicht zeigt mehrere Berichte in drei Spalten an**: Damit können Sie den Bereich für die Berichtsanzeige in drei Spalten aufteilen, um mehrere Berichte anzuzeigen.

  Für Berichte mit lokaler Option:
- **Drucken**: Klicken Sie auf das Symbol, um den Bericht zu drucken.

  Hinweis: Mit "Drucken", können Sie nur auf die ersten 50 Knoten oder Benachrichtigungen aus der Datenliste zugreifen.
- **Aktualisieren**: Klicken Sie darauf, um die Informationen mit Bezug zum Bericht zu aktualisieren.
- **E-Mail**: Sie können den Bericht per E-Mail versenden. Weitere Informationen finden Sie unter Bericht per E-Mail senden.

  Hinweis: Mit einer E-Mail können maximal 10.000 Datensätze exportiert werden.
- **Speichern**: Sie können diese Option verwenden, einen Bericht zu exportieren. Wählen Sie als Format **CSV**, **PDF** oder **HTML** aus, und klicken Sie dann im Dialogfeld, das unten auf der Seite angezeigt wird, auf **Öffnen** oder auf eine der Optionen zum **Speichern**, um den Bericht zu exportieren.

  Hinweis: Mit "Speichern" können Sie nur auf die ersten 10.000 Knoten oder Alerts aus der kompletten Datenliste zugreifen.

Arbeiten mit Arcserve UDP-Berichten

In diesem Abschnitt werden die folgenden Themen behandelt:

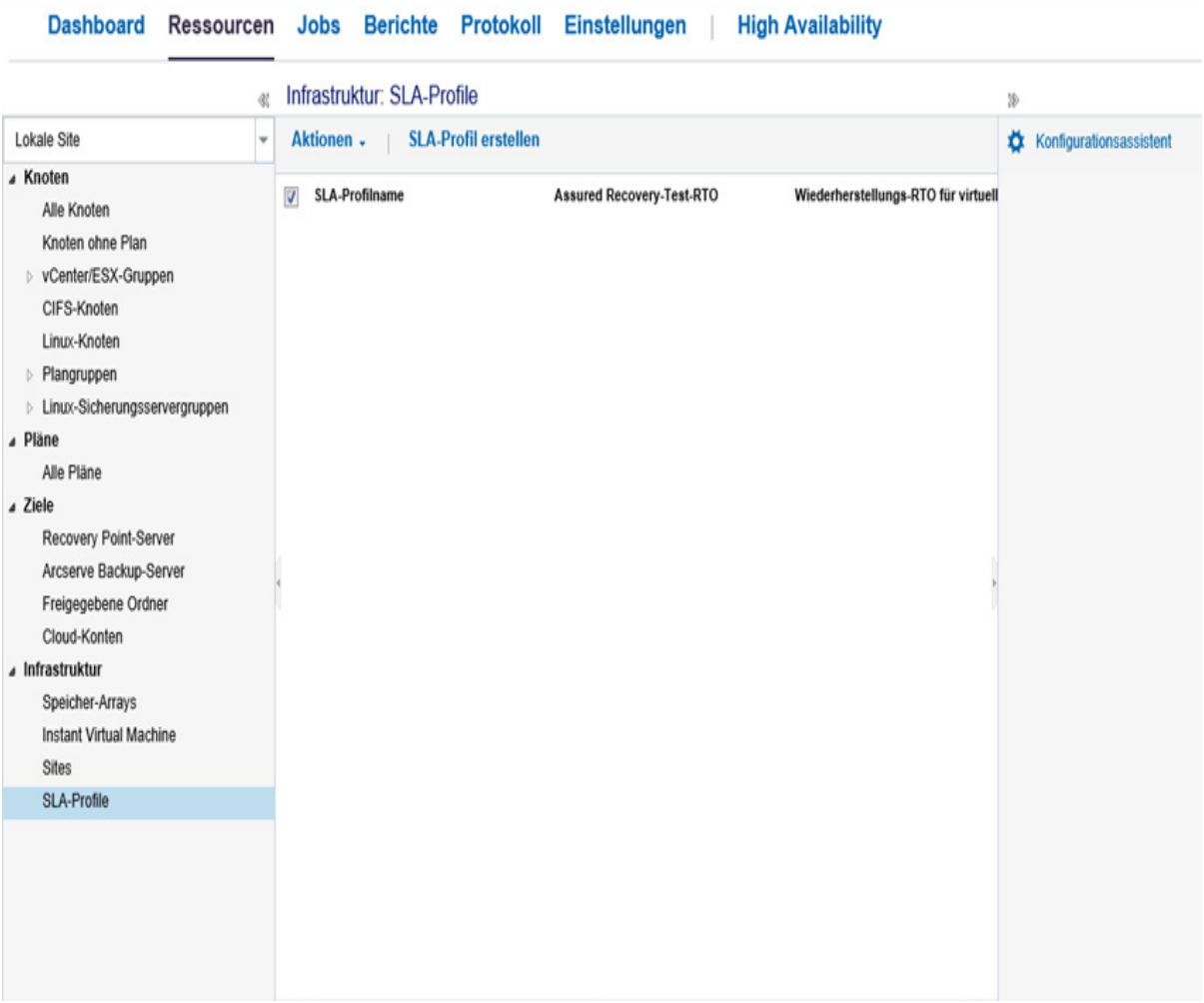
1. Erstellen von SLA-Profilen
2. Planen von E-Mails
3. Bericht per E-Mail senden
4. Erstellen von Berichten
5. Anpassen der Verweildauer in Tagen für einen Jobstatusbericht
6. Rohdatengröße im Bericht zur verwalteten Kapazität für hostbasierte agentenlose Sicherungen von VMs
7. Anzeigen tatsächlicher Werte an Quelle und Ziel für Jobtypen

Erstellen von SLA-Profilen

Sie müssen ein SLA-Profil erstellen, um RTO-Berichte zu generieren.

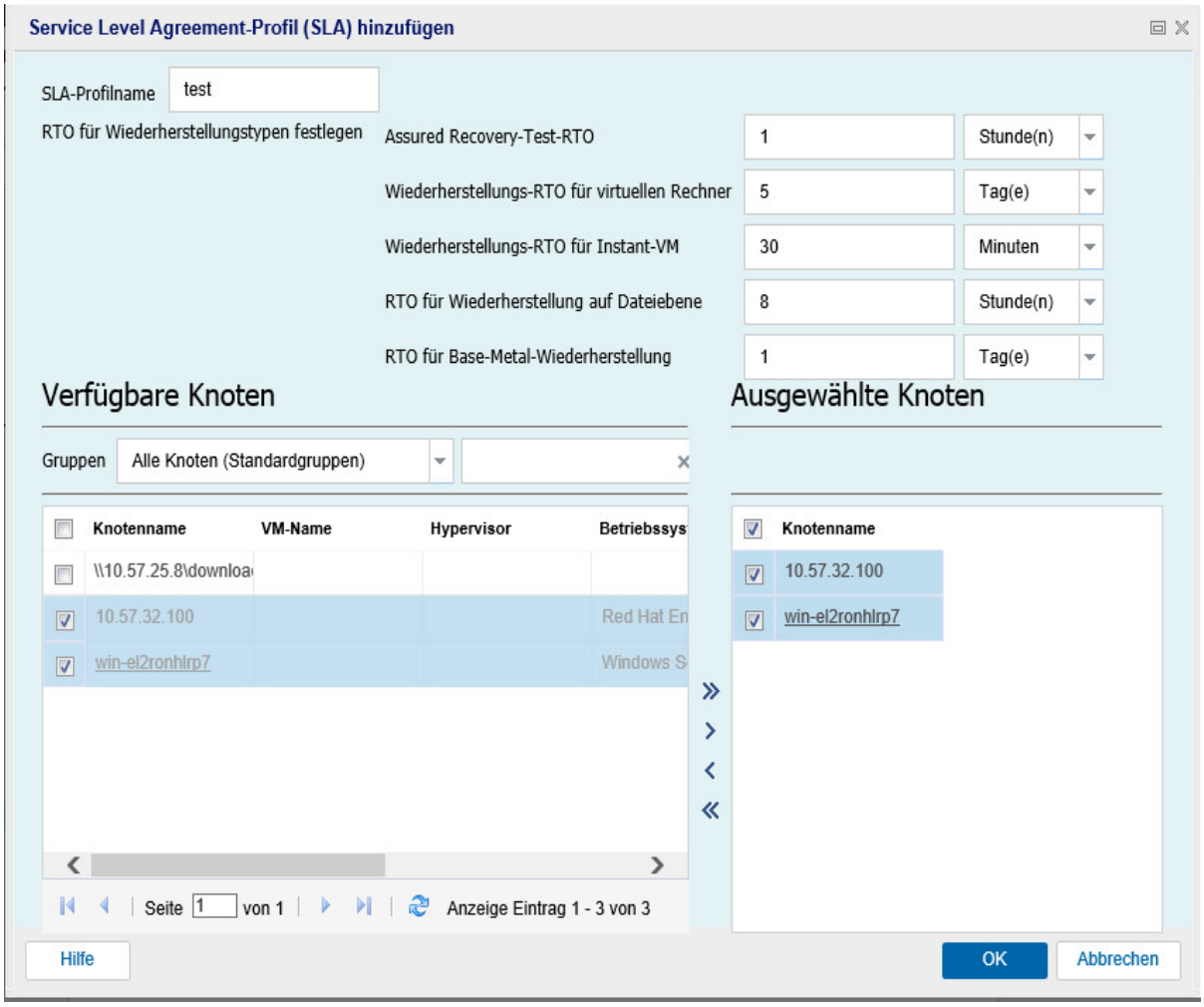
Gehen Sie wie folgt vor:

1. Navigieren Sie zum linken Fensterbereich der Registerkarte **Ressourcen**, und klicken Sie auf **Infrastruktur**>**SLA-Profil**.



2. Klicken Sie im mittleren Fensterbereich auf **Erstellen eines SLA-Profils**.

   Das Fenster zum **Hinzufügen des Service Level Agreement (SLA)-Profils** wird geöffnet.



3. Führen Sie im Fenster zum Hinzufügen des Service Level Agreement (SLA)-Profils die folgenden Schritte aus:

   a. Geben Sie einen **SLA-Profilnamen** ein.

   b. Geben Sie den Zeittyp und die Dauer für die gewünschten Optionen ein, um den **RTO für Wiederherstellungstypen festzulegen**.

      Hinweis: Bei allen Optionen können Sie die Zeit in Tagen, Stunden und Minuten auswählen.

   c. Aktivieren Sie im Abschnitt **Verfügbare Knoten** die Kontrollkästchen der Knoten, für die Berichte generiert werden sollen, und wechseln Sie zum Abschnitt **Ausgewählte Knoten**.

   d. Wählen Sie unter **Ausgewählte Knoten** einen oder mehrere Knoten aus, und klicken Sie auf **OK**.

Das SLA-Profil wird erstellt und unter dem SLA-Profilnamen hinzugefügt.

4. Um das vorhandene SLA-Profil zu ändern oder zu löschen, aktivieren Sie das Kontrollkästchen des entsprechenden Profils, und klicken Sie auf **Aktionen**.

Um sich über den Status aller definierten SLA-Profile zu informieren, zeigen Sie den **RTO**-Bericht über die Registerkarte **Berichte** an.

Planen von E-Mails

In Arcserve Unified Data Protection können Sie einen Ablaufplan erstellen, um Berichte per E-Mail an ausgewählte Empfänger zu senden.

Hinweis: Bevor Sie einen Ablaufplan für das Versenden einer E-Mail erstellen, konfigurieren Sie die E-Mail-Einstellungen. Weitere Informationen zur Konfiguration finden Sie unter "Konfigurieren von E-Mails und Alerts".

Sie können Ablaufpläne erstellen und bearbeiten.

Erstellen eines Ablaufplans

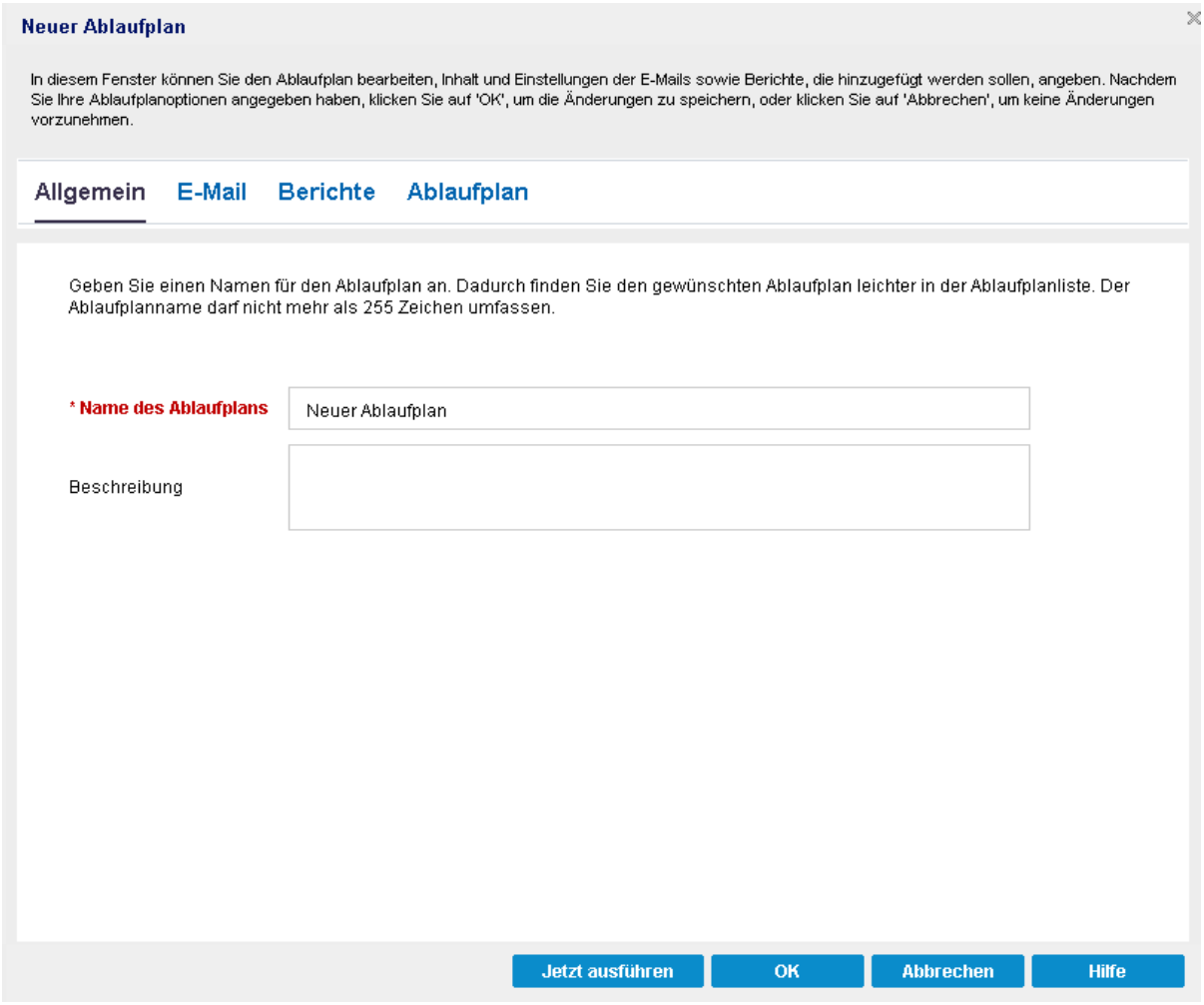
Sie können neue Ablaufpläne für den E-Mail-Bericht hinzufügen. Diese Bericht-E-Mails werden automatisch aktualisiert, erstellt und wie von Ihnen geplant gesendet. Sie können den Ablaufplan der Bericht-E-Mails anpassen. Die Anwendung lässt Sie die E-Mail-Inhalte festlegen, die anzuhängenden Berichte, die Empfänger der Berichte und das Datum und den Zeitpunkt, zu dem die Berichte gesendet werden sollen. Die ausgewählten Berichte werden innerhalb der E-Mail-Nachrichten mit ausführlichen Informationen im Tabellenformat angezeigt.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Arcserve Unified Data Protection an.
2. Klicken Sie in der Navigationsleiste auf **Berichte**.
3. Klicken Sie in der oberen rechten Ecke eines Berichts auf den globalen Abschnitt **Filter/Aktionen**.
4. Wählen Sie in der erweiterten Liste das E-Mail-Symbol aus, um das Dialogfeld **Planen, dass Berichte per E-Mail gesendet werden** zu öffnen.

   Das Dialogfeld **E-Mails planen** wird angezeigt.
5. Klicken Sie im Dialogfeld **E-Mails planen** auf **Neu**.

   Das Dialogfeld **Neuer Ablaufplan** wird angezeigt.



Die folgenden Registerkarten werden angezeigt:

- **Allgemein**: Geben Sie einen Namen und eine Beschreibung (optional) für den neuen Ablaufplan an.
- **E-Mail**: Geben Sie E-Mail-Einstellungen, Inhalt und Anhang für den E-Mail-Ablaufplan an.
- **Berichte**: Wählen Sie die spezifischen Berichte aus, die Sie zur E-Mail hinzufügen möchten.
- **Ablaufplan**: Geben Sie einen Ablaufplan für die E-Mail an.

6. Füllen Sie die erforderlichen Felder auf den einzelnen Registerkarten aus.
7. Klicken Sie auf **OK**, um den Ablaufplan zu speichern.

   Der neue Ablaufplan wird dem Dialogfeld **E-Mails planen** hinzugefügt.

   Hinweis: Klicken Sie nicht auf **OK**, wenn Sie den Bericht sofort anzeigen möchten.

8. (Optional) Um den Bericht sofort anzuzeigen, klicken Sie auf **Jetzt ausführen**.

   Der Bericht wird an die Empfänger gesendet.

Bearbeiten eines Ablaufplans

Mit Arcserve UDP können Sie Ablaufpläne aktualisieren, die Sie über die Ablaufplanerstellung hinzugefügt haben.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Arcserve Unified Data Protection an.
2. Klicken Sie auf die Registerkarte **Berichte**.
3. Klicken Sie auf den globalen Abschnitt **Filter/Aktionen**.
4. Wählen Sie in der erweiterten Liste das E-Mail-Symbol aus, um das Dialogfeld **E-Mails planen** zu öffnen.
5. Klicken Sie im Dialogfeld **E-Mails planen** auf **Bearbeiten**.

   Das Dialogfeld **Ablaufplan bearbeiten** wird angezeigt.
6. Aktualisieren Sie die Ablaufplandetails, und klicken Sie auf **OK**.

   Der aktualisierte Ablaufplan wird im Dialogfeld **E-Mails planen** angezeigt.

   Hinweis: Klicken Sie nicht auf **OK**, wenn Sie den Bericht sofort anzeigen möchten.
7. (Optional) Um den aktualisierten Bericht sofort anzuzeigen, klicken Sie auf **Jetzt ausführen**.

   Der Bericht wird an die Empfänger gesendet.

Senden von Berichten per E-Mail

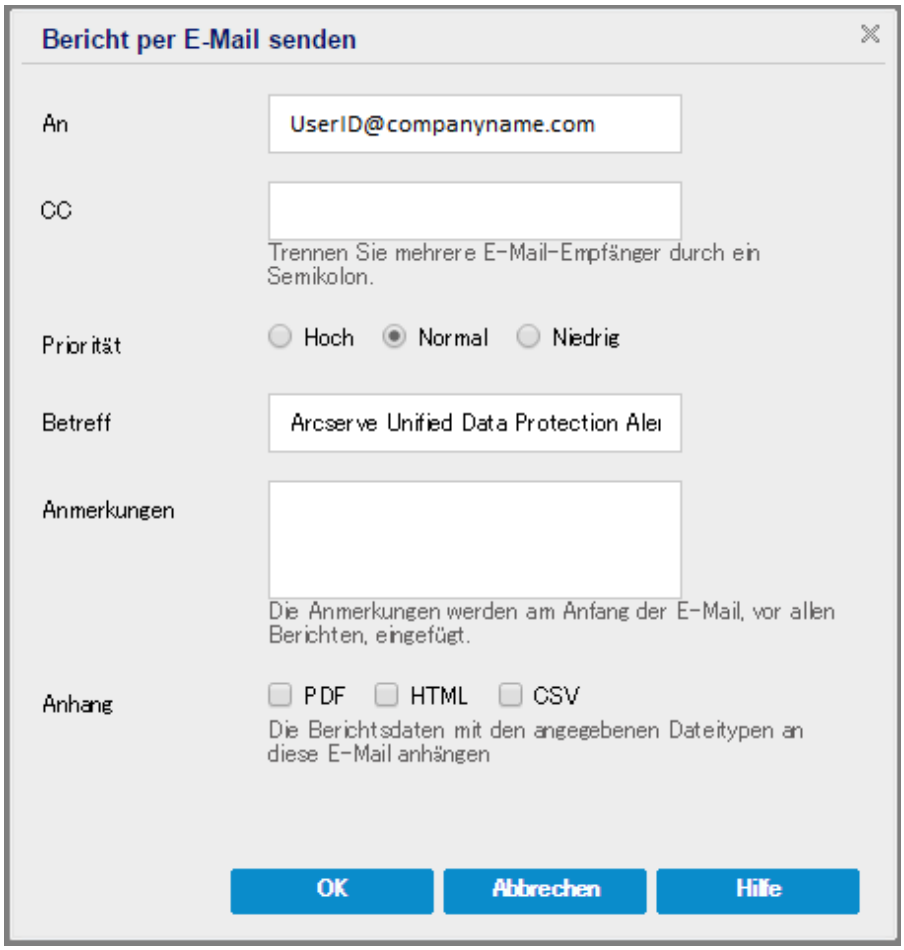
Mit Arcserve Unified Data Protection können Sie einzelne Berichte an spezifische Empfänger senden. Wenn Sie einen Bericht per E-Mail versenden, entspricht der Inhalt dem gedruckten Inhalt, und alle Diagramme werden als eingebettete Bilder gesendet.

Hinweis: Bevor Sie die Option **Bericht per E-Mail senden** verwenden, konfigurieren Sie die **E-Mail-Einstellungen**. Weitere Informationen zur Konfiguration finden Sie unter Konfigurieren von E-Mails und Alerts.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Arcserve Unified Data Protection an.
2. Klicken Sie in der Navigationsleiste auf **Berichte**, und wählen Sie einen der Berichte aus.
3. Klicken Sie auf den lokalen Abschnitt **Filter/Aktionen**, der unter dem Namen des ausgewählten Berichts verfügbar ist.
4. Wählen Sie in der erweiterten Liste das E-Mail-Symbol aus, um das Dialogfeld **Bericht per E-Mail senden** zu öffnen.

   Hinweis: Wenn die E-Mail-Konfiguration nicht abgeschlossen wurde, informiert Sie ein **Warnungsdialogfeld** darüber, dass keine E-Mail-Einstellungen angegeben wurden. Weitere Informationen zur Konfiguration finden Sie unter Konfigurieren von E-Mails und Alerts.



5. Füllen Sie die folgenden Felder aus:

   - **An** : Geben Sie den Empfänger der E-Mail an.

     Hinweis: Standardmäßig enthält dieses Feld die E-Mail-Adresse, die im E-Mail-Konfigurationsmodul angegeben wurde.

   - **CC** : Geben Sie weitere Empfänger an, denen Sie den Bericht per E-Mail zukommen lassen möchten. Trennen Sie die Adressen durch Strichpunkte.

   - **Priorität** : Geben Sie die Priorität der E-Mail an. Dieses Feld ist standardmäßig auf "Normal" gesetzt.

   - **Betreff**: Geben Sie den Betreff der E-Mail an. Dieses Feld enthält standardmäßig den ausgewählten Bericht.

   - **Kommentar**: (Optional) Geben Sie weitere Informationen an, die Sie teilen möchten.

   - **Anhang** : Wählen Sie die Formate für das Anhängen der Berichtsdaten aus.

6. Klicken Sie auf **OK**.

   Die E-Mail wurde erfolgreich gesendet.

Erstellen von Berichten

Auf der Registerkarte **Berichte** können Sie vordefinierte Berichte generieren. Sie können Berichte im CSV-, PDF- und HTML-Format generieren.

Gehen Sie wie folgt vor:

1. Navigieren Sie zur Registerkarte **Berichte**, und wählen Sie im linken Fensterbereich einen Bericht aus.
2. Klicken Sie auf die Drop-down-Liste für lokale **Filter/Aktionen**.
3. Geben Sie die Details in den Drop-down-Optionen für **Filter/Aktionen** an, oder wählen Sie sie aus.
4. Klicken Sie in der Drop-down-Liste der Schaltfläche **Speichern** auf **CSV**, **PDF** oder **HTML**.

   Hinweis: Große Bilder oder viele Daten auf einer Berichtsseite verdecken möglicherweise einige der Optionen, einschließlich der Schaltfläche "Speichern". Um diese Optionen anzuzeigen, klicken Sie auf "Erweitern".

Der Bericht wird im ausgewählten Format generiert.

Anpassen der Aufbewahrungszeit (Tage) für einen Jobstatus-Bericht

Die Standard-Aufbewahrungszeit für das Abrufen eines Jobstatus-Berichts ist 180 Tage. Sie können die Anzahl der Aufbewahrungstage in der Konfiguration ändern, die in der Datei "ConsoleConfiguration.xml" an folgendem Speicherort angegeben ist:

Programme\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml

Sie können die Anzahl an Aufbewahrungstagen in der Konfiguration gemäß Ihren Anforderungen ändern.

```
<PurgeConf>
<!-- retentionDays, Standardwert ist 180 (180 Tage).
Die Einheit ist Tage.
Anzahl an Tagen für die Aufbewahrung von Daten für die
Konsolendatenbank.-->
<retentionDays>180</retentionDays>
<!-- purgeHourOfDay, Standardwert ist 0 (0:00 Uhr).
Bereinigungsjob jeden Tag um diese Uhrzeit ausführen.-
->
<purgeHourOfDay>0</purgeHourOfDay>
</PurgeConf>
```

Rohdatengröße im Bericht zur verwalteten Kapazität für hostbasierte agentenlose Sicherungen von VMs

Sie können die folgenden Registrierungen auf Proxy-Ebene oder VM-Ebene konfigurieren:

Auf Proxy-Ebene für alle vom aktuellen Proxy geschützten VMs:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

"CountNtfsVolumeSize"=dword:00000001

"ReportZeroIfHavingNonNtfsVolume"=dword:00000001

"BackupZeroBlock"=dword:00000001

Auf VM-Ebene für eine bestimmte VM:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\{VM UUID}]

"CountNtfsVolumeSize"=dword:00000001

"ReportZeroIfHavingNonNtfsVolume"=dword:00000001

"BackupZeroBlock" = DWORD: 00000001

Hinweis: Die Registrierung auf VM-Ebene hat Vorrang vor der Registrierung auf Proxy-Ebene.

Die folgenden Verhalten werden beobachtet:

Registrierungsschlüssel	Standardeinstellung	Mögliche Werte	Zweck	Zusätzliche Informationen
GetVMGuestVolumeUsedSize	0	0 oder 1	Gibt an, ob der belegte Speicherplatz aller Volumes einer VM gezählt werden soll. 0 - zählt die Größe der	

			VMDK-Datei des virtuellen Rechners als die Rohdatengröße der VM. 1 - Ermittelt lediglich den verwendeten Speicherplatz der Volumes. **Hinweis:** Bei Windows-Gästen werden nur NTFS-Volumes berücksichtigt. Für Linux-Gäste zählen alle Volumes.	
ReportZeroIfHavingNonNtfsVolume	0	0 oder 1	Bestimmt das Verhalten für die Spalte zur Rohdatengröße im Bericht zur verwalteten Kapazität beim Vorliegen von nicht-NTFS-Volume(s) auf den virtuellen Com-	1. Ignoriert, wenn GetVMGuestVolumeUsedSize = 0 2 gilt nur für Windows VM

			putern. 0 - Die Größe von nicht-NTFS-Volume(s) zählt nicht als Teil der Spalte ROH-Datengröße. 1- die allgemeine Rohdatengröße wird beim Vorliegen von nicht-NTFS-Volume(s) auf dem virtuellen Computer als 0 angezeigt	
BackupZeroBlock	0	0 oder 1	Gibt an, ob alle Nulldatenblöcke in das Sicherungsziel geschrieben werden sollen. 1 - schreibt Null Datenblöcke auf das Sicherungsziel. 0 - ignoriert die Null Datenblöcke als Teil der Sicherung.	1. Ignoriert, wenn GetVMGuestVolumeUsedSize = 1 2. Wenn geändert, wird der Wert nur nach einer vollständigen Sicherung wirksam

Beispiel

Eine VM verfügt über eine Thin Provisioning-Partition mit der bereitgestellten Größe 1000 GB. Die Größe der VMDK-Datei des virtuellen Datenträgers beträgt 800 GB, von denen 200 GB an Datenblöcken reine Nulldatenblöcke sind. Auf dem Gast-BS dieser VM befinden sich 2 NTFS-Volumes, welche jeweils 100 GB und 200 GB belegen, sowie 1 FAT32-Volume mit einer Speicherplatzbelegung von 1 GB.

Schlüsselnamen	Standardwerte	Benutzerdefinierte Werte	Benutzerdefinierte Einstellung	Benutzerdefinierte Werte
GetVMGuestVolumeUsedSize	0	0	1	1
ReportZeroIfHavingNonNtfsVolume	N/V	N/V	1	1
BackupZero Block	0	1	N/V	N/V
Erwartete Rohdatengröße	600 GB (ausgenommen Null Datenblöcke)	800 GB (einschließlich Null Datenblöcke)	300 GB	0

Anzeigen tatsächlicher Werte an Quelle und Ziel für Jobtypen

In der folgenden Tabelle werden die tatsächlichen Werte an Quelle und Ziel für alle Jobtypen beschrieben, um den Jobstatusbericht verständlich zu machen:

Jobtyp	Tatsächlicher Wert an der Quelle	Tatsächlicher Wert am Ziel	Kommentare
FS-Sicherung in Datenspeicher (mit/ohne Deduplizierung): Windows, Linux-Knoten	Nicht verfügbar (N/V)	Angezeigt wie erwartet	
FS-Sicherung in Netzwerkfreigabe	N/V	Angezeigt wie erwartet	
FS-Wiederherstellung aus Netzwerkfreigabe	N/V	N/V	
CIFS-Sicherungsjobs – Datenspeicher ohne Deduplizierung	N/V	Angezeigt wie erwartet	
CIFS-Wiederherstellungsjobs – Datenspeicher ohne Deduplizierung	Angezeigt wie erwartet	N/V	
FS-Wiederherstellung aus Datenspeicher (mit/ohne Deduplizierung)	Angezeigt wie erwartet	N/V	
Dateikopie aus Datenspeicher (mit/ohne Deduplizierung), Dateikopie aus Replikationsdatenspeicher	Angezeigt wie erwartet	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
Dateiarchiv aus Datenspeicher (mit/ohne Deduplizierung), Dateiarchiv aus Replikationsdatenspeicher	Angezeigt wie erwartet	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
Dateikopie/Dateiarchiv in Netzwerkfreigabe	N/V	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
Wiederherstellung aus Dateikopie/Dateiarchiv	N/V	N/V	**Hinweis:** Hier werden die Spalten "Geschützte

			Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
Löschen von Dateiarchiv	N/V		**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
FS-Katalogjob (agen-tenbasiert/agentenlos)	Angezeigt wie erwartet	N/V	
CRP aus Datenspeicher (mit-/ohne Deduplizierung)	Angezeigt wie erwartet	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
CRP aus Netzwerkfreigabe, lokal	N/V	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
CRP-Wiederherstellung in Netzwerkfreigabe, lokal	N/V	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
IVM-Jobs	Angezeigt wie erwartet	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
Assured Recovery-Jobs	Angezeigt wie erwartet	N/V	
Bare-Metal-Recovery (BMR) aus Datenspeicher (mit/ohne Deduplizierung)	Angezeigt wie erwartet	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
Virtual Standby-Jobs	Angezeigt wie erwartet	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt

Jobs "Auf Band kopieren"	Angezeigt wie erwartet	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
Replikationsjobs, standortübergreifende Replikationsjobs	Angezeigt wie erwartet	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
MSP-Replikationsjobs	Angezeigt wie erwartet	Angezeigt wie erwartet	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
RPS Jumpstart aus Netzwerkfreigabe	Angezeigt wie erwartet	N/V	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt
RPS Jumpstart (Datenspeicher mit/ohne Deduplizierung)	Angezeigt wie erwartet	Angezeigt wie erwartet	**Hinweis:** Hier werden die Spalten "Geschützte Daten", "Verwendeter Speicher" ebenfalls als "N/V" angezeigt

Kapitel 7: Verwalten von High Availability

In diesem Abschnitt werden die folgenden Themen behandelt:

Funktionsweise von High Availability

In Unified Data Protection können Sie Arcserve High Availability-Funktionen über die Registerkarte **High Availability** überwachen und verwalten. Um diese Funktionen zu verwalten, müssen Sie sich zuerst bei "Steuerungsdienst" anmelden. Wenn Sie zum ersten Mal auf die Registerkarte **High Availability** klicken, wird das Dialogfeld **Steuerungsdienst hinzufügen** geöffnet. Dieses Dialogfeld wird später nicht mehr angezeigt.

Verwalten von Steuerungsdiensten für High Availability

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **High Availability**.

   Das Dialogfeld **Steuerungsdienst hinzufügen** wird geöffnet.

2. Geben Sie die Details zum Steuerungsdienst wie IP-Adresse, Kontonamen, Kennwort, Protokoll und Portnummer ein.

3. Klicken Sie auf **OK**.

   Der angegebene Steuerungsdienst wird im linken Fensterbereich unter Steuerungsdienste und Szenarien hinzugefügt. Um den Steuerungsdienst zu ändern oder zu löschen, wählen Sie den Steuerungsdienst aus, und klicken Sie mit der rechten Maustaste darauf, um die Optionen anzuzeigen. Sie können auch einen Steuerungsdienst im mittleren Fensterbereich auswählen und auf **Aktionen** klicken, um den Steuerungsdienst zu ändern oder zu löschen. Alternativ können Sie im Navigationsbereich mit der rechten Maustaste auf den Steuerungsdienst klicken.

   Hinweis: Blenden Sie den Steuerungsdienst ein, um Szenarien, Gruppen und weitere Details anzuzeigen.

Verwalten von High Availability-Lizenzen

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **High Availability**.
2. Klicken Sie im linken Bereich auf **Steuerungsdienste und Szenarien**.

   Die Seite **Steuerungsdienste und Szenarien** wird angezeigt.
3. Wählen Sie den Steuerungsdienst aus, und klicken Sie auf **Registrieren**.

   Das Dialogfeld **Registrieren** wird geöffnet.
4. Geben Sie den Registrierungsschlüssel ein
5. Klicken Sie auf **OK**.

   Die Lizenz ist registriert.

Verwalten von Szenarien

Mit Arcserve Unified Data Protection können Sie Ihre vorhandenen HA-Szenarien verwalten und Gesamtsystemszenarien erstellen. Sie können auch Szenariogruppen erstellen, um Ihre Szenarien zu organisieren. In den folgenden Abschnitten wird beschrieben, wie Sie HA-Szenarien verwalten:

- Verwalten von Szenariogruppen
- Erstellen von Gesamtsystemszenarien
- Verwalten von Szenarien
- Bearbeiten von Szenarien
- Verwalten von Szenario-Hosts
- Vorgänge auf Szenarien
- BMR und umgekehrte Replikation
- Überwachungsszenarien

Verwalten von Szenariogruppen

Mit Arcserve Unified Data Protection können Sie Gruppen in einem Steuerungsdienst verwalten. Sie können Gruppen hinzufügen, umbenennen, löschen, kennzeichnen und Kommentare posten.

Gehen Sie wie folgt vor:

1. Wählen Sie im linken Fensterbereich einen verwalteten Steuerungsdienst aus.

   Alle Gruppen im Steuerungsdienst werden im mittleren Fensterbereich aufgelistet.

2. Klicken Sie auf das Drop-down-Menü **Aktionen** und anschließend auf eine der folgenden Optionen:

   Szenariogruppe hinzufügen

   Erstellt eine Gruppe.

   Wählen Sie eine Gruppe aus, um folgende Aktionen auszuführen:

   Szenariogruppe umbenennen

   Benennt die Gruppe um.

   Szenariogruppe entfernen

   Löscht die Gruppe. Sie können keine Gruppe entfernen, wenn Sie Szenarien innerhalb der Gruppe haben.

   Flag und Kommentar

   Markiert die Gruppe in verschiedenen Farben, und ermöglicht es Ihnen, Kommentare für das Flag hinzuzufügen. Verwenden Sie Flags, um Ihre Gruppe persönlich anzupassen und einfach zu identifizieren.

3. Optional können Sie im linken Fensterbereich mit der rechten Maustaste auf eine Gruppe klicken, um eine Gruppe zum ausgewählten Steuerungsdienst hinzuzufügen, sie daraus zu löschen oder eine Gruppe umzubenennen.

   Die Gruppe wird hinzugefügt oder basierend auf Ihrer Auswahl aktualisiert.

Erstellen von Gesamtsystemszenarien

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Bereich auf **Steuerungsdienste und Szenarien**, und klicken Sie dann auf einen verwalteten Steuerungsdienst.

   Alle Szenariogruppen im Steuerungsdienst werden aufgelistet.

2. Klicken Sie auf eine Szenariengruppe.

   Die Seite **Szenarien** wird im mittleren Fensterbereich angezeigt.

3. Klicken Sie im mittleren Fensterbereich auf **Szenario erstellen**.

   Hinweis: Optional können Sie im linken Fensterbereich mit der rechten Maustaste klicken und anschließend auf **Szenario erstellen** klicken.

   Der Assistent für das **Erstellen eines Gesamtsystems** wird geöffnet, und das Dialogfeld **Server- und Produkttyp auswählen** wird geöffnet.

4. Geben Sie den Szenarionamen ein, wählen Sie den Produkttyp aus, und geben Sie an, ob Sie einen AR-Test durchführen möchten.

5. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Master- und Replikat-Host** wird angezeigt.

6. Geben Sie die Details zu Master und Replikat ein.

7. Klicken Sie auf **Weiter**.

   Wenn Sie die Option **Prozess auf Hosts überprüfen** aktiviert haben, werden die Prozesse auf den Hosts überprüft. Sie können auch Prozesse auf den Hosts installieren oder Prozesse von den Hosts deinstallieren.

8. Klicken Sie nach der Überprüfung der Prozesse auf **Weiter**.

   Das Dialogfeld **Volumeeinstellung** wird geöffnet.

9. Wählen Sie die zu schützenden Volumes aus.

   Hinweis: Wenn Sie die Option **Ausschlussverzeichnis und -dateien aktivieren** auswählen, werden die Dateien und Ordner "pagefile.sys", "hyberfil.sys", "system volume information", "Recycler" und "Recycled" standardmäßig gefiltert.

10. Klicken Sie auf **Weiter**.

    Das Dialogfeld **Ressourcenpool-Auswahl** wird geöffnet. Sie können den Ressourcenpool auswählen, in dem sich die VM nach dem Switchover oder während des AR-Tests befindet.

11. Klicken Sie auf **Weiter**.

    Das Dialogfeld **Speicherauswahl** wird eingeblendet.

12. Wählen Sie den Datenspeicher aus, um den virtuellen Rechner zu speichern. Wählen Sie optional die Option **Speicherplatz nach Bedarf zuordnen und übergeben (bei dynamischem Datenträger)** aus. Die generierte VM verwendet Thin Provision für die virtuellen Datenträger, wenn Sie diese Option auswählen.
13. Klicken Sie auf **Weiter**.

    Das Dialogfeld **Szenarioeigenschaften** wird geöffnet.
14. Erweitern Sie die Eigenschaften, ändern Sie sie nach Bedarf, und klicken Sie dann auf **Weiter**. Weitere Informationen finden Sie im Arcserve RHA-Administratorhandbuch.

    Das Dialogfeld **Master- und Replikateigenschaften** wird angezeigt.
15. Überprüfen Sie die Master- und Replikateigenschaften, und klicken Sie dann auf **Klicken Sie hier, um die Zuordnungen physischer Netzwerke zu bearbeiten**.

    Das Dialogfeld **High Availability-Netzwerkadapterzuordnung** wird geöffnet.

    Hinweis: Sollte sich sowohl auf dem Master- als auch auf dem Replikatserver lediglich ein Adapter für virtuelle Netzwerke befinden, werden diese automatisch zugeordnet.
16. Führen Sie die folgenden Schritte aus:
    a. Wählen Sie unter **Replikat-Netzwerkadapter** per Klick den Adapter aus, der dem aufgelisteten Adapter in der Spalte "Master-Netzwerkadapter" zugeordnet werden soll.
    b. Wählen Sie unter **Masteradapterinformationen anwenden** aus, ob der Masteradapter sich im DHCP-Modus befindet. (Standard)
    c. Wählen Sie unter **Adapterinformationen benutzerdefiniert anpassen** die Option aus, um die Einstellung "IP-Adresse", "Gateways", "DNS-Server" und "WINS-Server" zu aktivieren. "IP-Adresse", "Gateways", "DNS-Server" und "WINS-Server" können nach Bedarf hinzugefügt oder entfernt werden.
17. Klicken Sie auf "OK", um das Dialogfeld **Netzwerkadapter-Zuordnung** zu schließen, und klicken Sie auf **Weiter**, um fortzufahren.

    Das Dialogfeld **Switchover-Eigenschaften** wird geöffnet.
18. Erweitern Sie **Netzwerkverkehrsumleitung** sowie andere Eigenschaften, um die Werte zu überprüfen, und klicken Sie auf **Weiter**.

    Das Dialogfeld **Initiierung von Switchover und umgekehrter Replikation** wird eingeblendet.
19. Geben Sie den Switchover-Typ ein. Für Gesamtsystemszenarien ist die umgekehrte Replikation manuell.

20. Klicken Sie auf **Weiter**.

    Warten Sie, bis der Szenarioüberprüfungsvorgang abgeschlossen ist und das Dialogfeld **Szenarioüberprüfung** geöffnet wird.

    Sollte die Szenarioüberprüfung Fehler anzeigen, müssen Sie diese korrigieren, bevor Sie fortfahren können. Werden Warnungen angezeigt, sollten Sie auf diese ebenfalls entsprechend reagieren, um erfolgreich fortfahren zu können. Wenn Sie Änderungen vorgenommen haben, klicken Sie auf **Wiederholen**, um eine erneute Überprüfung durchzuführen.

21. Klicken Sie auf **Weiter**.

    Das Dialogfeld **Szenarioausführung** wird geöffnet.

22. Klicken Sie auf **Fertig stellen**, um die aktuellen Einstellungen zu speichern und das Szenario später auszuführen.

    Optional kann das Szenario sofort ausgeführt werden, indem Sie **Jetzt ausführen, nach dem Klicken auf die Schaltfläche 'Fertig stellen'** aktivieren und anschließend auf **Fertig stellen** klicken.

    Wählen Sie **Volumesynchronisation** für Gesamtsystemszenarien aus.

    Das Szenario wird erstellt.

Verwalten von Szenarien

Wenn Sie einen verwalteten Steuerungsdienst aus dem linken Fensterbereich auswählen, werden alle Szenarien in diesem Steuerungsdienst im mittleren Fensterbereich angezeigt. Die Szenarien werden inklusive Typ, Status, Produkt und Modus aufgelistet. Die Statistiken für RPO/RTO, Master-Spool-Verwendung und Synchronisationsfortschritt werden ebenfalls hier aufgelistet. Wenn Sie ein Szenario auswählen, können Sie verschiedene Vorgänge wie Löschen, Umbenennen, Kennzeichnen oder Kommentieren dafür durchführen.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Bereich auf **Steuerungsdienste und Szenarien**, und klicken Sie dann auf einen verwalteten Steuerungsdienst.

   Alle Szenariogruppen im Steuerungsdienst werden im mittleren Fensterbereich aufgelistet.

2. Klicken Sie im linken Fensterbereich auf eine Szenariogruppe.

   Die Szenarien in der Szenariogruppe werden im mittleren Fensterbereich aufgelistet.

3. Wählen Sie ein Szenario aus.

4. Klicken Sie auf das Drop-down-Menü **Aktionen** und anschließend auf eine der folgenden Optionen:

   Szenario umbenennen

   Benennt das Szenario um.

   Szenario entfernen

   Löscht das Szenario.

   Sie können keine Gruppe entfernen, wenn Sie Szenarien innerhalb der Gruppe haben.

5. Optional können Sie im linken Fensterbereich mit der rechten Maustaste auf ein Szenario klicken, um das Szenario zu entfernen oder umzubenennen.

   Das Szenario wird aktualisiert.

Bearbeiten von Szenarien

Mit Arcserve Unified Data Protection können Sie die Eigenschaften von Szenarien im angehaltenen Status bearbeiten. Sie können Hosts einfügen, umbenennen oder löschen und die Topologie eines Szenarios ändern.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Bereich auf **Steuerungsdienste und Szenarien**, und klicken Sie dann auf einen verwalteten Steuerungsdienst.

   Alle Szenariogruppen im Steuerungsdienst werden im mittleren Fensterbereich aufgelistet.

2. Klicken Sie im linken Fensterbereich auf eine Szenariogruppe, und klicken Sie dann auf ein Szenario.

   Die Seite "<Szenariogruppe>:<Szenario>" wird angezeigt.

3. Wählen Sie einen Host aus dem Szenario aus.

4. Klicken Sie auf die Registerkarte **Eigenschaften**, und wählen Sie eine der folgenden Optionen aus der Drop-down-Liste aus.

   Szenarioeigenschaften

   Aktualisiert die Szenarieneigenschaften.

   HA-Eigenschaften

   Aktualisiert die High Availability-Eigenschaften.

   Host-Eigenschaften

   Aktualisiert die Hosteigenschaften.

   Stammverzeichnisse

   Aktualisiert die Stammverzeichnisse.

   Hinweis: Dies gilt nur für Gesamtsystemszenarien.

5. Klicken Sie im Drop-down-Menü **Aktionen** auf **Speichern**.

   Die Szenarioeigenschaften werden aktualisiert.

   Bearbeiten der virtuellen Plattformeinstellungen für ein angehaltenes Gesamtsystemszenario:

   Gehen Sie wie folgt vor:

1. Wählen Sie einen Replikat-Host aus dem Szenario aus.

2. Klicken Sie auf die Registerkarte **Eigenschaften**, und wählen Sie in der Drop-down-Liste die Option **Host-Eigenschaften** aus.

3. Erweitern Sie **Virtueller Rechner**, und klicken Sie auf **Klicken Sie hier, um Einstellungen der virtuellen Plattform zu bearbeiten**.

   Der Assistent **Einstellungen der virtuellen Plattform** wird geöffnet.

4. Wählen Sie den **Typ der virtuellen Plattform** und die verknüpfte IP-Adresse oder den Hostnamen aus.
5. Wählen Sie den Ressourcenpool für ESX und vCenter oder den Hostserver für Citrix Xen aus.
6. Wählen Sie den Speicher aus. Durchsuchen Sie bei Hyper-V die Verzeichnisse, und wählen Sie den Speicherort der VM auf dem Hyper-V-Server aus.
7. Klicken Sie auf **Fertig stellen**.

Bearbeiten der Netzwerkadapter-Zuordnung für High Availability oder Assured Recovery:

Gehen Sie wie folgt vor:

1. Wählen Sie den Replikat-Host aus dem Szenario aus.
2. Klicken Sie auf die Registerkarte **Eigenschaften**, und wählen Sie in der Drop-down-Liste die Option **Host-Eigenschaften** aus.
3. Erweitern Sie **Virtueller Rechner** und **Einstellungen des virtuellen Rechners**.
4. Klicken Sie für die Eigenschaft **High Availability-Netzwerkadapterzuordnung** oder **Assured Recovery-Netzwerkadapterzuordnung** auf **Klicken Sie hier, um die Zuordnungen physischer Netzwerke zu bearbeiten**.

   Das Dialogfeld **High Availability-Netzwerkadapterzuordnung** wird geöffnet.

5. Wählen Sie die Replikat-Netzwerkadapter aus, um den Master-Netzwerkadapter zuzuordnen.

   Sie können die Adapterinformationen des Replikatadapters anpassen, indem Sie die IP-Adresse, Gateways, DNS-Server und WINS-Server einbeziehen.

6. Klicken Sie auf **OK**.

   Die Zuordnungen sind geändert und gespeichert.

Verwalten von Szenario-Hosts

Sie können Hosts in einem Szenario einfügen, löschen und umbenennen.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Bereich auf **Steuerungsdienste und Szenarien**, und klicken Sie dann auf einen verwalteten Steuerungsdienst.

   Alle Szenariogruppen im Steuerungsdienst werden im mittleren Fensterbereich aufgelistet.

2. Klicken Sie im linken Fensterbereich auf eine Szenariogruppe, und klicken Sie dann auf ein Szenario.

   Die Seite "<Szenariogruppe>:<Szenario>" wird angezeigt.

3. Wählen Sie einen Host aus dem Szenario aus.

4. Klicken Sie auf das Drop-down-Menü **Bearbeiten** und anschließend auf eine der folgenden Optionen:

   Host einfügen

   Fügt einen untergeordneten Host zum ausgewählten Host im Szenario hinzu.

   Host entfernen

   Löscht den ausgewählten Host aus dem Szenario.

   Host umbenennen

   Benennt den ausgewählten Host im Szenario um.

   Speichern

   Speichert alle Änderungen an den Szenarioeigenschaften.

   Aktualisieren

   Aktualisiert alle Änderungen.

   Die Szenarioeigenschaften sind bearbeitet.

Vorgänge auf Szenarien

Sie können verschiedene Vorgänge auf den Szenarien ausführen.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Bereich auf **Steuerungsdienste und Szenarien**, und klicken Sie dann auf einen verwalteten Steuerungsdienst.

   Alle Szenariogruppen im Steuerungsdienst werden im mittleren Fensterbereich aufgelistet.

2. Klicken Sie im linken Fensterbereich auf eine Szenariogruppe, und klicken Sie dann auf ein Szenario.

   Die Seite "<Szenariogruppe>:<Szenario>" wird angezeigt.

3. Klicken Sie auf das Drop-down-Menü **Aktionen** und anschließend auf eine der folgenden Optionen:

   Ausführen

   Nachdem Sie ein Szenario erstellt haben, müssen Sie es ausführen, um die Replikation zu starten. Üblicherweise müssen Master und Replikat zunächst synchronisiert werden, damit Datenänderungen auf dem Master auf dem Replikat repliziert werden können. Daher ist der erste Schritt beim Start der Replikation die Synchronisation von Master- und Replikatservern. Nach der Synchronisation der Server wird automatisch eine Online-Replikation gestartet, und der Replikatserver wird kontinuierlich mit allen Änderungen, die auf dem Master stattfinden, aktualisiert.

   Ausführen (Bewertungsmodus)

   Im Bewertungsmodus können Sie die Bandbreite und das Komprimierungsverhältnis, die für die Replikation erforderlich sind, präzise ermitteln, ohne die Daten tatsächlich zu replizieren. Wenn Sie diesen Befehl ausführen, werden statistische Daten gesammelt, ohne dass eine Replikation durchgeführt wird. Sobald die Bewertung beendet wird, wird ein Bericht erstellt.

   Anhalten

   Sie müssen laufende Szenarien anhalten, um Eigenschaften festzulegen oder zu ändern. Sie könnten Szenarien in ausgeführtem Status und im Bewertungsmodus anhalten.

   Synchronisieren

Synchronisation ist ein Prozess, über den Daten in Master und Replikat konsistent gehalten werden. Aktiviert die Synchronisation (unabhängig vom Ausführungsstatus der Replikation).

Vergleichsbericht

Ein Vergleichsbericht vergleicht die Unterschiede zwischen dem Master und den Replikat zu einem bestimmten Zeitpunkt. Der Vergleich wird mit denselben Algorithmen durchgeführt, die für die Synchronisation verwendet werden. Es werden jedoch keine Daten übertragen. Vergleichsberichte werden für jedes Replikat erstellt und am Ende des Vorgangs an den Manager gesendet. Dieser Bericht kann jederzeit erstellt werden.

Durchführen des Switchovers

Switchover (oder Failover) ist der Prozess, in dem Master und Replikat ihre Rollen wechseln. Dadurch wird der Masterserver zum Standby-Server und der Replikatserver zum aktiven Server.

Aktiven Server wiederherstellen

Wenn der Switchover-Vorgang nicht ordnungsgemäß abgeschlossen wurde, können Sie über den Vorgang "Aktiven Server wiederherstellen" manuell auswählen, welcher Server als aktiver Server fungieren soll.

"Ist aktiv"-Überprüfung anhalten

Unterbricht die "Ist aktiv"-Überprüfung, mit der überprüft wird, ob der aktive Server in Betrieb ist. Sie können diese Überprüfung für laufende HA-Szenarien manuell unterbrechen und wiederaufnehmen.

Replikat-Integritätstest

Mit der Option "Assured Recovery" kann ein vollständig automatischer Test der Wiederherstellbarkeit von Daten auf Replikatservern durchgeführt werden. Der getestete Replikatserver übernimmt bei Ausfällen die Funktion des Produktionsservers. Die Option "Assured Recovery" stellt einen vollumfänglichen Test des tatsächlichen Servers, der Anwendungen und Aktionen dar, die erforderlich sind, wenn der Replikatserver zum aktiven Server wird und dessen Funktionen übernehmen muss.

Virtuellen Rechner starten/anhalten

Verwenden Sie diesen Vorgang, um einen virtuellen Rechner mit dem Zustand des letzten Systemstatus oder einer Markierung zu starten oder anzuhalten. Sie können einen virtuellen Rechner starten oder anhalten, nachdem Sie ein Szenario erstellt und Master und Replikat synchronisiert haben. Verwenden Sie diese Funktion, wenn das Szenario nicht ausgeführt wird. Diese Funktion ist ver-

fügbar für vollständige Disaster Recovery- und High Availability-Szenarien. Starten/Anhalten ist eine Umschaltfläche im Menü.

Replikation unterbrechen

Die Aktualisierung auf dem Replikat-Host wird unterbrochen, um Wartungsarbeiten am System oder andere Arten der Verarbeitung vorzunehmen, bei denen die replizierten Daten auf dem Computer nicht geändert werden. Änderungen werden weiterhin erfasst, jedoch erst nach Wiederaufnahme der Replikation übermittelt und auf dem unterbrochenen Replikatserver angewendet. Während der Synchronisation kann die Replikation nicht unterbrochen werden.

Alle VM-Ressourcen löschen

Wenn Sie ein Gesamtsystemszenario ausführen, werden einige temporäre Ressourcen wie Datenträgerdateien, Snapshots und andere Dateien erstellt. Dieser Vorgang lässt Sie diese Ressourcen löschen und ist verfügbar, wenn das Szenario nicht ausgeführt wird.

Daten wiederherstellen

Stellt verloren gegangene oder beschädigte Masterdaten über einen Replikatserver durch eine Synchronisation in umgekehrter Richtung wieder her.

Rücklaufmarkierung setzen

Eine Markierung ist ein Checkpoint, der von Hand festgelegt wird, um einen Status zu kennzeichnen, zu dem Sie zurückkehren können. Diese manuelle Einstellung wird als Rücklaufmarkierung bezeichnet. Markierungen sollten vor jeder Aktivität gesetzt werden, die zu instabilen Daten führen kann. Markierungen werden in Echtzeit gesetzt und nicht für vergangene Ereignisse.

Der ausgewählte Vorgang wird ausgeführt.

BMR und umgekehrte Replikation

Mit Arcserve Unified Data Protection können Sie BMR und umgekehrte Replikation für Ihre Gesamtsystemszenarien verarbeiten.

Gehen Sie wie folgt vor:

1. Bereiten Sie einen Bare-Metal-Rechner vor, indem Sie den Computer über die BMR-CD starten.
2. Wählen Sie das Gesamtsystemszenario aus, und klicken Sie im Drop-down-Menü **Aktionen** auf **Wiederherstellen**.

   Der **Assistent zum Wiederherstellen von Daten** wird geöffnet.
3. Befolgen Sie die Anweisungen in den Fenstern des Assistenten, um das Wiederherstellungsszenario zu erstellen und auszuführen.

   Hinweis: Wenn die Volumes für Quelle und Ziel automatisch zugeordnet werden, ist die benutzerdefinierte Volume-Zuordnung auf der Seite **Volume-Zuordnung** deaktiviert. Um die benutzerdefinierte Volume-Zuordnung zu aktivieren, klicken Sie auf **Löschen**, um die vorhandene Zuordnung zu entfernen. Klicken Sie mit der rechten Maustaste auf das ausgewählte Volume, und wählen Sie **Benutzerdefinierte Volume-Zuordnung** aus, um das Dialogfeld **Volumegröße ändern** zu öffnen und die Größe bedarfsgerecht zu ändern.

Um die umgekehrte Replikation auszuführen, gehen Sie folgendermaßen vor:

1. Bereiten Sie einen Bare-Metal-Rechner vor, indem Sie den Computer über die BMR-CD starten.
2. Wählen Sie das Gesamtsystemszenario aus, das Switchover oder Failover ausgeführt hat, und klicken Sie im Drop-down-Menü **Aktionen** auf **Ausführen**.

   Der **Assistent zum Wiederherstellen von Daten** wird geöffnet.
3. Befolgen Sie die Anweisungen in den Fenstern des Assistenten, um das Wiederherstellungsszenario zu erstellen und auszuführen.

   Daten werden auf dem Bare-Metal-Rechner wiederhergestellt. Wenn Sie einen automatischen Switchover ausgewählt haben, wird der Switchover-Prozess initiiert, und der Bare-Metal-Rechner ist bereit. Wenn Sie das manuelle Switchover ausgewählt haben, müssen Sie den Switchover-Vorgang manuell initiieren.

Überwachungsszenarien

Mit Arcserve Unified Data Protection können Sie verschiedene Statistiken und Berichte für die Überwachung von DR- oder HA-Szenarien erstellen.

Gehen Sie wie folgt vor:

1. Wählen Sie im mittleren Fensterbereich ein Szenario aus.

   Der Status des ausgeführten Szenarios wird inklusive Details wie gesendete Daten, gesendete Dateien, empfangene Daten, empfangene Dateien usw. angezeigt.

2. Klicken Sie auf die Registerkarte **Statistik**, um weitere Details anzuzeigen. Die Registerkarte enthält die folgenden beiden Kategorien:

   Statistiken werden ausgeführt

   Zeigt detaillierte statistische Daten zur Szenarioausführung an.

   Historiendatensätze

   Zeigt Berichte für Synchronisation, Vergleichsberichte und AR-Tests an.

3. Klicken Sie auf die Registerkarte **Ereignisse**, um alle Ereignisse für ein ausgewähltes Szenario anzuzeigen. Um die Ereignisse zu kopieren oder zu löschen, wählen Sie die Ereignisse aus und klicken mit der rechten Maustaste darauf. Wählen Sie anschließend **Ereignisse anzeigen** aus, um das Dialogfeld "Ereignisse anzeigen" zu öffnen, in dem Sie die Ereignisse kopieren oder löschen können. Verwenden Sie die Umschalttaste und STRG, um mehrere Ereignisse gleichzeitig auszuwählen.

   Hinweis: Die Ereignisse werden automatisch aktualisiert. Die fünf aktuellsten kritischen Ereignisse werden im Bereich angezeigt, wenn Sie ein Szenario auswählen.

4. Wählen Sie die Szenariogruppe aus dem linken Fensterbereich aus. Alle Szenarien in der Gruppe werden im mittleren Fensterbereich aufgelistet. Sie können RPO/RTO, Master-Spool-Verwendung und Synchronisationsfortschritt in dieser Liste überprüfen.

5. Die Details im rechten Fensterbereich enthalten Szenarioinformationen wie Szenarionamen, Szenariostatus und Synchronisationsfortschritt.

   Hinweis: "Spool-Verwendung (% des Spool)" im rechten Fensterbereich steht für die Spool-Verwendung des Master im Szenario.

Remote-Installation

Mit Arcserve Unified Data Protection können Sie den Prozess von einem verwalteten Steuerungsdienst auf den Remote-Hosts bereitstellen. Sie könnten die Installation und Überprüfung auch von der Hostliste verwalten.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Bereich auf **Remote-Installation**.

   Die Seite **Remote-Installation** wird im mittleren Fensterbereich angezeigt.

2. Wählen Sie in der Drop-down-Liste **Steuerungsdienst** einen Steuerungsdienst aus, den Sie verwenden möchten, um den Prozess bereitzustellen.

   Die vorhandenen Hosts, auf denen der Prozess zuvor installiert oder überprüft wurde, werden im mittleren Fensterbereich aufgelistet.

3. Klicken Sie im Drop-down-Menü **Aktionen** auf **Hosts hinzufügen**.

   Das Dialogfeld **Hosts für die Installation des Prozesses** wird geöffnet.

4. Geben Sie den Hostnamen oder die IP-Adresse des Hosts ein, und klicken Sie auf **Hinzufügen**.

   Der Host wird der Liste hinzugefügt.

5. Klicken Sie auf **OK**.

   Das Dialogfeld **Hosts hinzufügen** wird geöffnet.

6. Wählen Sie eine der folgenden Optionen:

   Hosts bearbeiten

   Öffnet das Dialogfeld **Hosts für die Installation des Prozesses**, sodass Sie Hosts hinzufügen oder vorhandene Hosts verwalten können.

   Installationseinstellungen ändern

   Öffnet das Dialogfeld **Installationseinstellungen bearbeiten.** Sie können folgende Details angeben:

   Installationskonto

   Dienstkonto

   Port

   Verwenden Sie frühere Einstellungen, wenn Sie eine Neuinstallation oder ein Upgrade durchführen

   Aktualisiert oder installiert einen vorhandenen RHA-Prozess neu.

7. Klicken Sie auf **OK**.

8. Der Host wird auf der Seite **Remote-Installation** angezeigt.

   Die Spalte **Status** zeigt den Installationsstatus an.

   Hinweis: Platzieren Sie den Mauszeiger auf den Status, um Details abzurufen, wenn die Installation fehlschlägt.

Remote-Installationsaktionen

Sie können verschiedene Vorgänge auf hinzugefügten Hosts ausführen.

Gehen Sie wie folgt vor:

1. Wählen Sie ein Host im mittleren Fensterbereich aus.
2. Klicken Sie auf die Dropdown-Liste **Aktionen**, und wählen Sie eine der folgenden Optionen aus:

Hosts hinzufügen

Öffnet das Dialogfeld **Hosts für die Installation des Prozesses**. Weitere Informationen finden Sie unter Remote-Installation.

Installieren/Aktualisieren

Installiert oder aktualisiert den HA-Prozess auf dem ausgewählten Host.

Deinstallieren

Deinstalliert den HA-Prozess vom ausgewählten Host.

Einstellungen bearbeiten

Öffnet das Dialogfeld **Installationseinstellungen bearbeiten**.

Host-Status überprüfen

Überprüft die Existenz des Hosts.

Hosts entfernen

Entfernt den Host aus der Liste.

Anzeigen von Protokollen

Öffnet das Dialogfeld **Remote-Installationsprotokolle**, und zeigt die Protokolle aller Remote-Hosts an. Klicken Sie, um die Ansicht der aktuellsten Protokolle zu aktualisieren.

Der Vorgang wurde erfolgreich abgeschlossen.

High Availability-Berichte

Arcserve Unified Data Protection stellt verschiedene Berichte für die Überwachung des High Availability-Status zur Verfügung. Sie können Filter anwenden, um je nach Bedarf verschiedene Arten von Berichten zu generieren.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte **Steuerungsdienste und Szenarien**.
2. Klicken Sie im linken Fensterbereich auf **Berichte**.
3. Die Seite **Berichte** wird im mittleren Fensterbereich angezeigt.
4. Wählen Sie im mittleren Fensterbereich einen Steuerungsdienst aus der Drop-down-Liste **Steuerungsdienst** aus.
5. Geben Sie Details ein, und wenden Sie Filter bedarfsgerecht an.

   Der HA-Bericht wird generiert.

Kapitel 8: Verwenden des VSphereConfig-Hilfsprogramms

In diesem Abschnitt werden die folgenden Themen behandelt:

Aktivieren oder Deaktivieren des VSPhereBackupNFC-Tags mithilfe der Eingabeaufforderung

Wichtig! Aktivieren Sie das VSphereBackupNFC-Tag auf einem bestimmten Kernel-Adapter für die Sicherung (anstelle eines bestimmten Sicherungsnetzwerks), wenn eine Quell-VM ESXi Hypervisor hostet und die Sicherung VDDK7 oder höhere Versionen verwendet.

Mit Arcserve UDP können Sie das *VSphereBackupNFC*-Tag über die Eingabeaufforderung aktivieren oder deaktivieren. Mit dem Befehlszeilentool (*AFVSphereConfigTool.exe*) können Sie das VSphereBackupNFC-Tag auf einem bestimmten Kernel-Adapter aktivieren oder deaktivieren.

Dieser Abschnitt enthält Informationen zum Aktivieren oder Deaktivieren des *VSPhereBackupNFC*-Tags über die Eingabeaufforderung.

Gehen Sie wie folgt vor:

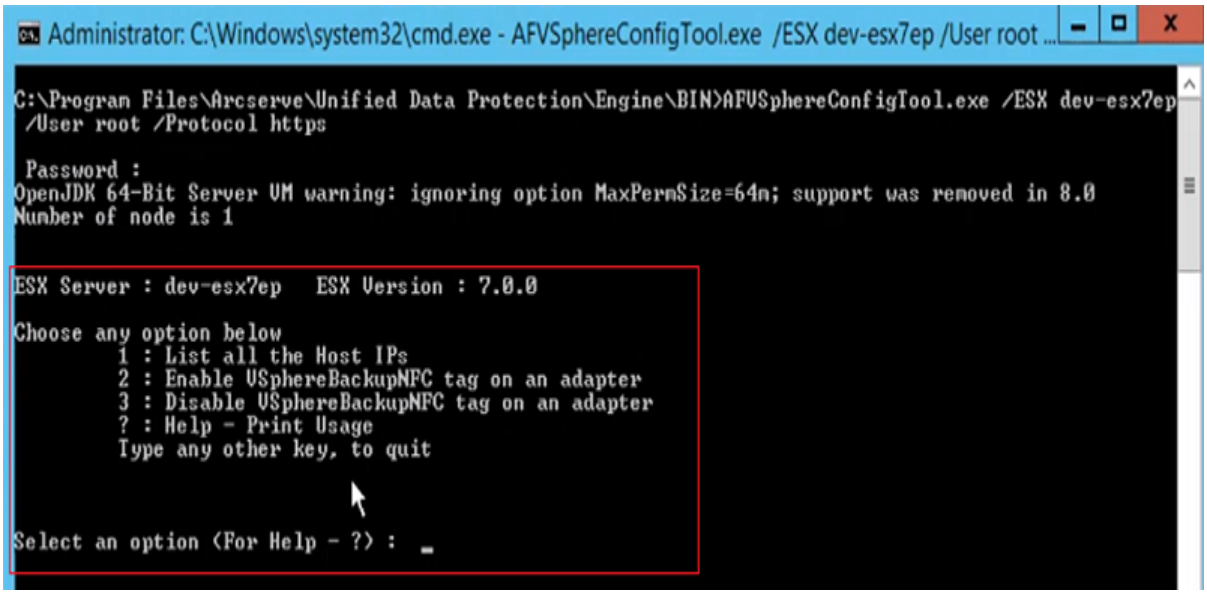
1. Öffnen Sie die Eingabeaufforderung, und navigieren Sie zu <Engine>\BIN>.

   Beispiel: C:\Programme\Arcserve\Unified Data Protection\Engine\BIN>

2. Stellen Sie über das Befehlszeilen-Tool (*AFVSphereConfigTool.exe*) eine Verbindung zum ESX-Server her, und geben Sie bei Aufforderung ein Kennwort ein.

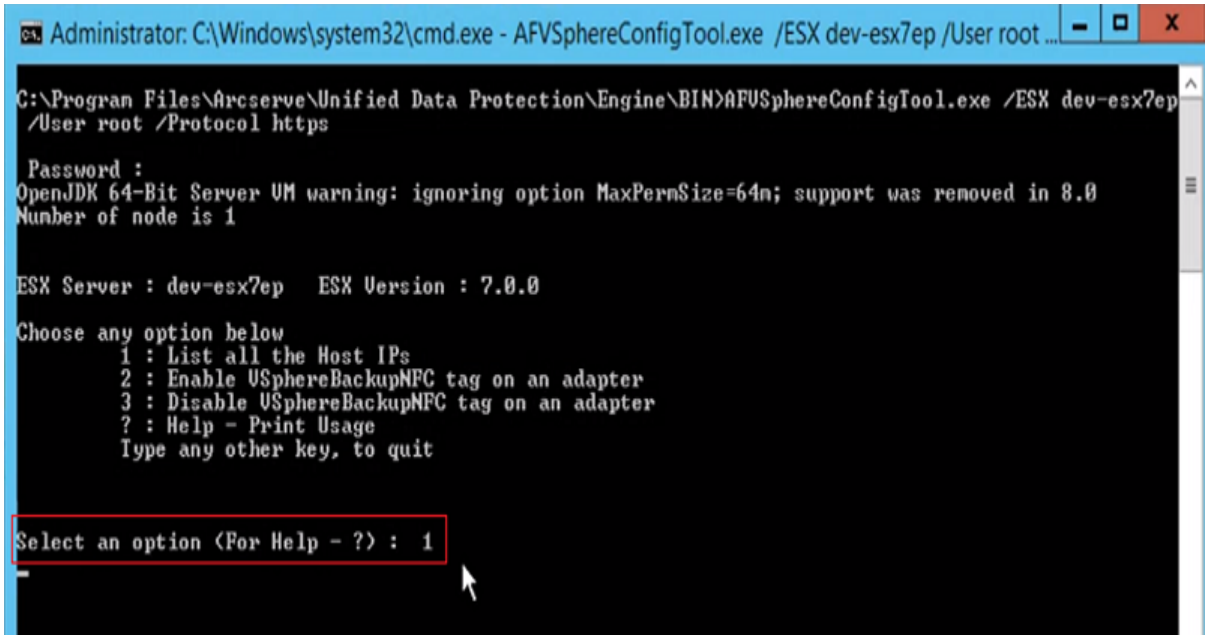
   AFVSphereConfigTool.exe/ESX dev-esx7ep/user root/protocol https

   Der ausgewählte ESX-Server (dev-esx7ep) ist jetzt verbunden.

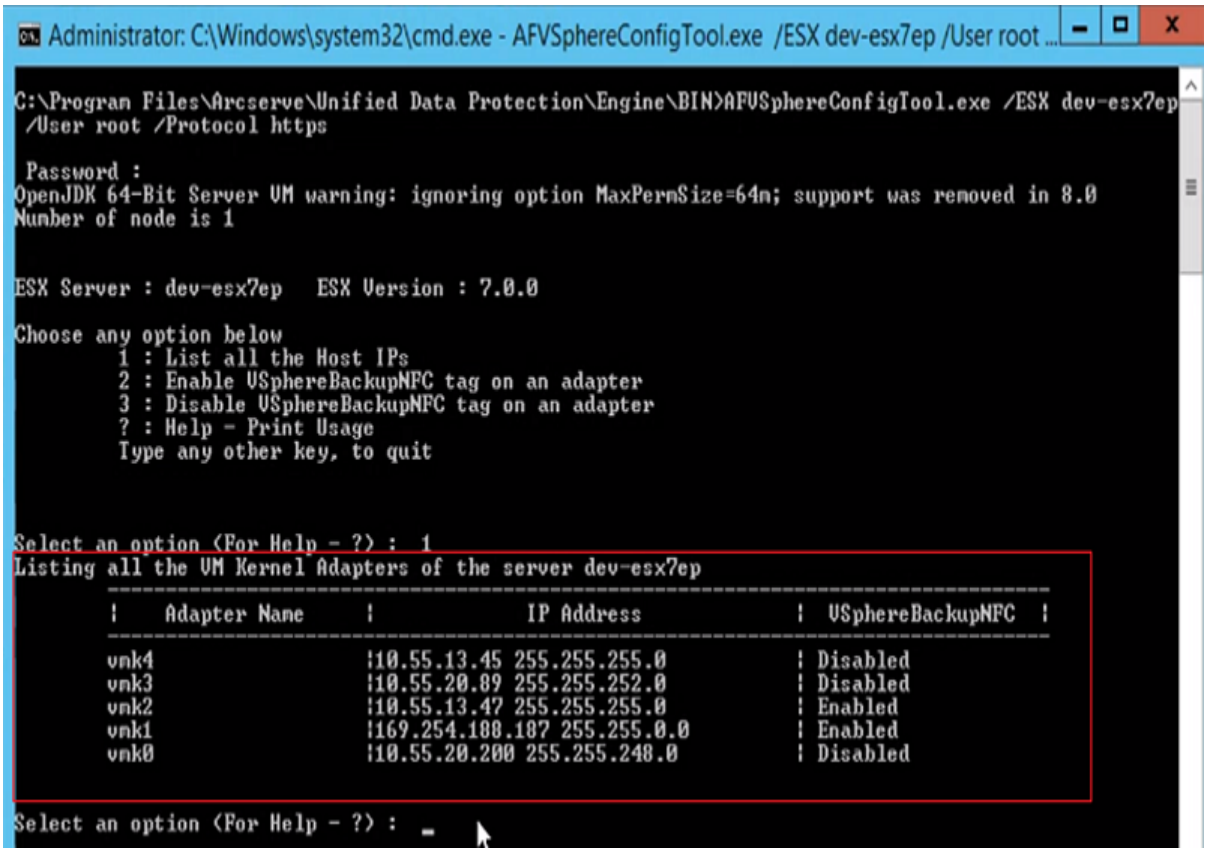


3. Wenn Sie nach dem erfolgreichen Herstellen der Verbindung zum ESX-Server aufgefordert werden, eine Option auszuwählen, gehen Sie folgendermaßen vor:

   - Geben Sie die Optionsnummer ein, um alle VM-Kernel-Adapter des ESX-Servers aufzulisten. Geben Sie beispielsweise 1 für die Option ein.

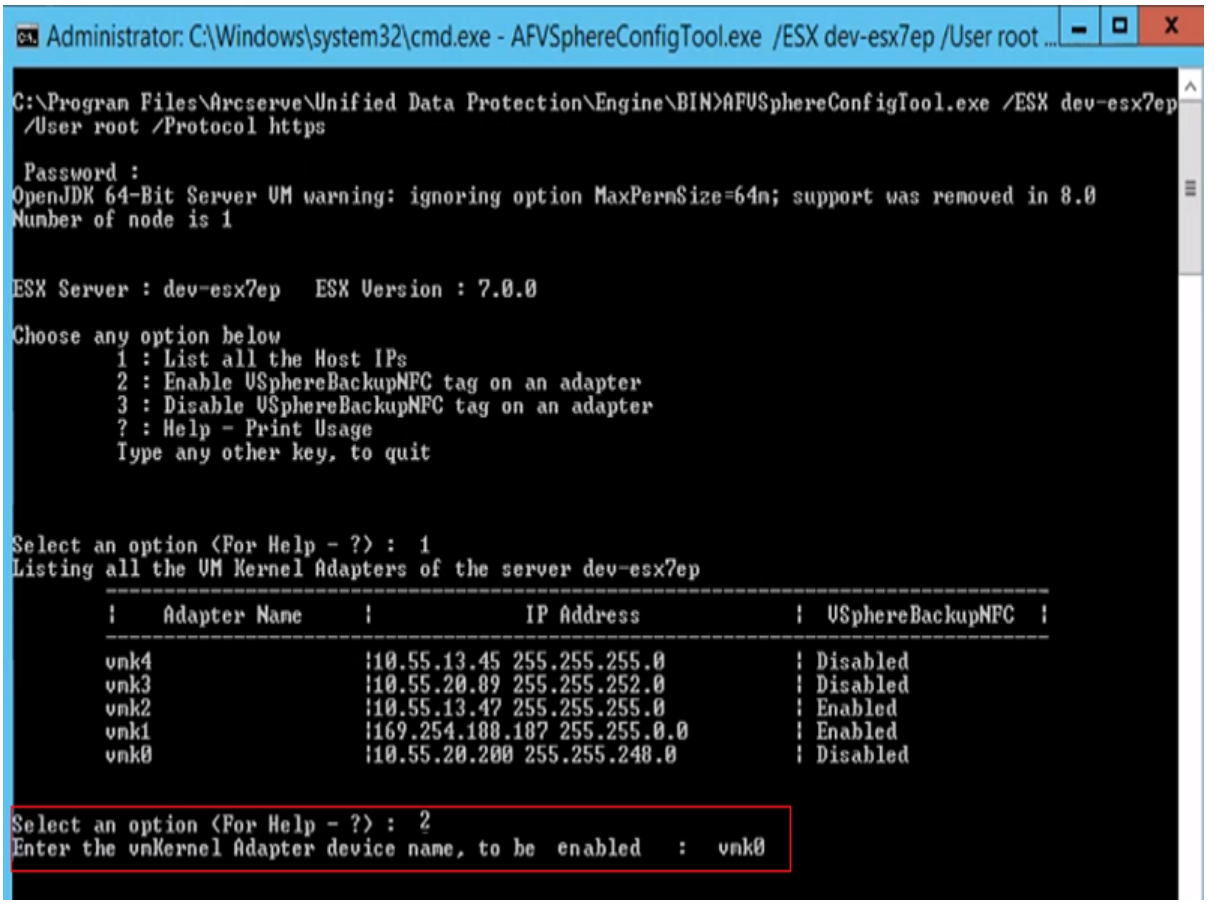


Eine Liste aller VM-Kernel-Adapter wird angezeigt.

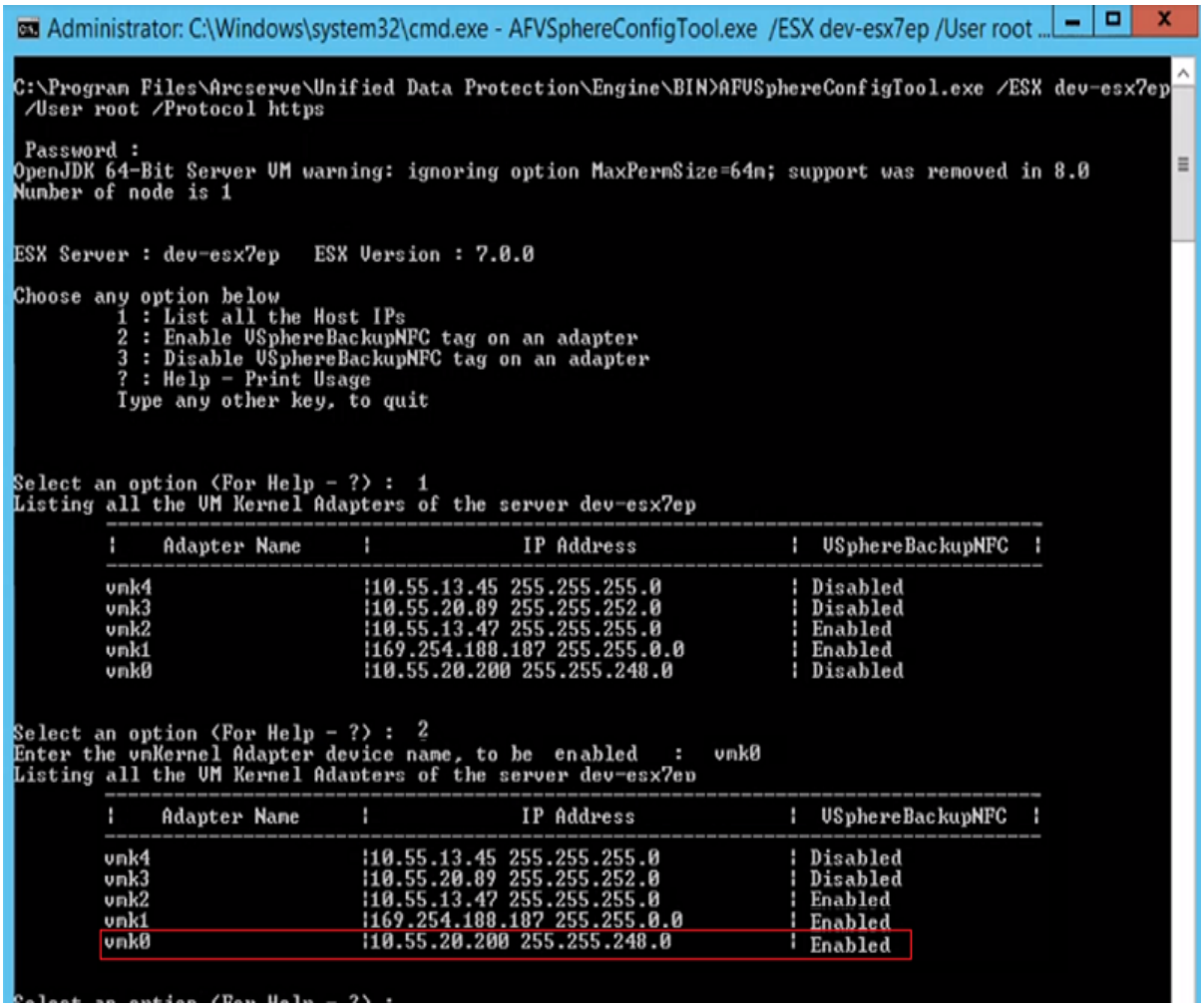


- Um das VSphereBackupNFC-Tag auf einem Adapter zu aktivieren, geben Sie die Optionsnummer ein. Geben Sie beispielsweise 2 für die Option ein.

  Wenn Sie aufgefordert werden, den Namen des VM-Kernel-Adapter-Geräts einzugeben, geben Sie den Gerätenamen ein.

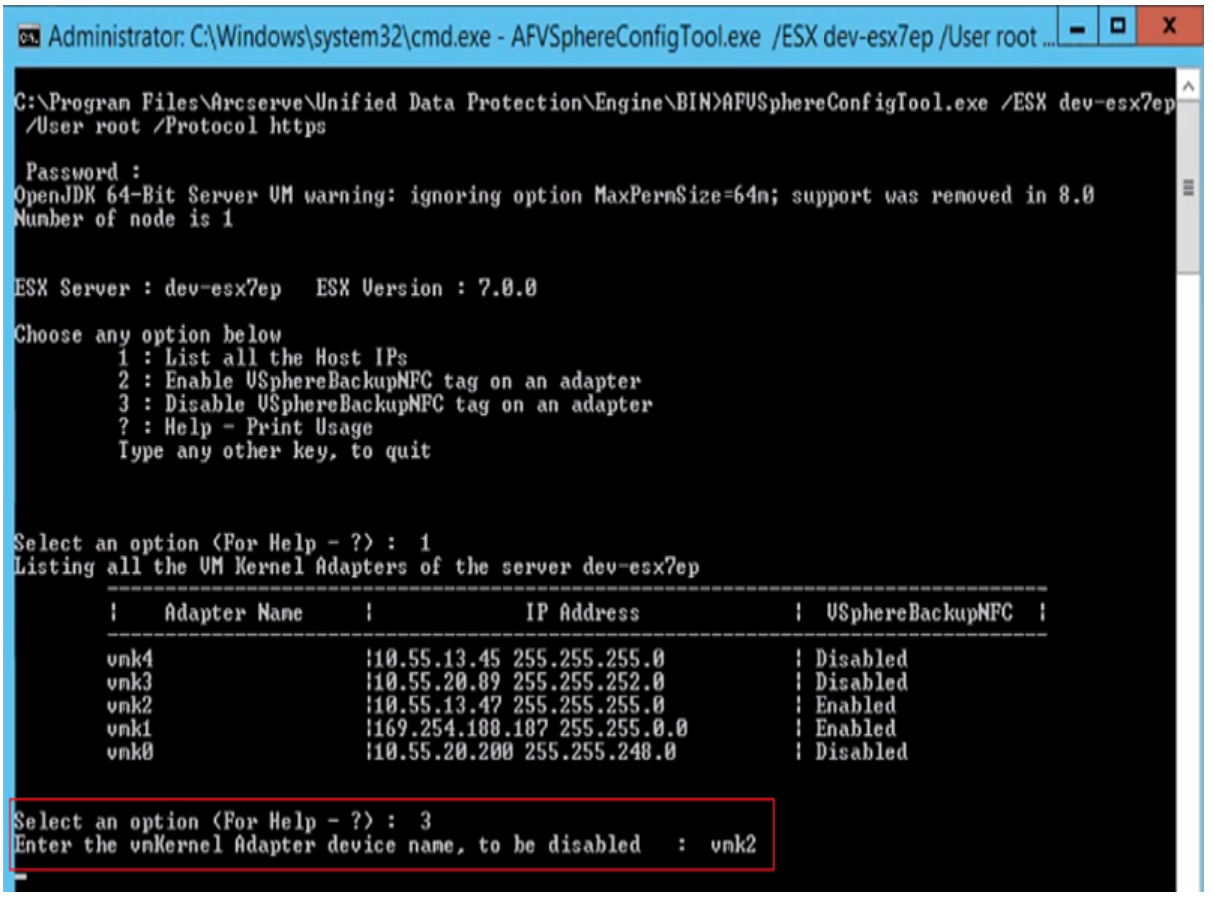


Das VSphereBackupNFC-Tag wird für den ausgewählten Adapter aktiviert.

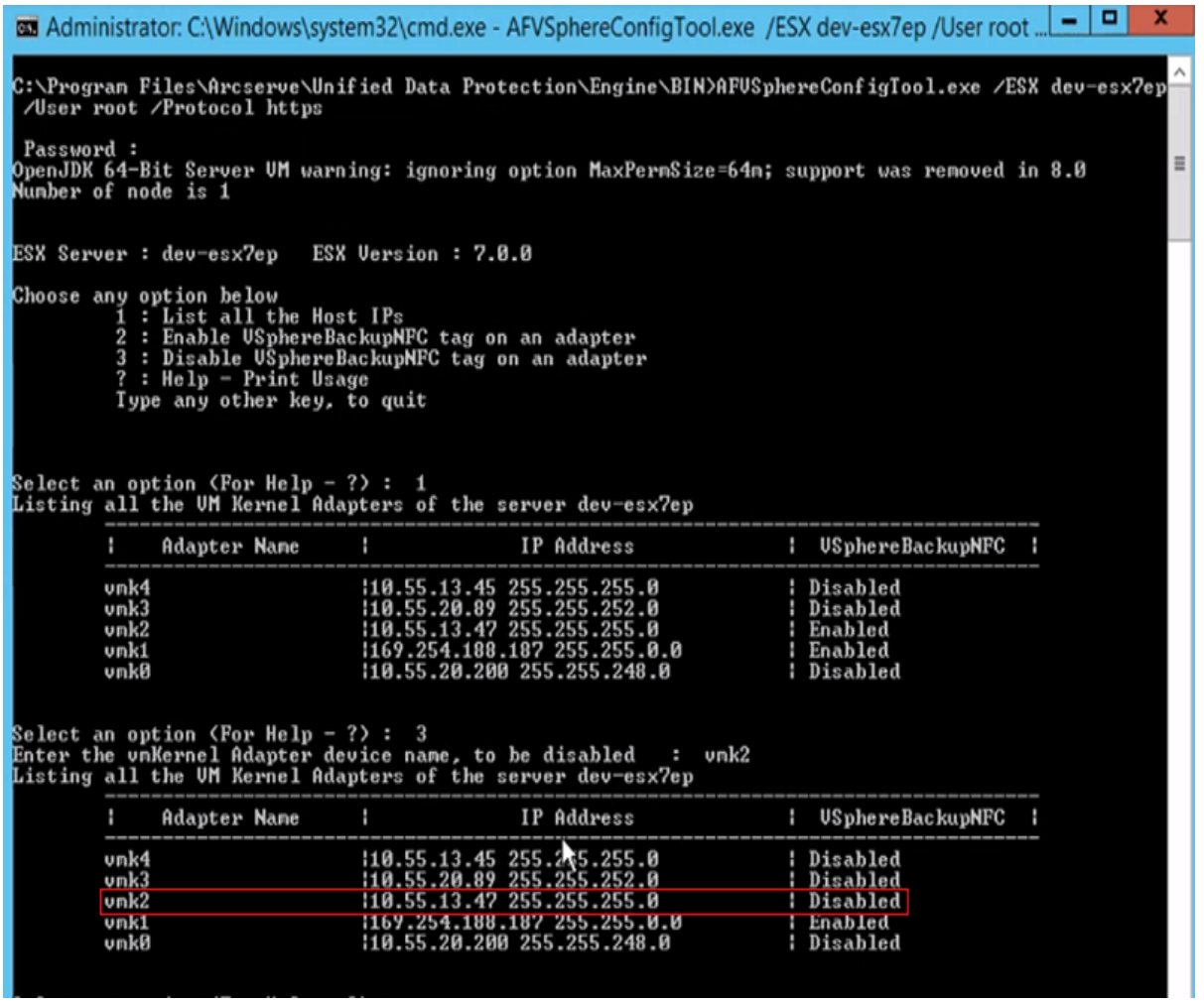


- Um das VSphereBackupNFC-Tag auf einem Adapter zu deaktivieren, geben Sie die Optionsnummer ein. Geben Sie beispielsweise 3 für die Option ein.

  Wenn Sie aufgefordert werden, den Namen des VM-Kernel-Adapter-Geräts einzugeben, geben Sie den Gerätenamen ein.



Das VSphereBackupNFC-Tag wird für den ausgewählten Adapter deaktiviert.



4. Geben Sie einen beliebigen Schlüssel ein (außer 1, 2, 3 und?) , um die Eingabeaufforderung zu schließen.

Kapitel 9: Verwenden des Diagnosehilfsprogramms

Mit dem Diagnosehilfsprogramm können Sie Protokolle von Ihren Rechnern erfassen. Wenn Sie das Arcserve-Support-Team zu einem Problem kontaktieren, verwendet das Support-Team die Protokolle, um das Problem zu untersuchen und zu beheben.

In diesem Abschnitt werden die folgenden Themen behandelt:

Erfassen der Diagnoseinformationen

Bei Diagnoseinformationen handelt es sich um eine Sammlung von Protokollen, Ereignissen, Registrierungs- und Anwendungsinformationen des Produkts und Systems, welche das Arcserve-Support-Team benötigt, um einen Fehler zu untersuchen. Mit Arcserve UDP können Sie alle diese Informationen an einem Speicherort, meist einem Netzwerkfreigabepfad, erfassen. Halten Sie diese Informationen bereit, wenn Sie den Arcserve-Support kontaktieren. Sie können die Diagnosedaten für Windows-, Linux-, VMware- und Hyper-V-Rechner erfassen.

Hinweis: Für Linux-Sicherungsserver ist die Option **Diagnosedaten erfassen** nur über die Ansicht **<Standortname>-Knoten: Linux-Sicherungsservergruppen** verfügbar.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Führen Sie einen der folgenden Schritte je nach Art des Knotens aus:

   Bei Linux-Sicherungsservern

   - Navigieren Sie im linken Navigationsbereich zu **Knoten**, und klicken Sie auf **Linux-Sicherungsservergruppen**.
   - Wählen Sie im mittleren Fensterbereich alle Linux-Knoten aus.

   Bei allen anderen Knoten und Servern

   - Navigieren Sie im linken Navigationsbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.
   - Wählen Sie im mittleren Fensterbereich alle erforderlichen Knoten aus.
3. Klicken Sie auf **Aktionen**, **Diagnosedaten erfassen**.

   Das Dialogfeld **Diagnoseinformationen erfassen** wird angezeigt.
4. (Optional) Aktivieren Sie das Kontrollkästchen.
5. Geben Sie den Netzwerkfreigabepfad zum Speichern der Daten an.

   Hinweise:

   - Wenn Sie Diagnoseinformationen für einen Remote-Standort erfassen, müssen Sie als Ziel den Gatewayserver oder einen anderen Rechner angeben, der Zugriff auf den Agenten oder RPS an diesem Standort hat.
   - Wenn Sie den lokalen Pfad als Ziel angeben möchten, konvertieren Sie den lokalen Pfad in den UNC-Pfad, und geben Sie den UNC-Pfad an. Zum Beispiel

kann **C:\test** als **\\<Name des lokalen Rechners>\C$\test** angegeben werden.

- Bei hostbasierten agentenlosen Sicherungen (VMs) werden mit der Funktion "Diagnosedaten erfassen" Daten vom Arcserve UDP-Proxy-Server erfasst.
- Die Funktion erfasst Daten von Computern, auf denen der Arcserve UDP-Agent installiert ist.

6. Klicken Sie auf **Übergeben**.

   Ein Job wird übermittelt, um die Daten zu erfassen.

   Nach erfolgreichem Abschluss des Jobs sehen Sie die Daten im freigegebenen Ordner. An den Namen der Zip-Datei wird der aktuelle Zeitstempel als Suffix angehängt.

Erfassen von Diagnoseinformationen von einem eigenständigen Agenten

Bei Diagnoseinformationen handelt es sich um eine Sammlung von Protokollen, Ereignissen, Registrierungs- und Anwendungsinformationen des Produkts und Systems, welche das Arcserve-Support-Team benötigt, um einen Fehler zu untersuchen. Mit Arcserve UDP Agent können Sie alle diese Informationen an einem Speicherort, meist einem Netzwerkfreigabepfad, erfassen. Halten Sie diese Informationen bereit, wenn Sie den Arcserve-Support kontaktieren.

Gehen Sie wie folgt vor:

1. Wechseln Sie über die Eingabeaufforderung zu folgendem Pfad:

   ```
   %Programme% \Arcserve\Unified Data Protection\Engine\BIN\DiagnosticUtility
   ```

2. Führen Sie folgenden Befehl aus, um zu erfahren, wie Sie die Batch-Datei ausführen können:

   ```
   arcserveAgentSupport.bat -help
   usage: arcserveAgentSupport.bat [OPTIONS]
   -help print help
   -pass <arg> usrPass (wenn es sich beim Exportpfad um eine Remote-Freigabe handelt, Benutzerkennwort für den Zugriff)
   -path <arg> export path (kann eine Remote-Freigabe sein)
   -user <arg> usrName (wenn es sich beim Exportpfad um eine Remote-Freigabe handelt, Benutzername für den Zugriff)
   -xmlConfig <arg> xmlConfigurationFile (optional)
   ```

3. Verwenden Sie folgenden Befehl, um die Diagnoseinformationen zu erfassen:

   ```
   arcserveAgentSupport.bat -path <remote share path> -user <username> -pass <password>
   ```

   Beispiel: arcserveAgentSupport.bat -path \\remote_share\data -user abc -pass xyz

   Dabei ist "\\remote_share\data" der Pfad, "abc" der Benutzername und "xyz" das Kennwort.

   Sie finden die Zip-Datei mit den Diagnoseinformationen in der Remote-Freigabe.

Hochladen von Diagnoseinformationen auf die Arcserve-Website über FTP

Sie können Protokolle oder Dateien auf den Arcserve-Support-FTP mithilfe eines File Transfer Protocol (FTP) hochladen. Allerdings können Benutzer (Anforderer des Tickets) den FTP-Link auch bei der anfänglichen Ticketerstellung oder beim Aktualisieren des Tickets online aktivieren. Nach Aktivierung generiert FTP den FTP-Link zusammen mit Anmeldeinformationen. Diese Informationen werden dem Benutzer über eine automatische E-Mail zur Verfügung gestellt. Sie können den über eine automatische E-Mail gesendeten Benutzernamen und das zugehörige Kennwort für das Hochladen und Herunterladen von Dateien vom FTP verwenden.

Wenn Sie sich beim FTP über ftp://supportftp.arcserve.com anmelden, wird der Stammordner angezeigt. Wenn Sie ein Ticket im Arcserve-Support-Portal erstellen, wird ein Unterordner mit der Ticketnummer im Stammordner erstellt. Zum Beispiel: Wenn Sie ein Ticket mit der Ticketnummer Ticket-00XXXX30 erstellen, wird ein Unterordner namens Ticket-00XXXX30 im Stammordner erstellt.

ftp://supportftp.arcserve.com/Ticket-00XXXX30/

Benutzername und Kennwort: Verwenden Sie automatisch generierte Benutzernamen und Kennwörter, die über automatische E-Mail gesendet wurden.

Ordner: Ticket-00XXXX30

Hinweis: Bei japanischen Benutzern ist das Kennwort die E-Mail-Adresse des Anforderers ohne den Domänennamen. Wenn zum Beispiel die registrierte E-Mail-Adresse abc@yahoo.jp ist, ist das Kennwort abc.

Wenn das Ticket bearbeitet wurde, erhält der FTP-Server eine Benachrichtigung. Der Ordner wird dann komprimiert, und der ursprüngliche Ordner wird gelöscht. Der komprimierte Ordner steht für die nächsten drei Monate zur Verfügung und wird danach endgültig gelöscht.

Wichtig! Geben Sie Ihren Benutzernamen nicht an Dritte weiter.

Befolgen Sie diese Schritte, um Dateien auf die Website von Arcserve über FTP hochzuladen:

1. Der Ticketanforderer (Benutzer) oder Arcserve-Support-Mitarbeiter meldet sich beim Arcserve-Support-Portal an und erstellt ein Support-Ticket.

   Der Arcserve-Support-Mitarbeiter oder der Ticketanforderer aktiviert das Kontrollkästchen im Support-Ticket und aktualisiert das Ticket.

Ein FTP-Link wird automatisch für den FTP-Stammordner generiert. Die Berechtigung wird ausschließlich für den Anforderer festgelegt, der das Ticket geöffnet hat.

Zum Beispiel ist der folgende Ordner Ihr FTP-Ordner:

ftp://supportftp.arcserve.com/<Ticket_number>

2. Sobald der FTP-Link erstellt wurde, sendet Arcserve-Support automatisch eine E-Mail mit dem FTP-Link und den Anmeldeinformationen an den Ticketanforderer (Benutzer).
3. Der Benutzer meldet sich über den FTP-Link an und lädt die Dateien hoch.

   Sie haben den Prozess zum Hochladen von Dateien auf den Arcserve-FTP-Server erfolgreich abgeschlossen.

Extrahieren der Agentenprotokolle

Die Protokolldateien, die vom Diagnosehilfsprogramm generiert werden, liegen im ZIP-Format vor. Um die Protokolldateien anzuzeigen, müssen Sie die Dateien extrahieren.

Gehen Sie wie folgt vor:

1. Kopieren Sie die .arcZIP-Datei auf den Rechner, auf dem der UDP-Agent installiert ist.

   Die .arcZIP-Datei wird mit dem Diagnosehilfsprogramm erstellt.

2. Wechseln Sie über die Eingabeaufforderung zu folgendem Pfad:

   ```
   %Programme% \Arcserve\Unified Data Protection\Engine\BIN\DiagnosticUtility
   ```

3. Führen Sie folgenden Befehl aus, um zu erfahren, wie Sie die Batch-Datei ausführen können:

   ```
   arcserveAgentSupportInternal.bat -help
   ```

   ```
   BaseOperation loadDefaultValue
   ```

   ```
   INFO: Installationspfad C:\Programme\Arcserve\Unified Data Protection\Engine des Agenten laden
   ```

   ```
   Verwendung: arcserveAgentSupportInternal.bat [OPTIONS] rawfile
   ```

   ```
   -help          Hilfe drucken
   ```

   ```
   -keepFile      Temporäre Datei beibehalten
   ```

   ```
   -path <arg>    Pfad, in dem der Inhalt extrahiert werden muss
   ```

   Der Abschnitt "Hilfe" wird angezeigt.

4. Extrahieren Sie die Datei mit dem folgenden Befehl:

   ```
   arcserveAgentSupportInternal.bat -path <sollte_der_gleiche_Rechner_sein_auf_dem_extrahiert_werden_soll> <Name_der_Zip_Datei>
   ```

   Die Agentenprotokolle werden extrahiert.

Extrahieren der Konsolenprotokolle

Die Protokolldateien, die vom Diagnosehilfsprogramm generiert werden, liegen im ZIP-Format vor. Um die Protokolldateien anzuzeigen, müssen Sie die Dateien extrahieren.

Gehen Sie wie folgt vor:

1. Kopieren Sie die .arcZIP-Datei auf den Rechner, auf dem die UDP-Konsole installiert ist.

   Die .arcZIP-Datei wird mit dem Diagnosehilfsprogramm erstellt.

2. Wechseln Sie über die Eingabeaufforderung zu folgendem Pfad:

   ```
   %ProgramFiles%\Arcserve\Unified Data Protection\Management\BIN\DiagnosticUtility
   ```

3. Führen Sie folgenden Befehl aus, um zu erfahren, wie Sie die Batch-Datei ausführen können:

   ```
   arcserveConsoleSupportInternal.bat -help
   BaseOperation loadDefaultValue
   INFO: Installationspfad C:\Programme\Arcserve\Unified Data Protection\Management\ des Agenten laden
   Verwendung: arcserveConsoleSupportInternal.bat [OPTIONS] rawfile
   -help          Hilfe drucken
   -ignoreFailed   Fehlgeschlagene Importtabelle ignorieren
   -keepFile       Temporäre Datei beibehalten
   -noClean        Datenbank nicht bereinigen
   -path <arg>     Pfad, in dem der Inhalt extrahiert werden muss
   -u              Nur Datei extrahieren
   ```

   Der Abschnitt "Hilfe" wird angezeigt.

4. Extrahieren Sie die Datei mit dem folgenden Befehl:

   ```
   arcserveConsoleSupportInternal.bat -path <sollte_der_gleiche_Rechner_sein_auf_dem_extrahiert_werden_soll> <Name_der_Zip_Datei>
   ```

   Hinweis: Durch den Befehl wird die Datenbank der Konsole nicht überschrieben. Wenn die Konsolendatenbank überschrieben werden soll, bearbeiten Sie den

Befehl in *arcserveConsoleSupportInternal.bat* und entfernen Sie *-u* aus der Datei. Speichern Sie danach die Datei.

Die Konsolenprotokolle werden extrahiert.

Überspringen der Inhalte des Protokollverlaufsordners über die Registrierung

Sie können UDP Agent verwenden, um alle Protokolle einschließlich des Protokollverlaufs vom Prozess zu erfassen. Manchmal werden die Dateien beim Erfassen des Protokollverlaufs vom UDP Agent langsam verarbeitet, was dazu führt, dass sie größer erscheinen. Um diese Abweichungen zu vermeiden, können Sie den Ordner "LogHistory" ausschließen.

Gehen Sie wie folgt vor:

1. Fügen Sie den Schlüssel an folgendem Speicherort in der Registrierung hinzu:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

2. Geben Sie die folgenden Details ein:

   Schlüsselname: *SkipLogHistory*

   Typ: *DWORD(32-bit)*

   Wert: 1 (der Wert "1" wird verwendet, um "LogHistory" zu überspringen, während "0" verwendet wird, um "LogHistory" zu erfassen)

Erfassen des Protokolls vom Gateway-Rechner über die Befehlszeile

Um Protokolle über die Befehlszeile erfassen zu können, muss das Arcserve UDP-Gateway-Produkt installiert sein.

Gehen Sie folgendermaßen vor, um Protokolle über die Befehlszeile zu erfassen:

1. Öffnen Sie die Eingabeaufforderung und navigieren Sie zu *<Gateway-Installationsverzeichnis>\BIN\Diagnostic Utility*.

   Beispiel: C:\Programme\Arcserve\Unified Data Protection\Gateway\BIN\Diagnostic Utility\

2. Um die Protokolle zu packen, führen Sie den folgenden Befehl aus:

   arcserveGatewaySupport.bat -Path "<Zielpfad>"

3. Um die Protokolle zu entpacken, führen Sie den folgenden Befehl aus:

   arcserveGatewayInternalSupport.bat -Path "<Zielpfad>" "<Quellpfad>"

Sammeln von Protokollen aus dem RPS über die Befehlszeile

Sie müssen das Arcserve UDP-Produkt mit RPS-Komponente installiert haben, um RPS-Protokolle von der Befehlszeile aus zu sammeln.

Gehen Sie folgendermaßen vor, um Protokolle über die Befehlszeile zu erfassen:

1. Öffnen Sie die Eingabeaufforderung und navigieren Sie zu *<Agent Installationsverzeichnis>\BIN\Diagnostic Utility*.

   Beispiel: C:\Program Files\Arcserve\Unified Data ProtectionEngine\BIN\Diagnostic Utility\

2. Um die Protokolle zu packen, führen Sie den folgenden Befehl aus:

   arcserveAgentSupport.bat -path <remote share path> -user <username> -pass <password>

3. Um die Protokolle zu entpacken, führen Sie den folgenden Befehl aus:

   arcserveAgentSupportInternal.bat –path <destination> <source(rawfile)>

Hinweise:

- RPS-Protokolle haben die Jobprotokolle, die auf RPS ausgeführt werden.
- RPS-Protokolle können nur über die Befehlszeile und nicht über die Konsolenoberfläche erfasst werden.
- Einige RPS-bezogene Jobprotokolle können nicht von der Konsolenoberfläche erfasst werden, wenn VM-Protokolle von der Konsole erfasst werden.

Beispiel: Wenn ein MSP-Replikationsauftrag konfiguriert ist, konfigurieren Sie die Aufgaben mit zwei Konsolen, wobei Konsole-1 die Sicherung als Hauptaufgabe und die Replikation als Nebenaufgabe hat. In Konsole-2 wird der per Remote-Zugriff verwaltete Replikationsauftrag konfiguriert und mit der Konsole-1 geteilt.

In diesem Szenario können Sie in Konsole-2 keine Replikationsjobprotokolle erfassen, wenn Sie VM-Protokolle von der Konsole aus erfassen. Sie müssen diese Replikationsprotokolle von der Befehlszeile auf dem RPS-Rechner, der das Ziel des Replikationsjob ist, sammeln.

Erfassen von Stub-Protokollen von Hyper-V mit installiertem Agenten

Stub-Protokolle können über Hyper-V mit installiertem Agenten erfasst werden. Hyper-V kann als Proxy fungieren, um die Erfassung der Hyper-V-Stub-Protokolle zu unterstützen.

Wenn Hyper-V selbst als Proxy fungiert (auf dem Hyper-V-Rechner muss der Agent installiert sein)

Öffnen Sie die Eingabeaufforderung und navigieren Sie zu *<Agent-Installationsverzeichnis>\BIN\ Diagnostic Utility*.

Beispiel: *C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Diagnostic Utility*

- So werden die Protokolle gepackt: Führen Sie *arcserveAgentSupport.bat -Path "Zielpfad"* aus.
- So werden die Protokolle entpackt: Führen Sie *arcserveAgentInternalSupport.bat -Path "Zielpfad" "Quellpfad"* aus.

Wenn Hyper-V nicht als Proxy fungiert (Erfassen des gesamten UDP-Host-basierten VM-Sicherungsordners)

Voraussetzung: Auf dem Rechner muss Java installiert sein.

Gehen Sie wie folgt vor:

1. Importieren Sie die Registrierung aus dem folgenden Pfad auf dem Rechner, auf dem Agent installiert ist:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine.

2. Kopieren Sie auf einem Rechner, auf dem der Agent bereits installiert ist, den gesamten Ordner "DiagnosticUtility" und fügen Sie den Ordner unter dem folgenden Pfad ein:

   C:\Programme\Arcserve\Unified Data Protection\Engine\BIN

   Hinweis: Sie müssen Sie diese Verzeichnisstruktur manuell erstellen.

3. Erstellen Sie einen leeren Ordner mit dem Namen "Logs" (oder "Protokolle") unter dem folgendem Pfad:

   C:\Programme\Arcserve\Unified Data Protection\Engine

4. Kopieren Sie den Ordner "Common" von einem Rechner, auf dem der Agent bereits installiert ist, in den folgenden Pfad:

   C:\Programme\Arcserve\Unified Data Protection

   - So werden die Protokolle gepackt: Führen Sie *arcserveAgentSupport.bat -Path "Zielpfad"* aus.
   - So werden die Protokolle entpackt: Führen Sie *arcserveAgentInternalSupport.bat -Path "Zielpfad" "Quellpfad"* aus.

Erfassen von Meldungen aus der Hyper-V-Ereignisanzeige

Meldungen können aus der Hyper-V-Ereignisanzeige mit installiertem Agenten und dem Ordnernamen *hyperVEventViewerFiles* erfasst werden.

Gehen Sie folgendermaßen vor, um Meldungen aus der Ereignisanzeige über die Befehlszeile zu erfassen:

1. Öffnen Sie die Eingabeaufforderung und navigieren Sie zu *<Agent-Installationsverzeichnis>\BIN\ Diagnostic Utility*

   Beispiel: C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Diagnostic Utility\

2. Führen Sie zum Packen der Meldungen aus der Ereignisanzeige *arcserveAgentSupport.bat -Path "Zielpfad"* aus.
3. Führen Sie zum Entpacken der Meldungen aus der Ereignisanzeige *ArcserveAgentInternalSupport.bat -Path "Zielpfad"* aus.

Erfassen des Ordners "Ca_lic" und der OLF-Dateien

"CA_LIC" und OLF-Dateien werden in den Protokollen erfasst, wenn Sie sie auf dem Rechner erfassen, auf dem der Agent bereits mit dem Ordnernamen "CA_LIC" installiert ist.

- Erfassen über die Befehlszeilenschnittstelle: Öffnen Sie die Eingabeaufforderung´, und navigieren Sie zu *<Agent-Installationsverzeichnis>\BIN\ Diagnostic Utility*.

  Beispiel: *C:\Programme (x86)\Arcserve\SharedComponents\CA_LIC*

- Erfassen über die Konsole: Navigieren Sie zum Agentenknoten, klicken Sie mit der rechten Maustaste darauf, und klicken Sie auf **Diagnoseinformationen erfassen**.

- So werden die Protokolle gepackt: Führen Sie *arcserveAgentSupport.bat -Path "Zielpfad"* aus.
- So werden die Protokolle entpackt: Führen Sie *arcserveAgentInternalSupport.bat -Path "Zielpfad" "Quellpfad"* aus.

Erfassen der Verzeichnisliste für Verzeichnisse im Sicherungsziel/Datenspeicher

Verzeichnisliste für die Ordner "Engine" und "Management"

Engine: Dieses Protokoll wird mit dem Namen *EngineDirectoryBrowseInfo.log* unter dem Ordner *AgentLogs* (nach dem Entpacken von "arczip") erfasst.

Verwaltung: Dieses Protokoll wird mit dem Namen *ManagementDirectoryBrowseInfo.log* unter dem Ordner *consoleLogs* (nach dem Entpacken von "arczip") erfasst.

Verzeichnisliste für Datenspeicher:

- **Ohne Deduplizierung:** Dieses Protokoll für Datenspeicher ohne Deduplizierung wird mit dem Namen *CommonStorePathDirectoryBrowseInfo.log* (nach dem Entpacken von "arczip") im Ordner *agentLogs* erfasst.
- **Deduplizierung:** Vier Protokolle für Datenspeicher mit Deduplizierung (nach dem Entpacken von "arczip") werden im Ordner *agentLogs* mit den folgenden Namen erfasst:
    1. *CommonStorePathDirectoryBrowseInfo.log*
    2. *HashRolePathDirectoryBrowseInfo.log*
    3. *IndexRolePathDirectoryBrowseInfo.log*
    4. *DataRolePathDirectoryBrowseInfo.log*

Kapitel 10: Manuelles Installieren von Sophos Intercept X Advanced for Server auf Arcserve UDP

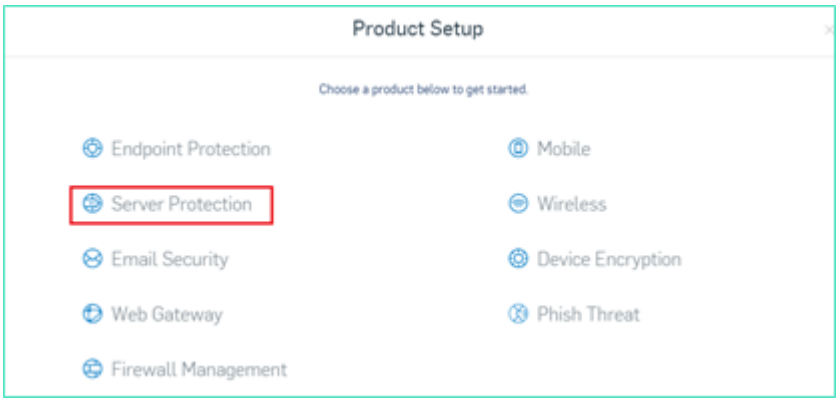
Die Installation von Sophos Intercept X Advanced for Server auf Arcserve UDP bietet Folgendes:

- Schützt Daten und Systemsicherungen vor Ransomware und anderen Angriffen
- Endpunktschutz, der signaturbasierte und signaturlose Malware-Erkennung kombiniert.
- Tief lernendes neuronales Netzwerk
- Anti-Exploit-Technologie
- CyptoGuard Anti-Ransomware- und WipeGuard-Technologien und mehr, um die breiteste Palette von Endpunktbedrohungen zu stoppen

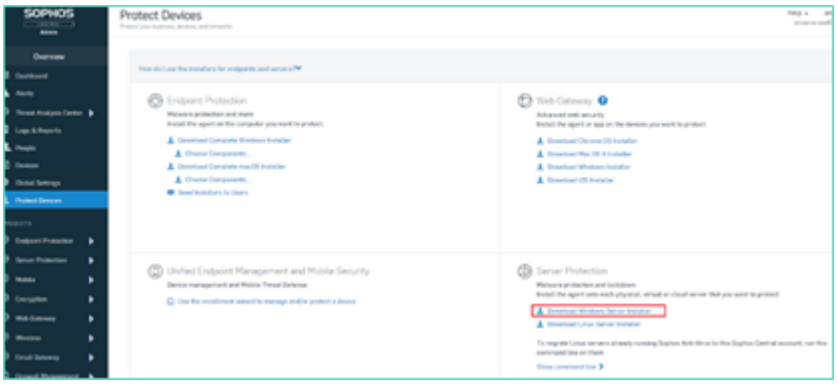
Befolgen Sie diese Schritte:

1. Erstellen Sie auf der Arcserve Support-Website ein Konto.
2. Um eine kostenlose Kopie von Sophos Intercept X Advanced anzufordern, geben Sie alle relevanten Details in das Sophos-Anfrageformular ein und senden es an den Arcserve-Support. Die E-Mail-ID und die Bestell-ID müssen angegeben werden. Sie erhalten eine automatisch generierte E-Mail-Bestätigung.

   Nachdem Sie Ihre E-Mail-ID bestätigt haben, verarbeitet Arcserve Ihre Anfrage, erstellt ein Konto auf der Sophos Central und sendet eine E-Mail mit Anweisungen zum Erstellen eines Kennworts.
3. Um ein Passwort für Ihr neues Konto auf Sophos Central zu erstellen, folgen Sie den Anweisungen in der E-Mail.
4. Melden Sie sich bei Sophos Central an.
5. Öffnen Sie das Dialogfeld Produkteinrichtung, und wählen Sie dann **Serverschutz** aus.



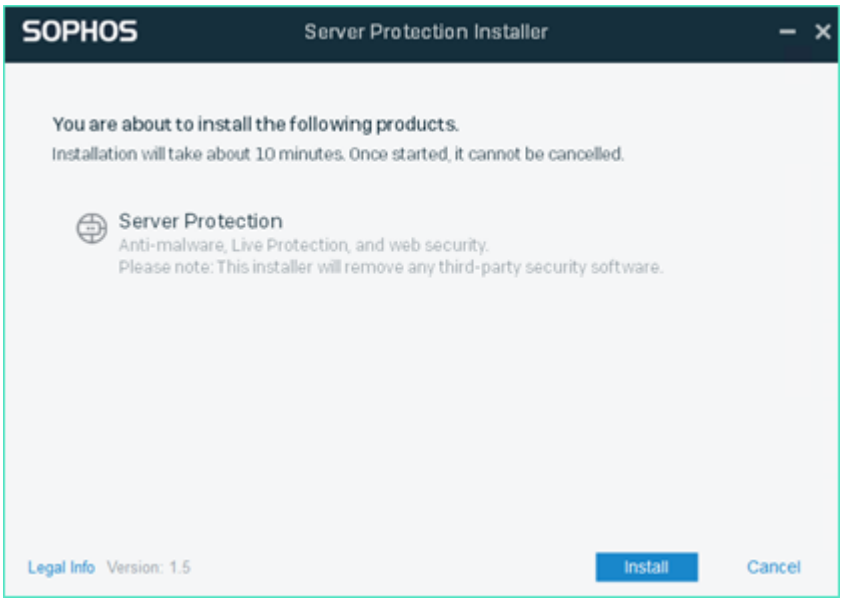
6. Klicken Sie im Abschnitt "Serverschutz" auf **Windows Server Installer herunterladen**, und speichern Sie dann das Installationsprogramm **SophosSetup.exe** in einem Ordner dem UDP-Rechner.



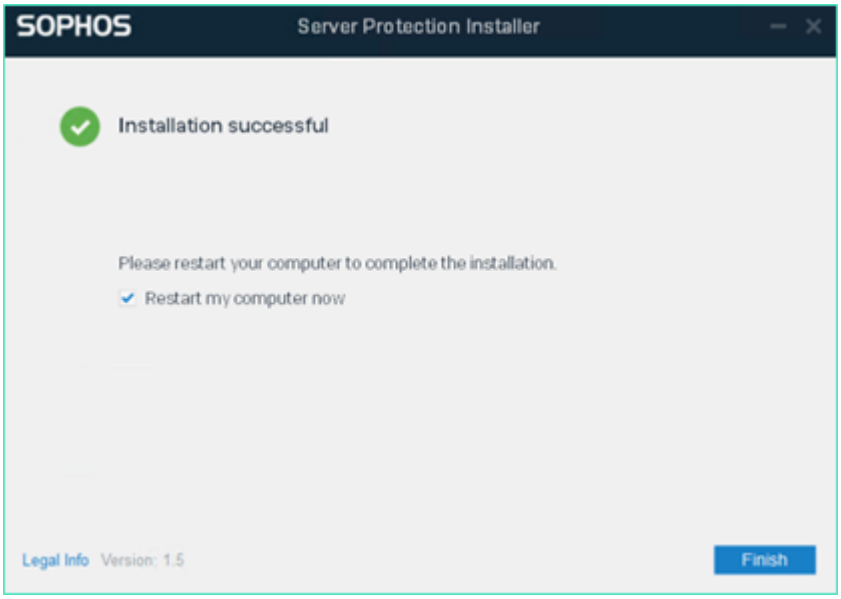
7. Um das Installationsprogramm zu starten, öffnen Sie den Ordner, und doppelklicken Sie dann auf **SophosSetup.exe**.

   Hinweis: Um unerwartetes Verhalten während der Installation von Sophos Intercept-X zu vermeiden, deaktivieren Sie Windows Defender und\oder andere Antivirensoftware auf dem Server. Sophos entfernt einige Sicherheitsprodukte anderer Hersteller von den Windows-Servern. Weitere Informationen finden Sie unter Sophos CRT: Liste der Sicherheitssoftware von Drittanbietern, die von Sophos entfernt wurde.

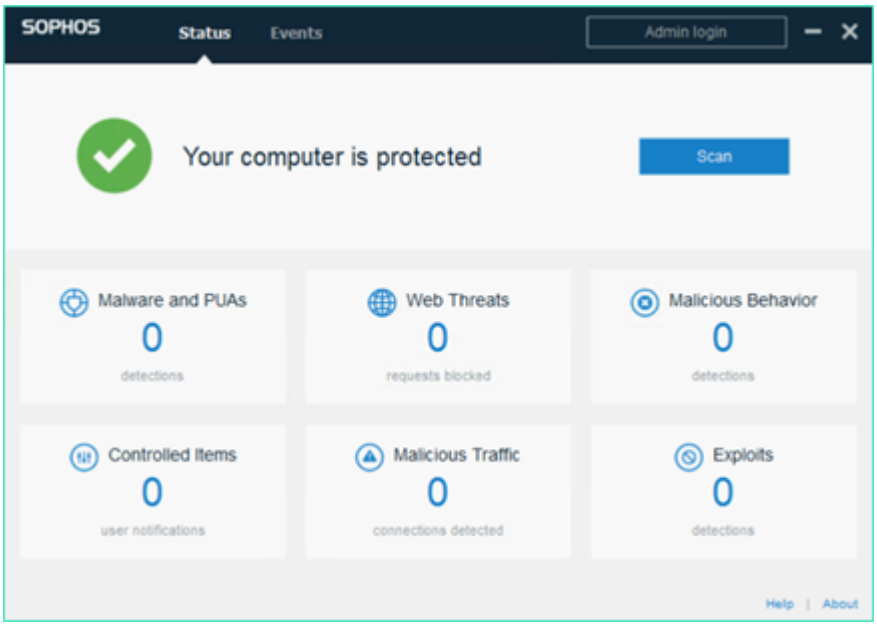
8. Klicken Sie auf **Installieren**.



9. Um das System sofort neu zu starten, klicken Sie auf **Fertig stellen**. Um die später neu zu starten, deaktivieren Sie die Option **Jetzt Computer neu starten**.



10. Um den Schutzstatus anzuzeigen, öffnen Sie die Schnittstelle **Sophos Intercept X**.



Der Status gibt an, dass Arcserve UDP 8.0 vor Ransomware-Angriffen, Malware, Webbedrohungen und Zero-Day-Exploits geschützt ist.

11. Um auf Sophos Central zuzugreifen, klicken Sie auf **Admin Login**. Es ermöglicht Ihnen, Sophos Intercept X Advanced Server zu verwalten, Warnungen und Richtlinien festzulegen usw.

    Hinweise:

    - Sie müssen in Arcserve UDP über Internetzugriff verfügen, um *Sophos Intercept X Advanced* und alle zugehörigen Updates zu installieren. Sophos Intercept X ist Cloud-basiert, und es sind keine Offline-Installationsprogramme verfügbar.
    - Wenn Sie bereits eine andere UDP-Instanz erworben haben und über ein Sophos-Konto über Arcserve verfügen, verwenden Sie dasselbe Konto für alle Arcserve UDP 8.0-Instanzen.
    - Wenn Sie bereits ein Sophos-Konto über einen anderen Kauf haben, z. B. direkt von Sophos, geben Sie eine andere E-Mail-Adresse für ein separates Konto bei Sophos Central an.
    - Wenn die Sophos-Installation aus irgendeinem Grund fehlschlägt, befolgen Sie die Anweisungen auf dem Bildschirm oder per E-Mail, die zusammen mit der Fehlermeldung bereitgestellt werden.
    - Um Updates für Sophos Intercept X Advanced for Server wie z. B. Malwaredefinitionsupdates und Versionsaktualisierungen zu erhalten, benötigen Sie einen gültigen und aktiven Wartungsvertrag oder ein Abonnement für Arcserve UDP.

Für weitere Unterstützung wenden Sie sich bitte telefonisch an den technischen Support von Arcserve (+1.844.765.7043), oder online, oder an Ihr lokales Arcserve-Supportbüro.

Kapitel 11: Best Practices

In diesem Abschnitt werden die folgenden Themen behandelt:

Best Practices für den Schutz des Arcserve UDP-Servers

Sie können ohne Datenverlust die Konsole vom alten Server auf einen neuen Server migrieren.

- Halten Sie die Backup-Lösung nicht in derselben Active Directory-Domäne.
- Verwenden Sie Backup-Konten.
- Verwenden Sie keine Domänenadministrator-Konten. Zum Beispiel ein Administrator, der Administratorrechte zum Lesen von E-Mails, Online-Browsing usw. verwendet.
- Trennen Sie die UDP-Konsole von RPS und erstellen Sie VSB für die UDP-Konsole.
- Verwenden Sie wenn möglich dediziertes Backup-Netzwerk / Vlan.
- Deaktivieren Sie wenn möglich SMBv1.

  Hinweis: Nicht deaktivierbar bei Verwendung von Red Hat / Centos v6.6 und älter, da diese SMB v1 verwenden.

Ausschließen von Dateien vom Antivirusscanning

Antivirus-Software kann die reibungslose Ausführung des Virtual Standby-Prozesses behindern, indem sie den Zugriff auf Dateien vorübergehend blockiert oder Dateien, die fälschlicherweise als verdächtig oder gefährlich klassifiziert werden, in Quarantäne stellt oder löscht. Sie können die meisten Antivirenprogramme so konfigurieren, dass sie bestimmte Dateien oder Ordner ausschließen, so dass Sie das Scannen bestimmter Daten überspringen können. Es ist wichtig, Ihre Antivirus-Software richtig zu konfigurieren, damit sie keine Sicherungs- und Wiederherstellungsvorgänge oder andere Prozessarten behindert.

In Hyper-V-Servern beschädigt die Antivirus-Software die VM-Konfigurationsdatei. Der Hyper-V-Server ändert den VM-Status in den Modus "save" um, und die VM wird beschädigt und kann nicht mehr verwendet werden. In solchen Fällen müssen Sie die VM löschen und eine vollständige Konvertierung durchführen, um eine neue VM zu erstellen.

Um sicherzustellen, dass der lokale und entfernte virtuelle Standby ordnungsgemäß funktioniert und um zu verhindern, dass die VM in den Speichermodus wechselt, schließen Sie die folgenden Dateien aus, die auf virtuelle Hyper-V-Maschinen ausgerichtet sind:

- Verzeichnis der Konfigurationsdateien des virtuellen Rechners:

  (Standard) C:\ProgramData\Microsoft\Windows\Hyper-V

  Verzeichnis der Konfigurationsdateien des virtuellen Arcserve UDP-Virtual Standby-Rechners

- Verzeichnis der virtuellen Festplattendateien des virtuellen Rechners:

  (Standard) C:\Benutzer\Öffentlich\Dokumente\Hyper-V\Virtual Hard Disks

  Verzeichnis der Festplattendateien des virtuellen Arcserve UDP-Virtual Standby-Rechners

- Snapshot-Dateienverzeichnis:

  (Standard) %systemdrive%\ProgramData\Microsoft\Windows\Hyper-V\Snapshots

  Verzeichnis der Snapshot-Dateien des virtuellen Arcserve UDP-Virtual Standby-Rechners

Konfigurieren von Multistreaming-Parametern

Einstellungen für Replikationen über das WAN sind unter folgendem Registrierungsschlüssel gespeichert:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\Network]

Die folgende Liste enthält die Registrierungsschlüssel und die dazugehörigen Standardwerte:

- "WAN_EnableAutoTunning"=REG_DWORD:0x00000001 (1)
- "WAN_ChunkSizeByte"=REG_DWORD:0x000010000 (65536)
- "WAN_NumberofStreams"=REG_DWORD:0x00000005 (5)
- "WAN_RTT_Threshold"=REG_DWORD:0x00000014 (20)
- "WAN_MultiStreamsMaxCacheSize"=REG_DWORD:0x04000000 (67108864)
- "WAN_SendCommandFragDataMerged"=REG_DWORD:0x00000000 (0)

Nachstehend werden die Einstellungen der Registrierungsschlüssel beschrieben:

WAN_EnableAutoTunning

Legt den Schalter für das Aktivieren bzw. Deaktivieren von Multistreaming fest. Bei einem Wert von 0 ist Multistreaming deaktiviert. Bei anderen Werten ist Multistreaming aktiviert. Der Standardwert für aktiviertes Multistreaming ist 1.

WAN_ChunkSizeByte

Gibt die Datenblockgröße für die einzelnen Pakete an. Die Paketgröße wirkt sich auf den Durchsatz aus. Bei einer höheren WAN-Bandbreite können die Datenblöcke weiter vergrößert werden.

Der Standardwert ist 64 KB. Zulässige Werte im Code sind 512 Byte bis 1 MB.

WAN_NumberofStreams

Gibt die Anzahl der Streams an, die im WAN erstellt werden müssen, wenn die Latenz über der angegebenen Anzahl für WAN_RTT_Threshold liegt. Die Standardanzahl von Streams ist 5. Zulässige Werte sind 1 bis 10.

WAN_RTT_Threshold

Wenn RTT höher als WAN_RTT_Threshold ist, werden mehrere Sockets erstellt. Die Einheit für WAN_RTT_Threshold ist Millisekunden (ms). Der Standardwert ist 20 Millisekunden. Zulässige Werte sind 20 ms bis 600 ms.

WAN_MultiStreamsMaxCacheSize

Gibt an, dass die Speichergröße zugeteilt wird, wenn Multistreaming aktiviert ist. Dieser Speicherpuffer wird verwendet, um empfangenen fragmentierten Speicher zwischenzuspeichern. Der Bereich reicht von 16MB bis 64MB. Der Standardwert beträgt 64 MB. Wenn der Wert 0 ist, wird er auf 64 MB festgelegt. Als Einheit für diesen Wert werden Byte verwendet.

WAN_SendCommandFragDataMerged

Gibt an, dass die Kommunikationsbibliothek Dateien in kleinen Gruppen zusammenfasst und in einem Block versendet, wenn der Wert nicht 0 ist. Wenn der Wert 0 ist, werden kleine Dateien einzeln versendet. Der Standardwert ist 0.

Hinweise:

- In Replikationsjobs ist die Socket-Verbindungszahl möglicherweise nicht mit der Registrierung WAN_NumberofStreams konsistent.

  Replikationsjob von nicht globaler Deduplizierung zu nicht globaler Deduplizierung

  Wenn RTT höher als WAN_RTT_Threshold ist, stimmt die Anzahl der Socket-Verbindungen mit WAN_NumberofStreams überein.

  Replikationsjob von nicht globaler Deduplizierung zu globaler Deduplizierung oder von globaler Deduplizierung zu globaler Deduplizierung

  Es gibt vier Arten von Verbindungen. Bei der Multistreaming-Funktion funktioniert nur die Datenblockverbindung. Wenn RTT höher als WAN_RTT_Threshold ist, beträgt die Socket-Verbindung insgesamt 3+WAN_NumberofStreams.

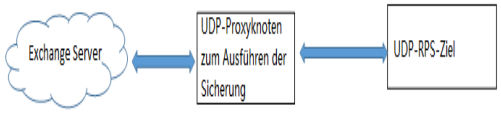
- Der Replikationsjob erkennt den Netzwerkstatus, um festzustellen, ob es sich um eine WAN-Verbindung handelt. Bei schwachem Netzwerkstatus kann LAN als WAN akzeptiert werden.

Infos zu Exchange Online

In diesem Abschnitt werden die folgenden Themen behandelt:

Konfiguration für optimale Leistung

Mögliche Topologie:



Sie können Proxy entweder auf dem RPS oder separat installieren. Für optimale Leistung empfehlen wir jedoch, beide im selben Knoten abzulegen.

Empfohlene Konfiguration für Proxy

- Architektur: 64-Bit-Windows-Computer. Für weitere Informationen über die unterstützten Betriebssysteme für Arcserve UDP, klicken Sie hier.
- Arbeitsspeicher: 8 GB oder höher
- CPU: 2 Prozessorkerne

Empfohlene Konfiguration für Recovery Point-Server:

Siehe Versionshinweise für Systemanforderungen.

Best Practices für Sicherungen

- Rechnen Sie mit längeren Sicherungszeiten während der ersten vollständigen Sicherung, die die Daten vom Microsoft Exchange Online-Server über eine WAN-Verbindung bezieht.
- Da die erste vollständige Sicherung lange dauert, stellen Sie die erforderliche Konfiguration für Hardware, Netzwerk und Ressourcen (z. B. Speicherplatz im Ziel, Arbeitsspeicher, CPU usw.) während der Sicherung bereit, um Unterbrechungen durch äußere Ausfälle zu vermeiden.
- Nehmen Sie die Sicherung vom Haltepunkt aus während eines der folgenden Szenarien wieder auf:
  - Stellen Sie sicher, dass eine Sicherung nicht während einem geplanten Ausfall oder einem Netzwerkausfall. Wenn eine Sicherung ausgeführt wird, brechen Sie sie ab. Wenn Sie eine Sicherung abbrechen, behält sie den teilweise gesicherten Wiederherstellungspunkt und die nächste geplante Sicherung kann vom Haltepunkt wiederaufgenommen werden.
  - Wenn der Rechner während der Sicherung unerwartet heruntergefahren wird oder der Prozess unerwartet beendet wird, wird der Wiederherstellungspunkt des ausgeführten Jobs entfernt. Starten Sie die Sicherung erneut. Sicherung wird nicht vom Haltepunkt aus gestartet. Alle Daten werden erneut gesichert.
- Wir empfehlen immer, einen Knoten mit automatischem Schutzmechanismus zu verwenden, um alle Postfächer zu schützen, einschließlich neu erstellter Postfächer nach der Erstellung des Plans.
- In Arcserve UDP ist die unterstützte Größe der geschützten Daten standardmäßig auf 8 Terabyte (komprimiert) begrenzt. Zum Konfigurieren der Größe können Sie den folgenden Registrierungswert auf dem Proxy-Knoten erstellen:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<NodeGUID>]

  " VirtualDiskSize "=dword:00000002

  Im obige Beispiel wird die Größe auf 2 TB festgelegt

  Hinweis: Wenn Sie die Größe des virtuellen Laufwerks vergrößern, wird der nächste inkrementelle Sicherungsauftrag in den vollen Zustand versetzt und wirkt sich auch auf die Geschwindigkeit der folgenden Aufträge aus:

Auf Band kopieren, Replikation, Wiederherstellungspunkte in die Cloud kopieren

- Wählen Sie die Größe des virtuellen Laufwerks basierend auf der aktuellen Größe und dem Wachstum der Quelldaten aus.

  Beispiel: Wenn die Gesamtgröße aller Benutzer 5 TB und das durchschnittliche Datenwachstum pro Tag 1 % beträgt, also 50 GB, benötigen Sie 5 TB + 50 GB * 30 Tage = 6.5 TB Speicherplatz für die ersten vollständigen und 30 tägliche inkrementelle Backups für einen Monat.

  Daher beträgt die erforderliche Mindestgröße des Datenträgers 7 TB (nicht komprimiert). Wenn Sie mehr Wiederherstellungspunkte beibehalten möchten, verwenden Sie die gleiche Methode zur Größenberechnung.

- Verwenden Sie die Drosselungspläne ordnungsgemäß, um sicherzustellen, dass dem Backup die gewünschte Bandbreite außerhalb der Geschäftszeiten zur Verfügung steht. Führen Sie eine kleine Sicherung mit wenigen Benutzern durch, um die Netzwerklast durch den Sicherungsauftrag einzuschätzen und die Drosselungswerte entsprechend anzupassen.

- Stellen Sie sicher, dass das Backup-Konto die obligatorischen Voraussetzungen erfüllt. Weitere Informationen finden Sie unter link.

- Wenn die für die Verbindung des Exchange Online-Servers genutzte Netzwerkverknüpfung instabil ist und regelmäßige Sicherungsabbrüche hervorruft, konfigurieren Sie die Richtlinie zur Aufbewahrung von Wiederherstellungspunkten, um eine große Anzahl von nicht zusammengeführten Sitzungen zu sichern.

  Standardwert für tägliche inkrementelle Backups: 7

  Standardwert für manuelle Backups: 31

  Konfigurieren Sie den Ablaufplan/die Ablaufpläne so, dass Sie mindestens einen täglichen, wöchentlichen und monatlichen Backup beibehalten.

- Vergewissern Sie sich, dass für die Installation ausreichend Lizenzen vorliegen. Sie können Lizenzen über den Lizenz-Manager verwalten. Weitere Informationen finden Sie unter Frage 4 im Abschnitt Häufig gestellte Fragen.

Best Practices zur Wiederherstellung

Stellen Sie sicher, dass das für die Wiederherstellung verwendete Konto über die Berechtigungen, die Identität des ausgewählten Zielnutzers anzunehmen, verfügt. Weitere Informationen finden Sie unter Link.

Häufig gestellte Fragen zu Exchange Online

1. Kann ich den RPS direkt zur Sicherung von Exchange Online-Benutzern ohne Anwendung eines Proxy verwenden?

   Ja.

2. Benötige ich ein Administrator-/ Gruppenadmin-Konto, um Exchange Online-Postfächer zu sichern?

   Nein, das Backup-Konto benötigt lediglich bestimmte Berechtigungen. Weitere Informationen finden Sie unter Link.

3. Welchen Durchsatz kann ich bei Exchange Online-Backups erwarten, wenn meine Internetbandbreite gut ist?

   Neben der Netzwerkbandbreite ist für den Durchsatz auch die Leserate der Daten vom Exchange-Server, die von der Beschaffung des Exchange Servers abhängig ist, ausschlaggebend.

   Manchmal verweigert der Exchange-Server die Verbindung mit Arcserve UDP, um Daten zu lesen. In solchen Fällen versucht Arcserve UDP erneut, eine erfolgreiche Verbindung herzustellen. Die längere Wartezeit führt zu niedrigeren Durchsatzzahlen.

4. Falls die Anzahl konfigurierter Benutzer im im Sicherungsplan die Anzahl der Lizenzen übersteigt, kann ich teilweise Backups für die lizenzierten Benutzer ausführen?

   Nein, das ist nicht möglich. Wenn Sie eine Sicherung für mehr Benutzer als die Anzahl der verfügbaren Lizenzen ausführen, schlägt die Sicherung für alle Benutzer fehl. Wenn Sie z. B. 100 zu schützende Benutzer in der Konsole Arcserve UDP konfiguriert haben und nur 90 verfügbare Lizenzen haben, schlägt die Sicherung fehl. Zum erfolgreichen Ausführen der Sicherung müssen Sie mindestens 10 Benutzer aus der Liste der geschützten Benutzer entfernen.

5. Wie kann ich die Leistung des Sicherungsdurchsatzes verbessern?

   Berücksichtigen Sie die folgenden Punkte, um eine optimale Durchsatzleistung zu sichern:

   - Unterteilen Sie eine große Sicherung in kleinere überschaubare Backup-Jobs.
   - Schließen Sie die Ordner, die nicht gesichert werden sollen, von den Planeinstellungen aus. z. B. Clutter, Synchronisierungsprobleme, u.s.w.

- Führen Sie eine periodische Überprüfung der internen und externen Netzwerkinfrastruktur durch.

Infos zu Microsoft Azure

In diesem Abschnitt werden die folgenden Themen behandelt:

Best Practices für eine Instant-VM auf Microsoft Azure

Um die Knoten im lokalen Netzwerk zu schützen, müssen Sie die UDP-Konsole auf dem Host installieren.

- Wählen Sie bei der Installation der UDP-Komponenten HTTPS als Protokoll aus.
- Am einfachsten lässt sich eine Ressourcengruppe erstellen, indem Sie mindestens eine Test-VM erstellen. Azure führt Sie durch die Schritte zur Erstellung aller Ressourcen für die Test-VM, die Sie für eine Standby-VM verwenden können.
- (Optional) Erstellen Sie einen RPS in Azure.

  Befolgen Sie diese Schritte:

  1. Öffnen Sie die eingehenden TCP-Ports 8014 und 8015.
  2. Wenn Sie von einem Remote-Webbrowser aus auf den RPS zugreifen, lösen Sie den Namen des RPS-Servers in die öffentlichen IP-Adresse auf.
  3. Verwenden Sie zur Replikation den freigegebenen Plan-Task "Auf remote verwalteten RPS replizieren".

Bereitstellen von Arcserve UDP für Microsoft Azure

Beachten Sie die folgenden Best Practices, bevor Sie Arcserve UDP in Microsoft Azure bereitstellen:

1. Sie müssen die Arcserve UDP-Konsole lokal installieren, um die Knoten zu schützen, die sich im lokalen Netzwerk befinden.
2. Wählen Sie das HTTPS-Protokoll während der Installation von Arcserve UDP-Komponenten aus.
3. Am einfachsten können Sie Azure-Ressourcen erstellen, indem Sie mindestens einen virtuellen Testrechner erstellen, den Sie später als Standby-VM verwenden können.

4. Erstellen Sie den Arcserve UDP-Recovery Point-Server in Azure.
    - Öffnen Sie die TCP-Ports 8014 und 8015 für eingehende Verbindungen.
    - Sie müssen den Namen des Recovery Point-Servers in die öffentliche IP-Adresse auflösen, wenn Sie auf über einen Remote-Webbrowser auf den Recovery Point-Server zugreifen.
    - Verwenden Sie zur Replikation von Tasks den freigegebenen Plan-Task **Auf remote verwalteten RPS replizieren**.

Kapitel 12: Fehlerbehebung

Dieser Abschnitt enthält folgende Themen:

Bei Arcserve UDP-Kommunikationsfehlern

Dieser Abschnitt enthält die folgenden Fehlerbehebungsthemen im Zusammenhang mit Arcserve UDP-Kommunikationsfehlern:

- Arcserve UDP kann nicht mit Windows-Knoten kommunizieren.
- Es können keine E-Mail-Alerts vom Gmail-Konto empfangen werden
- Arcserve UDP kann nicht mit dem Arcserve UDP Linux-Sicherungsserver auf Remote-Knoten kommunizieren
- Arcserve UDP kann nicht mit dem Arcserve UDP Recovery Point Server auf Remote-Knoten kommunizieren.
- Arcserve UDP kann nicht mit dem Arcserve Backup-Server auf Remote-Knoten kommunizieren
- Arcserve UDP kann nicht mit dem Remote-Standort kommunizieren.

Arcserve UDP kann nicht mit Windows-Knoten kommunizieren

Gilt für Windows-Betriebssysteme

Problem

Arcserve UDP kann nicht mit Windows-Knoten kommunizieren.

Lösung

Die folgende Tabelle enthält verschiedene Gründe, aufgrund derer Arcserve UDP nicht mit Windows-Knoten kommunizieren kann, sowie entsprechende Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Das Netzwerk war bei der Anwendung der Pläne nicht verfügbar oder instabil.	Stellen Sie sicher, dass das Netzwerk verfügbar und stabil ist, und versuchen Sie es dann erneut. Arcserve UDP kann den Remote-Knoten pingen, und der Remote-Knoten kann Arcserve UDP zurückpingen.
Die Netzwerkfreigabe "Admin$" des Remote-Knotens war beim Kommunikationsversuch von Arcserve UDP mit dem Knoten nicht verfügbar.	Stellen Sie sicher, dass der Netzwerk-Admin$ auf dem Remote-Knoten ausgeführt wird, und versuchen Sie es erneut.
Beim Versuch von Arcserve UDP, mit dem Knoten zu kommunizieren, konnte der Arcserve Unified Data Protection Agent für Windows-Knoten die Last nicht verarbeiten.	Stellen Sie sicher, dass sich die CPU auf dem Remote-Knoten von Arcserve Unified Data Protection Agent für Windows in einem Normalzustand befindet, und versuchen Sie die Kommunikation erneut.
Der Arcserve Unified Data Protection Agent für Windows-Dienst des Remote-Knotens war beim Kommunikationsversuch von Arcserve UDP mit dem Knoten nicht verfügbar.	Stellen Sie sicher, dass der Arcserve Unified Data Protection Agent für Windows-Dienst auf dem Remote-Knoten ausgeführt wird, und versuchen Sie es erneut.
Es wurde ein falsches Protokoll oder ein falscher Port zur Kommunikation mit dem Knoten verwendet.	Verwenden Sie das richtige Protokoll oder den richtigen Port, um den Remote-Knoten in der Arcserve UDP-Knotenansicht hinzuzufügen bzw. ihn zu aktualisieren.
Die Kommunikation des Arcserve Unified Data Protection Agent für Windows-Diensts ist nicht korrekt ausgefallen.	Starten Sie den Arcserve Unified Data Protection Agent für Windows-Dienst auf dem Remote-Knoten neu, und versuchen Sie es erneut.

Es können keine E-Mail-Alerts vom Gmail-Konto empfangen werden

Das Gmail-Konto wird von Google blockiert, wenn Sie das Gmail-Konto in Ihren E-Mail-Einstellungen verwenden.

Gültig auf Windows-Plattformen.

Problem

Wenn Sie Gmail-Konten konfigurieren, erhalten Sie keine E-Mail-Alerts. Wenn Sie versuchen, das Gmail-Konto für E-Mail-Alerts zu konfigurieren und auf "Test-E-Mail senden" klicken, wird Sie eine der folgenden Fehlermeldungen angezeigt:

Die Test-E-Mail ist aufgrund falscher Benutzeranmeldeinformationen fehlgeschlagen.

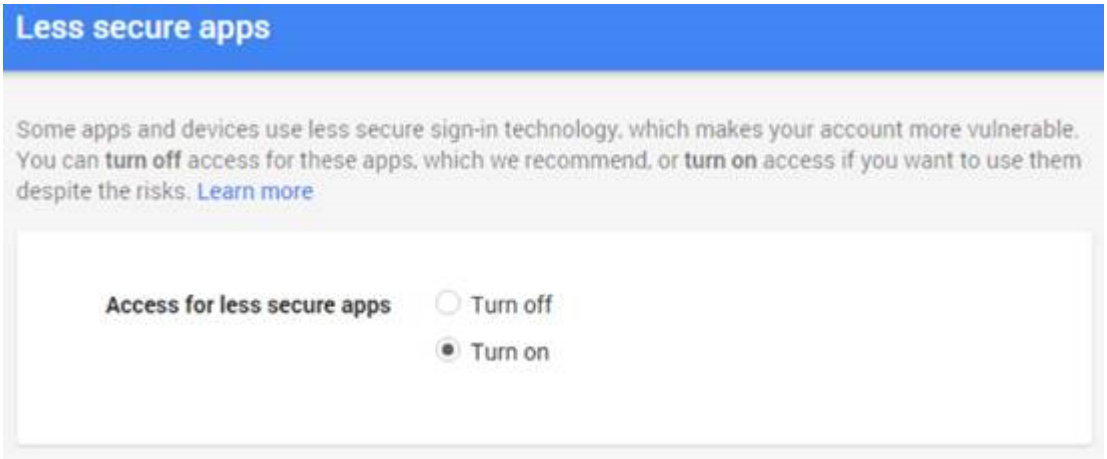
oder

Das Senden der Test-E-Mail ist fehlgeschlagen: Ungültige Benutzeranmeldeinformationen.

Lösung

1. Geben Sie die richtigen Anmeldeinformationen ein, und versuchen Sie es erneut.
2. Die Google-Sicherheit blockiert E-Mails von Gmail-Konten, die außerhalb von Google konfiguriert wurden. Um dies zu vermeiden, ändern Sie Einstellungen unter dem folgenden Link durch Auswahl von "Aktivieren", um Zugriff für weniger sichere Apps zu verwenden:

   https://www.google.com/settings/security/lesssecureapps



Arcserve UDP kann nicht mit dem Arcserve UDP Linux-Sicherungsserver auf Remote-Knoten kommunizieren

Gilt für Linux Betriebssysteme

Problem

Arcserve UDP kann nicht mit dem Arcserve UDP Linux-Sicherungsserver auf Remote-Knoten kommunizieren.

Lösung

Die folgende Tabelle enthält verschiedene Gründe, aufgrund derer Arcserve UDP nicht mit dem Arcserve UDP Linux-Sicherungsserver auf Remote-Knoten kommunizieren kann, sowie entsprechende Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Das Netzwerk war nicht verfügbar oder instabil, als Arcserve UDP versuchte, mit dem Knoten des Linux-Sicherungsservers zu kommunizieren.	Stellen Sie sicher, dass das Netzwerk verfügbar und stabil ist, und versuchen Sie es dann erneut. Arcserve UDP kann den Remote-Knoten des Linux-Sicherungsservers pingen, und der Remote-Knoten kann Arcserve UDP zurückpingen.
Beim Versuch von Arcserve UDP, mit dem Knoten zu kommunizieren, konnte der Arcserve UDP Linux-Sicherungsserverknoten die Last nicht verarbeiten.	Stellen Sie sicher, dass sich die CPU auf dem Arcserve UDP Linux-Sicherungsserverknoten im Normalzustand befindet, und versuchen Sie es erneut.
Der Arcserve UDP Linux-Sicherungsserver-Dienst auf dem Remote-Knoten wurde nicht ausgeführt, als Arcserve UDP versuchte, mit dem Knoten zu kommunizieren.	Stellen Sie sicher, dass der Arcserve UDP Linux-Sicherungsserver-Dienst auf dem Remote-Knoten ausgeführt wird, und versuchen Sie es erneut.
Der Arcserve UDP Linux-Sicherungsserver-Dienst hat nicht ordnungsgemäß kommuniziert.	Starten Sie den Arcserve UDP Linux-Sicherungsserver-Dienst auf dem Remote-Knoten neu, und versuchen Sie es erneut.

Arcserve UDP kann nicht mit dem Arcserve UDP Recovery Point Server auf Remote-Knoten kommunizieren.

Gilt für Windows-Betriebssysteme.

Problem

Arcserve UDP kann nicht mit dem Arcserve UDP-Recovery Point Server auf Remote-Knoten kommunizieren.

Lösung

Die folgende Tabelle beschreibt Gründe und die entsprechenden Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Das Netzwerk war beim Versuch von Arcserve UDP, mit dem Recovery Point Server-Knoten zu kommunizieren, nicht verfügbar.	Stellen Sie sicher, dass das Netzwerk verfügbar und stabil ist, und versuchen Sie es dann erneut. Arcserve UDP kann den Remote-Recovery Point Server-Knoten anpingen, und der Remote-Recovery Point Server-Knoten kann einen Ping an Arcserve UDP zurücksenden.
Die Freigabe des Arcserve UDP-Recovery Point Server-Knotens vom Netzwerkadministrator war beim Kommunikationsversuch von Arcserve UDP mit dem Knoten nicht verfügbar.	Stellen Sie sicher, dass der Netzwerk-Admin$ auf dem Recovery Point Server-Knoten ausgeführt wird, und versuchen Sie es erneut.
Beim Versuch von Arcserve UDP, mit dem Server zu kommunizieren, konnte der Arcserve UDP-Recovery Point Server-Knoten die Last nicht verarbeiten.	Stellen Sie sicher, dass sich die CPU auf dem Remote-Recovery Point Server-Knoten im Normalzustand befindet, und versuchen Sie es erneut.
Der Arcserve UDP-Agent-Dienst, der Arcserve UDP-RPS-Datenspeicherdienst oder der Arcserve UDP-RPS-Portfreigabedienst auf dem Remote-Knoten wurde nicht ausgeführt, als Arcserve UDP versuchte, mit dem Knoten zu kommunizieren.	Überprüfen Sie, ob der Arcserve UDP-Agent-Dienst, der Arcserve UDP-RPS-Datenspeicherdienst und der Arcserve UDP-RPS-Portfreigabedienst auf dem Remote-Knoten ausgeführt werden, und versuchen Sie es erneut.
Es wurde ein falsches Protokoll oder ein falscher Port zur Kommunikation mit dem Recovery Point Server-Knoten verwendet.	Verwenden Sie das richtige Protokoll bzw. den richtigen Port, um den Recovery Point Server-Knoten in der Arcserve UDP-Zielknotenansicht hinzuzufügen bzw. zu aktualisieren.
Der Arcserve UDP-Agent-Dienst, der Arcserve UDP-RPS-Datenspeicherdienst oder	Starten Sie den Arcserve UDP-Agent-

der Arcserve UDP-RPS-Portfreigabedienst hat nicht richtig kommuniziert.	Dienst, den Arcserve UDP-RPS-Daten-speicherdienst und den Arcserve UDP-RPS-Portfreigabedienst auf dem Remote-Knoten neu, und versuchen Sie es erneut.

Arcserve UDP kann nicht mit dem Arcserve Backup-Server auf Remote-Knoten kommunizieren

Gilt für Windows-Betriebssysteme

Problem

Arcserve UDP kann nicht mit dem Arcserve Backup-Server auf Remote-Knoten kommunizieren.

Lösung

Die folgende Tabelle enthält verschiedene Gründe, aufgrund derer Arcserve UDP nicht mit dem Arcserve UDP-Server auf Remote-Knoten kommunizieren kann, sowie entsprechende Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Das Netzwerk war beim Versuch von Arcserve UDP, mit dem Knoten des Arcserve Backup-Servers zu kommunizieren, nicht verfügbar.	Stellen Sie sicher, dass das Netzwerk verfügbar und stabil ist, und versuchen Sie es dann erneut. Arcserve UDP kann den Remote-Knoten des Arcserve Backup-Servers pingen, und der Remote-Knoten kann Arcserve UDP zurückpingen.
Beim Versuch von Arcserve UDP, mit dem Knoten zu kommunizieren, konnte der Arcserve Backup-Serverknoten die Last nicht verarbeiten.	Stellen Sie sicher, dass sich die CPU auf dem Arcserve Backup-Server-Remote-Knoten im Normalzustand befindet, und versuchen Sie es erneut.
Der Arcserve Backup-Server-Dienst auf dem Remote-Knoten wurde nicht ausgeführt, als Arcserve UDP versuchte, mit dem Knoten zu kommunizieren.	Stellen Sie sicher, dass der Arcserve Backup-Server auf dem Remote-Knoten ausgeführt wird, und versuchen Sie es erneut.
Es wurde ein falsches Protokoll oder ein falscher Port zur Kommunikation mit dem Arcserve Backup-Server-Knoten verwendet.	Verwenden Sie das richtige Protokoll bzw. den richtigen Port, um den Knoten des Arcserve Backup-Servers in der Arcserve UDP-Zielknotenansicht hinzuzufügen bzw. zu aktualisieren.
Die Kommunikation beim Arcserve Backup-Server-Dienst hat nicht ordnungsgemäß funktioniert.	Starten Sie den Arcserve Backup-Server-Dienst auf dem Remote-Knoten neu, und versuchen Sie es erneut.

Arcserve UDP kann nicht mit dem Remote-Standort kommunizieren

Gilt für Windows-Betriebssysteme

Problem

Arcserve UDP kann nicht mit dem Remote-Standort kommunizieren.

Lösung

Die folgende Tabelle enthält verschiedene Gründe, aufgrund derer Arcserve UDP nicht mit dem Remote-Standort kommunizieren kann, sowie entsprechende Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Das Netzwerk ist nicht verfügbar oder instabil.	Stellen Sie sicher, dass das Netzwerk verfügbar und stabil ist, und versuchen Sie es dann erneut.
Arcserve UDP wird neu installiert, und der Remote-Standort ist in Arcserve UDP nicht registriert.	Registrieren Sie den Remote-Standort bei Arcserve UDP.
Der Hostname oder die IP-Adresse von Arcserve UDP hat sich geändert, und der Remote-Standort ist in Arcserve UDP nicht registriert.	Registrieren Sie den Remote-Standort bei Arcserve UDP.
Den Hostname oder die IP-Adresse des Remote-Standorts hat sich geändert, und der Remote-Standort ist in Arcserve UDP nicht registriert.	Registrieren Sie den Remote-Standort bei Arcserve UDP.

Bei Plänen, Jobs und Einstellungen

Dieser Abschnitt enthält die folgenden Fehlerbehebungsthemen im Zusammenhang mit Sicherungsjob und Einstellungen:

- Fehlgeschlagener Sicherungsjob nach Änderung von Hostname/IP-Adresse der Konsole
- Hinzufügen eines Verschlüsselungskennworts für ein vorhandenes verschlüsseltes Ziel
- Anwendung von Sicherungseinstellungen für Knoten nicht möglich
- Fehlgeschlagene Planbereitstellung nach Änderung des Kennworts des agentenlosen Sicherungs-Proxy-Rechners
- Einstellungen beim Öffnen der Agent-Benutzeroberfläche deaktiviert
- Unterbrechen und Wiederaufnehmen schlägt fehl, wenn Agent nicht mit dem Netzwerk verbunden ist
- Arcserve UDP Agent-Dienst wird nur langsam ausgeführt
- Konfigurieren der Registrierung, um einen Kopie auf Band-Job erneut auszuführen
- Konfigurieren der Registrierung, um mehrere Wiederherstellungspunkte desselben Typs im gleichen Job auf Band zu kopieren
- Datei/Ordner fehlte in der Sicherung des freigegebenen NFS-Ordners oder Datei-/Ordnername wurde in einen unbrauchbaren Namen umgewandelt
- Die Sicherung des freigegebenen NFS-Ordners schlägt fehl
- Falscher Servername bei Lizenzanforderung für UNC-Pfade
- Zurücksetzen der MFA-aktivierten UDP-Konsole, wenn TOTP nicht verfügbar ist

Fehlgeschlagener Sicherungsjob nach Änderung von Hostname/IP-Adresse der Konsole

Problem

Konsole und RPS-Server wurden auf demselben Rechner installiert. Die Sicherung funktionierte anfangs problemlos, doch seit einer Änderung des Hostnamens oder der IP-Adresse der Konsole schlägt der Sicherungsjob fehl.

Lösung

Dieses Problem tritt auf, wenn Pläne zu Knoten zugewiesen sind und Sie den Hostnamen oder die IP-Adresse dieses Rechners ändern.

Um dieses Problem zu lösen, aktualisieren Sie den Agentenknoten manuell, und führen Sie den Sicherungsjob erneut aus.

Befolgen Sie diese Schritte:

1. Navigieren Sie zur Seite "Knoten": "Alle Knoten".
2. Wählen Sie den Knoten aus.
3. Klicken Sie mit der rechten Maustaste, und wählen Sie **Aktualisieren** aus.
4. Klicken Sie auf **OK**.

Die Knoten werden aktualisiert.

So fügen Sie ein Verschlüsselungskennwort für ein vorhandenes verschlüsseltes Ziel hinzu

Problem

Sie haben vergessen, das Verschlüsselungskennwort für das Dateikopieziel anzugeben.

Lösung

Sie können das Verschlüsselungskennwort jetzt hinzufügen.

Gehen Sie wie folgt vor:

1. Öffnen Sie den Plan.
2. Öffnen Sie das Dateikopieziel, in dem Sie das Verschlüsselungskennwort hinzufügen müssen.
3. Ändern Sie den Zieltyp von "Cloud-Speicher\Netzwerkfreigabe" in "Netzwerkfreigabe\Cloud-Speicher".
4. Geben Sie eine Netzwerkfreigabe oder einen Cloud-Speicher an, und speichern Sie.
5. Öffnen Sie den Plan erneut, und wechseln Sie zum Dateikopieziel.
6. Ändern Sie das Ziel in "Cloud-Anbieter\Netzwerkfreigabe".
7. Wählen Sie den Cloud-Anbieter oder die Netzwerkfreigabe aus, und wählen Sie dann den Bucket oder Container\Anbieter-Pfad.
8. Geben Sie das richtige Verschlüsselungskennwort ein.
9. Speichern Sie den Plan.

Anwendung von Sicherungseinstellungen für Knoten nicht möglich

Problem

Ich habe zwei Konsolen: Konsole A und Konsole B. Ich füge einen Recovery Point Server (RPS) zu Konsole A hinzu und erstelle einen Plan für den RPS. Anschließend füge ich den RPS zu Konsole B hinzu. Jetzt wird dieser RPS von Konsole B verwaltet. Beim Aktualisieren des Agentenknoten über Konsole A, die auf dem RPS gesichert ist, erhalte ich jedoch den folgenden Fehler:

"Sicherungseinstellungen" lassen sich nicht auf Knoten anwenden. (Der Plan des Arcserve-UDP-Recovery Point-Servers wurde auf diesem Server nicht gefunden.)

Lösung

Um diesen Fehler zu vermeiden, folgen Sie diesen Schritten:

1. Wählen Sie den Plan über Konsole A aus,
2. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, und wählen Sie dann "**Jetzt bereitstellen**" aus.

   Der Plan wird erneut bereitgestellt und die Sicherungseinstellungen werden auf den Knoten angewendet.

Fehlgeschlagene Planbereitstellung nach Änderung des Kennworts des agentenlosen Sicherungs-Proxy-Rechners

Problem

Wenn sich die Konsole und der Proxy-Server auf unterschiedlichen Rechnern befinden, schlägt die erneute Bereitstellung des Plans nach dem Ändern des Kennworts für den Proxy-Rechner fehl. Die Fehlermeldung gibt an, dass die Anmeldeinformationen nicht korrekt sind.

Lösung

Führen Sie diese Schritte aus, um das Problem zu beheben:

1. Aktualisieren Sie in der Knotenansicht der Konsole den Proxy-Server mit neuen Anmeldeinformationen.
    a. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.
    b. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie **Aktualisieren**, um den Proxy-Server zu aktualisieren.
2. Wenn sich die Konsole und der Proxy-Server auf dem gleichen Rechner befinden, aktualisieren Sie den RPS mit neuen Anmeldeinformationen.
    a. Gehen Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.
    b. Klicken Sie im mittleren Fensterbereich mit der rechten Maustaste auf den RPS, und wählen Sie **Aktualisieren**.
3. Starten Sie den Arcserve UDP Agent-Dienst auf dem Proxy-Rechner neu.
4. Stellen Sie den Plan erneut bereit.

Einstellungen beim Öffnen der Agent-Benutzeroberfläche deaktiviert

Wenn Knoten von Arcserve UDP Agent (Windows) vor der Deinstallation der Arcserve UDP-Konsole nicht von der Arcserve UDP-Benutzeroberfläche entfernt werden, sind die Einstellungen deaktiviert, wenn die Agent-Benutzeroberfläche auf diesen Knoten von Arcserve UDP Agent (Windows) geöffnet wird.

Problem

Der Arcserve UDP Agent (Windows)-Knoten wird nicht benachrichtigt, dass die Arcserve UDP-Konsole deinstalliert wurde. Er verhält sich wie ein verwalteter Knoten.

Lösung

Entfernen Sie im Knoten von Arcserve UDP Agent (Windows) die Dateien "RegConfigPM.xml" und "BackupConfiguration.xml" aus dem Verzeichnis "<UDP_ENGINE_HOME>\Configuration", und starten Sie den Windows-Dienst "Arcserve UDP Agent Service" neu.

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Unterbrechen und Wiederaufnehmen schlägt fehl, wenn Agent nicht mit dem Netzwerk verbunden ist

Problem

Wenn versucht wird, einen Plan zu unterbrechen, wenn der Agent nicht mit dem Netzwerk verbunden ist, wird der Plan nicht unterbrochen. Wenn versucht wird, einen Plan zu wiederaufzunehmen, wenn der Agent nicht mit dem Netzwerk verbunden ist, wird der Plan nicht wiederaufgenommen.

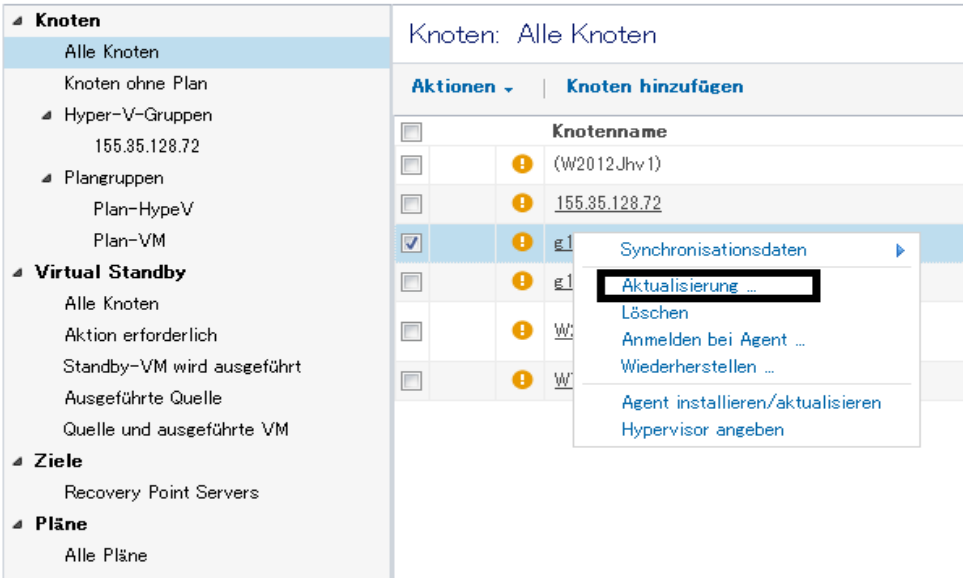
Lösung

Sie können dieses Problem beheben, indem Sie den Knoten manuell über die Konsole aktualisieren.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte Ressourcen.
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf Alle Knoten.

   Alle hinzugefügten Knoten werden im mittleren Fensterbereich angezeigt.
3. Wählen Sie den Knoten im mittleren Fensterbereich aus.
4. Klicken Sie mit der rechten Maustaste, und wählen Sie **Aktualisieren** aus.



Der Knoten und der Plan werden aktualisiert.

Der Arcserve UDP Agent-Dienst wird nur langsam ausgeführt.

Gültig auf Windows-Betriebssystemen

Symptom 1:

Die Ausführung des Arcserve UDP-Agent-Diensts auf Arcserve UDP-Agentensystemen ist langsam. Es kann zu weiteren Symptomen kommen, wie:

- Der Arcserve UDP-Agent-Dienst reagiert nicht mehr oder belegt 100 % der CPU-Ressourcen.
- Arcserve UDP-Agentenknoten funktionieren nicht ordnungsgemäß oder können nicht mit dem Webservice kommunizieren.

Lösung 1:

In mehreren Umgebungskonfigurationen ist feststellbar, dass der Arcserve UDP-Agent-Dienst zu viel CPU-Zeit in Anspruch nimmt oder die Reaktionszeit zu lange ist. Standardmäßig wird Tomcat konfiguriert, um den Knoten einen beschränkten Speicher zuzuweisen, der möglicherweise nicht für Ihre Umgebung geeignet sind. Um diesem Problem nachzugehen, überprüfen Sie folgende Protokolldateien:

<D2D_home>\TOMCAT\logs\casad2dwebsvc-stdout.*.log
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stder.*.log
<D2D_home>\TOMCAT\logs\catalina.*.log
<D2D_home>\TOMCAT\logs\localhost.*.log

Suchen Sie die folgende Meldung:

java.lang.OutOfMemoryError

Um dieses Problem zu beheben, erhöhen Sie den zugewiesenen Speicher.

Führen Sie folgende Schritte aus, um den Speicher zu erhöhen:

1. Öffnen Sie den Registrierungs-Editor, und wählen Sie den folgenden Schlüssel aus:

   x86-Betriebssysteme:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java

   x64-Betriebssysteme:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java

2. Verwenden Sie eine der folgenden Optionen:

- Wenn folgende Meldung in der Protokolldatei angezeigt wird:

  java.lang.OutOfMemoryError: PermGen-Bereich

  Hängen Sie Folgendes dem Wert der Optionen an.

  -XX:PermSize=128M -XX:MaxPermSize=128M

  Hinweis: Möglicherweise müssen Sie den Wert "-XX:MaxPermSize" erhöhen, um Ihre Umgebung anzupassen.

- Wenn eine der folgenden Meldung in der Protokolldatei angezeigt wird:

  java.lang.OutOfMemoryError: Java heap space
  java.lang.OutOfMemoryError: GC overhead limit exceeded

  Erhöhen Sie den Wert des folgenden DWORD:

  JvmMx

3. Starten Sie den Arcserve UDP-Agent-Dienst neu.

Symptom 2

Geplante Sicherungen werden übersprungen und nicht mehr ausgeführt.

Lösung 2

Wenn Sie den maximalen Wert für gleichzeitige Sicherungen auf 20 oder weniger festlegen, gehen Sie wie folgt vor:

1. Erhöhen Sie den Wert des folgenden DWORD:

   JvmMx=256

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.

2. Hängen Sie Folgendes dem Wert der Optionen an.

   -XX:MaxPermSize=128M

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.

Wenn Sie den maximalen Wert für gleichzeitige Sicherungen auf mehr als 20 aber unter 50 festlegen, gehen Sie wie folgt vor:

1. Erhöhen Sie den Wert des folgenden DWORD:

   JvmMx=512

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.

2. Hängen Sie Folgendes dem Wert der Optionen an.

   -XX:MaxPermSize=256M

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.

Konfigurieren der Registrierung, um einen Kopie auf Band-Job erneut auszuführen

Problem

Der Kopie auf Band-Job wurde aufgrund eines Datenträgerfehlers nicht ausgeführt, und Sie möchten den Job erneut auszuführen.

Lösung

Sie können die Anzahl der Wiederholungsversuche und das Zeitintervall der wiederholten Jobs für den "Kopie auf Band"-Task mit den folgenden zwei Registrierungsschlüsseln steuern. Beide Registrierungsschlüssel befinden sich auf dem Rechner, auf dem Sie Arcserve Backup Server installiert haben:

NumberOfRetryCopyToTapeJob

Wenn ein Kopie auf Band-Job fehlschlägt, wird der fehlgeschlagene Job von Arcserve UDP wiederholt. Die Anzahl der Wiederholungsversuche wird mit dem Registrierungsschlüssel **NumberOfRetryCopyToTapeJob** konfiguriert. Wenn jedoch Informationen zum Kopierziel (Knoten) oder Wiederherstellungspunkt im Job geändert werden, setzt Arcserve UDP die akkumulierte fehlgeschlagene Anzahl auf 0 zurück. In diesem Fall kann der Kopie auf Band-Job ausgeführt werden, ohne durch die Anzahl der Wiederholungsversuche begrenzt zu werden. Auch wenn der Arcserve Backup-Webservice neu gestartet wird, setzt Arcserve UDP die akkumulierte fehlgeschlagene Anzahl auf 0 zurück.

Der Registrierungsschlüssel befindet sich auf dem Arcserve Backup Server an folgendem Speicherort:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo\NumberOfRetryCopyToTapeJob

Der Typ ist DWORD.

Standard: 1

TimeIntervalOfRetryCopyToTapeJob

Steuert das Zeitintervall der Wiederholungsversuche für den fehlgeschlagenen Kopie auf Band-Job. Dieser Registrierungsschlüssel wird in Verbindung mit **NumberOfRetryCopyToTapeJob** verwendet.

Der Registrierungsschlüssel befindet sich auf dem Arcserve Backup Server an folgendem Speicherort:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo\TimeIntervalOfRetryCopyToTapeJob

Der Typ ist DWORD.

Standard: 1 Stunde

Konfigurieren der Registrierung, um mehrere Wiederherstellungspunkte desselben Typs im gleichen Job auf Band zu kopieren

Problem

Bei einem "Kopie auf Band"-Job werden standardmäßig alle qualifizierten Wiederherstellungspunkte auf Band kopiert, auch wenn sie zu demselben Typ gehören. Infolgedessen wird mehr Speicherplatz verbraucht und der Kopiervorgang nimmt viel Zeit in Anspruch. Sie sollten nur den neuesten der qualifizierten Wiederherstellungspunkte kopieren.

Lösung

Sie können die Registrierung auf dem Arcserve Backup-Serverknoten so konfigurieren, dass der neueste Wiederherstellungspunkt eines Typs auf Band kopiert wird.

Gehen Sie wie folgt vor:

1. Fügen Sie auf dem Arcserve Backup-Serverknoten den folgenden DWORD-Wert unter [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo] zur Registrierung hinzu:

   "CopyLatestRecoveryPointOfSameType"=dword:00000001

2. Starten Sie den Arcserve Backup-Server-Webdienst neu, damit die Änderungen wirksam werden.

   Bei allen "Kopie auf Band"-Jobs auf dem Arcserve Backup-Serverknoten wird der neueste Wiederherstellungspunkt eines Typs auf Band kopiert.

Datei/Ordner fehlte in der Sicherung des freigegebenen NFS-Ordners oder Datei-/Ordnername wurde in einen unbrauchbaren Namen umgewandelt

Problem

Wenn die Sicherung des freigegebenen NFS-Ordners durchgeführt wird, fehlen in den Sicherungsdaten einige Dateien/Ordner oder der Name einer Datei bzw. eines Ordners wird in einen unbrauchbaren Datei-/Ordnernamen umgewandelt.

Lösung

Dieses Problem tritt auf, wenn eine Datei bzw. ein Ordner im freigegebenen NFS-Ordner einen Namen mit einer Sprachcodierung aufweist, die nicht unterstützt wird. Exportieren Sie als Lösung einen freigegebenen SMB-Ordner an Stelle eines freigegebenen NFS-Ordners. Ziehen Sie auch das Hinzufügen eines UNC- oder NFS-Pfades mit SMB-Protokoll in Erwägung.

Weitere Informationen über das Hinzufügen eines UNC-Pfades und die unterstützte Sprachcodierung finden Sie unter Hinzufügen eines UNC-Pfades.

Die Sicherung des freigegebenen NFS-Ordners schlägt fehl

Problem

Wenn die Sicherung des freigegebenen NFS-Ordners durchgeführt wird, schlägt der Job fehl.

Lösung

Dieses Problem tritt auf, wenn die GID (Gruppen-ID) und die UID (Benutzer-ID) Werte geändert und die Standardwerte nicht mehr verwendet werden. Verwenden Sie stets ausschließlich die GID- und UID-Standardwerte für den NFS-Client und den NFS-Server.

Zurücksetzen der MFA-aktivierten UDP-Konsole, wenn TOTP nicht verfügbar ist

Problem

Nachdem der Anmeldeprozess für die Multi-Faktor-Authentifizierung (MFA) auf der UDP-Konsole aktiviert wurde, können Sie:

- Der QR-Code muss nicht gescannt werden
- Verlust des mobilen Geräts, das eine Authentifizierungs-App enthält
- Deinstallieren der Authentifikator-App

Lösung 1

Wenn Sie Super-Administrator oder Administrator oder Nicht-Administrator sind, wenden Sie sich an Ihren Administrator oder andere Admin-Benutzer von UDP, um den QR-Code von der UDP-Konsole zurückzusetzen.

Lösung 2

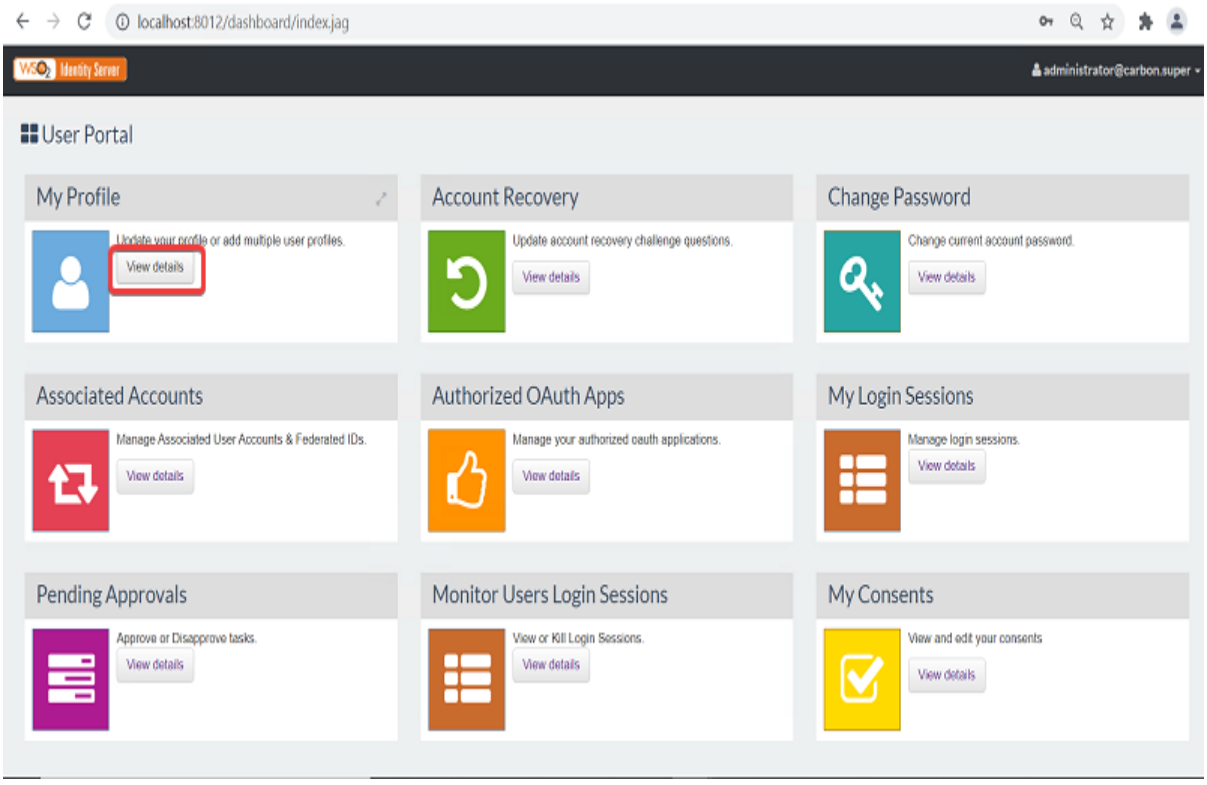
Wenn Sie Super-Administrator oder Administrator sind, können Sie das QR-Code-Image mithilfe des Identity Server-Dashboard-Portals nach einem neuen TOTP durchsuchen.

Befolgen Sie diese Schritte:

1. Melden Sie sich beim Identity Server-Dashboard an.

   Zum Beispiel: *https://localhost:8012/dashboard*

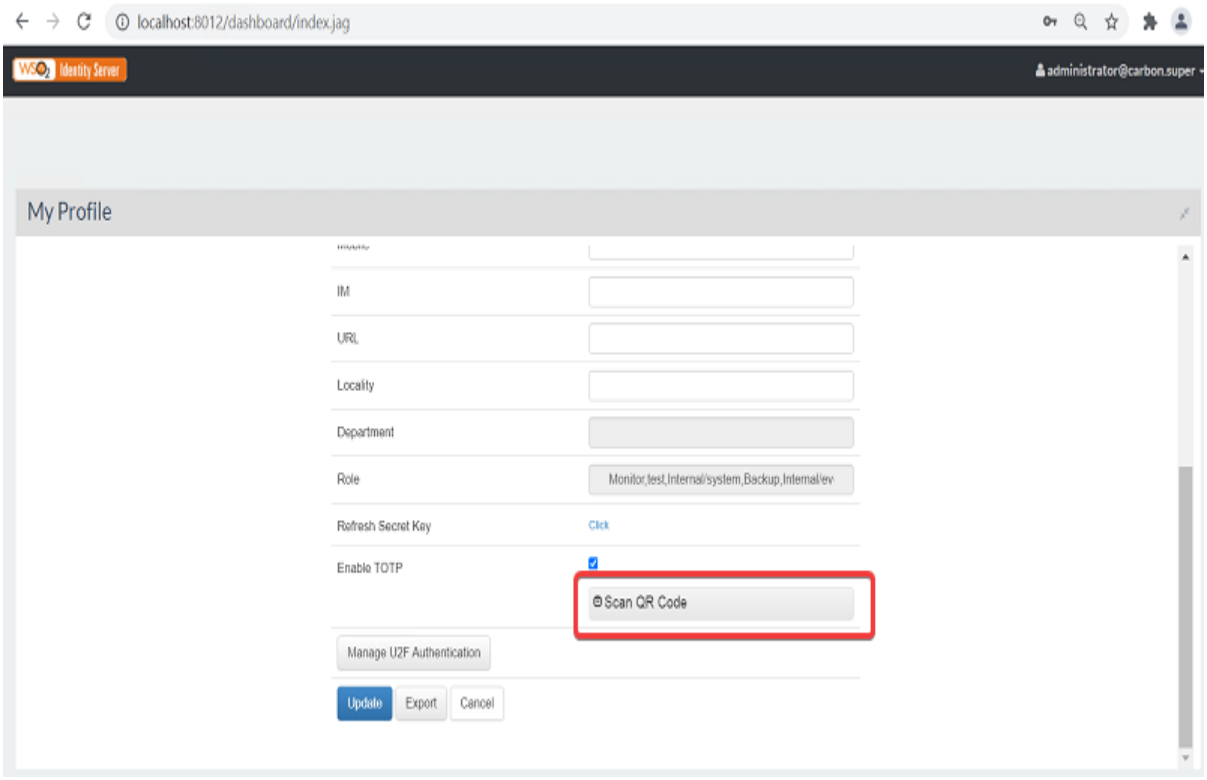
   Die Seite Benutzerportal wird angezeigt:



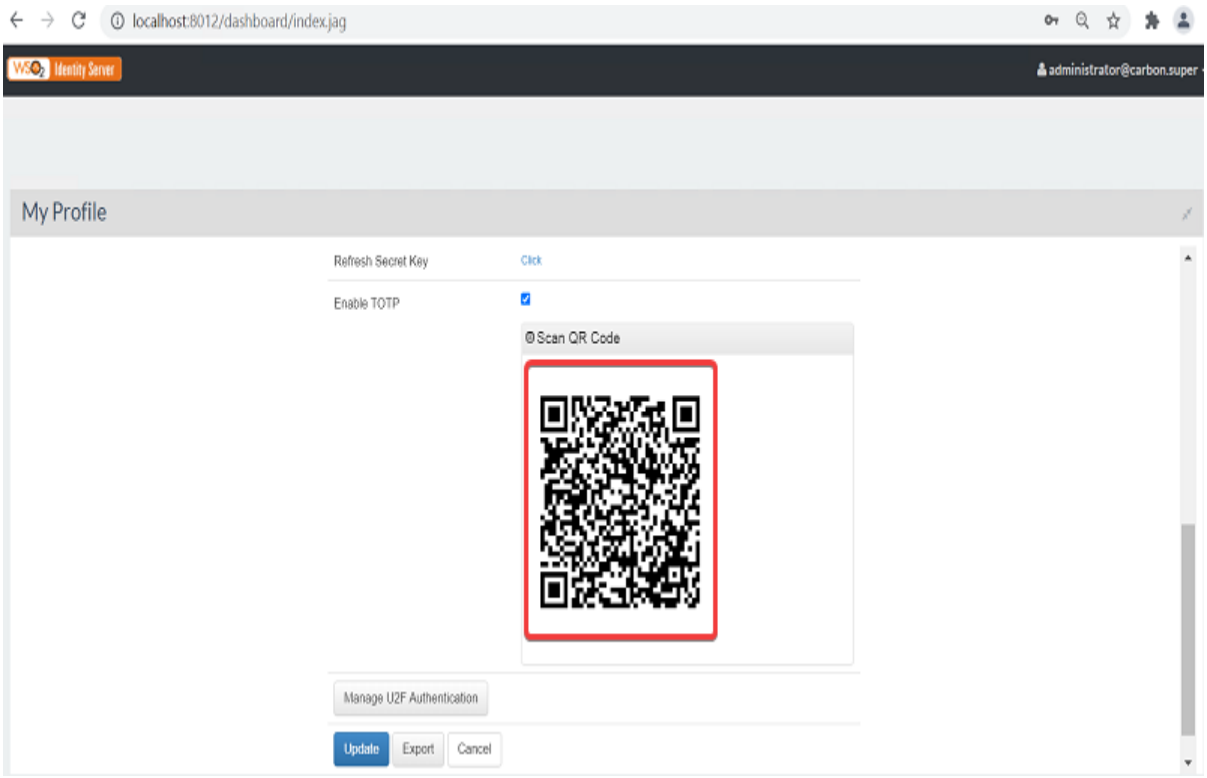
2. Klicken Sie auf der Seite Benutzerportal auf **Details anzeigen**.

   Die Seite "Mein Profil" wird angezeigt.

3. Klicken Sie auf der Seite Mein Profil unter TOTP aktivieren auf **QR-Code durchsuchen**, um ein Bild mit dem QR-Code anzuzeigen.



4. Scannen Sie das QR-Code-Bild mithilfe einer Authentifizierungs-App, um den TOTP zu generieren.



5. Gehen Sie zur Anmeldeseite der UDP-Konsole, und melden Sie sich dann mit dem neu generierten TOTP an.

Lösung 3

Wenn Sie ein Super-Administrator sind, können Sie die vorhandenen Einstellungen vollständig entfernen.

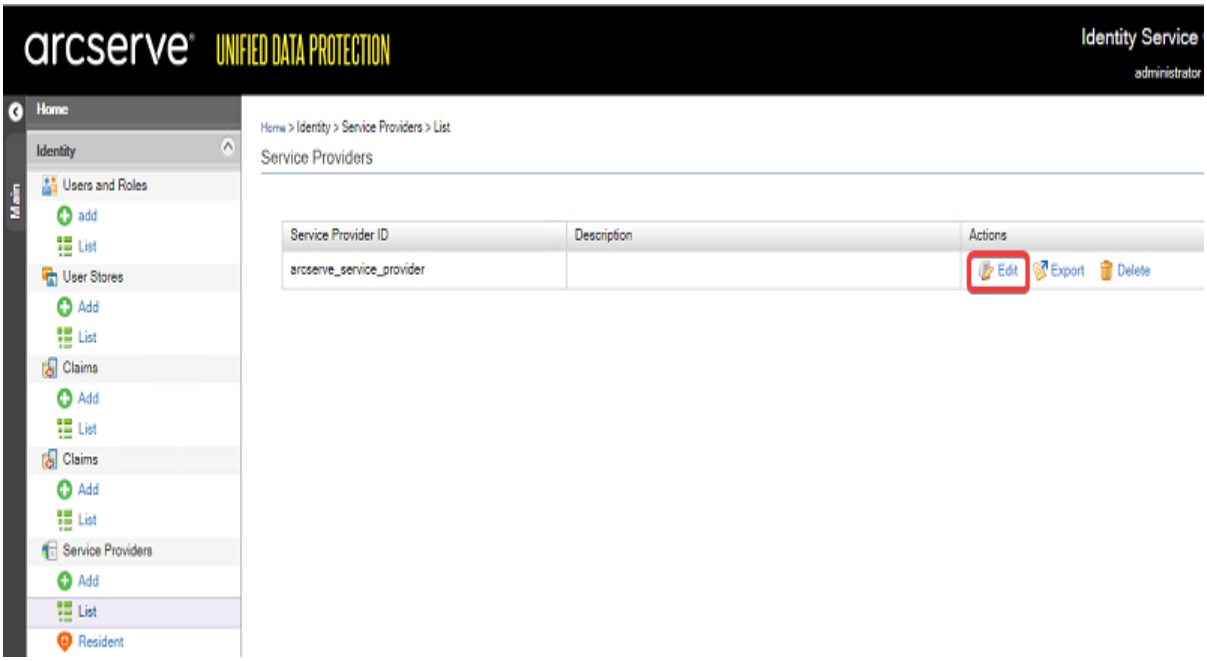
Befolgen Sie diese Schritte:

1. Navigieren Sie zum Pfad *…\Programme\Arcserve\Unified Data Protection\Management\IdentityServer\Repository\conf*, und öffnen Sie die Datei *carbon.xml* mit einem Editor.
2. Kommentieren Sie in der Datei carbon.xml die XML-Tags *HideMenuItemIds* aus, und speichern Sie die Datei.

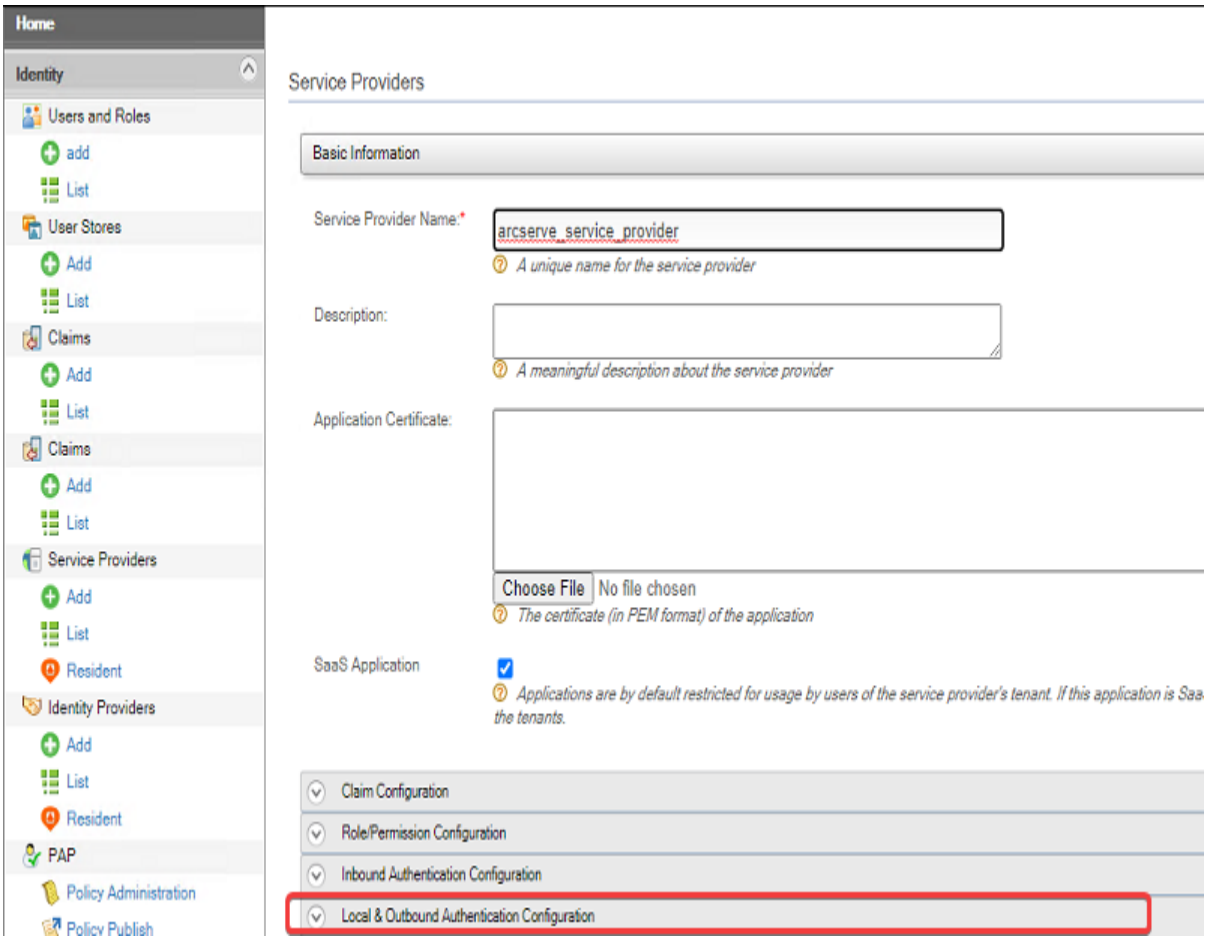
```
</Security>
    <!--HideMenuItemIds> <HideMenuItemId>generic_sts_menu</HideMenuItemId> <HideMenuItemId>manage_saml_sso</HideMenuItemId>
    <HideMenuItemId>oauth_menu</HideMenuItemId> <HideMenuItemId>scim_menu</HideMenuItemId>
    <HideMenuItemId>userstores_mgt_menu</HideMenuItemId> <HideMenuItemId>claim_mgt_menu</HideMenuItemId>
    <HideMenuItemId>comp-mgt_menu</HideMenuItemId> <HideMenuItemId>keystores_menu</HideMenuItemId>
    <HideMenuItemId>logging_menu</HideMenuItemId> <HideMenuItemId>identity_emailtemplate_menu</HideMenuItemId>
    <HideMenuItemId>bam_service_data_publisher_menu</HideMenuItemId>
    <HideMenuItemId>bam_message_tracer_handler_menu</HideMenuItemId> <HideMenuItemId>server-roles-mgt_menu</HideMenuItemId>
    <HideMenuItemId>govern_add_tenants_menu</HideMenuItemId> <HideMenuItemId>govern_view_tenants_menu</HideMenuItemId>
    <HideMenuItemId>service_store_menu</HideMenuItemId> <HideMenuItemId>policy_tryit_menu</HideMenuItemId>
    <HideMenuItemId>tools_saml_validator_resp_menu</HideMenuItemId>
    <HideMenuItemId>tools_saml_validator_req_menu</HideMenuItemId> <HideMenuItemId>add_service_providers_menu</HideMenuItemId>
    <HideMenuItemId>list_service_providers_menu</HideMenuItemId> <HideMenuItemId>identity_providers_add</HideMenuItemId>
    <HideMenuItemId>identity_providers_list</HideMenuItemId> <HideMenuItemId>policy_pap_menu</HideMenuItemId>
    <HideMenuItemId>policy_publish_menu</HideMenuItemId> <HideMenuItemId>pdp_policy_menu</HideMenuItemId>
    <HideMenuItemId>pdp_config_menu</HideMenuItemId> <HideMenuItemId>policy_search_menu</HideMenuItemId>
    <HideMenuItemId>shutdown_restart_menu</HideMenuItemId> <HideMenuItemId>resource_browser_menu</HideMenuItemId>
    <HideMenuItemId>registry_search_menu</HideMenuItemId> <HideMenuItemId>app_log_menu</HideMenuItemId>
    <HideMenuItemId>statistics_menu</HideMenuItemId> <HideMenuItemId>logs_menu</HideMenuItemId>
    <HideMenuItemId>tracer_menu</HideMenuItemId> </HideMenuItemIds-->
```

3. Starten Sie den Arcserve UDP Identity Service neu.
4. Die Benutzerverwaltungskonsole starten Weitere Informationen finden Sie unter Starten der Arcserve UDP-Benutzerverwaltungskonsole.

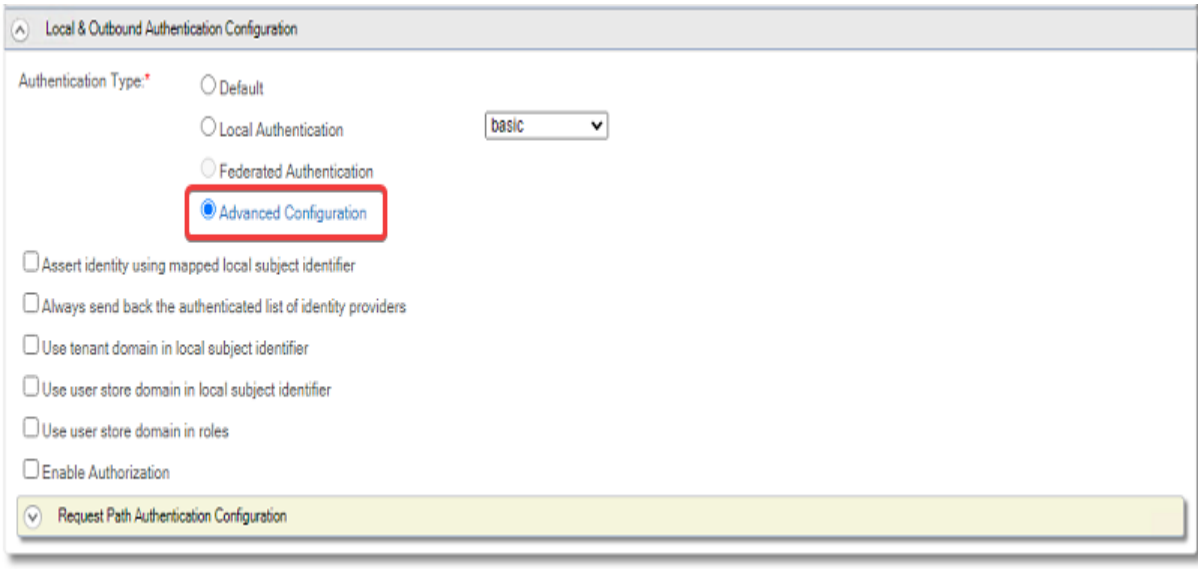
   Die "Identitätsdienstkonsole" wird angezeigt.
5. Gehen Sie zu **Start** > **Identität** > **Serviceanbieter** > **Liste**.



6. Klicken Sie in der Liste der Dienstanbieter für *arcserve_service_provider* auf **Bearbeiten**.



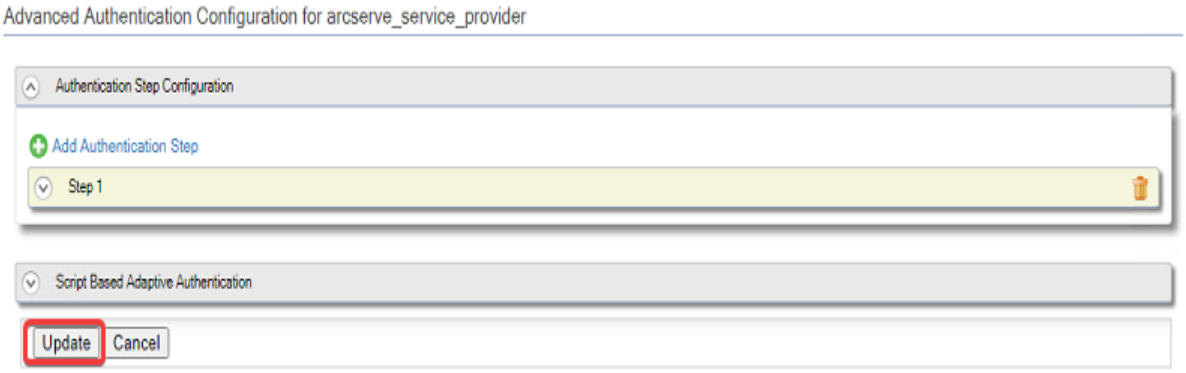
7. Erweitern Sie das Drop-down-Menü **Lokale & ausgehende Authentifizierung konfigurieren**, und wählen Sie dann **Erweiterte Konfiguration** aus.



Die Seite *Advanced Configuration for arcserve_service_provider* wird angezeigt.

8. Klicken Sie auf der Seite *Erweiterte Konfiguration für arcserve_service_provider* unter Konfiguration des Authentifizierungsschritts, um Schritt 2 zu entfernen, auf das Symbol **Löschen**.

9. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.



Die vorhandenen Einstellungen werden entfernt.

10. Gehen Sie zur UDP-Anmeldeseite, und melden Sie sich dann mit dem Benutzernamen und dem Kennwort an.
11. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung**.
12. **Deaktivieren** Sie im Abschnitt "Multi-Faktor-Authentifizierung" die Einstellung, um MFA zu deaktivieren.

13. Klicken Sie auf **Speichern**.

    Die Einstellungen für die MFA-Anmeldung wurden erfolgreich entfernt.

Hinweise zu Instant VMs

Dieser Abschnitt enthält die folgenden Fehlerbehebungsthemen im Zusammenhang mit der Instant VM:

- Fehlgeschlagene Erstellung einer Instant VM in VMware aufgrund eines doppelten NFS-Datenspeichernamens
- Fehlgeschlagene Erstellung einer Instant VM mit Windows 2008 als Wiederherstellungsserver für VMware- oder Windows 2008 R2 Hyper-V-Server
- Eine Instant VM kann nicht gestartet werden, wenn es sich bei dem Quellrechner um einen Windows 2008/2012/2016 AD-Server handelt
- Einschalten der VM nach der Wiederherstellung von Hyper-V ist fehlgeschlagen
- Instant VM-Job schlägt aufgrund eines Windows NFS-Dienstfehlers fehl
- Zugreifen auf oder Löschen von Instant VM-Dateiordner auch mit Administratorrechten nicht möglich
- Instant VM kann nach dem Neustart des Wiederherstellungsservers nicht in Hyper-V gestartet werden
- Fehlgeschlagene Erstellung eines VMware-NFS-Datenspeichers und Anzeige des Fehlers "Auflösen des Hostnamens" nicht möglich
- Fehler beim Bereitstellen des Integrationsdiensts auf der Gast-VM in Hyper-V
- Linux-Instant VM-Fehler auf einem nicht englischen Hyper-V-Server
- Zusätzlicher Lizenzverbrauch für UNC-Pfade, die sich auf einer VM unter einem lizenzierten Hyper-V befinden
- Lizenzfehler wird angezeigt, wenn die Lizenz-Edition/der Lizenztyp geändert und eine Instant VM erstellt wird

Fehler bei der Erstellung einer Instant VM in VMware aufgrund eines doppelten NFS-Datenspeichernamens

Problem

Die Instant VM-Erstellung schlägt fehl, und es wird die folgende Fehlermeldung angezeigt:

Fehler beim Erstellen des NFS-basierten Datenspeichers [arcserve_UDP_<Host-nam/IP>] mit dem NFS-Freigabenamen [arcserve_UDP_IVM_{GUID}]. Fehlercode: 12. Fehlermeldung: Der angegebene Schlüssel, Name oder die ID ist bereits vorhanden (Details:).

Die Ursache für diesen Fehler könnte darin bestehen, dass bereits ein NFS-Datenspeicher mit demselben Namen vorhanden ist und nicht entfernt wurde oder das vCenter bzw. der Host immer noch Referenzen auf den NFS-Datenspeicher in den Datensätzen enthält. Wenn Sie sich jedoch direkt bei dem Host anmelden, sehen Sie einen NFS-Datenspeicher. Dieser Datenspeicher ist sehr wahrscheinlich als inaktiv gekennzeichnet und ausgegraut.

Lösung

So beheben Sie dieses Problem:

1. Melden Sie sich beim ESX-Host an und entfernen Sie den NFS-Datenspeicher.
2. Starten Sie die Management-Agenten auf dem ESX-Host mit dem folgenden Befehl neu:

   ```
   /sbin/services.sh restart
   ```

Weitere Informationen zum Arbeiten auf dem ESX-Host finden Sie in der VMware-Dokumentation.

Fehlgeschlagene Erstellung einer Instant VM mit Windows 2008 R2 als Wiederherstellungsserver für VMware oder Windows 2008 R2 Hyper-V Server

Problem

Die Instant VM konnte nicht erstellt werden. Im Aktivitätsprotokoll zum Job wird folgender Fehler angezeigt:

Die digitale Signatur für diese Datei kann von Windows nicht bestätigt werden. Durch eine aktuelle Änderung der Hardware oder Software ist möglicherweise eine Datei installiert worden, die falsch signiert oder beschädigt ist, oder bei der es sich um Schadsoftware aus einer unbekannten Quelle handelt.

Lösung

Diese Instant VM kann nicht erstellt werden, da der Treiber der Instant M mit einem gesicherten digitalen Zertifikat signiert ist, das unter Windows 2008 R2 nur dann unterstützt werden kann, wenn Sie ein Patch von Microsoft anwenden.

Wenden Sie das Microsoft-Patch 3033929 an, und versuchen Sie erneut, die Instant VM zu erstellen.

Eine Instant VM kann nicht gestartet werden, wenn es sich bei dem Quellrechner um einen Windows 2008/2012/2016 AD-Server handelt

Problem

Eine Instant VM kann nicht gestartet werden, wenn die VM ein Windows 2008 Active Directory-Server ist.

Wenn der Quellrechner ein Windows Active Directory-Server ist, der einen Instant VM-Job ausführt, kann die Instant VM nicht gestartet werden, und es wird ein blauer Bildschirm mit der folgenden Meldung angezeigt:

STOPP: c00002e2 Verzeichnisdienste konnten aufgrund von folgendem Fehler nicht gestartet werden: Ein Gerät, das an das System angehängt wurde, funktioniert nicht. Fehlerstatus: 0xc0000001.

Lösung 1:

Wenn der Ziel-Hypervisor ein Hyper-V ist, fügen Sie dem HyperV-Hypervisor den folgenden Registrierungsschlüssel hinzu, und lösen Sie dann den IVM-Job aus.

Wenn der Ziel-Hypervisor ein ESX/Vcenter ist, fügen Sie den folgenden Registrierungsschlüssel auf dem Proxy-Rechner hinzu, der zum Ausführen des Instant VM-Jobs verwendet wird, und lösen Sie dann den IVM-Job aus.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\InstantVM
```

Reg-Typ: DWORD-Wert

Name: RenameADLog

Wert: 1

Einschränkungen:

- Wenn sich die NTDS-Datenbank und die NTDS-Protokolldateipfade auf unterschiedlichen Volumes befinden, ist die obige Lösung nicht geeignet.
- Ab sofort ist die obige Lösung nur für Windows 2008 Active Directory Server gültig.

Lösung 2:

Sie können das Problem manuell lösen, indem Sie sich bei der Instant VM anmelden.

Gehen Sie wie folgt vor:

1. Schalten Sie die Instant VM ein.
2. Wenn der Rechner eingeschaltet wird, drücken Sie F8, bevor das Betriebssystem zu laden beginnt, und wählen den Modus für **Verzeichnisdienstwiederherstellung** aus.
3. Benennen Sie alle *.log-Dateien im Ordner *C:\Windows\NTDS* um. Benennen Sie zum Beispiel die Datei "edb.log" in "edb.log.old" um.
4. Führen Sie folgenden Befehl aus:

   ```
   esentutl /p "C:\Windows\NTDS\ntds.dit"
   ```

5. Starten Sie das System neu.

Hinweis: Die obige Lösung gilt für alle Versionen von Windows-Servern, auf denen Active Directory installiert ist.

Einschalten der VM nach der Wiederherstellung von Hyper-V ist fehlgeschlagen

Problem

Nach der Wiederherstellung der virtuellen Hyper-V-Maschine kann die virtuelle Maschine nicht mehr eingeschaltet werden. Der folgende Fehler wird angezeigt:

Synthetischer Ethernet-Port (Instanz-ID....): Einschalten fehlgeschlagen mit Fehlversuch, auf eine ungültige Adresse zuzugreifen'.

Lösung

Dieser Fehler tritt auf, da die MAC-Adresse der wiederhergestellten VM mit den vorhandenen VMs kollidiert. Entfernen Sie den NIC-Adapter aus der wiederhergestellten VM und fügen Sie dann manuell einen neuen hinzu, um das Problem zu beheben und das Gerät erfolgreich einzuschalten.

Instant VM-Job schlägt aufgrund eines Windows NFS-Dienstfehlers fehl

Problem

Wenn auf dem Instant VM-Wiederherstellungsserver Arcserve UDP Agent und Arcserve Backup installiert sind, wird der Windows-NFS-Dienst beim Erstellen einer Instant VM für den VMware ESX(i)-Server nicht gestartet, und der Instant VM-Job schlägt fehl.

Lösung

Der Grund hierfür ist, dass die standardmäßige Portnummer des Windows-NFS-Dienstes 111 ist und sie vom **Remoteprozeduraufruf-Server** für den Arcserve Backup-Dienst verwendet wird.

Um dieses Problem zu lösen, ändern Sie die standardmäßige Portnummer des **Remoteprozeduraufruf-Servers** für den Arcserve Backup-Dienst in einen anderen Port, und versuchen Sie erneut, die Instant VM zu erstellen. Weitere Informationen zum Ändern des standardmäßigen Ports finden Sie unter Ändern der Portkonfigurationsdatei und Kommunikationsports von Primär- und Mitgliedsservern in der Arcserve Backup-Dokumentation.

Zugreifen auf oder Löschen von Instant VM-Dateiordner ist auch mit Administratorrechten nicht möglich.

Problem

Der Benutzer kann aufgrund des Fehlers "Administratorrechte erforderlich" nicht auf den Instant VM-Ordner zugreifen oder diesen löschen, obwohl er über Administratorrechte verfügt.

Lösung

Hierbei handelt es sich um ein Problem von NFS. Sie müssen zuerst die NFS-Freigabe entfernen, dann können Sie den Ordner löschen. Verwenden Sie die folgende Befehlszeile zum Löschen des Ordners:

nfsshare /delete [Name der NFS-Freigabe]

Instant VM kann nach dem Neustart des Wiederherstellungsservers nicht in Hyper-V gestartet werden.

Problem

Wenn ich die IVM (Instant Virtual Machine) starte und dann den Hyper-V-Wiederherstellungsserver neu starte, wird die IVM nicht hochgefahren.

Lösung

Um diesen Boot-Fehler zu beheben, starten Sie die IVM neu.

Fehlgeschlagene Erstellung eines VMware-NFS-Datenspeichers und Anzeige des Fehlers "Auflösen des Hostnamens nicht möglich"

Gültig für VMware

Problem

Die Instant VM-Erstellung schlägt fehl, und es wird die folgende Fehlermeldung angezeigt:

Fehlgeschlagene Erstellung des VMware-NFS-Datenspeichers durch Server <hostname of recovery server>.

Fehlermeldung: Während der Hostkonfiguration ist ein Fehler aufgetreten.

Details: Vorgang ist fehlgeschlagen, Diagnosebericht: Hostname <one hostname but not recovery server> kann nicht aufgelöst werden.

Beispiel

Fehlgeschlagene Erstellung des VMware-NFS-Datenspeichers durch Server 'host1'.

Fehlermeldung: Während der Hostkonfiguration ist ein Fehler aufgetreten.

Details: Vorgang ist fehlgeschlagen, Diagnosebericht: Hostname 'host2' kann nicht aufgelöst werden.

Lösung

Der Grund für diesen Fehler ist, dass der ESX-Server alle NFS-Datenspeicher aufführt, wenn Sie Instant VM-NFS-Datenspeicher erstellen, selbst wenn einige Datenspeicher nicht mehr verfügbar sind. Beispielsweise ist der NFS-Datenspeicher, der von **host2** erstellt wurde, immer noch vorhanden, selbst wenn **host2** nicht verfügbar ist, da der Rechner gelöscht wurde. Daher kann der ESX-Server den Hostnamen nicht auflösen.

Um dieses Problem zu beheben, löschen Sie den nicht verfügbaren Datenspeicher vom ESX-Server.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim ESX-Server mit SHH an.
2. Geben Sie folgenden Befehl ein:

   ```
   esxcfg-nas -l
   ```

   Der gleiche Fehler wird in der Befehlszeile angezeigt.

```
Fehler beim Durchführen des Vorgangs: Hostname 'host2'
kann nicht aufgelöst werden.
```

3. Fügen Sie eine Zuordnung in der Datei **/etc/hosts** des ESX-Servers hinzu, um dieses Problem zu beheben.

   <IP address> <hostname>

   Hinweis: Die IP-Adresse sollte erreichbar sein.

   Beispiel: 10.57.X.X host2

4. Listen Sie alle NFS-Datenspeicher mithilfe des folgenden Befehls auf:

   ```
   esxcfg-nas –l
   ```

   ```
   arcserve_UDP_<hostname> is /arcserve_UDP_IVM_{ESX_gene-
   rated_number} from <hostname> unmounted unavailable
   ```

   Beispiel: esxcfg-nas –l

   arcserve_UDP_host2 is /arcserve_UDP_IVM_{991555E6-09A4-4D80-A47E-522831A62Axx} from host2 unmounted unavailable

5. Mit dem folgenden Befehl können Sie den nicht verfügbaren Datenspeicher löschen:

   ```
   esxcfg-nas -d arcserve_UDP_host2
   ```

6. Entfernen Sie die Zuordnung für <hostname> in der Datei **/etc/hosts** vom ESX-Server.

   Jetzt können Sie die NFS-Funktion wie gewohnt verwenden.

   Hinweis: Weitere Informationen zu diesem Problem finden Sie in folgendem VMware-KB-Artikel:

Fehler beim Bereitstellen des Integrationsdiensts auf der Gast-VM in Hyper-V

Problem

Wenn Sie einen virtuellen Rechner sichern, auf dem die Anwendung (SQL oder Exchange) installiert ist, enthält der Wiederherstellungspunkt keine Writer-Informationen, und das Aktivitätsprotokoll des Sicherungsjobs zeigt die folgende Warnung an:

Der Integrationsdienst für den virtuellen Rechner konnte nicht bereitgestellt werden.

Lösung

Dieses Problem tritt häufig auf, wenn die Windows-Verwaltungsinstrumentation (WMI) durch die Firewall auf der Gast-VM deaktiviert wird. Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Melden Sie sich bei der Gast-VM an.
2. Öffnen Sie die Systemsteuerung.
3. Öffnen Sie die Windows-Firewall.
4. Klicken Sie auf "Eine App oder ein Feature durch die Windows-Firewall zulassen".
5. Aktivieren Sie die Windows-Verwaltungsinstrumentation (WMI).
6. Klicken Sie auf "OK".

Linux-Instant VM-Fehler auf einem nicht englischen Hyper-V-Server

Linux-Instant VM-Fehler auf einem nicht englischen Hyper-V-Server aufgrund eines Verbindungsfehlers, auch wenn die Firewall deaktiviert ist.

Problem

Die Instant VM-Erstellung schlägt fehl, und es wird die folgende Fehlermeldung angezeigt:

Verbindung zum Hyper-V-Host [Hyper-V-Zielservername] fehlgeschlagen Überprüfen Sie, ob die Adresse des Hosts korrekt ist und die Anmeldeinformationen gültig sind.

Lösung

Eine fehlerhafte Konfiguration für Hyper-V-Serververbindungsinformationen könnte dieses Problem verursachen.

Weitere Details finden Sie unter **Konfigurieren der Verbindungsinformationen von Hyper-V-Servern für Instant VM** im *Arcserve UDP Agent for Linux-Benutzerhandbuch*.

Zusätzlicher Lizenzverbrauch für UNC-Pfade, die sich auf einer VM unter einem lizenzierten Hyper-V befinden

Problem

UNC-Pfade, die sich auf einer VM unter einem Hypervisor befinden, verbrauchen eine zusätzliche Socket-Lizenz, auch wenn die Lizenz bereits zuvor auf den Hypervisor-Host angewendet wurde. Dieser Fehler führt zum Verbrauch von zusätzlichen Lizenzen.

Lösung

Hypervisor-Host-Backup und UNC-Pfade, die sich auf demselben Hypervisor befinden, benötigen die gleiche Lizenz. Beim Sichern von UNC-Pfaden, die sich in einer VM befinden, die sich unter demselben Hypervisor befindet, verbrauchen die UNC-Pfade/Shares jedoch eine zusätzliche Lizenz. Dieses Problem tritt nur auf, wenn die VM nicht als Knoten zur Konsole hinzugefügt/importiert wird, und auch, wenn UNC-Pfade mit einem anderen Namen als dem beim Hinzufügen der VM zur Konsole angegebenen Namen hinzugefügt werden.

Gehen Sie wie folgt vor:

1. Fügen Sie entweder den Knoten (die VM mit UNC-Pfaden) zur Konsole hinzu und geben Sie Hypervisor-Details zum Knoten an oder importieren Sie den Knoten aus dem Hypervisor.
2. Fügen Sie UNC-Pfade/Shares mit dem gleichen Namen wie in Schritt 1 eingefügt hinzu.

Lizenzfehler wird angezeigt, wenn Sie die Lizenzedition/den Lizenztyp ändern und eine Instant-VM erstellen

Problem

Nachdem Sie einen Lizenztyp oder eine Edition in der Konsole hinzugefügt oder geändert und eine Instant-VM ohne Sicherungsjob erstellt haben, wird eine Fehlermeldung zum Lizenzfehler angezeigt. Wenn Sie jedoch das nächste Mal eine Instant-VM ausführen, identifiziert sie die neue Lizenz erfolgreich und erstellt eine Instant-VM.

Lösung

Gehen Sie wie folgt vor:

1. Nachdem der UDP-Konsole eine neue Lizenz hinzugefügt wurde, führen Sie für den vorhandenen Plan den Sicherungsjob aus.
2. Erstellen Sie nun eine Instant-VM.

Bei Linux-Agenten

Dieser Abschnitt enthält die folgenden Fehlerbehebungsthemen im Zusammenhang mit dem Arcserve UDP-Linux-Agent:

- Deaktivierte Sicherungsziel-Einstellungen bei Verwendung der Benutzeroberfläche des Linux-Agent
- Jobstatus, Jobübersicht und Aktivitätsprotokoll nicht sichtbar

Deaktivierte Sicherungsziel-Einstellungen bei Verwendung der Benutzeroberfläche des Linux-Agent

Wenn der Linux-Sicherungsserver nicht aus der Arcserve UDP-Konsole entfernt wird, bevor die Konsole deinstalliert wird, werden die Sicherungszieleinstellungen beim Öffnen der Benutzeroberfläche des Sicherungsservers deaktiviert.

Problem

Der Sicherungsserver wird nicht benachrichtigt, dass die Arcserve UDP-Konsole deinstalliert wurde. Der Sicherungsserver nimmt an, dass er weiterhin von der Konsole verwaltet wird.

Lösung

Melden Sie sich beim Sicherungsserver an und führen Sie den folgenden Befehl aus:

```
# /opt/Arcserve/d2dserver/bin/d2dreg -release
```

Der Sicherungsserver wird aus der Konsole entfernt. Sie können die Sicherungseinstellungen nun auf der Benutzeroberfläche des Sicherungsservers ändern.

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Jobstatus, Jobübersicht und Aktivitätsprotokoll nicht sichtbar

Problem

Jobstatus, Jobübersicht und Aktivitätsprotokoll für Linux-Knoten werden in der Arcserve UDP-Konsole nicht angezeigt.

Lösung

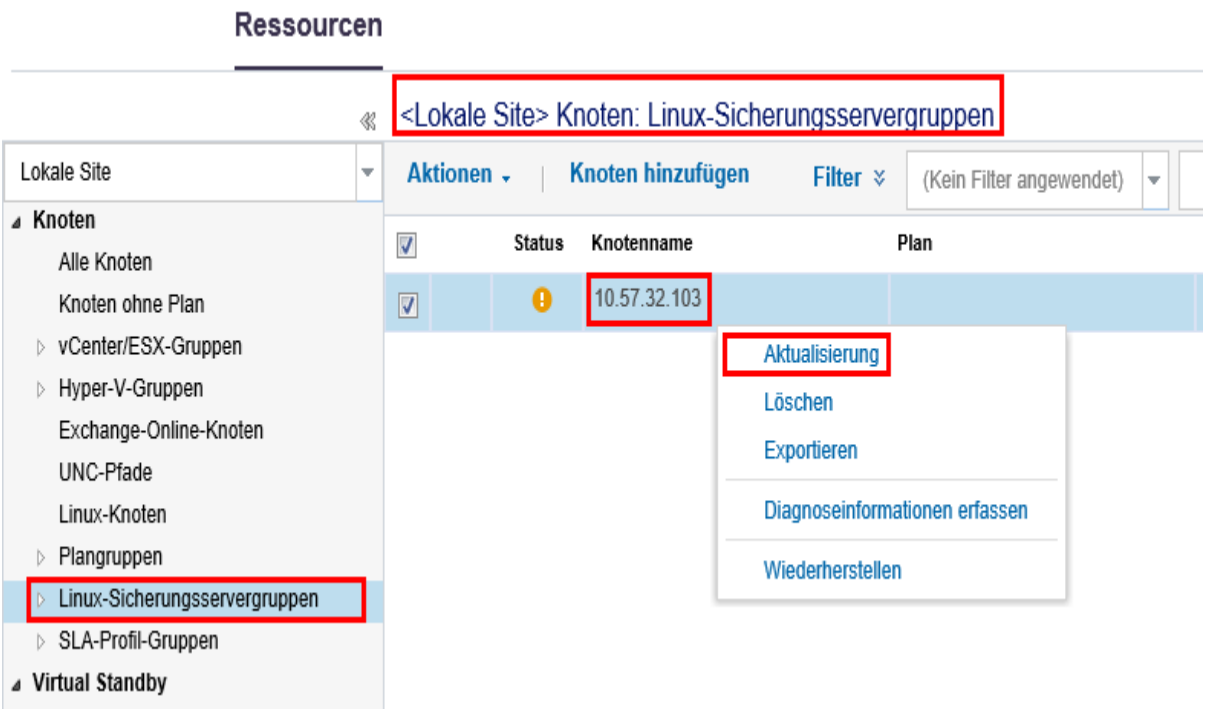
Der Linux-Sicherungsserver kann mit dem Hostnamen keine Verbindung mit Arcserve UDP herstellen.

Gehen Sie wie folgt vor:

1. Erstellen Sie die Datei server_ip.ini an folgendem Speicherort von Arcserve UDP:

   "UDP-Installationspfad"\Management\Configuration\server_ip.ini
2. Geben Sie die IP-Adresse von Arcserve UDP in dieser Datei ein.
3. Melden Sie sich bei der Arcserve UDP-Konsole an und aktualisieren Sie den Linux-Sicherungsserver und Linux-Knoten.

   Hinweis: Der Linux-Sicherungsserver kann nur über "Linux-Sicherungsservergruppen", wo alle Linux-Sicherungsserver aufgelistet werden, aktualisiert werden.



Jobstatus, Jobübersicht und Aktivitätsprotokoll sind nun sichtbar.

System-Volume des SUSE15 mit XFS-Dateisystem konnte nicht wiederherstellen

Das Systemvolume des SUSE15 mit XFS-Dateisystem konnte nicht wiederhergestellt.

Problem

Der Wiederherstellungsauftrag des SUSE15-Knotens mit dem XFS-Dateisystem konnte nicht ausgeführt werden.

Lösung

Das Problem tritt auf, weil das System-Volume nicht installiert wurde. Erstellen Sie eine CentOS 7.5 Live-CD und verwenden Sie diese Live-CD, um BMR/Instant BMR durchzuführen.

Wenn das Problem weiterhin besteht, verwenden Sie Live-Chat, um sich mit dem Arcserve-Support in Verbindung zu setzen. Mit dem Live-Chat können Sie Ihre Kommunikation mit dem Team für technischen Support optimieren. Bedenken und Fragen können noch bei bestehendem Zugriff auf das Produkt umgehend behandelt werden.

Infos zu Wiederherstellungen

Dieser Abschnitt enthält die folgenden Fehlerbehebungsthemen im Zusammenhang mit der Wiederherstellung:

- Wiederherstellung von Dateien nicht möglich
- Hinzufügen der wiederhergestellten Inhaltsdatenbank zur ursprünglichen Webanwendung
- Datenbank kann nicht geladen werden, während die Microsoft Exchange-Datenbank wiederhergestellt wird
- Feld "Von" wird für E-Mails nicht richtig angezeigt, die von Benutzern mit Vertretungsrechten für ein freigegebenes Postfach gesendet wurden
- Wiederherstellungsaufträge schlagen nach Light-Integration-Backups fehl

Wiederherstellung von Dateien nicht möglich

Problem

Aufgrund einer Beschränkung von Microsoft können Dateidaten auf den NTFS-Deduplizierungsvolumes aus Windows 2012 R2-Systemen in Windows 2012-Systemen nicht gelesen werden. Wenn UDP Agent in einem Windows 2012 System verwendet wird, um eine VM mit Windows 2012 R2-Gastbetriebssystem und NTFS-Deduplizierungsvolumes wiederherzustellen, kann das folgende Problem auftreten. Das Problem tritt nur bei Wiederherstellungsvorgängen auf Dateiebene oder mit geladenen Wiederherstellungspunkten auf.

Die Datei bzw. das Verzeichnis ist beschädigt und nicht lesbar.

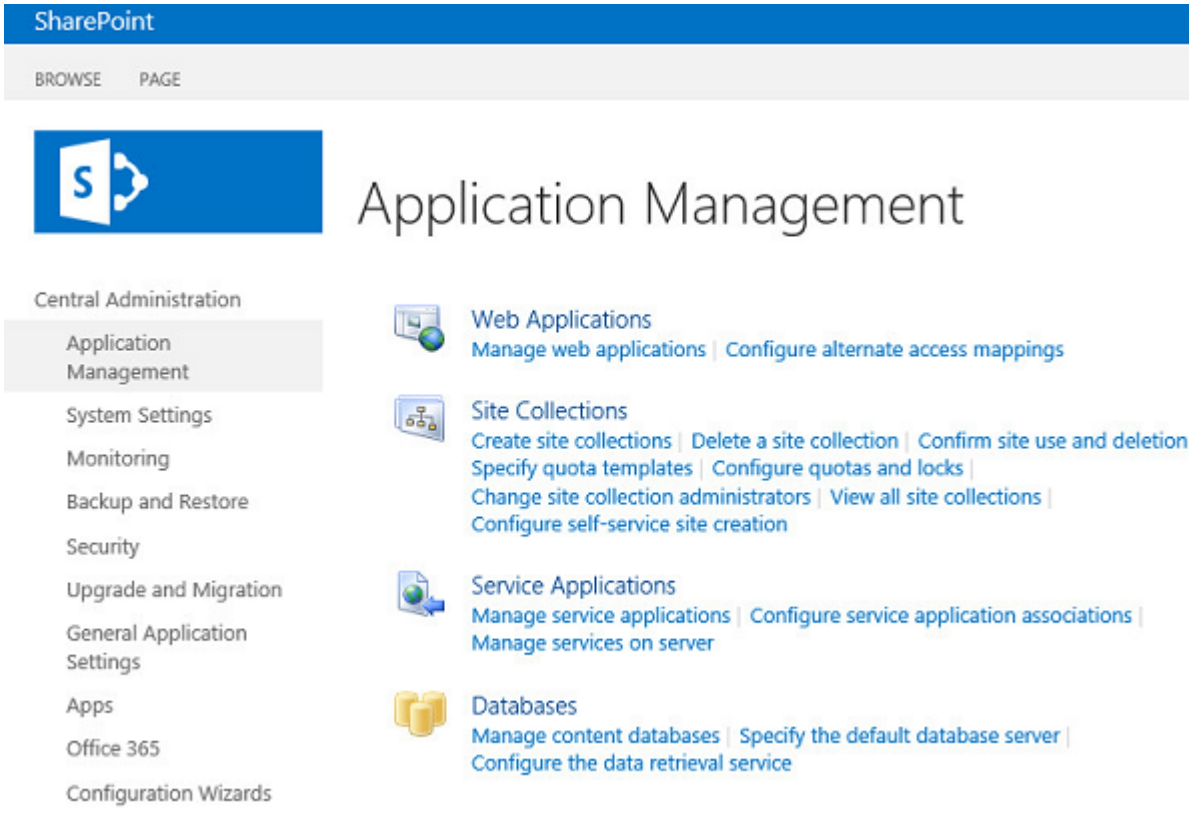
Lösung

Wenn dieses Problem auftritt, starten Sie die Wiederherstellung über einen UDP Agent, der auf einem Windows 2012 R2-System installiert ist.

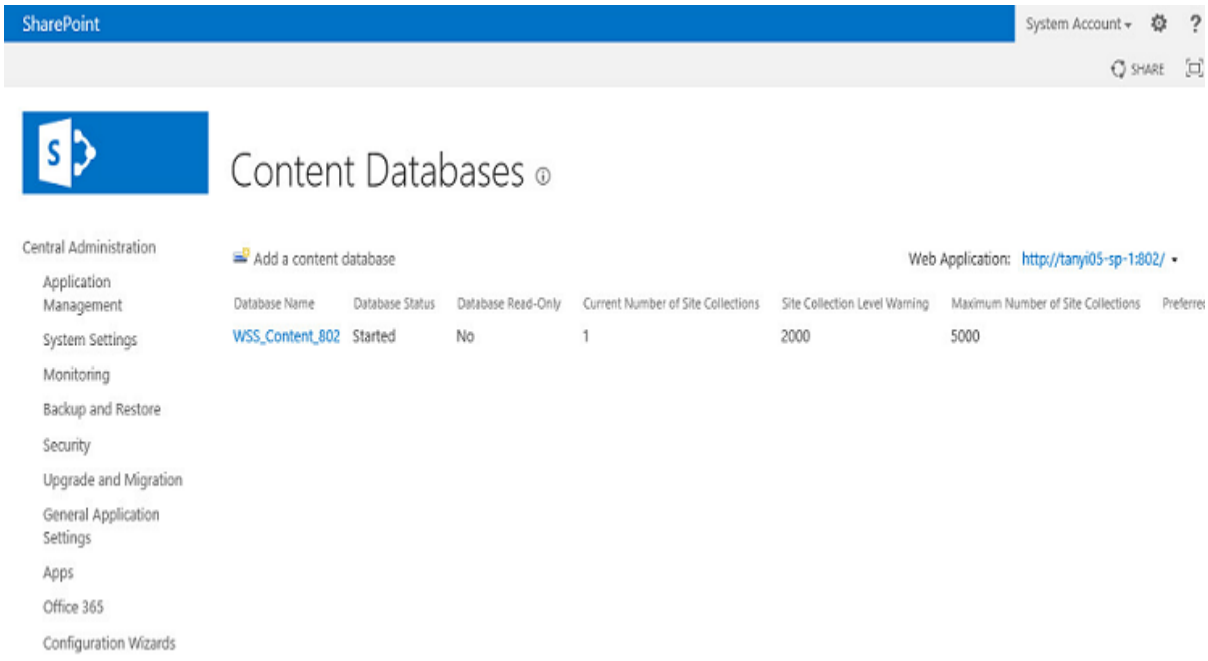
Hinzufügen der wiederhergestellten Inhaltsdatenbank zur ursprünglichen Webanwendung

Gehen Sie wie folgt vor:

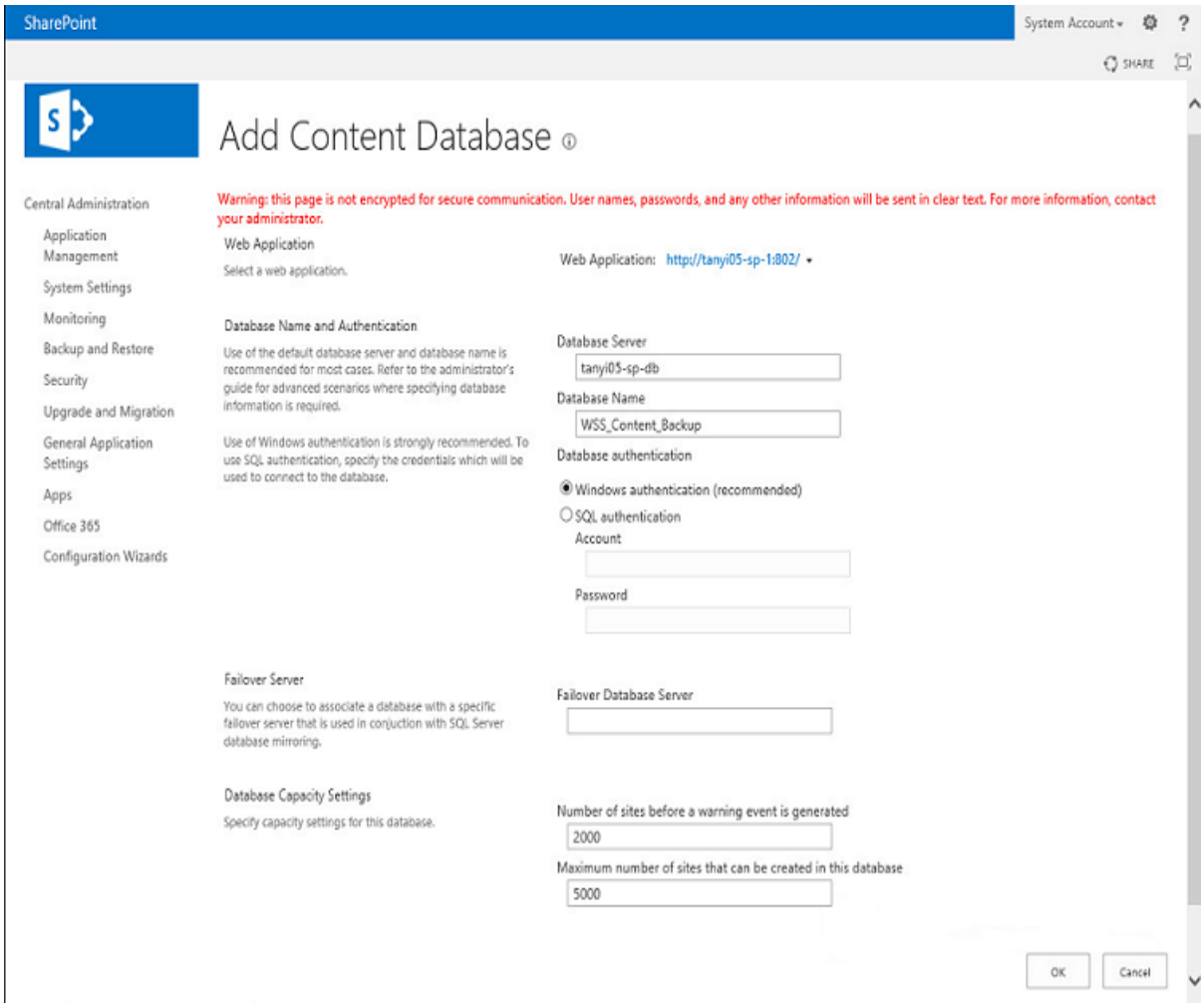
1. Öffnen Sie die SharePoint-Zentraladministration, und wählen Sie "Anwendungsverwaltung" aus.



2. Wählen Sie "Inhaltsdatenbanken verwalten" aus.



3. Wählen Sie die Webanwendung aus, und klicken Sie auf "Inhaltsdatenbank hinzufügen".
4. Geben Sie den Datenbankserver und den Datenbanknamen (z. B. WSS_Content_Backup) ein, und klicken Sie dann auf "OK".



Die Inhaltsdatenbank ist jetzt der ursprünglichen zugehörigen Webanwendung zugeordnet.

Datenbank kann nicht geladen werden, während die Microsoft Exchange-Datenbank wiederhergestellt wird

Problem

Wenn Sie eine Microsoft Exchange-Datenbank wiederherstellen, kann die Datenbank nicht geladen werden. Die erforderlichen Protokolle fehlen, oder die Transaktionsprotokolle sind nicht fortlaufend. Es liegen Ereignisfehler wie 454, 455 und 2006 im Ereignisprotokoll vor.

Die folgenden zwei Ursachen könnten zu dem Datenbankladefehler führen.

Ursache 1: Die Option "Exchange-Protokoll bereinigen" ist in den UDP-Einstellungen aktiviert. Bei dieser Einstellung werden die Transaktionsprotokolle nach jeder Sicherung gelöscht. Die Benutzer versuchen dann, die vorherige Sitzung wiederherzustellen, nachdem mehrere Sicherungen erfolgt sind, in denen der Protokollbereinigungsvorgang stattfand.

Ursache 2: Benutzer haben manuell Transaktionsprotokolle gelöscht, oder die Protokolle werden von anderen Programmen wie Antivirensoftware gelöscht.

Lösung

Lösung 1: Wenn Sie die Option "Exchange-Protokoll bereinigen" aktiviert haben und die Transaktionsprotokolle nicht fortlaufend sind, dann stellen Sie alle Sitzungen einzeln wieder her, beginnend mit der letzten Sitzung, bis die Wiederherstellung der Sitzung fehlschlägt. Wenn die aktuelle Sitzung nicht wiederhergestellt werden kann, versuchen Sie es mit Lösung 2.

Lösung 2: Wenn Lösung 1 nicht funktioniert, verwenden Sie Lösung 2. Diese Lösung behebt beide Probleme.

Beispiel: Sie möchten die Testdatenbank in Sitzung 1 wiederherstellen. In den folgenden Schritten wird der Datenbankname als Test verwendet.

1. Melden Sie sich bei dem Exchange-Server an, auf dem sich die Datenbank befindet.
2. Löschen Sie alle Dateien (wie z. B. *.edb, *. log, *.jrs, *.chk) aus dem Datenbankordner.
3. Stellen Sie die Datenbank bereit, um eine leere Datenbank zu erstellen.

   Mount-Database -Identity Test
4. Stellen Sie dieselbe Sitzung am ursprünglichen Speicherort wieder her.

Wenn die Wiederherstellung erfolgreich ist, brauchen Sie die folgenden Schritte nicht auszuführen. Wenn die Wiederherstellung fehlschlägt, fahren Sie mit den folgenden Schritten fort.

5. Laden Sie die Datenbank erneut.

   Mount-Database -Identity Test

6. Erstellen Sie eine temporäre Datenbank.

   new-mailboxdatabase -name OtherDatabase

7. Verschieben Sie das Postfach in eine andere Datenbank.

   get-mailbox -datatbase Test -resultsize unlimited | new-moverequest -targetdatabase OtherDatabse

8. Entfernen Sie die Postfachdatenbank vom Zielrechner.

   remove-mailboxdatabase -identity Test

9. Erstellen Sie eine Postfachdatenbank mit demselben Namen.

   new-mailboxdatabase -name Test

10. Stellen Sie dieselbe Sitzung am ursprünglichen Speicherort wieder her.

    Die Datenbank wird erfolgreich geladen.

Feld "Von" wird für E-Mails nicht richtig angezeigt, die von Benutzern mit Vertretungsrechten für ein freigegebenes Postfach gesendet wurden

Problem

Wenn der Benutzer Exchange-E-Mails wiederherstellt, werden für E-Mails, die von einem Benutzer mit Vertretungsrechten für ein freigegebenes Postfach gesandt wurden, nach der Wiederherstellung die "Von"-Informationen nicht richtig angezeigt. Das Feld "Von" zeigt nur den <host sender>-Namen.

Lösung

Führen Sie diese Schritte aus, um das Problem zu beheben:

1. Führen Sie eine der folgenden Aktionen durch:

   Für agentenlose Sicherungen

   - Erstellen Sie auf dem HBBU-Proxy-Server eine Datei "grtcfg.ini" im Ordner "Configuration":

     [product_installed_path]\ Engine\Configuration

   Für agentenbasierte Sicherungen

   - Erstellen Sie auf dem Agentenrechner eine Datei "grtcfg.ini" im Ordner "Configuration":

     [product_installed_path]\ Engine\Configuration

2. Fügen Sie der Datei "grtcfg.ini" folgenden Inhalt hinzu:

   [common]

   0xFF07_enable=1

3. Übergeben Sie den Wiederherstellungsjob erneut.

Wiederherstellungsaufträge schlagen nach Light-Integration-Backups fehl

Problem

Wenn Sie Light-Integration-Backups aus dem Arcserve Backup Manager hinzufügen, um einen Exchange Online-Knoten über einen RPS Server zu sichern, ist der Knoten bereits mit einer Kopie-auf-Band-Sitzung gesichert. Die Aufträge schlagen fehl, wenn die Quelldaten Arcserve D2D-Sitzungen enthalten, die zuvor von Arcserve Backup gesichert wurden. Die Fehlermeldung AW0813 wird im Aktivitätsprotokoll angezeigt.

Lösung

Das designbedingte Verhalten von ARCserve Backup ist für dieses Verhalten verantwortlich. Sie müssen dieses Verhalten anpassen, um Arcserve Backup die Sicherung von Arcserve D2D-Sitzungen zu erlauben, die zuvor gesichert wurden.

Gehen Sie wie folgt vor:

1. Öffnen Sie den Windows Registry Editor über den Arcserve D2D-Server(-knoten), den Sie sichern.
2. Öffnen Sie den folgenden Schlüssel:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\ClientAgent\Parameters\AllowRedundantD2DBackups
3. Ändern Sie den Wert "DWORD" für "AllowRedundantD2DBackups" auf 1.

   Hinweis: Wenn der oben beschriebene Registrierungsschlüssel auf dem Knoten, den Sie sichern, nicht vorhanden ist, müssen Sie den Schlüssel erstellen.
4. Schließen Sie den Windows-Registrierungs-Editor.

   Weitere Informationen finden Sie im KB-Artikel.

Bei Wiederherstellung auf einem freigegebenem NFS Ordner wird der Dateiname in einen unbrauchbaren Namen geändert

Problem:

Beim Wiederherstellen auf einem freigegebenem NFS Ordner werden die Dateien/Ordner mit einem unbrauchbaren Namen wiederhergestellt.

Lösung:

UDP unterstützt die Wiederherstellung der Dateien und Ordner in einem freigegebenen NFS Ordner nicht. Es wird empfohlen, einen freigegebenen SMB-Ordner (Server Message Block) zu exportieren und anschließend im gleichen Ordner wiederherzustellen.

Hinweis: Wenn der Datei-/Ordnername während der NFS-Sicherungssitzung in einen unbrauchbaren Namen umgewandelt wird, bleibt der Name auch nach der Wiederherstellung unbrauchbar.

Bei Gateway, RPS, Datenspeicher, Konsole und Datenbank

Dieser Abschnitt enthält die folgenden Fehlerbehebungsthemen im Zusammenhang mit Recovery Point Server (RPS), Datenspeicher und Datenbank:

- Datenspeichername wird bereits verwendet
- Verbindung mit dem Datenspeicher aufgrund eines DNS-Fehlers nicht möglich
- Datenspeicher wechselt in den Modus für "Nur Wiederherstellen"
- Fehler, wenn RPS-Version niedriger ist als Konsolenversion
- Hinzufügen derselben Ressource an verschiedenen Standorten wird nicht unterstützt
- Aktivieren von Protokollkürzungen, wenn die SQL-Datenbank sich im vollständigen Wiederherstellungsmodus befindet
- Beim Durchsuchen von Wiederherstellungspunkten werden keine verfügbaren Wiederherstellungspunkte angezeigt, wenn RPS mit FQDN konfiguriert sind
- Zugriffsverweigerung beim Hinzufügen von RPS
- Wechsel zu UDP-Ansicht für Wiederherstellungspunkt nicht möglich
- Zugriffsverweigerung beim Hinzufügen oder Aktualisieren von Knoten
- UDP-Konsole wird nicht geöffnet, wenn SQL-Administratorkennwort geändert wird
- Fehler beim Laden von Wiederherstellungspunkten aufgrund eines Zeitlimits
- Aktualisieren der Anmeldeinformationen des Gateway-Servers
- Aktualisieren des Gateways, wenn die Gateway-Proxy-Anmeldeinformationen geändert werden
- Konsole zeigt Meldung "Identitätsdienst wird gestartet"

Datenspeichername wird bereits verwendet

Problem:

Wenn ich einen Datenspeicher erstelle, wird manchmal die folgende Meldung angezeigt, auch wenn ich einen neuen Datenspeichernamen angebe:

Dieser Name wird bereits von einem anderen Datenspeicher auf dem Server verwendet. Legen Sie einen anderen Datenspeichernamen fest.

Lösung:

Dies tritt auf, wenn Sie einen vorhandenen Datenspeicher haben und die Datenspeicher-UUID auf der Registrierung aus irgendeinem Grund beschädigt ist. Sie können den Datenspeicher aus der grafischen Benutzeroberfläche löschen, der Name verbleibt jedoch in der Registrierung des Recovery Point Servers.

Um das Problem zu beheben, geben Sie einen neuen Namen an.

Verbindung mit dem Datenspeicher aufgrund eines DNS-Fehlers nicht möglich

Problem:

Während der BMR kann ich keine Verbindung mit dem freigegebenen Ordner für RPS herstellen. Obwohl ich den richtigen Benutzernamen und das richtige Kennwort eingebe, kann ich keine Knoten auf dem RPS durchsuchen.

Lösung:

Wenn Windows UAC auf dem RPS-Server aktiviert ist, kann auch ein Konto, das zur lokalen Administratorgruppe gehört, möglicherweise nicht auf einen freigegebenen Ordner des Datenspeichers zugreifen, wenn diesem Konto nicht explizit Zugriff auf diese Freigabe gewährt wurde.

Verwenden Sie den integrierten Administrator von RPS, um für das während der BMR verwendete Konto Lese-/Schreibzugriff auf den freigegebenen Ordner des bestimmten Datenspeichers zu gewähren.

Datenspeicher wechselt in den Modus für "Nur Wiederherstellen"

Problem

Ein Datenspeicher wechselt in den Modus für "Nur Wiederherstellen" und lässt keine Sicherungen von Daten zu.

Lösung

Wenn der Speicherplatz eines Datenträgers, der von einem Datenspeicher verwendet wird, ausgeschöpft ist, wechselt der Datenspeicher in den Modus für "Nur Wiederherstellen". In diesem Modus können Sie Wiederherstellungen durchführen, doch Sie können keine Daten im Datenspeicher sichern. Wenn die angegebene Zuweisung von virtuellem Speicher vollständig ausgelastet ist, können Sie zudem entweder die Zuordnung von Arbeitsspeicher erhöhen oder den Datenspeicher vom Speichermodus in den SSD-Modus ändern. Sogar in solchen Fällen wechselt der Datenspeicher in den Modus "Nur Wiederherstellen".

Um solche Probleme zu lösen, verschieben Sie den Datenspeicher auf einen größeren Datenträger, indem Sie ihn importieren.

Kopieren Sie zunächst die Ordner, die sich auf dem vollen Datenträger befinden, auf einen größeren Datenträger mit mehr freiem Speicherplatz, und importieren Sie danach den Datenspeicher aus der Konsole.

Mit der Funktion "**Datenspeicher importieren**" können Sie einen Datenspeicher zum Recovery Point Server hinzufügen. Sie können alle vorhandenen Datenspeicher zu einem Recovery Point Server importieren. Datenspeicher, die Sie zu einem früheren Zeitpunkt aus einem Recovery Point Server gelöscht haben, stehen für den Import zur Verfügung.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Ziele**, und klicken Sie auf **Recovery Point Server**.

   Die Seite **Ziele: Recovery Point Server** wird angezeigt.
3. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie mit der rechten Maustaste auf einen Recovery Point Server.
   - Wählen Sie einen Recovery Point Server aus, und klicken Sie im mittleren Menü auf die Drop-down-Liste **Aktionen**.
4. Klicken Sie auf "**Datenspeicher importieren**".

Die Seite "**Datenspeicher importieren**" wird angezeigt.

5. Führen Sie folgende Aktionen durch, und klicken Sie auf "**Weiter**":
   - **Durchsuchen** Sie Ihr System, um den **Ordner des Sicherungsziels** auszuwählen, aus dem Sie den Datenspeicher importieren möchten.
   - Geben Sie das **Verschlüsselungskennwort** ein.

   Hinweis: Lassen Sie das Feld leer, wenn der Datenspeicher nicht verschlüsselt ist.

   Nach der Authentifizierung des **Ordners des Sicherungsziels** wird die Seite "**Datenspeicher importieren**" angezeigt. Sie enthält die Details zum Datenspeicher.

6. Ändern Sie die Details bei Bedarf, und klicken Sie auf "**Speichern**".

   Wenn Sie Ordner für Datenziel, Index-Ziel und Hash-Ziel für Deduplizierungs-Datenspeicher kopiert haben, ändern Sie den Ordnerpfad.

   Hinweis: Sie können die Verschlüsselungsoption für vorhandene Datenspeicher nicht aktivieren oder deaktivieren.

   Der Datenspeicher wird zum Recovery Point Server hinzugefügt und im Dialogfeld **Ziele: Recovery Point Server** angezeigt.

   Nun ist der Datenspeicher für Sicherungen verfügbar.

Fehler, wenn RPS-Version niedriger ist als Konsolenversion

Problem

Es ist ein Plan mit einem Sicherungs-Task oder Replikations-Task vorhanden, und das Ziel ist Recovery Point Server (RPS). Der Recovery Point Server ist eine ältere Version, und die Konsole ist die neueste Version. Wenn ich einen Plan erstelle, ändere, erneut bereitstelle, unterbreche oder wiederaufnehme und eine oder mehrere ältere Versionen von RPS vorhanden sind, wird folgende Fehlermeldung angezeigt:

Die Version des Ziel-Recovery Point Server "rps1" ist niedriger als die Version der aktuellen Konsole. Um fortzufahren, müssen Sie ein Upgrade und eine Aktualisierung für den Recovery Point Server durchführen.

Lösung

Dieser Fehler tritt auf, wenn Sie für Ihren Plan eine ältere Version von RPS verwenden. Um diesen Fehler zu beheben, aktualisieren Sie den Recovery Point Server, der im Plan verwendet wird. Wenn Sie den RPS manuell (außerhalb der Konsole) aktualisieren, vergessen Sie nicht, den Recovery Point Server auch auf der Konsole zu aktualisieren.

Aktualisieren Sie den Recovery Point Server in der folgenden bevorzugten Reihenfolge:

Replikation auf einen remote verwalteten RPS (RPS3) > Replikations-Task (RPS2) > Sicherungs-Task (RPS1)

Aktualisieren Sie zuerst RPS3 und dann RPS2. Aktualisieren Sie zuletzt RPS1.

Führen Sie diese Schritte durch, um zu aktualisieren:

1. Navigieren Sie über die Registerkarte **Ressourcen** zu "Ziele": Seite "Recovery Point Server".
2. Wählen Sie den Recovery Point Server aus.
3. Klicken Sie mit der rechten Maustaste, und wählen Sie **Recovery Point Server installieren/aktualisieren**.
4. Klicken Sie auf **OK**.

Führen Sie diese Schritte durch, um das Update durchzuführen:

1. Navigieren Sie auf der Registerkarte **Ressourcen** zu "Ziele" im linken Fensterbereich und klicken Sie auf "Recovery Point Server".
2. Wählen Sie den Recovery Point Server aus.

3. Klicken Sie mit der rechten Maustaste, und wählen Sie **Aktualisieren** aus.
4. Klicken Sie auf **OK**.

Hinzufügen derselben Ressource an verschiedenen Standorten wird nicht unterstützt

Problem

Wenn ich einen Datenspeicher am Remote-Standort hinzufüge, erhalte ich folgende Fehlermeldung:

Job kann nicht für eine Hyper-V-VM oder ESX-VM übergeben werden.

Lösung

Der Fehler tritt auf, weil dieselbe Ressource (Knoten, RPS-Server, ASBU-Server, Hyper-V-Server, ESX-Server, Proxy-Server) bereits an einem anderen Standort vorhanden ist. Um diesen Fehler zu beheben, löschen Sie die Ressource aus allen Standorten, und fügen Sie die Ressource nur zu einem Standort hinzu.

Aktivieren von Protokollkürzungen, wenn die SQL-Datenbank sich im vollständigen Wiederherstellungsmodus befindet

Problem

Wenn sich die Datenbank im vollständigen Modus befindet und eine vollständige Datenbanksicherung durchgeführt wird, kann das SQL-Kürzungsprotokoll nicht gekürzt werden.

Lösung

Um dieses Problem zu beheben, fügen Sie zwei Registrierungswerte hinzu, damit Arcserve UDP den Befehl BACKUP LOG ausführen kann, um das Transaktionsprotokoll zu sichern. Mit diesem Befehl wird der Speicherplatz, der in der Datenbankdatei bereits beschrieben ist, als wiederverwendbar markiert.

Führen Sie diese Schritte aus, um den Registrierungswert hinzuzufügen:

1. Öffnen Sie den Registrierungstabellen-Editor auf dem Agentenrechner mit dem folgenden Befehl:

   ```
   regedit
   ```

2. Rufen Sie folgende Schlüssel ab, je nachdem, ob eine agentenbasierte oder agentenlose Sicherung erfolgt:

   Navigieren Sie für die agentenbasierte Sicherung für 32-Bit und 64-Bit-Betriebssysteme auf dem Agentenrechner zu folgendem Schlüssel:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Wenn Sie eine Version unter Arcserve UDP v6.5 Update 2 verwenden, navigieren Sie für agentlose Sicherungen zum untenstehenden Schlüssel. Erstellen Sie den Registrierungstabellenwert auf dem virtuellen Rechner, den Sie auf dem Proxy-Server sichern möchten. Wenn der Schlüssel der Registry-Tabelle nicht verfügbar ist, erstellen Sie den vollständigen Schlüsselpfad.

   - **32-Bit-BS:**

     HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   - **64-Bit-BS:**

     HKEY_LOCAL_MACHINE\SOFTWARE\WoW6432Node\Arcserve\Unified Data Protection\Engine\AFBackupDll

3. Erstellen Sie die folgenden beiden Registrierungswerte, und legen Sie für beide den Wert auf 1 fest:
   - dword-Wert mit dem Namen "BackupSQLLog4Purge"
   - dword-Wert mit dem Namen "ForceShrinkSQLLog"

     Der Registrierungswert wird hinzugefügt.

   Die Lösung tritt in Kraft, wenn der nächste Bereinigungsjob durchgeführt wird.

Beim Durchsuchen von Wiederherstellungspunkten werden keine verfügbaren Wiederherstellungspunkte angezeigt, wenn RPS mit FQDN konfiguriert sind

Gültig auf Windows-Betriebssystemen

Problem

Wenn der RPS sich nicht in einer Domäne befindet, wenn Sie den FQDN in der UDP-Konsole konfigurieren (durch Hinzufügen des DNS-Suffix), werden beim Durchsuchen der Wiederherstellungspunkte keine genauen Ergebnisse angezeigt. Obwohl Sie einige Sitzungen auf RPS sichern, wird die Anzahl der Wiederherstellungspunkte als Null angezeigt.

Der Grund dafür ist folgender: Wenn der RPS sich nicht in einer Domäne befindet, kann der RPS sich selbst nicht unter Verwendung des FQDN identifizieren.

Lösung

Um dieses Problem zu beheben, fügen Sie das DNS-Suffix zum RPS-Host hinzu.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Systemsteuerung, und navigieren Sie zu **System und Sicherheit**, **Systeme**.
2. Klicken Sie auf **Einstellungen ändern** für Computername, Domäne sowie Workgroup-Einstellungen.

   Das Dialogfeld "Systemeigenschaften" wird angezeigt.
3. Klicken Sie auf der Registerkarte **Computername** auf **Änderungen**.

   Das Dialogfeld **Änderungen für Computername/Domäne** wird geöffnet.
4. Klicken Sie auf **Mehr**.

   Das Dialogfeld **DNS-Suffix und NetBIOS-Computername** wird geöffnet.
5. Fügen Sie im Feld "Primäres DNS-Suffix dieses Computers" das Netzwerk-DNS-Suffix hinzu, und klicken Sie auf **OK**.

   Fügen Sie beispielsweise ABC.com hinzu.
6. Starten Sie das System neu.

Zugriffsverweigerung beim Hinzufügen von RPS

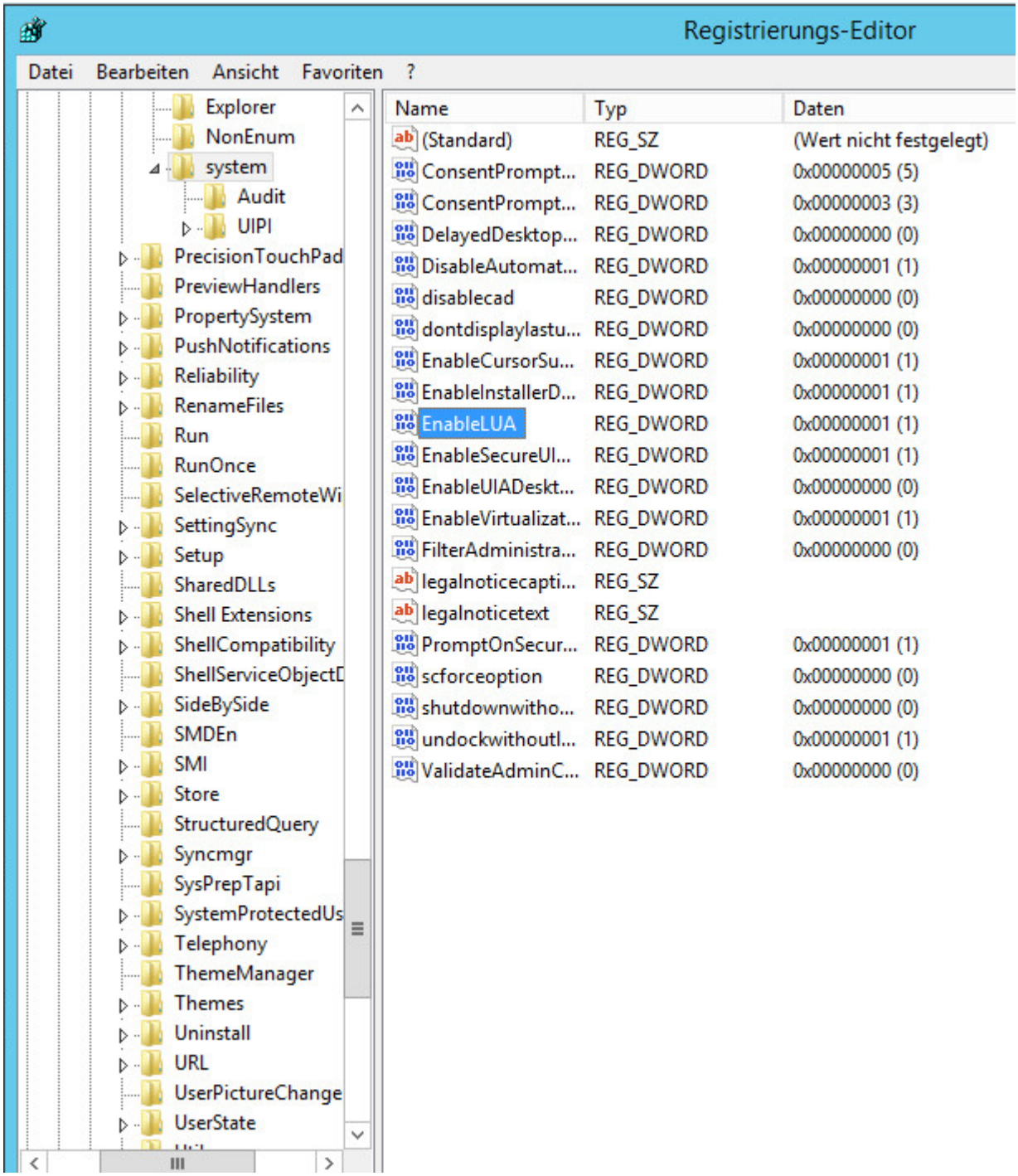
Problem:

Wenn Sie Windows 10 als RPS hinzufügen und auch wenn UAC nicht ausgeführt wird, wird eine Fehlermeldung angezeigt:

Zugriff verweigert. Das Konto verfügt möglicherweise nicht über Administratorrechte oder das Konto ist ein nicht integriertes Administratorkonto und UAC ist eingeschaltet.

Lösung:

Um die UAC unter Windows 10 zu deaktivieren, ändern Sie den Wert des Registrierungsschlüssels, indem Sie in der Systemsteuerung nicht nur die Ebene in "Nie benachrichtigen" ändern, sondern auch entsprechend des Registrierungsdiagramms unten.



Legen Sie die Registrierung "EnableLUA" auf 0 fest, um UAC vollständig zu deaktivieren und den Rechner neu zu starten.

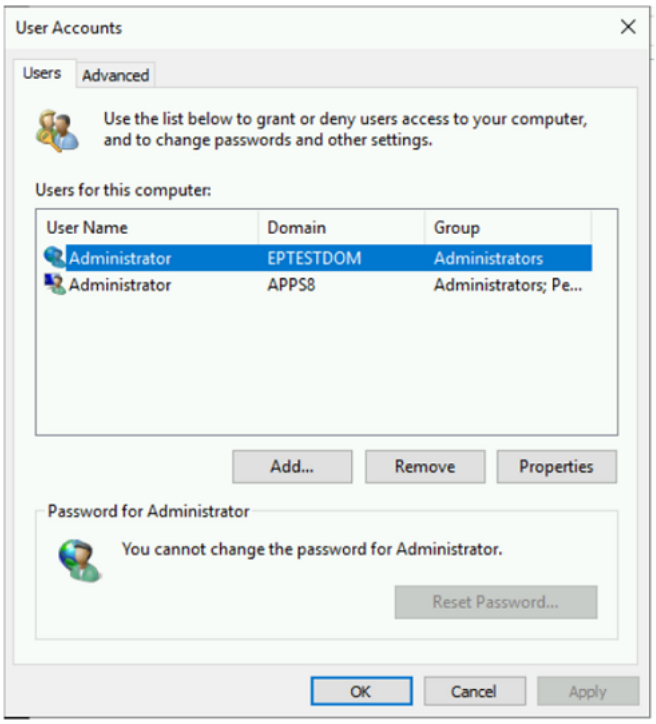
Fügen Sie dann Windows 10 in der Konsole als RPS hinzu.

Zuweisen von Administratorrechten und -rollen zu einem Domänenbenutzer

Dieser Abschnitt enthält Informationen zum Zuweisen von Administratorrechten und -rollen zu einem Domänenbenutzer.

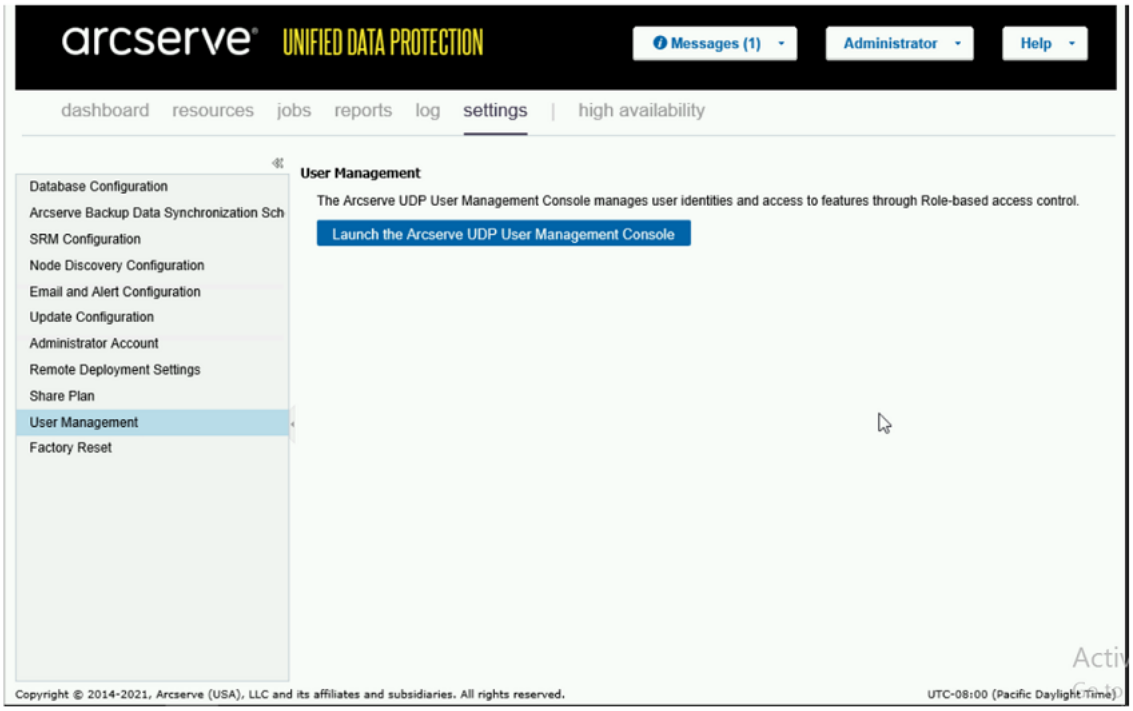
Gehen Sie wie folgt vor:

1. Um den UDP-Konsolenrechner für die Domäne zu konfigurieren, verwenden Sie die Anmeldeinformationen des Administrators.
2. Stellen Sie sicher, dass der Domänenbenutzer Teil der Administratorgruppe ist. Um einen Benutzer zur Administratorgruppe hinzuzufügen, klicken Sie im Fenster "Benutzerkonten" auf die Schaltfläche **Hinzufügen**.



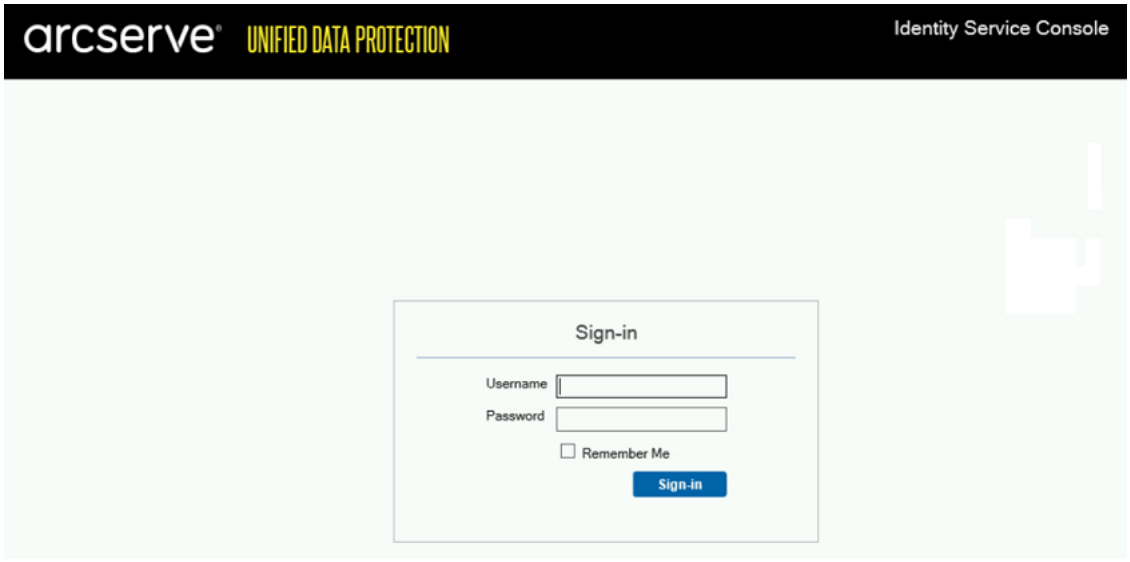
3. Nachdem Sie den Benutzer zur Administratorgruppe hinzugefügt haben, starten Sie den Verwaltungsdienst neu.
4. Gehen Sie wie folgt vor, um einem Domänenbenutzer mit der Arcserve UDP-Benutzerverwaltungskonsole die Administratorrolle hinzuzufügen:
    a. Melden Sie sich mit den Anmeldeinformationen des Administrators bei der Arcserve UDP-Konsole an.
    b. Klicken Sie auf die Registerkarte **Einstellungen**.
    c. Klicken Sie im linken Fensterbereich auf **Benutzerverwaltung**.

Die Seite "Benutzerverwaltung" wird geöffnet.



d. Klicken Sie auf die Schaltfläche **Starten Sie die Arcserve UDP-Benutzerverwaltungskonsole**.

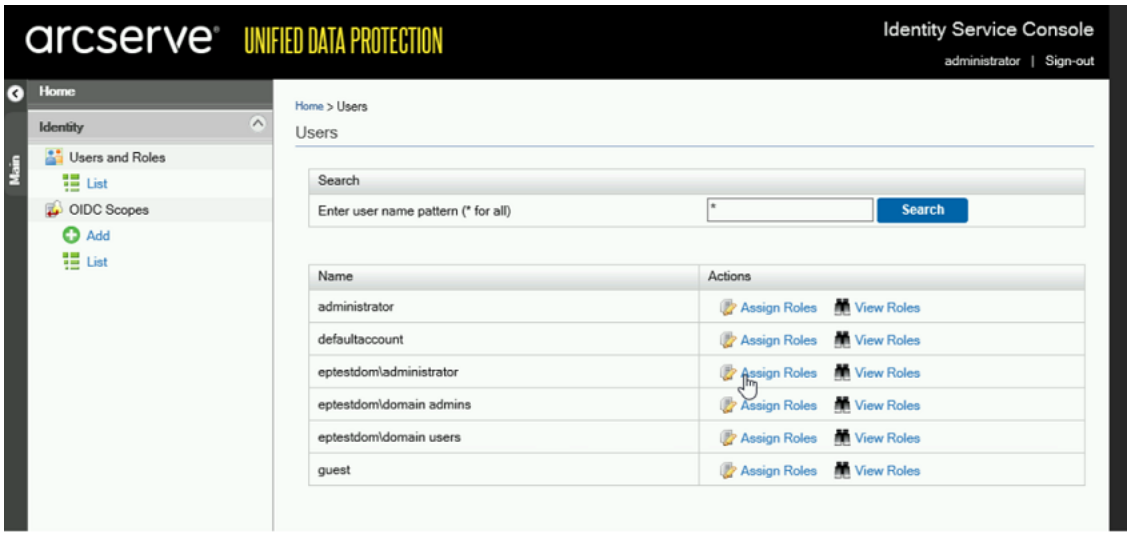
Die Identitätsdienstkonsole wird in einem neuen Fenster geöffnet.



e. Geben Sie die Administrator-Anmeldeinformationen wie Benutzername und Kennwort an, und klicken Sie dann auf **Anmelden**.

Die Startseite der Identitätsdienstkonsole wird geöffnet.

f. Navigieren Sie zur Seite **Benutzer**, und wählen Sie dann aus einer Liste von Benutzern einen Benutzer aus, und klicken Sie auf **Rollen zuweisen**, um Administratorberechtigungen anzuwenden.



g. Melden Sie sich mit Domänen-Anmeldeinformationen bei der UDP-Konsole an.

Umschalten in die UDP-Ansicht für Wiederherstellungspunkt nicht möglich

Problem:

Wenn Sie die Ansicht für einen RPS-Wiederherstellungspunkt in die UDP-Ansicht umstellen, erhalten Sie manchmal Fehlermeldungen, wie z. B. Zugriff verweigert.

Lösung:

Deaktivieren Sie die UAC, um das Problem zu lösen. Weitere Informationen finden Sie unter Deaktivieren einer Remote-UAC für einen nicht integrierten Administrator.

Zugriffsverweigerung beim Hinzufügen oder Aktualisieren von Knoten

Gültig auf Windows-Betriebssystemen

Problem

Wenn Sie Knoten hinzufügen oder aktualisieren, erhalten Sie in manchen Fällen den folgenden Fehler:

Zugriff verweigert. Das Konto verfügt evtl. nicht über Administratorrechte, oder das Konto ist ein nicht integriertes Administratorkonto, und die UAC wird aktiviert.

Lösung

Der Fehler tritt in folgenden Szenarios auf:

- Sie haben sich als lokaler Benutzer oder Domänenbenutzer angemeldet, der sich nicht in der lokalen Administratorengruppe des Knotens befindet, um Knoten hinzuzufügen oder zu aktualisieren.
- Sie haben sich als Benutzer angemeldet, der sich in den Gruppen lokaler Administrator des Knotens befindet, jedoch über ein nicht integriertes Administratorkonto des Knotens verfügt, um Knoten hinzuzufügen oder zu aktualisieren.

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Fügen Sie die lokalen oder Domänenbenutzer zu den lokalen Administratorgruppen dieses Knotens hinzu.
2. Deaktivieren Sie die UAC dieses Knotens.

   Führen Sie diese Schritte aus, um die UAC zu deaktivieren:

   a. Klicken Sie auf "Start", geben Sie "regedit" im Feld "Programme/Dateien durchsuchen" ein, und drücken Sie die Eingabetaste.

   b. Der Registrierungs-Editor von Windows wird geöffnet.

      Hinweis: Möglicherweise müssen Sie Administrator-Anmeldeinformationen angeben, um den Windows-Registrierungs-Editor zu öffnen.

   c. Suchen Sie den folgenden Registrierungsschlüssel, und klicken Sie darauf:

      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

   d. Klicken Sie im Menü "Bearbeiten" auf "Neu" und anschließend auf "DWORD-Wert (32-Bit)".

e. Geben Sie "LocalAccountTokenFilterPolicy" als Namen des neuen Eintrags ein, und drücken Sie die Eingabetaste.

f. Klicken Sie mit der rechten Maustaste auf "LocalAccountTokenFilterPolicy" und anschließend auf "Ändern".

g. Geben Sie im Datenfeld "Wert" "1" ein, und klicken Sie auf "OK".

h. Verlassen Sie den Registrierungseditor.

Hinweise:

- Dieser Vorgang weicht vom Deaktivieren der UAC grundsätzlich ab. Mit diesem Vorgang können Sie bestimmte Funktionen der UAC deaktivieren.
- Da für den Import die Technologie der Windows-Verwaltungsinstrumentation (WMI) eingesetzt wird, stellen Sie sicher, dass WMI nicht durch die Firewall blockiert ist.

Weitere Informationen zum Verhalten von Windows finden Sie in der Microsoft-Dokumentation.

UDP-Konsole wird bei Änderung des SQL-Administratorkennworts nicht geöffnet

Problem:

Die Arcserve UDP-Konsole nutzt SQL Server als Datenbank und den SQL-Administrator "SA", um sich mit der Datenbank zu verbinden. Wenn das "SA"-Kennwort geändert wird, kann die Konsolenstartseite nicht geöffnet werden und es wird die folgende Meldung angezeigt:

SQL Server ist zurzeit nicht verfügbar. Überprüfen Sie den Dienststatus, und starten Sie den Arcserve UDP-Verwaltungsdienst neu.

Lösung:

1. Führen Sie <homedir>\Management\BIN\DBAccountUpdate.bat aus.
2. Geben Sie Folgendes ein: updatePassword
3. Geben Sie das neue Kennwort ein, und drücken Sie EINGABE.

Fehler beim Laden von Wiederherstellungspunkten aufgrund eines Zeitlimits

Problem

Wenn der RPS ausgelastet ist, benötigt das Betriebssystem länger, um das geladene Volume anzuhängen. Das Laden von Wiederherstellungspunkten schlägt fehl. In den Aktivitätsprotokollen wird die folgende Meldung angegeben:

Das Laden des Volume dauert länger als erwartet (2 Minuten). Dies geschieht, wenn Ihr Server ausgelastet ist. Versuchen Sie es erneut, wenn die Auslastung des Servers weniger hoch ist, oder informieren Sie sich in der Online-Dokumentation über die Fehlerbehebung, um das Zeitlimit zu erhöhen.

Lösung

Um dieses Problem zu beheben, erhöhen Sie das Zeitlimit.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim RPS an, und navigieren Sie zu folgendem Speicherort:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFStorHBAMgmt
   ```

   ```
   "WaitDeviceReadyTimeoutS"=dword:00000078
   ```

   Standard: 120 Sekunden

2. Ändern Sie das Zeitlimit in einen höheren Wert.

   Ändern Sie zum Beispiel das Zeitlimit in 600 Sekunden (10 Minuten).

Aktualisieren der Anmeldeinformationen des Gateway-Servers

Problem

Wenn der Benutzername für die Gateway-Installation geändert wird oder das Kennwort abgelaufen ist, erhalten Sie während der Planbereitstellung folgenden Fehler:

Agent-Bereitstellung fehlgeschlagen.

Benutzer, der Arcserve Remote Management Gateway mit den gespeicherten Anmeldeinformationen installiert hat, kann nicht imitiert werden. Überprüfen Sie, ob die Anmeldeinformationen noch gültig sind, und stellen Sie den Agenten erneut bereit.

Lösung

Um dieses Problem zu lösen, aktualisieren Sie Benutzername oder Kennwort für das Gateway-Konto.

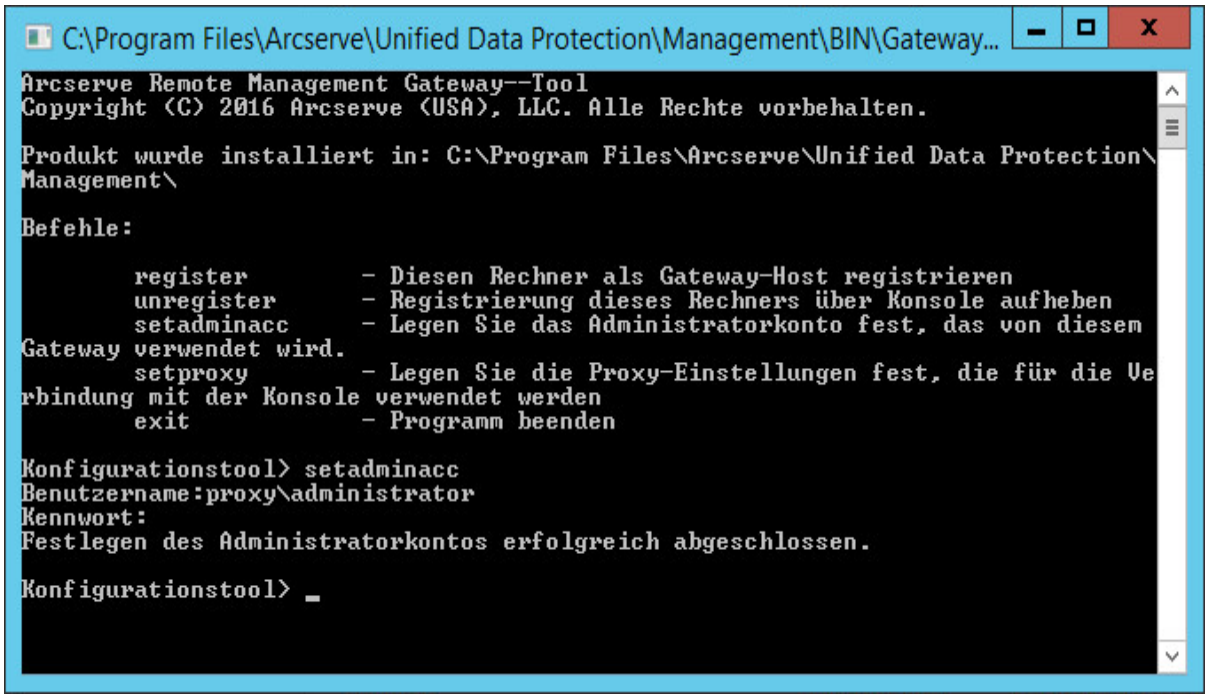
Gehen Sie wie folgt vor:

1. Melden Sie sich beim Gateway-Server an.
2. Navigieren Sie zum Ordner "BIN" im Installationsverzeichnis von Arcserve UDP.

   Beispiel: C:\Programme\Arcserve\Unified Data Protection\Management\BIN\GatewayTool.exe
3. Klicken Sie mit der rechten Maustaste auf GatewayTool.exe, und klicken Sie auf "Als Administrator ausführen".
4. Geben Sie im Eingabeaufforderungsfenster **setadminacc** ein.
5. Geben Sie den neuen Benutzernamen an.
6. Geben Sie das neue Kennwort an.

   Wenn alle Details richtig sind, wird die folgende Meldung angezeigt:

   ```
   Festlegen des Administratorkontos erfolgreich
   ```



7. Stellen Sie den Plan erneut bereit.

Aktualisieren des Gateways, wenn die Gateway-Proxy-Anmeldeinformationen geändert werden

Problem

Wenn die Proxy-Server-Anmeldeinformationen geändert werden, ist die Verbindung zum Gateway unterbrochen. Sie erhalten die folgende Fehlermeldung, bei dem Versuch, eine Verbindung zum Gateway herzustellen:

Keine Verbindung zum Gateway-Standort-Proxy möglich. Überprüfen Sie den Status des Standorts, und stellen Sie sicher, dass dieses Gateway ausgeführt wird.

Lösung

Um dieses Problem zu beheben, aktualisieren Sie die Parameter in GatewayTool.exe Setproxy.

Führen Sie diese Schritte aus, um den Gateway-Server zu aktualisieren:

1. Melden Sie sich beim Gateway-Server an.
2. Navigieren Sie zum Ordner "BIN" im Installationsverzeichnis von Arcserve UDP.

   Beispiel: C:\Programme\Arcserve\Unified Data Protection\Management\BIN\GatewayTool.exe
3. Klicken Sie mit der rechten Maustaste auf GatewayTool.exe, und klicken Sie auf "Als Administrator ausführen".
4. Geben Sie im Eingabeaufforderungsfenster **setproxy** ein.
5. Geben Sie **2** ein, um "Benutzerdefinierter Proxy" auszuwählen, da der IE-Proxy aktuell keine Anmeldeinformationen unterstützt.
6. Geben Sie die IP-Adresse für den Proxy-Server an.
7. Geben Sie den Port für den Proxy-Server an.
8. Geben Sie zur Authentifizierung **Y** ein.

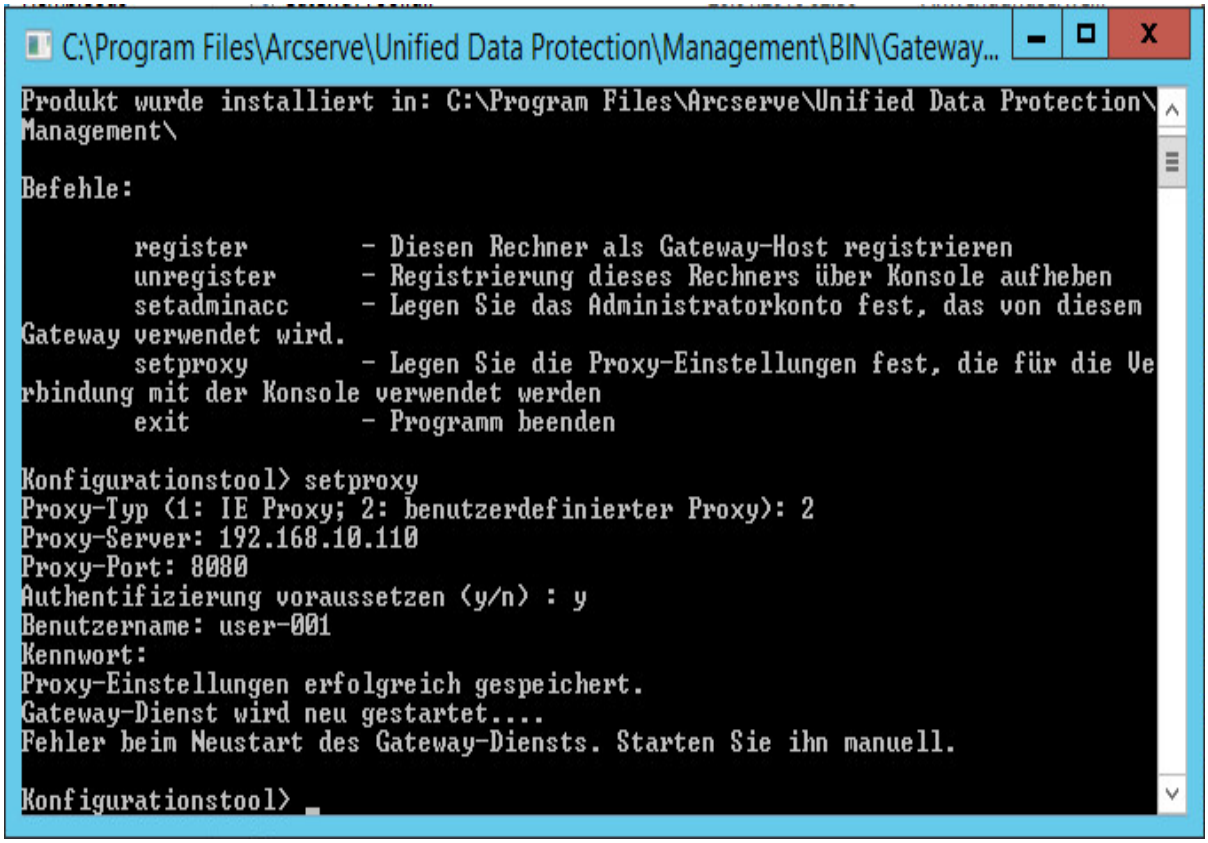
   Hinweis: Wenn Sie "N" eingeben, werden die Anmeldeinformationen deaktiviert.
9. Geben Sie den neuen Benutzernamen an.
10. Geben Sie das neue Kennwort an.

    Wenn alle Details richtig sind, wird die folgende Meldung angezeigt:

    ```
    Proxy-Einstellungen wurden erfolgreich gespeichert.
    Der Gateway-Dienst wird neu gestartet.
    ```

Hinweis: Wenn die Gateway-Proxy-Anmeldeinformationen in einem Plan aktiviert sind, aktualisieren Sie Proxy-Benutzernamen und Proxy-Kennwort im Plan.

In gleicher Weise können Sie andere Einstellungen wie Proxy-Typ, IP-Adresse und Portnummer in **setproxy** ändern.



Wenn die Meldung **Gateway-Dienst konnte nicht neu gestartet werden, manuell starten** in der Eingabeaufforderung angezeigt wird, gehen Sie folgendermaßen vor:

a. Führen Sie **services.msc** aus, um nach **Arcserve remote management gateway service** zu suchen, und starten Sie dann den Remote Management Gateway Service.

b. Wenn der Remote-Dienst nach dem Neustart beendet wird, verwenden Sie den Task-Manager, um den Task **tomcat8.exe** manuell zu beenden.

c. Aktualisieren Sie **services.msc**, und starten Sie **Arcserve remote management gateway service** neu.

Konsole zeigt Meldung "Identitätsdienst wird gestartet"

Problem

Anmeldung bei der Arcserve UDP-Konsole nicht möglich. Die Konsole zeigt die folgenden Meldungen, selbst fünf Minuten, nachdem Sie sich angemeldet haben:

Identitätsdienst wird gestartet

Lösung

Um dieses Problem zu beheben, öffnen Sie die Windows-Dienstkonsole, und starten Sie den Arcserve UDP-Konsolendienst **Arcserve UDP Management Service** neu.

Bei Sicherung und Wiederherstellung des virtuellen Rechners

Dieser Abschnitt enthält die folgenden Fehlerbehebungsthemen im Zusammenhang mit Recovery Point Server (RPS), Datenspeicher und Datenbank:

- Hinzufügen von Berechtigungen für VDDK auf Ebene des vCenter-Servers
- Jobs für die Sicherung von VM-Vorlagen werden immer in eine vollständige Sicherung konvertiert
- Unabhängige Datenträger werden bei der Sicherung von VM-Vorlagen übersprungen
- Die Sicherung von in SMB 3.0-Freigaben abgelegten VMs schlägt mit einer Fehlermeldung fehl
- VM-Wiederherstellungsjobs schlagen fehl bei der Wiederherstellung von VMs in eine Windows-Standarddateifreigabe
- Volume-Informationen für den Wiederherstellungspunkt nicht verfügbar
- Berechtigungen für die hostbasierte agentenlose Sicherung und virtuelles Standby auf vCenter Server-Ebene
- Konvertierung von inkrementellen Sicherungen in Überprüfungssicherungen aufgrund Snapshots virtueller Rechner, die seit dem letzten Sicherungsjob geändert wurden oder konsolidiert werden müssen
- Agentenlose Sicherung für VMware-VM schlägt bei CD/DVD-Gerät der VM fehl
- Agentenlose hostbasierte Sicherung für Hyper-V schlägt nach dem Aktualisieren von Arcserve UDP fehl
- Hostbasierte agentenlose Sicherung schlägt in VMware ESXi 6.0 fehl
- Fehler beim Erstellen eines Snapshot für virtuelle Hyper-V-Rechner bei mehreren ausgeführten Jobs
- Sicherung von virtuellem Datenträger ist fehlgeschlagen. Systemfehler=[The device is not ready(21)]
- Fehlgeschlagene Sicherungsjobs
- Fehler beim Importieren von VMware-VMs aus vCenter
- Anwendung von Sicherungseinstellungen für Knoten nicht möglich
- Sicherungen schlagen wegen ESXi-Lizenz fehl

- Hostbasierte agentenlose Sicherung verwendet keinen HotAdd-Transportmodus
- Der HotAdd-Transportmodus funktioniert nicht, wenn Sie versuchen, eine VMware-VM zu sichern.
- Hostbasierter agentenloser Sicherungs- oder Wiederherstellungsjob verwendet den NBD- oder den NBDSSL-Transportmodus auch dann, wenn der SAN-Modus möglich ist
- Genauere Steuerung für VSS Windows Gast-BS Quiescings
- Wiederherstellungsvorgänge schlagen fehl, wenn Daten im HotAdd- oder SAN-Transportmodus wiederhergestellt werden
- Wiederherstellung der VM schlägt fehl, wenn ein nicht standardmäßiger Port angegeben wird
- Geplante Zuwachssicherungsjobs oder vollständige Sicherungsjobs für Hyper-V-VMs schlagen fehl
- Hyper-V VSS NTDS-Writer schlägt bei der Erstellung des Snapshot in der VM fehl
- Änderungen der MAC-Adresse werden nach der VM-Wiederherstellung nicht beibehalten
- Hyper-V konnte keinen VSS-Snapshot erstellen
- VMDK-Dateien konnten nicht geöffnet werden
- Probleme durch doppelte VM-UUID
- Dateisystem-Katalogjob schlägt fehl oder die Überprüfung des Wiederherstellungspunktes für die hostbasierte agentenlose Sicherung schlägt fehl
- Inkrementelle Sicherung wird zu Überprüfungssicherung konvertiert, oder die Sicherungsgröße in Hyper-V wird erhöht.
- Hostbasierte agentenlose Sicherung schlägt für Hyper-V-VM mit spezieller Konfiguration differenzierender Datenträger fehl
- Sicherungsjob für VMware-VM schlägt fehl
- Deaktivieren des erneuten Durchsuchens von Host-Bus-Adaptern, wenn sich Quelle und Proxy auf unterschiedlichen VMware-ESX-Servern befinden
- Deaktivieren der aufeinander folgenden Erstellung von Snapshots in VMware-VM für eine Sicherung

- Agentenlose hostbasierte Sicherung stürzt ab, wenn Windows 2003 R2 (64 Bit) als Sicherungs-Proxy verwendet wird
- Nach Wiederherstellung von einem Host mit höherer ESXi-Version auf einen Host mit niedrigerer ESXi-Version hängt sich die VM beim Booten auf
- RAM-Auslastung erreicht 99 %, wenn Sicherungsjobs an die VM übergeben werden
- Hyper-V-Wiederherstellungsjob schlägt fehl, kann keine Verbindung zum Dienstprogramm auf Host herstellen
- Automatischer Schutz erkennt und schützt virtuellen Computer nicht
- Aktivieren Sie beim Sichern der VMDK-Datei das Lesen der Blockgröße

Hinzufügen von Berechtigungen für VDDK auf Ebene des vCenter-Servers

Wenn Sie nicht über die entsprechenden Berechtigungen verfügen, dann werden der Sicherungsjob für hostbasierte virtuelle Rechner und der Virtual Standby-Job fehlschlagen.

Um dieses Problem zu vermeiden, stellen Sie sicher, dass Sie über die entsprechenden Berechtigungen verfügen. Wenn Sie ein vCenter-Benutzer sind, benötigen Sie keine Administratorrechte auf der vCenter-Serverebene, jedoch müssen Sie über Administratorrechte auf der Datencenter-Ebene verfügen. Außerdem müssen Sie folgende Berechtigungen auf vCenter-Serverebene haben:

- Global, DisableMethods und EnableMethods
- Global, Lizenz

Weitere Informationen finden Sie im VMware-KB-Artikel.

Weitere Informationen zur Berechtigung finden Sie unter Berechtigungen für die hostbasierte agentenlose Sicherung und Virtual Standby auf vCenter-Serverebene.

Berechtigungen für die hostbasierte agentenlose Sicherung und virtuelles Standby auf vCenter Server-Ebene

Wenn Sie vCenter konfigurieren, um virtuelle Rechner zu verwalten, richten Sie im Allgemeinen Benutzer oder Gruppen mit vCenter-Administratorrechten ein. Diese Vorgehensweise hilft, sicherzustellen, dass die vCenter-Konten uneingeschränkten Zugriff auf die vCenter-Funktionen und -Tasks haben. Optional können Sie vCenter-Benutzer und Gruppen erstellen, die verwendet werden können, um entweder nur Sicherungen oder Sicherungen mit Wiederherstellung zu erleichtern.

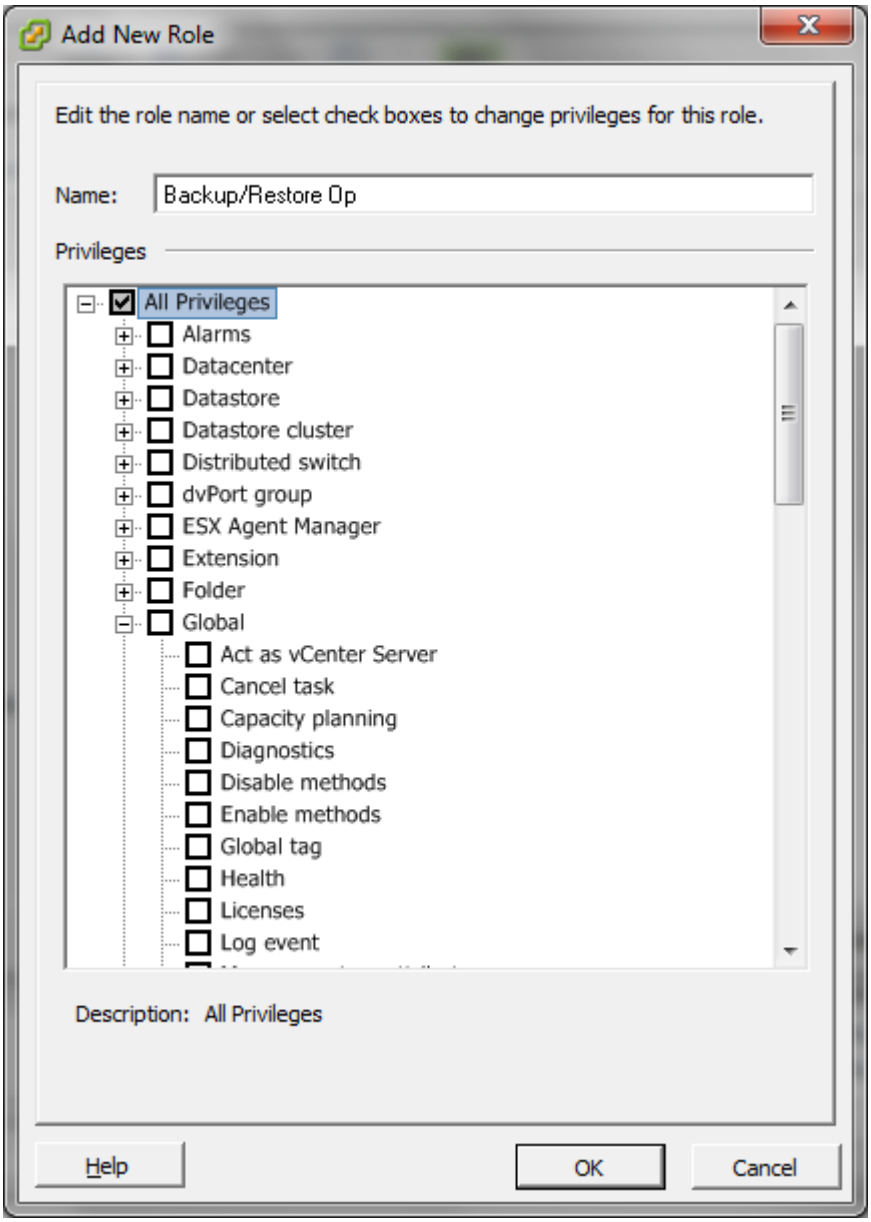
Werden nicht administrative vCenter-Konten verwendet, um Sicherung und Wiederherstellungsvorgänge zu erleichtern, erstellen Sie vCenter-Rollen, weisen den Rollen Berechtigungen zu, und wenden dann die Rolle auf individuelle Benutzer oder Gruppen an.

Hinweis: Als bewährtes Verfahren empfiehlt VMware, es den nicht administrativen vCenter-Benutzerkonten zu ermöglichen, Mitglied einer lokalen Windows-Administratorgruppe zu sein.

Wichtig! Die folgenden Schritte setzen voraus, dass Sie mit der Konfiguration von vCenter-Benutzern, -Gruppen, -Rollen und -Berechtigungen vertraut sind. Lesen Sie Bedarf die vCenter-Dokumentation.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei vCenter mithilfe des VI-Client an.
2. Öffnen Sie das Dialogfeld "Add New Roles", und geben Sie einen Namen für die Rolle an.



3. Blenden Sie alle Berechtigungen ein.
4. **(Optional)** Um es der Rolle zu ermöglichen, **nur Sicherungsvorgänge zu erleichtern**, geben Sie die folgenden Berechtigungen an:

   Wichtig! Um es der Rolle zu ermöglichen, Sicherungs- und Wiederherstellungsvorgänge zu erleichtern, fahren Sie zum nächsten Schritt fort.

   - Blenden Sie "Virtual machine" und "Configuration" ein, und geben Sie die folgenden Berechtigungen an:
     - Verfolgen von Datenträgeränderungen
     - Leasen von Datenträgern
     - Vorhandenen Datenträger hinzufügen

- Neuen Datenträger hinzufügen
- Gerät hinzufügen oder entfernen
- Ressource ändern
- Datenträger entfernen
- Einstellungen

- Blenden Sie "Virtual machine" und "Provisioning" ein, und geben Sie die folgenden Berechtigungen an:
  - Schreibgeschützten Datenträger-Zugriff erlauben
  - Download durch virtuellen Rechner erlauben
- Blenden Sie "Virtual machine" ein, und geben Sie die folgenden Berechtigungen an:

  vSphere 4: Blenden Sie "State" ein und geben Sie "Create Snapshot and Remove snapshot" an.

  vSphere 5: Blenden Sie "Snapshot management" und dann "State" ein und geben Sie dann "Create Snapshot and Remove snapshot" an.
- Blenden Sie "Global" ein und geben Sie die folgenden Berechtigungen an:
  - Methoden deaktivieren
  - Methoden aktivieren
  - Lizenzen

  Fahren Sie mit Schritt 6 fort.

5. Um es der Rolle zu ermöglichen, **nur Sicherungs und Wiederherstellungsvorgänge zu erleichtern**, geben Sie die folgenden Berechtigungen an:
   - Blenden Sie "Datastore" ein und geben Sie die folgenden Berechtigungen an:
     - Speicherplatz zuweisen
     - Datenspeicher durchsuchen
     - Dateioperationen auf niedriger Ebene
   - Blenden Sie "Global" ein und geben Sie die folgenden Berechtigungen an:
     - Methoden deaktivieren
     - Methoden aktivieren
     - Lizenzen
   - Blenden Sie "Host" und "Local Operations" ein, und geben Sie dann "Reconfigure virtual machine" an.

Hinweis: Diese Berechtigung wird nur zur Durchführung von Sicherungs- und Wiederherstellungsvorgängen unter Verwendung des HotAdd-Transport-Modus benötigt.

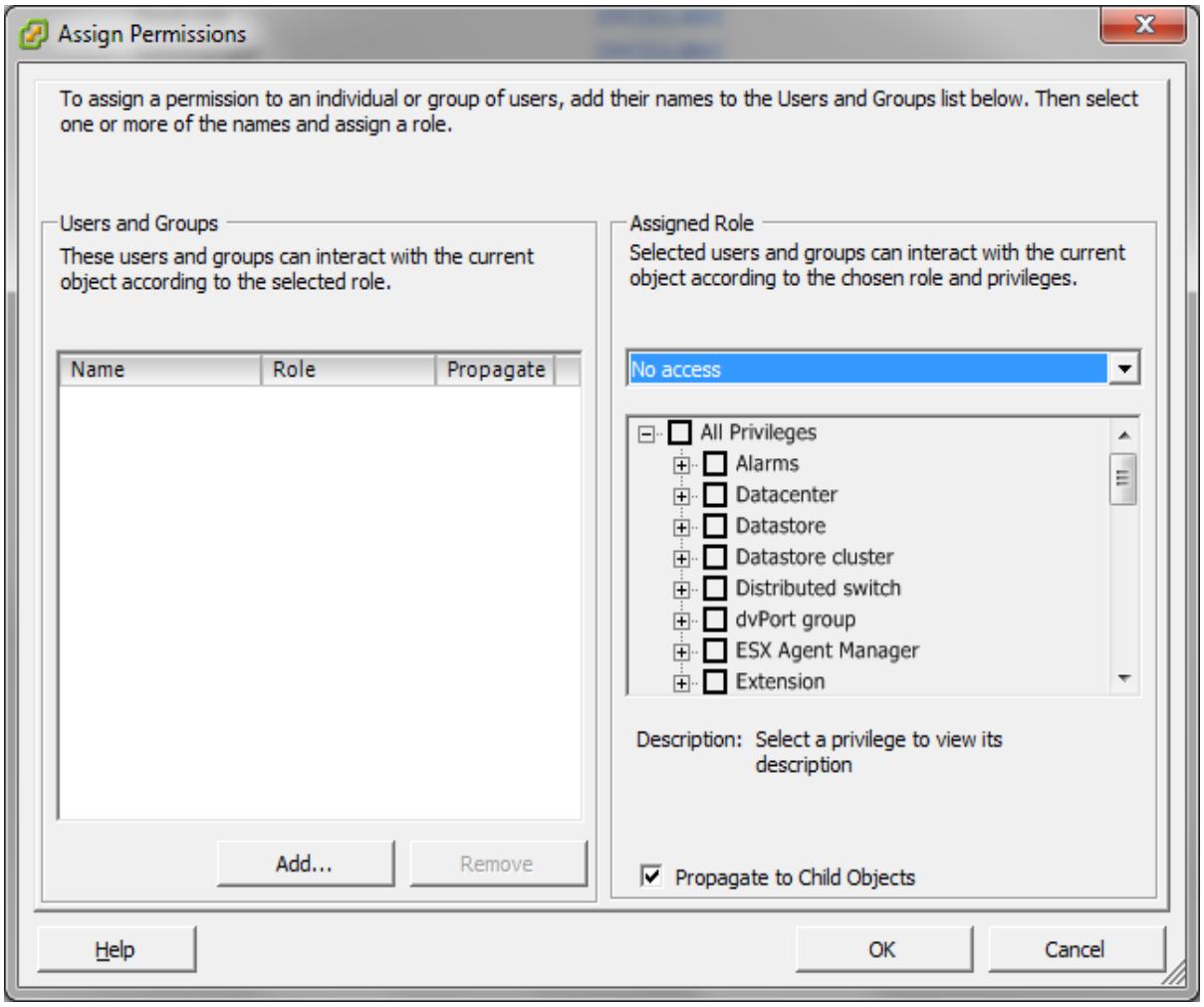
- Blenden Sie "Network" ein und geben Sie "Assign Network" an.
- Blenden Sie "Resource" ein und klicken Sie auf "Assign Virtual Machine to resource pool".
- Blenden Sie "Virtual machine" und "Configuration" ein, und geben Sie die folgenden Berechtigungen an:
  - Vorhandenen Datenträger hinzufügen
  - Neuen Datenträger hinzufügen
  - Gerät hinzufügen oder entfernen
  - Erweitert
  - CPU-Anzahl ändern
  - Ressource ändern
  - Verfolgen von Datenträgeränderungen
  - Leasen von Datenträgern
  - Host-USB-Gerät
  - Arbeitsspeicher
  - Geräteeinstellung ändern
  - Unformatiertes Medium
  - Von Pfad laden
  - Datenträger entfernen
  - Umbenennen
  - Gastinformationen zurücksetzen
  - Einstellungen
  - Auslagerungsdatei platzieren
  - Virtuelle Hardware aktualisieren
- Blenden Sie "Virtual machine" und "Guest Operations" ein, und geben Sie die folgenden Berechtigungen an:
  - Gastvorgang-Änderungen
  - Gastvorgang-Programmausführung
  - Gastvorgang-Abfragen (vSphere 5)

- Blenden Sie "Virtual machine" und "Interaction" ein, und geben Sie die folgenden Berechtigungen an:
  - Ausschalten
  - Einschalten
- Blenden Sie "Virtual machine" und "Inventory" ein, und geben Sie die folgenden Berechtigungen an:
  - Neu erstellen
  - Registrieren
  - Entfernen
  - Registrierung aufheben
- Blenden Sie "Virtual machine" und "Provisioning" ein, und geben Sie die folgenden Berechtigungen an:
  - Festplattenzugriff erlauben
  - Schreibgeschützten Datenträger-Zugriff erlauben
  - Download durch virtuellen Rechner erlauben
- Blenden Sie "Virtual machine" ein, und geben Sie die folgenden Berechtigungen an:

  vSphere 4: Blenden Sie "State" ein und geben Sie "Create snapshot", "Remove snapshot" und "Revert to snapshot" an.

  vSphere 5: Blenden Sie "Snapshot management" und "State" ein, und geben Sie "Create snapshot", "Remove snapshot" und "Revert to snapshot" an.

6. Klicken Sie auf "OK", um die Rolle zu erstellen.
7. Öffnen Sie das Dialogfeld "Assign Permissions", um die neu erstellte Rolle Benutzern, Gruppen, oder beiden zuzuweisen.



8. Wählen Sie in der Liste "Users and Groups" den benutzerdefinierten Benutzer aus, den Sie für Sicherungen und Wiederherstellungen verwenden wollen.

   Geben Sie in der Drop-down-Liste "Assigned Role" die Rolle an, die Sie auf die Benutzer oder Gruppen anwenden wollen.

9. Klicken Sie auf "OK", um die Rolle auf die Benutzer oder Gruppen anzuwenden.

   Die Berechtigungen sind jetzt für vCenter-Rollen definiert.

Jobs für die Sicherung von VM-Vorlagen werden immer in eine vollständige Sicherung konvertiert, und das Volumen der Sicherungsdaten entspricht der Bereitstellungsgröße des virtuellen Datenträgers

Problem

Beim Sichern einer VM-Vorlage wird der Sicherungsjob in eine vollständige Sicherung konvertiert, und das verarbeitete Datenvolumen entspricht der Bereitstellungsgröße des virtuellen Datenträgers. Im Aktivitätsprotokoll wird die folgende Warnmeldung angezeigt:

Da der virtuelle Rechner als Vorlage konfiguriert ist, ist der Job eine vollständige Sicherung, und die virtuellen Datenträger werden als komplette Datenträger gesichert.

Lösung

Bei diesem Verhalten handelt es sich um erwartetes Verhalten bei der Sicherung von VM-Vorlagen. Eine mögliche Problemumgehung besteht darin, die Vorlage zu Beginn der Sicherung in eine VM zu konvertieren, die VM zu sichern und sie nach Abschluss des Sicherungsjobs wieder in eine Vorlage zu konvertieren. Falls Sie diese Problemumgehung bevorzugen, müssen Sie wie folgt einen Registrierungswert auf dem Proxy-Rechner festlegen:

1. Melden Sie sich beim Proxy-Rechner an.
2. Erstellen Sie einen Registrierungswert auf Ebene des Proxy-Servers oder auf VM-Ebene.

   Hinweis: Wenn Sie den Registrierungswert auf VM-Ebene und auf Proxy-Ebene hinzufügen, hat die Einstellung in der Registrierung auf VM-Ebene Vorrang vor der Einstellung in der Registrierung auf Proxy-Ebene.

   Auf Ebene des Proxy-Servers (gilt für alle Sicherungsjobs, die auf dem jeweiligen Proxy-Server ausgeführt werden)

   a. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

   b. Fügen Sie einen DWORD-Wert mit dem Namen *TemplateDirectBackup* hinzu, und setzen Sie diesen Wert auf "0".

   Auf VM-Ebene

a. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Fügen Sie einen DWORD-Wert mit dem Namen *TemplateDirectBackup* hinzu, und setzen Sie diesen Wert auf "0".

Hinweis: Sobald diese Option aktiviert ist, lässt sich die VM bei einem abnormen Abbruch des Sicherungsjobs (z. B. bei einem Absturz des Jobs oder einem Neustart des Proxy-Rechners) nicht wieder in eine Vorlage konvertieren.

Unabhängige Datenträger werden bei der Sicherung von VM-Vorlagen übersprungen

Problem

Beim Sichern von VM-Vorlagen überspringt der Sicherungsjob unabhängige Datenträger, und im Aktivitätsprotokoll wird die folgende Warnmeldung angezeigt:

Der virtuelle Datenträger [datastore_720_4] shuli02-t235/shuli02-t235_1.vmdk konnte nicht gesichert werden, weil es sich um einen unabhängigen Datenträger handelt.

Lösung

Bei diesem Verhalten handelt es sich um erwartetes Verhalten bei der Sicherung von VM-Vorlagen. Die Ursache ist eine VMware-Einschränkung, aufgrund derer Sicherungsanwendungen die VMDK unabhängiger Datenträger nicht öffnen können. Eine mögliche Problemumgehung ist es, unabhängige Datenträger zu Beginn der Sicherung in abhängige Datenträger zu konvertieren, die abhängigen Datenträger zu sichern und sie nach Abschluss des Sicherungsjobs wieder in unabhängige Datenträger zu konvertieren. Falls Sie diese Problemumgehung bevorzugen, müssen Sie wie folgt einen Registrierungswert auf dem Proxy-Rechner festlegen:

1. Melden Sie sich beim Proxy-Rechner an.
2. Erstellen Sie einen Registrierungswert auf Ebene des Proxy-Servers oder auf VM-Ebene.

   Hinweis: Wenn Sie den Registrierungswert auf VM-Ebene und auf Proxy-Ebene hinzufügen, hat die Einstellung in der Registrierung auf VM-Ebene Vorrang vor der Einstellung in der Registrierung auf Proxy-Ebene.

   Auf Ebene des Proxy-Servers (gilt für alle Sicherungsjobs, die auf dem jeweiligen Proxy-Server ausgeführt werden)

   a. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

   b. Fügen Sie einen DWORD-Wert mit dem Namen *ConvertIndependentVMDK* hinzu, und setzen Sie diesen Wert auf "1".

   Auf VM-Ebene

   a. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Fügen Sie einen DWORD-Wert mit dem Namen *ConvertIndependentVMDK* hinzu, und setzen Sie diesen Wert auf "1".

Hinweise:

- Nachdem Sie diese Option aktiviert haben, können Sie die unabhängigen Laufwerke nicht zurücksetzen, falls die Sicherung anormal abgebrochen wird (beispielsweise durch einen Absturz des Auftrags oder wenn der Proxy-Rechner neu gestartet wird).
- Diese Option funktioniert nicht, wenn die Option "Vorlage wird während der Sicherung für VM konvertiert" aktiviert ist (der Registry-Wert TemplateDirectBackup wird mit dem Wert 0 erstellt).

Die Sicherung von in SMB 3.0-Freigaben abgelegten VMs schlägt mit einer Fehlermeldung fehl

Hinweis: Gilt für Hyper-V.

Problem

Die VM wird unter Hyper-V 2012 oder 2012 R2 gehostet und enthält Dateien in einer SMB 3.0-Freigabe. Der Sicherungsauftrag schlägt mit einer der folgenden Fehlermeldungen weiterhin fehl:

Fehler bei der VSS-Snapshot-Erfassung. Systemfehler=[VSS_E_VOLUME_NOT_SUPPORTED_BY_PROVIDER]

Fehler bei der VSS-Snapshot-Erfassung. Systemfehler=[VSS_E_BAD_STATE]

Lösung

1. Wenn die SMB-Freigabe von einem Windows-Dateiserver gehostet wird, fügen Sie die Rolle File Server VSS Agent Service auf dem Dateiserver hinzu und stellen Sie sicher, dass Microsoft File Server Shadow Copy Agent Service installiert ist.
2. Wenn die SMB-Freigabe von NAS-Geräten von Drittanbietern oder ähnlichen Lösungen gehostet wird, überprüfen Sie, ob diese Geräte oder Lösungen die VSS-Protokolle SMB 3.0 und File Server Remote unterstützen. Weitere Informationen erhalten Sie bei einem Drittanbieter.

Hinweis:

- Der Schattenkopie-Agent-Dienst für Dateiserver ist für VMs unter Hyper-V 2016 nicht erforderlich.
- Sie müssen die SMB 3.0-Freigabe ordnungsgemäß konfigurieren, damit Arcserve UDP VMs sichern kann, die in ihr abgelegt sind. Alle Anforderungen für SMB 3.0-Freigaben finden Sie im Abschnitt "Anforderungen und unterstützte Konfigurationen" in der Dokumentation von Microsoft.

VM-Wiederherstellungsjobs schlagen fehl bei der Wiederherstellung von VMs in eine Windows-Standarddateifreigabe

Hinweis: Gilt für Hyper-V.

Problem

Wird bei der VM-Wiederherstellung eine Windows-Standarddateifreigabe als Zielpfad angegeben (z. B. "\\hostname\C$\abc"), schlägt der Wiederherstellungsjob fehl, und die folgende Fehlermeldung wird angezeigt:

Der VM-Wiederherstellungsjob konnte den neuen virtuellen Rechner nicht erstellen.

Lösung

Das Fehlschlagen des Jobs ist ein erwarteter Fehler, da VM-Dateien unter Windows nicht in einer Standarddateifreigabe gespeichert werden dürfen. Es werden ausschließlich Microsoft SMB 3.0-Dateifreigaben unterstützt. Weitere Details finden Sie in der *Dokumentation von Microsoft*.

Volume-Informationen für den Wiederherstellungspunkt nicht verfügbar

Problem

Im Assistenten zum Wiederherstellen von VMs/Dateien werden beim Bereitstellen oder Kopieren eines Wiederherstellungspunkts kein Volume und keine Datei auf dem Bildschirm für Wiederherstellungspunkte angezeigt. Stattdessen wird die folgende Meldung angezeigt:

Volume-Informationen sind für diesen Wiederherstellungspunkt nicht verfügbar.

Lösung

Dieses Verhalten wird erwartet, wenn die Quell-VM kein Windows-Betriebssystem hat. Daher ist Arcservev UDP nicht in der Lage, virtuelle Festplatten der VM zu analysieren, um Volumendaten zu erhalten. Sie können die gesamte VM wiederherstellen oder den Wiederherstellungspunkt kopieren. Wenn die Quell-VM über ein Linux-VM-Betriebssystem verfügt, können Sie Dateien auch von dem Wiederherstellungspunkt wiederherstellen, indem Sie einen Linux-Sicherungsserver verwenden.

Konvertieren von Zuwachssicherungen in Überprüfungssicherungen, weil Snapshots virtueller Rechner seit dem letzten Sicherungsjob geändert wurden oder konsolidiert werden müssen

Hinweis: Gilt für Windows-Plattformen.

Problem

Die Zuwachssicherungen für virtuelle VMware-Rechner werden in Überprüfungssicherungen konvertiert. Das Aktivitätsprotokoll zeigt folgende Meldung an:

Zuwachssicherung in Überprüfungssicherung konvertieren, weil die Snapshots von virtuellen Rechnern sich seit dem letzten Sicherungsjob geändert haben oder eine Konsolidierung benötigen.

Lösung

Verwenden Sie den VMware vSphere Client, um die Snapshots virtueller Rechner zu konsolidieren. Weitere Details zum Konsolidieren von Snapshots finden Sie im folgenden Artikel der VMware Knowledge Base.

Hinweis: Die Konsolidierung von Snapshots für einen virtuellen Rechner kann aufgrund gesperrter Dateien fehlschlagen. Wenn der Sicherungsjob den HotAdd-Transportmodus verwendet, stellen Sie sicher, dass die Einstellungen des virtuellen Sicherungs-Proxy-Rechners auf dem ESXi-Server keine Festplatten enthalten, die über HotAdd hinzugefügt wurden. Konsolidieren Sie danach die Snapshots der virtuellen Rechner.

Agentenlose Sicherungen von VMware-VMs schlagen fehl, wenn das CD/DVD-Gerät der VM mit einem ISO-Image auf einem nicht verbundenen NFS-Daten-speicher verbunden ist

Problem

Führen Sie die folgenden Schritte aus, um das Problem zu reproduzieren:

1. Bereiten Sie ein ISO-Image auf einem NFS-Datenspeicher vor, der mit dem ESX-Host verbunden ist.
2. Verbinden Sie das ISO-Image mit dem CD/DVD-Gerät einer VM.
3. Trennen Sie den NFS-Datenspeicher vom Netzwerk.
4. Führen Sie eine agentenlose Sicherung der VM durch.

In diesem Fall schlägt der Job mit einer Fehlermeldung wie "Could not take snaps-hot of the virtual machine. ESX Server/vCenter Server reported the following error: A general system Error occurred." (Snapshot des virtuellen Rechners konnte nicht erstellt werden. ESX Server/vCenter Server hat folgenden Fehler gemeldet: all-gemeiner Systemfehler.) fehl.

Lösung

Aufgrund einer Beschränkung in ESX kann kein Snapshot erstellt werden, wenn die VM keine Verbindung mit dem mit ihr verbundenen ISO-Image hat. Trennen Sie das ISO-Image vor der Sicherung vom CD/DVD-Gerät der VM, um dieses Problem zu umgehen.

Agent-lose hostbasierte Sicherung für Hyper-V-VM schlägt nach dem Aktualisieren von Arcserve UDP fehl

Gilt für Hyper-V

Problem

Nach dem Upgrade von Arcserve UDP von Version 5.0 Update 2 oder einer älteren Version auf die neueste Version schlägt die agentenlose hostbasierte Sicherung mit der folgenden Meldung fehl:

Der Sicherungsjob wurde abgebrochen. Für einen VSS-Snapshot muss der Hyper-V-VSS Writer den virtuellen Rechner speichern. Dies wird im aktuellen Plan nicht berücksichtigt. Ändern Sie die Einstellung für die Hyper-V-Snapshot-Methode im Plan, um den Sicherungsjob neu zu starten. Weitere Informationen zum Konfigurieren der Hyper-V-Snapshot-Methode in einem Plan finden Sie in der Produktdokumentation.

Die agentenlose hostbasierte Sicherung hat vor dem Upgrade funktioniert.

Lösung

In Arcserve UDP Version 5.0 Update 2 und älteren Versionen wird standardmäßig die Offline-Sicherungsmethode verwendet, wenn der virtuelle Rechner die Online-Sicherungsmethode nicht unterstützt. Die Offline-Sicherungsmethode speichert den virtuellen Rechner, während der Snapshot erstellt wird. Im Zustand "Gespeichert" ist kein Zugriff auf den virtuellen Rechner möglich. Wichtige virtuelle Rechner müssen jedoch ständig erreichbar sein.

In Version 5.0 Update 3 und neueren Versionen wird der Sicherungsjob standardmäßig abgebrochen, wenn der virtuelle Rechner in den Zustand "Gespeichert" versetzt werden muss, um einen Ausfall des virtuellen Rechners zu verhindern. Wenn Sie nicht möchten, dass der Job abgebrochen wird, ändern Sie die Option **Hyper-V-Snapshot-Methode** im Plan. Weitere Informationen zur Option "Hyper-V-Snapshot-Methode" im Plan finden Sie unter "Erstellen eines hostbasierten Sicherungsplans für virtuelle Rechner".

Weitere Details zu diesem Problem finden Sie außerdem in diesem KB-Artikel von Arcserve.

Hostbasierte agentenlose Sicherung schlägt in VMware ESXi 6.0 fehl

Problem

Agentenlose Arcserve UDP-Sicherungen schlagen fehl, wenn Sie versuchen, einen virtuellen Rechner in VMware ESXi 6.0 zu sichern und die Funktion CBT (Change Block Tracking) aktiviert ist.

Dies ist ein bekanntes Problem mit VMware. Wenn die Sicherung fehlschlägt, können die folgenden beiden Verhalten auftreten:

- Arcserve UDP stellt möglicherweise keine Verbindung zur CBT-Funktion des ESXi-Hosts her. Infolgedessen kann Arcserve UDP keine verwendeten oder geänderten Datenblockinformationen vom virtuellen Rechner erhalten.
- Arcserve UDP kann möglicherweise nicht die stillgelegten Snapshots des virtuellen Rechners aufnehmen. (Dies kann jedes Mal vorkommen, wenn Arcserve UDP einen Snapshot aufnimmt, oder wenn Sie manuell einen Snapshot im vSphere-Client aufnehmen.)

Lösung

VMware hat dieses Problem im aktuellen Build, ESXi 6.0 Build 2715440, gelöst. Sie können den Patch ESXi600-201505001 installieren, um dieses Problem zu beheben. Weitere Informationen zum Herunterladen und Installieren des Patches finden Sie in diesem VMware-KB-Artikel.

Wenn Sie den Patch nicht anwenden können, können Sie das Problem lösen, indem Sie die folgenden Änderungen am Registrierungsschlüssel vornehmen:

Lösung für den CBT-Verbindungsfehler

Wenn Arcserve UDP keine Verbindung zu CBT herstellen kann, kann Arcserve UDP anstelle eines Fehlschlags mit dem Sicherungsjob fortfahren. Allerdings führt Arcserve UDP anstelle einer Zuwachssicherung standardmäßig eine vollständige Sicherung des virtuellen Rechners durch. Wenn Sie nicht automatisch eine vollständige Sicherung durchführen möchten, können Sie einen Registrierungsschlüssel hinzufügen, um das Standardverhalten zu ändern. Wenn Sie den Schlüssel hinzufügen und den Wert auf 1 setzen, lässt Arcserve UDP den Sicherungsjob fehlschlagen, wenn ein CBT-Fehler auftritt.

Sie können diesen Registrierungsschlüssel auf dem Proxy-Server wie folgt hinzufügen:

Auf Proxy-Server-Ebene (gilt für alle Sicherungsjobs, die auf diesem Proxy-Server ausgeführt werden)

1. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

2. Geben Sie folgendes DWORD ein:

   "BackupEntireDiskOnCBTBitmapFailure"=dword:00000001

3. Speichern Sie den Registrierungsschlüssel.

Auf VM-Ebene

1. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

2. Geben Sie folgendes DWORD ein:

   "BackupEntireDiskOnCBTBitmapFailure"=dword:00000001

3. Speichern Sie den Registrierungsschlüssel.

Hinweis: Wenn Sie den Registrierungsschlüssel sowohl im VM als auch in der Registrierung auf Proxy-Ebene hinzufügen, hat die Einstellung in der Registrierung auf VM-Ebene Priorität über die Einstellung in der Registrierung auf Proxy-Ebene.

Lösung für Fehler mit stillgelegtem Snapshot

Vergewissern Sie sich, dass die Option **Snapshot ohne Stilllegung des Gasts aufnehmen, wenn Stilllegungs-Snapshot fehlschlägt** auf der Registerkarte "Quelle" des hostbasierten agentenlosen Sicherungsplans ausgewählt ist.

Die agentenlose hostbasierte Sicherung stürzt ab, wenn Windows 2003 R2 64-Bit-als Sicherungs-Proxy verwendet wird.

Die agentenlose hostbasierte Sicherung für eine VMware-VM stürzt ab, wenn Windows 2003 R2 64-Bit-als Sicherungs-Proxy verwendet wird.

Gültig für VMware

Problem

Wenn ein Rechner mit Windows 2003 R2 64-Bit als Sicherungs-Proxy-Server zum Schützen einer VMware-VM verwendet wird, stürzt der Sicherungsjob manchmal ab. In der Debug-Protokolldatei des Sicherungsjobs können Fehlermeldungen wie die folgenden angezeigt werden:

[2016/01/21 10:18:11:316 00 03820 03336] [VDDKLOG] VixDiskLib: VixDiskLib_OpenEx: Open a disk. {AFBackend.exe::AFBackupVirtual.dll(1746.0)}
[2016/01/21 10:18:11:316 00 03820 03336] [VDDKLOG] VixDiskLibVim: VixDiskLibVim_GetNfcTicket: Get NFC ticket for [datastore1 (3)] VMname/VMware_1.vmdk. {AFBackend.exe::AFBackupVirtual.dll(1746.0)}
[2016/01/21 10:19:11:691 00 03820 03336] [VDDKLOG] VixDiskLibVim: Error 18000 (listener error GVmomiFaultInvalidResponse). {AFBackend.exe::AFBackupVirtual.dll (1746.0)}
[2016/01/21 10:19:11:691 00 03820 03336] [VDDKLOG] VixDiskLibVim: Login failure. Callback error 18000 at 2439. {AFBackend.exe::AFBackupVirtual.dll(1746.0)}
[2016/01/21 10:19:11:691 00 03820 03336] [VDDKLOG] VixDiskLibVim: Failed to find the VM. Error 18000 at 2511. {AFBackend.exe::AFBackupVirtual.dll(1746.0)}

Lösung

In Arcserve UDP Version 7.0 ist VMware VDDK 6.x integriert. VDDK 6.x unterstützt jedoch offiziell nicht Windows 2003 R2. Zur Umgehung des Problems können Sie eine der folgenden Optionen verwenden:

- Verwenden Sie einen Proxy, der von VDDK 6.x offiziell unterstützt wird. Zum Beispiel ein Proxy mit Windows 2008 R2, Windows 2012 oder Windows 2012 R2.
- Ersetzen Sie die integrierte Version VDDK 6.x durch VDDK 5.5, die auch von UDP 7.0 unterstützt wird. Ausführliche Informationen zum Ersetzen von VDDK finden Sie unter *So wenden Sie eine andere Version von VDDK als die integrierte Version in Arcserve UDP an.*

Hostbasierte agentenlose Sicherung verwendet keinen HotAdd-Transportmodus

Problem

Um Daten zu sichern, verwendet der hostbasierte Sicherungsjob den HotAdd-Transportmodus nicht, auch wenn dieser verfügbar ist. Dies geschieht, wenn der virtuelle Quellrechner von einem ESX-Host auf die Arcserve UDP-Konsole importiert wird (statt vom vCenter-Server) und der ESX-Host von einem vCenter-Server verwaltet wird.

Lösung

Gehen Sie folgendermaßen vor, um diesen Fehler zu beheben:

- Löschen Sie diesen virtuellen Rechnerknoten aus der Arcserve UDP-Konsole. Importieren Sie den Knoten erneut aus dem vCenter-Server, der den ESX-Host verwaltet.
- Trennen Sie den ESX vom vCenter-Server.

Hostbasierter agentenloser Sicherungs- oder Wiederherstellungsjob verwendet den NBD- oder den NBDSSL-Transportmodus auch dann, wenn der SAN-Modus möglich ist

Gilt für Windows-Plattformen. Gilt nur für VMware-VMs.

Problem

Obwohl der SAN-Transportmodus möglich ist, verwendet der agentenlose Sicherungs- oder Wiederherstellungsjob weiter den Transportmodus "NBD" oder "NBDSSL".

Lösung

Um den SAN-Transportmodus für agentenlose Sicherungs- und Wiederherstellungsjobs nutzen zu können, müssen folgende Voraussetzungen gegeben sein.

- Der Proxy-Rechner muss ein physischer Rechner sein. (Er darf kein virtueller Rechner sein.)
- Der Proxy-Rechner muss mit einer SAN-LUN verbunden sein, auf der sich der virtuelle Rechner befindet.
- Auf dem Proxy-Rechner muss die SAN-Richtlinie des SAN-Datenträgers auf "OnlineAll" konfiguriert sein.

  Zum Konfigurieren des Datenträgers gehen Sie wie folgt vor:

  1. Melden Sie sich über ein Konto mit Administratorrechten beim Sicherungs-Proxy-System an.
  2. Öffnen Sie die Windows-Befehlszeile.
  3. Geben Sie in der Befehlszeile folgende Befehle ein

     a. Geben Sie "diskpart" ein, und drücken Sie die Eingabetaste.
     b. Geben Sie "SAN" ein, und drücken Sie die Eingabetaste.

        Die aktuelle SAN-Richtlinie wird angezeigt.

     c. Geben Sie "SAN POLICY=OnlineAll" ein, und drücken Sie die Eingabetaste.
- Wenn Sie die VM-Wiederherstellung mit dem SAN-Transportmodus ausführen möchten, muss der SAN-Datenträger so konfiguriert sein, dass er beschrieben werden kann.

  Gehen Sie wie folgt vor, um die Schreibschutzkennzeichnung zu entfernen:

1. Melden Sie sich über ein Konto mit Administratorrechten beim Sicherungs-Proxy-System an.
2. Öffnen Sie die Windows-Befehlszeile.
3. Geben Sie in der Befehlszeile folgende Befehle ein
   a. Geben Sie "diskpart" ein, und drücken Sie die Eingabetaste.
   b. Geben Sie "list disk" ein, und drücken Sie die Eingabetaste.

      Die Liste der Datenträger wird angezeigt.
   c. Geben Sie "select disk xxx" ein, und drücken Sie anschließend die Eingabetaste, um den SAN-Datenträger auszuwählen, der als beschreibbar konfiguriert werden soll.
   d. Geben Sie "attribute disk clear readonly" ein, und drücken Sie anschließend die Eingabetaste.

- Der SAN-Transportmodus bietet bei der VM-Wiederherstellung optimale Leistung auf Thick-Datenträgern, jedoch sehr schlechte Leistung auf Thin-Datenträgern. Daher verwendet die VM-Wiederherstellung standardmäßig den Transportmodus "NBD" oder "NBDSSL" für Thin-Datenträger. Wenn Sie den SAN-Transportmodus auch für Thin-Datenträger verwenden möchten, können Sie einen Zeichenfolgenwert "EnforceTransportForRecovery" mit Wert "SAN" unter "HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFRestoreDll" hinzufügen (erstellen Sie den Schlüssel "AFRestoreDll", wenn er nicht vorhanden ist).
- Wenn während der Sicherung ein Snapshot erstellt wird, werden weitere Dateien generiert. Es wird also ein bestimmter freier Speicherplatz im Speichergerät benötigt, auf dem sich die VMDK-Dateien der VMs befinden. Für den SAN-Transportmodus wird mehr freier Speicherplatz benötigt als für den NBD/NBDSSL-Transportmodus. Achten Sie also darauf, dass in der SAN-LUN genügend freier Speicherplatz vorhanden ist, wenn Sie den SAN-Transportmodus verwenden möchten.

Fehler beim Erstellen eines Snapshot für virtuelle Hyper-V-Rechner bei mehreren ausgeführten Jobs

Problem

Wenn mehrere Jobs ausgeführt werden, beansprucht die Snapshot-Erstellung für virtuelle Hyper-V-CSV-Rechner zu viel Zeit und schlägt fehl. Sie schlägt auch bei mehreren Versuchen fehl. Die folgende Meldung wird im Aktivitätsprotokoll des jeweiligen virtuellen Rechners angezeigt.

Snapshot wird zurzeit erstellt. Es können nicht mehr als ein Snapshot gleichzeitig erstellt werden.

Versuchen Sie es in 600 Sekunden erneut.

Lösung

Dieses Problem kann auftreten, da nicht mehrere Snapshot-Erstellungen gleichzeitig ausgeführt werden können.

Um das Problem zu lösen, können Sie die Anzahl von Versuchen erhöhen oder das Zeitintervall für Wiederholungen verlängern. Sie können auch die Anzahl von Jobs, die Sie gleichzeitig ausführen können, erhöhen.

Hinweis: Der standardmäßige Wiederholungswert ist 3, und der standardmäßige Intervallwert beträgt 10 Minuten.

Um die Anzahl von Wiederholungen zu erhöhen, führen Sie für den Proxy-Server folgende Schritte aus:

1. Öffnen Sie die Windows-Registrierung.
2. Navigieren Sie zu HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Erstellen Sie einen Schlüssel namens **VSSWrap**.
4. Klicken Sie mit der rechten Maustaste auf **VSSWrap**, wählen Sie **Neu** und anschließend den Wert **DWORD (32-Bit)** aus, und geben Sie als Namen **VssAsynchMaxRetryTimes** an.
5. Geben Sie den Wert bedarfsgerecht an.

Um das Intervall zwischen den einzelnen Versuchen zu verlängern, führen Sie für den Proxy-Server folgende Schritte aus:

1. Öffnen Sie die Windows-Registrierung.
2. Navigieren Sie zu HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Erstellen Sie einen Schlüssel namens **VSSWrap**.

4. Klicken Sie mit der rechten Maustaste auf **VSSWrap**, wählen Sie **Neu** und anschließend den Wert **DWORD (32-Bit)** aus, und geben Sie als Namen **VssAsynchRetryInterval** an.
5. Geben Sie den Wert bedarfsgerecht an.

Um die Anzahl von gleichzeitigen Jobs erhöhen, führen Sie für den Proxy-Server folgende Schritte aus:

1. Öffnen Sie die Windows-Registrierung.
2. Navigieren Sie zu HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Klicken Sie mit der rechten Maustaste auf **HyperVMaxJobNum**, wählen Sie **Ändern** aus, und geben Sie den erforderlichen Wert an.

Hyper-V konnte keinen VSS-Snapshot erstellen

Die hostbasierte Sicherung von Hyper-V-VMs auf einem Hyper-V-Host schlägt fehl, und es wird folgende Meldung angezeigt:

Failed to take VSS snapshot. (VSS-Snapshot konnte nicht erstellt werden.)

Problem

Der Sicherungsfehler kann folgende Ursachen haben:

- Mindestens ein Volume auf dem Hyper-V-Host ist nicht mit NTFS/Refs formatiert.
- Mindestens ein Volume auf dem Hyper-V-Host hat weniger als 100 MB freien Speicherplatz.
- Es gab übermäßige Datenträgeraktivitäten zum Zeitpunkt der Sicherung.

Lösung

Beheben Sie die Probleme in der Umgebung, und führen Sie die Sicherung erneut aus.

Fehlschlag der Sicherung von virtuellem Datenträger wegen Systemfehler=[The device is not ready(21)]

Gilt für Windows-Plattformen.

Problem

Wenn während der Ausführung einer Sicherung ein Netzwerkfehler auftritt oder ein Hyper-V-Server neu gestartet wird, wird im Aktivitätsprotokoll angegeben, dass ein Netzwerkfehler oder Dateisystemfehler aufgetreten ist.

Lösung

Starten Sie den Sicherungsjob nach dem Neustart des Hyper-V-Servers erneut.

Fehlgeschlagene Sicherungsjobs

Problem

Ein Sicherungsjob schlägt mit folgender Fehlermeldung in den Aktivitätsprotokollen fehl:

Die Neukonfiguration für Sicherungen kann im aktuellen Zustand nicht ausgeführt werden. Fahren Sie den virtuellen Rechner herunter, und versuchen Sie, den Sicherungsjob erneut auszuführen. (Der virtuelle Rechner kann während oder nach der Snapshot-Phase eingeschaltet werden).

Lösung

Legen Sie die Registrierungswerte so fest, dass disk.enableUUID nicht neu konfiguriert wird.

Gehen Sie wie folgt vor:

Gilt für die Proxy-Ebene und wirkt sich auf alle VMware-VMs aus.

1. Melden Sie sich beim Sicherungs-Proxy-Server an.
2. Öffnen Sie den Registrierungs-Editor von Windows und suchen Sie nach dem folgenden Schlüssel:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll
3. Fügen Sie einen DWORD-Wert mit Namen DoNotReconfigDiskUUID hinzu, und legen Sie für seinen Wert 1 fest.

Gilt für die Ebene der spezifischen VM, wirkt sich nur auf die betroffene VM aus.

1. Melden Sie sich beim Sicherungs-Proxy-Server an.
2. Öffnen Sie den Registrierungs-Editor von Windows und suchen Sie nach dem folgenden Schlüssel:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM-InstanceUUID>

   Hinweis: Ersetzen Sie <VM-InstanceUUID> durch den UUID-Wert des virtuellen Rechners, für den diese Einstellung gilt. Sie finden den Wert in der URL des virtuellen Rechners, der verwendet wird, wenn eine Verbindung mit Arcserve UDP Agent hergestellt wird.
3. Fügen Sie einen DWORD-Wert mit Namen DoNotReconfigDiskUUID hinzu, und legen Sie für seinen Wert 1 fest.

Beachten Sie folgende Punkte:

- Wenn sowohl auf VM-Ebene als auch auf Proxy-Ebene Registrierungen konfiguriert sind, hat die VM-Ebene Vorrang.
- Wenn die Registrierung nicht vorhanden ist, wird als implizierter Registrierungswert 0 angenommen, was bedeutet, dass Sie disk.enableUUID neu konfigurieren müssen.
- Wenn Sie angegeben haben, dass der disk.EnableUUID-Parameter nicht neu konfiguriert werden soll, ist der Status der gesicherten Daten möglicherweise nicht konsistent.

Weitere Informationen zu diesem Problem finden Sie im entsprechenden Artikel der VMware-Knowledge-Base.

Fehler beim Importieren von VMware-VMs aus vCenter

Problem

Arcserve UDP kann keine VMware-VMs aus vCenter importieren, obwohl der vCenter-Server betriebsbereit ist und eine Verbindung mit dem Browser und dem vSphere-Client herstellen kann. Die Fehlermeldung in der Datei "ARCAPP-Gateway.log" des Arcserve UDP-Konsolenservers lautet folgendermaßen:

com.sun.xml.ws.client.ClientTransportException: HTTP transport error: javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: Certificates does not conform to algorithm constraints

Wenn Sie jedoch die folgenden beiden Zeilen in der Datei "C:\Programme\Arcserve\Unified Data Protection\Common\JRE\lib\security\java.security" ändern und den Arcserve UDP-Verwaltungsdienst neu starten, kann er eine Verbindung mit demselben vCenter-Server über Arcserve UDP herstellen:

Vorhandene Zeilen:

jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024

jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768

Geänderte Zeilen:

jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 512

jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 512

Ursache:

vCenter Server hat ein Zertifikat mit einem kurzen öffentlichen Schlüssel oder der Algorithmus wird durch die JRE in Arcserve UDP deaktiviert. Ein Zertifikat mit einer öffentlichen Schlüssellänge, die kürzer als 1024 Bit ist, wird als unsicher betrachtet (gilt auch für den MD5-Algorithmus). Sie werden durch die von Arcserve UDP verwendete JRE deaktiviert.

Lösung

Generieren Sie ein neues Zertifikat für den vCenter-Server. Stellen Sie sicher, dass das neue Zertifikat über einen öffentlichen Schlüssel verfügt, der größer als 1024 Bit ist und einen stärkeren Algorithmus verwendet.

Sicherungen schlagen wegen ESXi-Lizenz fehl

Gilt für Windows-Plattformen

Problem

Vollständige Sicherungen, Zuwachssicherungen und Überprüfungssicherungen schlagen fehl. Die folgende Meldung wird im Arcserve UDP-Aktivitätsprotokoll angezeigt:

VM-Server <Servername> hat keine bezahlte ESX-Lizenz.

Lösung

Aufgrund einer VMware-Einschränkung können virtuelle Rechner, die auf ESXi-Servern mit einer kostenlosen Lizenz ausgeführt werden, nicht gesichert werden. Verwenden Sie eine gekaufte Lizenz, um diese VMs zu schützen.

Der HotAdd-Transportmodus funktioniert nicht, wenn Sie versuchen, eine VMware-VM zu sichern.

Problem

Der HotAdd-Übertragungsmodus wird nicht für diese VM unterstützt. Das heißt, es erfolgt ein Failover der Sicherung zum NBDSSL-Modus (verschlüsseltes Netzwerk-Blockgerät). (Der Sicherungsjob wird langsam ausgeführt.) Die Sicherung einer VMware-VM verwendet nicht die HotAdd-Übertragung. Weitere Informationen zu HotAdd-Transport finden Sie unter Link.

Überprüfen Sie die folgenden HotAdd-Voraussetzungen:

- Der HotAdd-Sicherungs-Proxy muss ein virtueller Rechner sein. HotAdd umfasst das Anhängen eines virtuellen Datenträgers an den Sicherungs-Proxy (wie das Anhängen eines Datenträgers an einen virtuellen Rechner).
- Der HotAdd-Proxy muss Zugriff auf denselben Datenspeicher wie der virtuelle Zielrechner haben.
- Die VMFS-Version und die Datenblockgrößen für die Ziel-VM müssen dem Datenspeicher entsprechen, auf dem sich der HotAdd-Proxy befindet. Wenn der HotAdd-Proxy ein virtueller Rechner ist, der sich auf einem VMFS-3-Volume befindet, wählen Sie ein Volume mit einer Blockgröße, die der maximalen Größe des virtuellen Datenträgers virtueller Rechner angemessen ist, die Kunden sichern möchten (siehe VMFS-3-Blockgröße für HotAdd-Sicherungs-Proxy). Diese Einschränkung gilt nicht für VMFS-5-Volumes, die immer eine Dateiblockgröße von 1 MB haben.

  Die folgende Tabelle enthält die VMFS-3-Blockgröße für den HotAdd-Sicherungs-Proxy:

VMFS-Blockgröße	Maximale Größe des Zieldatenträgers
1 MB	256 GB
2 MB	512 GB
4 MB	1024 GB
8 MB	2048 GB

- In vSphere 5.1 und niedriger beträgt die maximale unterstützte VMDK-Größe 1,98 TB.
- Die Datenträger, für die HotAdd durchgeführt werden soll, müssen SCSI-Datenträger sein. IDE-Laufwerke sind nicht mit HotAdd kompatibel.

- VMware Tools muss auf der VM und auf dem Sicherungs-Proxy installiert und auf dem aktuellen Stand sein.
- Der Datenspeicher benötigt genügend Speicherplatz für einen VM-Snapshot.
- HotAdd schlägt möglicherweise fehl, wenn ein Datenträger mit einer neueren Hardwareversion als die gesicherte VM erstellt wurde. Zum Beispiel wenn ein Datenträger von einer VM mit Hardwareversion 8 auf eine VM mit Hardwareversion 7 verschoben wurde. Um dieses Problem zu lösen, aktualisieren Sie die Hardwareversion der VM.
- Ein einzelner SCSI-Controller kann höchstens 15 angehängte Datenträger aufweisen. Um mehrere gleichzeitige Jobs mit mehr als 15 Datenträgern auszuführen, müssen Sie weitere SCSI-Controller zu Ihrem Sicherungs-Proxy-Rechner hinzufügen.
- Bei einer eigenständigen ESX-Verbindung (ESX-Server wird nicht von vCenter verwaltet) können Sie HotAdd nur für Datenträger von VMs durchführen, die sich auf demselben ESX wie der Sicherungs-Proxy-Rechner befinden.
- HotAdd schlägt evtl. fehl, wenn Sie versuchen, die VM über einen ESX zu sichern, der als eigenständiger Server zu UDP hinzugefügt, jedoch tatsächlich von vCenter verwaltet wird.
- HotAdd kann fehlschlagen, wenn sich die VM, die Sie sichern möchten, und der Proxy-Server in unterschiedlichen Clustern befinden.

Lösung

Deaktivieren Sie "automount" auf dem Sicherungs-Proxy-Rechner mithilfe des Hilfsprogramms "diskpart".

Genauere Steuerung für VSS Windows Gast-BS Quiescings

Problem

Ich möchte eine detailliertere Kontrolle für VSS beim Erstellen von Ruhephasen-Snapshot für Windows-Gastbetriebssysteme festlegen.

Lösung

Ab vSphere 6.5 ermöglicht die vSphere Webservice-API die folgenden detaillierteren Steuerelemente für VSS beim Erstellen von Stilllegungs-Snapshots für Windows-Gastbetriebssysteme:

- Sie können den Timeout (Standard 15 Minuten) für die Aktivierung virtueller Maschinen von fünf Minuten bis vier Stunden beliebig konfigurieren.
- Der VSS Sicherungstyp - VSS_BT_COPY wurde bisher als Standard bei der Erstellung von Snapshots verwendet. Aber jetzt sind auch VSS_BT_FULL, VSS_BT_INCREMENTAL, VSS_BT_DIFFERENTIAL und VSS_BT_LOG verfügbar. Die Protokolltrunkierung wird entsprechend den Anwendungseinstellungen ausgelöst.
- Der VSS-Sicherungskontext wird eingeführt, um eine Stilllegung der Anwendung (Kontext VSS_CTX_BACKUP) oder des Dateisystems (Kontext VSS_CTX_FILE_SHARE_BACKUP) zu erzwingen.

Unter Arcserve UDP können Sie die Parameter in der Registrierung angeben, um das Steuerelement zu implementieren.

Hinweis: Zur Spezifizierung benötigen Sie VMware Tools 10.1.0 oder höher, die auf dem Gastbetriebssystem der VM installiert sind.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Proxy-Rechner an.
2. Erstellen Sie einen Registrierungswert auf Ebene des Proxy-Servers oder auf VM-Ebene.

   Hinweis: Wenn Sie den Registrierungswert auf VM-Ebene und auf Proxy-Ebene hinzufügen, hat die Einstellung in der Registrierung auf VM-Ebene Vorrang vor der Einstellung in der Registrierung auf Proxy-Ebene.

   Auf Ebene des Proxy-Servers (gilt für alle Sicherungsjobs, die auf dem jeweiligen Proxy-Server ausgeführt werden)

a. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

b. Fügen Sie folgende DWORD-Werte mit den richtigen Werten hinzu:

- VssUseEnhancedSnapshot
- VssTimeoutMinute
- VssBackupType
- VssBackupContext
- VssBootableSystemState
- VssPartialFileSupport

Auf VM-Ebene

a. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Fügen Sie folgende DWORD-Werte mit den richtigen Werten hinzu:

- VssUseEnhancedSnapshot
- VssTimeoutMinute
- VssBackupType
- VssBackupContext
- VssBootableSystemState
- VssPartialFileSupport

Mögliche Werte der Registrierungswerte:

VssUseEnhancedSnapshot

- 0 - Verwenden Sie keine erweiterte Steuerung und die niedrigeren Registrierungswerte sind nicht wirksam.
- 1 - Verwenden Sie eine verbesserte Steuerung und die niedrigeren Registrierungswerte sind wirksam.

VssTimeoutMinute

Bereich von 5 bis 240

VssBackupType

- 0 - VSS_BT_COPY (Standard)
- 1 - VSS_BT_FULL
- 2 - VSS_BT_INCREMENTAL
- 3 - VSS_BT_DIFFERENTIAL
- 4 - VSS_BT_LOG

VssBackupContext

- 0 - ctx_auto
- 1 - Ctx_backup (Standard)
- 2 - ctx_file_share_backup

VssBootableSystemState

- 0 – False
- 1 - True (Standardeinstellung)

VssPartialFileSupport

- 0 - False (Standard)
- 1 - True

Die virtuelle Maschine kann nicht konfiguriert werden, um den Parameter "Disk.EnableUUUID" zu aktivieren.

Problem

Es tritt ein Fehler während der Rekonfiguration der virtuellen Maschine auf, um den Parameter'disk.EnableUUUID' zu aktivieren, der für eine anwendungskonsistente Datensicherung erforderlich ist. Dieses Problem tritt auf, wenn sich die virtuelle Umgebung nach einem Fehler wieder erholt hat.

Lösung

Dieses Problem tritt nur bei VMware Environment auf. Dieses Problem tritt auf, wenn das Microsoft VSS versucht, einen anwendungsbezogenen Snapshot durchzuführen, aber den Wert für die Festplatten-UUID oder die Seriennummer für eine oder mehrere Festplatten der virtuellen Maschine nicht liest.

Der Parameter "disk.EnableUUID" der VM muss konfiguriert sein. Für VMs, die unter Version 4.1 oder höher erstellt wurden, ist dieser Parameter standardmäßig aktiviert. Der Sicherungsauftrag wird automatisch konfiguriert, um Dateninkonsistenzen zu vermeiden und anwendungskonsistente Sicherungen

durchzuführen. Wenn der Sicherungsauftrag die Festplatte.EnableUUUID nicht aktiviert, konfigurieren Sie den Parameter manuell mit den folgenden Schritten:

Gehen Sie wie folgt vor:

1. Schalten Sie die virtuelle Maschine aus.
2. Melden Sie sich auf dem vCenter-Server oder dem ESXi/ESX-Host mithilfe des vSphere-Clients an.
3. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und danach auf "Einstellungen bearbeiten".
4. Klicken Sie auf die Registerkarte "Optionen".
5. Navigieren Sie zu Erweitert > Allgemein > Konfigurationsparameter.
6. Fügen Sie die Zeile disk.EnableUUUID hinzu oder ändern Sie sie und setzen Sie sie auf True.
7. Klicken Sie zum Speichern auf OK.
8. Klicken Sie zum Beenden auf OK.
9. Starten Sie die virtuelle Maschine neu, damit Änderungen wirksam werden.

Hinweis: Wenn der Parameter bereits auf True gesetzt ist, gibt es eine unterbrechungsfreie Lösung, nämlich die vmx zu bearbeiten und den Wert disk.enableUUUID auf false zu setzen, dann vMotion die vm (auf einen beliebigen anderen Host), um die vmx im Hostspeicher neu zu laden. Dadurch wird die Stillegung auf Anwendungsebene effektiv deaktiviert (die Stillegung des Dateisystems ist jedoch weiterhin verfügbar).

Wiederherstellungsvorgänge schlagen fehl, wenn Daten im HOTADD- oder SAN-Transportmodus wiederhergestellt werden

Gilt für Windows-Plattformen.

Problem

Wiederherstellungsvorgänge schlagen fehl, wenn Daten im HOTADD- oder SAN-Transportmodus wiederhergestellt werden. Folgende Meldung wird im Aktivitätsprotokoll angezeigt:

Ein unbekannter Fehler ist aufgetreten. Kontaktieren Sie den Technischen Support.

Lösung

Wiederherstellungsvorgänge schlagen im HOTADD-Transportmodus oder im SAN-Transportmodus fehl, wenn die Datenträgereinstellungen nicht ordnungsgemäß konfiguriert sind.

Führen Sie folgende Schritte aus, um den Datenträger zu konfigurieren:

1. Melden Sie sich über ein Konto mit Administratorrechten beim Sicherungs-Proxy-System an.
2. Öffnen Sie die Windows-Befehlszeile.
3. Geben Sie in der Befehlszeile folgenden Befehl ein:

   diskpart

   Drücken Sie die Eingabetaste.
4. Gaben Sie "SAN" ein, und drücken Sie die Eingabetaste.

   Die aktuelle SAN-Richtlinie wird angezeigt.
5. Geben Sie folgenden Befehl ein, und drücken Sie EINGABE:

   SAN POLICY = OnlineAll

   Die SAN-Richtlinie wird so konfiguriert, dass SAN-gehostete Volumes nicht automatisch geladen werden.
6. Um das schreibgeschützte Attribut des spezifischen SAN-Datenträgers zu löschen, wählen Sie den Datenträger aus der Datenträgerliste aus, geben Sie den folgenden Befehl ein, und drücken Sie EINGABE:

   attribute disk clear readonly
7. Gaben Sie "exit" ein, und drücken Sie die Eingabetaste.

   Der Datenträger ist nun konfiguriert, und Sie können den Job erneut übergeben.

Wenn der Job erneut fehlschlägt, laden Sie die HOTADD-Datenträger manuell über die Datenträgerverwaltung des Proxysystems.

Um die Datenträger manuell zu laden, gehen Sie wie folgt vor:

1. Melden Sie sich über ein Konto mit Administratorrechten beim Sicherungs-Proxy-System an.
2. Öffnen Sie Windows-Systemsteuerung, und doppelklicken Sie auf "Verwaltung".

   Das Fenster "Verwaltung" wird geöffnet.
3. Doppelklicken Sie in der Liste "Favoriten" auf "Computerverwaltung".

   "Computerverwaltung" wird geöffnet.
4. Erweitern Sie den Bereich "Speicherung", und klicken Sie auf "Datenträgerverwaltung".

   Die Datenträger werden angezeigt.
5. Klicken Sie mit der rechten Maustaste auf den zu entfernenden Datenträger, und klicken Sie auf "Online".

   Der Datenträger ist nun geladen, und Sie können den Job erneut übergeben.

VM-Wiederherstellung schlägt fehl, wenn ein nicht standardmäßiger Port angegeben ist

Problem

Die VM-Wiederherstellung schlägt fehl, wenn ein nicht standardmäßiger Port für den VMware vCenter-Server angegeben ist.

Lösung

Um das Problem zu lösen, stellen Sie die nicht standardmäßige Portnummer für vCenter in der Registrierung des Sicherungs-Proxy-Rechners auf den Wert "VDDK-port" um.

Um die Nummer von VDDKport festzulegen, führen Sie auf dem Proxy-Server folgende Schritte aus:

1. Öffnen Sie die Windows-Registrierung.
2. Navigieren Sie zu HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Klicken Sie mit der rechten Maustaste auf "VDDKport", wählen Sie "Ändern" aus, und geben Sie den erforderlichen Wert an.

Geplante Zuwachssicherungsjobs oder vollständige Sicherungsjobs für Hyper-V-VMs schlagen fehl

Problem

In manchen Fällen schlagen die geplanten Jobs für Zuwachssicherungen oder vollständige Sicherungen für virtuelle Hyper-V-Rechner fehl. In der Ereignisanzeige des Hyper-V-Hosts werden folgende Fehler angezeigt:

- DM-Vorgang zum Hinzufügen für den virtuellen Rechner <VM-Name> schlug mit folgender Fehlermeldung fehl: Nicht genügend Arbeitsspeicher (0x8007000E) (Virtual machine ID <VM-ID>)
- Sicherungsprüfpunkt für virtuellen Rechner <VM-Name> konnte nicht erstellt werden: Element nicht gefunden. Dieser Vorgang wurde zurückgegeben, da der Zeitüberschreitungszeitraum abgelaufen ist. (0x800705B4). (Virtual machine ID <VM-ID>)
- Sicherungsprüfpunkt für virtuellen Rechner <VM-Name> konnte nicht erstellt werden: Element nicht gefunden. Element nicht gefunden. (0x80070490). (Virtual machine ID <VM-ID>)
- VSS-Writer im virtuellen Rechner <VM-Name> konnten BackupComplete auf den zugehörigen Schattenkopie(VSS-Snapshot)-Satz nicht auszuführen: Ein Funktionsaufruf erfolgte, als das Objekt sich in einem falschen Status für diese Funktion (0 x 80042301) befand. (Virtual machine ID)
- Der Hyper-V-VSS-Writer hat beim Verarbeiten dieses virtuellen Rechners einen Fehler gefunden. (Weitere Informationen zu Hyper-V-VSS-Writer-Fehlern finden Sie in der Produktdokumentation).

Lösung 1

Die Lösung besteht darin, die RAM-Größe auf dem Hyper-V-Server zu erhöhen und den Sicherungsjob danach erneut zu übergeben.

Lösung 2

Wenn der VSS-Writer im virtuellen Rechner nicht ordnungsgemäß arbeitet, schlägt der Sicherungsjob fehl. Um das Problem zu lösen, überprüfen Sie das Ereignisprotokoll des Hyper-V-Hosts und des virtuellen Rechners. Überprüfen Sie die VSS-Warnungen und Fehler, und führen Sie entsprechende Aktionen aus.

Hyper-V VSS NTDS-Writer schlägt bei der Erstellung des Snapshot in der VM fehl

Problem

Wenn die AutoMount-Funktion in einer Domänen-Controller-VM nicht aktiviert ist, schlägt der VSS NTDS-Writer bei der Aufnahme des Snapshot in der VM fehl. Dadurch kann der Hyper-V-VSS-Writer im Hyper-V-Host keinen VSS-Snapshot aufnehmen.

Der Hyper-V-HBBU-Sicherungsjob schlägt mit folgendem Eintrag im Aktivitätsprotokoll fehl:

Der Hyper-V-VSS-Writer hat beim Verarbeiten dieses virtuellen Rechners einen Fehler gefunden. (Weitere Informationen zu Hyper-V-VSS-Writer-Fehlern finden Sie in der Produktdokumentation).

Lösung

Aktivieren Sie die Funktion *AutoMount* in der VM.

Gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster mit der Eingabeaufforderung.
2. Öffnen Sie diskpart, und führen Sie folgenden Befehl aus:

   automount enable

Änderungen der MAC-Adresse werden nach der VM-Wiederherstellung nicht beibehalten

Gültig auf Windows-Plattformen und VMware-VMs

Problem

Die MAC-Adressen der virtuellen Rechner werden nicht beibehalten, nachdem virtuelle Rechner wiederhergestellt wurden.

Lösung

MAC-Adressen werden während der Wiederherstellung nicht beibehalten, um Duplikate zu verhindern. Um MAC-Adressen beizubehalten, legen Sie folgenden Registrierungsschlüssel auf dem Proxy-Server fest:

Speicherort: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
Schlüsselname: RetainMACForVDDK
Werttyp: Zeichenfolge

Schlüsselwert: 1

VM-Wiederherstellung schlägt fehl mit folgender Fehlermeldung – Öffnen der VMDK-Dateien nicht möglich

Problem

Die Wiederherstellung des virtuellen Rechners schlägt fehl, und es wird folgende Fehlermeldung in den Protokollen angezeigt:

Fehler beim Öffnen der VMDK-Datei (auf .vmdk endender Dateiname). VMware meldet den folgenden Fehler: Sie haben keine Zugriffsrechte für diese Datei. Weitere Informationen finden Sie im Debugging-Protokoll zur Wiederherstellung. Wenden Sie sich, falls erforderlich, an den Arcserve-Support.

Im Debugging-Protokoll zur Wiederherstellung werden die folgenden Meldungen angezeigt

- [VDDKLOG] CnxAuthdConnect: Gibt "False" aus, da die angeforderte SSL-Überprüfung und Ziel-Authd SSL nicht unterstützen.
- [VDDKLOG] CnxConnectAuthd: Gibt "False" aus, da CnxAuthdConnect fehlgeschlagen ist.
- [VDDKLOG] Cnx_Connect: Gibt "False" aus, da CnxConnectAuthd fehlgeschlagen ist.
- [VDDKLOG] Cnx_Connect: Fehlermeldung: SSL erforderlich

Lösung

Die Ursache könnte darin liegen, dass auf dem ESX-Host die SSL-Authentifizierung deaktiviert ist. Wenden Sie eine der folgenden Methoden an, um das Problem zu lösen:

Per vSphere-Client:

1. Melden Sie sich beim vCenter/ESX-Server an.
2. Rufen Sie die ESX Server-Einstellungen auf:

   Konfiguration, Erweiterte Einstellungen, Konfiguration, Standardsicherheit
3. Aktivieren Sie folgende Option:

   config.defaults.security.host.ruissl

Verwenden der Befehlszeile

1. Stellen Sie mithilfe von SSH eine Verbindung zum ESX-Host her.
2. Öffnen Sie die folgende Datei:

/etc/vmware/config

3. Setzen Sie den Eintrag security.host.ruissl auf "TRUE".
4. Speichern Sie die Datei, und starten Sie den Management-Agenten neu.

Probleme durch doppelte VM-UUID

Problem 1

VM-Knoten wird nach dem Importieren von einem anderen VM-Knoten in die Konsole überschrieben.

Beispiel: Sie haben 2 virtuelle Rechner VM1 und VM2 mit dem gleichen UUID (dieser wird für VMware als Instanzen-UUID für Hyper-V als VM-UUID bezeichnet) in den ESXi-Hosts, die von unterschiedlichen vCenter Systemen verwaltet werden: VC1 und VC2. Sie importieren VM1 in die Konsole und der virtuelle Rechner wird in der Knotenlistenansicht der Konsole angezeigt. Später importieren Sie VM2 in die Konsole. In der Knotenlistenansicht wird VM1 mit VM2 überschrieben (oder anders ausgedrückt, VM2 wird hinzugefügt und VM1 ist nicht mehr vorhanden).

Problem 2

Die VM-Knoteninformationen in der Spalte "Hypervisor" ändern sich stetig, während die Auto-Discovery ausgeführt wird.

Beispiel: Sie haben 2 virtuelle Rechner VM1 und VM2 mit dem gleichen UUID (dieser wird für VMware als Instanzen-UUID für Hyper-V als VM-UUID bezeichnet) in den ESXi-Hosts, die von unterschiedlichen vCenter Systemen verwaltet werden: VC1 und VC2. Sie importieren VM1 in die Konsole. Außerdem importieren Sie mindestens einen virtuellen Rechner von vCenter VC2, sodass sowohl VC1 als auch VC2 zu der Knoten-Discovery-Liste hinzugefügt werden (diese finden Sie auf der Seite "Knoten-Discovery-Konfiguration" auf der Registerkarte "Einstellungen"). Wenn die Knoten-Discovery ausgeführt wird, stellt die Funktion zunächst eine Verbindung mit VC1 her und erkennt VM1 durch den UUID. Die Spalte "Hypervisor" wird dann mit Informationen über VC1 aktualisiert. Später stellt die Funktion eine Verbindung mit VC2 her, erkennt VM2 durch den UUID und die Spalte "Hypervisor" wird mit Informationen über VC2 aktualisiert.

Lösung

Arcserve UDP verwendet zur Identifizierung eines VM-Knotens den UUID des virtuellen Rechners (dieser wird für VMware als Instanzen-UUID und für Hyper-V als VM-UUID bezeichnet). Es kommt zwar nur selten vor, dass VMs doppelte UUIDs haben, ein derartiger Fall kann aber zu problematischen Funktionsweise in Arcserve UDP führen.

Um die Probleme zu lösen, führen Sie die folgenden Schritte aus, um den UUID eines virtuellen Rechners manuell zu ändern (nur für VMware-VMs). Nachdem Sie den UUID des virtuellen Rechners manuell geändert haben, löschen Sie die Original-VM aus der Arcserve UDP-Konsole, und importieren Sie die VM neu.

1. Öffnen Sie die folgende URL-Adresse:

   https://<vCenter host name>/mob/

2. Melden Sie sich als Administrator an.
3. Suchen Sie "Inhalt" in der Spalte "NAME", und klicken Sie auf den Link in der Spalte "WERT" in der gleichen Zeile.
4. Suchen Sie in der Spalte "NAME" nach "rootFolder", und klicken Sie auf den Link in der Spalte "WERT" in der gleichen Zeile.
5. Suchen Sie "childEntity" in der Spalte "NAME". Suchen Sie in der gleichen Zeile in der Spalte "WERT" nach dem Datencenter, in dem sich der virtuelle Rechner befindet, und klicken Sie auf dessen Link.
6. Suchen Sie "VmFolder" in der Spalte "NAME", und klicken Sie auf den Link in der Spalte "WERT" in der gleichen Zeile.
7. Suchen Sie "childEntity" in der Spalte "NAME". Klicken Sie in der Spalte "VALUE" in der gleichen Zeile auf "Mehr...", um die Liste der virtuellen Rechner zu erweitern. Suchen Sie den gewünschten virtuellen Rechner, und klicken Sie auf den Link.
8. Suchen Sie in der Tabelle mit den Methoden nach "ReconfigVM_Task", und klicken Sie auf den Link.
9. Entfernen Sie in dem neu geöffneten Browser alle Inhalte im Feld "VALUE", und geben Sie den folgenden Code ein:

   ```
   <spec>
   <instanceUuid>2499952a-6c85-480e-b7df-4cb-
   d2137eb69</instanceUuid>
   </spec>
   ```

   Hinweis: Die oben genannte Zeichenfolge "2499952a-6c85-480e-b7df-4cb-d2137eb69" ist ein Beispiel für einen UUID. Sie sollten sie mit dem UUID ersetzen, den Sie anwenden möchten.
10. Klicken Sie auf den Link "Aufrufmethode", um den neuen UUID anzuwenden.
11. Um sicherzustellen, dass der neue UUID angewendet wurde, schließen Sie den geöffneten Browser, und kehren Sie zur Seite aus Schritt 8 zurück.
12. Suchen Sie in der Spalte "NAME" nach "config", und klicken Sie in der gleichen Zeile auf den Link in der Spalte "WERT".
13. Suchen Sie in der Spalte "NAME" nach "instanceUuid". Der UUID des virtuellen Rechners wird in der Spalte "WERT" in der gleichen Zeile angezeigt.

Dateisystem-Katalogjob schlägt fehl oder die Überprüfung des Wiederherstellungspunktes für die hostbasierte Agent-lose Sicherung schlägt fehl

Gilt für Windows-Plattformen. Gilt nur für VMware-VMs.

Problem

- Dateisystem-Katalogjob für hostbasierte agentenlose Sicherung von Wiederherstellungspunkten schlägt fehl
- Überprüfung des Wiederherstellungspunktes schlägt bei hostbasiertem agentenlosem Sicherungsjob fehl, und die nächste Zuwachssicherung wird in einen Verifizierungsjob konvertiert.

Lösung

Möglicherweise ist dies auf ein bekanntes Problem bei VMware zurückzuführen (siehe VMware-KB-Artikel). Wenn Sie eine VMware-VM stilllegen, enthält der Snapshot beschädigte Daten. Die Sicherung liest Daten vom Snapshot, sodass auch die gesicherten Daten beschädigt werden.

Hinweis: Dieses Problem kann bei allen VMware ESXi-Versionen und auf VMs mit Windows 2008 R2 SP1 und Windows 2012 als Gastbetriebssystem auftreten. In Arcserve UDP kann das Datenbeschädigungsproblem nicht erkannt werden, weil VMware in diesen Fällen keinen Fehler ausgibt. Sie erkennen das Problem möglicherweise erst, wenn Sie versuchen, Daten wiederherzustellen.

Sie können dem Arcserve-KB-Artikel folgen, um zu überprüfen, ob das Problem durch dieses bekannte VMware-Problem verursacht wird. Die von VMware vorgeschlagene Umgehungslösung besteht darin, die VSS-Writer wie MSSearch Service Writer (ignorieren, wenn nicht installiert) und Shadow Copy Optimization Writer (in der Regel auf allen Windows-VMs vorhanden) auf dem Gastbetriebssystem des virtuellen Rechners zu deaktivieren. Sie können die Writer entsprechend den Anweisungen im VMware-KB-Artikel manuell deaktivieren.

Mit Arcserve UDP lassen sich die Writer zudem auf einfache Art und Weise deaktivieren, wenn die Stilllegungsmethode für Snapshots von VMware Tools verwendet wird. Führen Sie diese Schritte aus, um die Writer zu deaktivieren:

Auf Proxy-Server-Ebene (auf durch diesen Proxy-Server geschützte VMs anwendbar)

1. Melden Sie sich beim Proxy-Server an.
2. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]
```

3. Erstellen Sie einen Multistring-Wert mit dem Namen *DisableSpecificVSSwriters*.
4. Geben Sie die Namen des VSS-Writer ein, der deaktiviert werden soll (jeder Writer-Name belegt eine Zeile).
5. Speichern Sie den Registrierungsschlüssel.

Auf VM-Ebene

1. Melden Sie sich beim Proxy-Server an.
2. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]
```

3. Erstellen Sie einen Multistring-Wert mit dem Namen *DisableSpecificVSSwriters*.
4. Geben Sie die Namen des VSS-Writer ein, der deaktiviert werden soll (jeder Writer-Name belegt eine Zeile).
5. Speichern Sie den Registrierungsschlüssel.

Hinweise:

- Wenn Sie den Registrierungsschlüssel in der Registrierung sowohl auf Ebene des virtuellen Rechners als auch auf Proxyebene hinzufügen, dann hat die Einstellung in der Registrierung auf Ebene des virtuellen Rechners Vorrang vor der Einstellung in der Registrierung auf Proxyebene.
- Diese Einstellung in der Registrierung funktioniert nur, wenn im Sicherungsplan die Stilllegungsmethode für Snapshots von VMware Tools verwendet wird.
- Wenn Sie auf dem Gastbetriebssystem des virtuellen Rechners bereits Writer gemäß dem VMware-KB-Artikel manuell konfiguriert haben, wird Ihre Konfiguration überschrieben.
- Beim Namen des Writers wird zwischen Groß- und Kleinschreibung unterschieden und es muss eine genaue Übereinstimmung wie in der Ausgabe von "Vssadmin List Writers" angezeigt vorliegen.
- Wenn Sie alle Writer erneut aktivieren möchten, löschen Sie nicht den Registrierungswert *DisableSpecificVSSwriters*. Behalten Sie stattdessen den Registrierungswert bei, aber entfernen Sie den Inhalt der Registrierung. Wenn *DisableSpecificVSSwriters* nicht vorhanden ist, geht Arcserve UDP davon aus, dass in Bezug auf das Aktivieren bzw. Deaktivieren von VSS-Writern keine Änderung erfolgen muss.

Inkrementelle Sicherung wird zu Überprüfungssicherung konvertiert oder die Sicherungsgröße in Hyper-V wird erhöht.

Gilt für Hyper-V-VMs

Problem

- Auf einem virtuellen Hyper-V-Rechner wurde eine inkrementelle Änderung vorgenommen. Beim Durchführen einer Zuwachssicherung wird anstelle der geänderten Daten der komplette virtuelle Rechner gesichert.
- Der Benutzer hat einen Proxy-Server mit Arcserve UDP Version 7.0, und die Lösung sichert einen virtuellen Rechner von einem Hyper-V-Host (Beispiel: HOST1). Der Benutzer hat einen weiteren Proxy-Server mit einer älteren Version von Arcserve UDP, und die Lösung sichert einen virtuellen Rechner vom gleichen Hyper-V-Host (HOST1). In solchen Fällen ist die Funktion der Verfolgung geänderter Blöcke (CBT) inaktiv, und die Zuwachssicherungsjobs werden nicht ausgeführt. Die inkrementelle Sicherung geht in eine Überprüfungssicherung über.

Lösung

Für die oben genannten Symptome kann es folgende Gründe geben:

- Der Verlust von CBT (Change Block Tracking)-Daten. Die folgenden Umstände führen zum Verlust von CBT-Daten:
  - Der Hyper-V-Host stürzt ab oder wird nicht ordnungsgemäß ausgeschaltet.
  - Der CBT-Dienst wird angehalten oder nicht ordnungsgemäß beendet.
  - Die Aktionen des CBT-Diensts wurden beim Herunterfahren des Hyper-V-Hosts nicht abgeschlossen.
- Der Hyper-V-Server und der Proxy-Server nutzen unterschiedliche CBT-Versionen.

  Beispiel: Betrachten Sie, dass Sie zwei Arcserve UDP-Umgebungen haben, eine ist Arcserve UDP Version 6.0 und eine andere ist Arcserve UDP Version 7.0. Diese beiden Arcserve UDP-Umgebungen sichern verschiedene VMs im selben Hyper-V-Server. Die ältere Version von CBT wird von der Arcserve UDP Version 7.0-Umgebung auf dem Hyper-V-Server automatisch erkannt und auf die neueste Version aktualisiert. In solchen Fällen konvertiert die Arcserve UDP Ver-

sion 5-Umgebung die verbleibende geplante Zuwachssicherung in eine vollständige Sicherung.

Wenn Arcserve UDP unterschiedliche CBT-Versionen erkennt, dann zeigt das Aktivitätsprotokoll einen Warnhinweis an.

Die Lösung besteht darin, für alle Proxy-Server, die virtuelle Rechner von einem Hyper-V-Host schützen, ein Upgrade auf die gleiche Arcserve UDP-Version durchzuführen.

Hostbasierte Sicherung schlägt für Hyper-V-VM mit spezieller Konfiguration differenzierender Datenträger fehl

Gültig für Hyper-V-VM

Problem

Wenn ein differenzierender Datenträger in einer Hyper-V-VM konfiguriert ist, schlägt der Sicherungsjob für diesen virtuellen Rechner fehl. Im Aktivitätsprotokoll wird die folgende Fehlermeldung angezeigt:

"Failed to prepare for backup of the virtual machine".

Die folgende Fehlermeldung wird in der Sicherungsjob-Protokolldatei unter C:\Programme\Arcserve\Unified Data Protection\Engine\Logs angezeigt:

"The virtual disk file \\?\UNC\<IP_Address_VM>\HYPERV_HBBU_SNAPSHOT@<snapshot_name>\WIN12-SQL\VIRTUAL HARD DISKS\WIN12-SQL-1.VHDX was not exposed."

Das Problem tritt nur auf, wenn der virtuelle Rechner über die folgenden Konfigurationen der differenzierenden Datenträger verfügt. Alle Konfigurationen müssen zutreffen.

- Der virtuelle Rechner verfügt über eine reguläre virtuelle Festplatte (festgesetzte Größe oder dynamische Erweiterung), Disk1, die mit einem IDE- oder SCSI-Controller des virtuellen Rechners verknüpft ist.
- Der virtuelle Rechner verfügt über eine differenzierende virtuelle Festplatte (Disk2), die ebenfalls mit einem IDE- oder SCSI-Controller des virtuellen Rechners verknüpft ist.
- Der übergeordnete Datenträger von Disk2 wird als Disk1 angegeben.

Lösung

Dieser Fehler tritt aufgrund einer ungewöhnlichen oder falschen Konfiguration auf. Um diesen Fehler zu beheben, heben Sie die Verknüpfung des differenzierenden Datenträgers oder seines übergeordneten Datenträgers mit dem virtuellen Rechner auf. Arcserve UDP unterstützt solche Konfigurationen differenzierender Datenträger nicht.

Sicherungsjob für eine VMware-VM schlägt fehl

Gültig für VMware-VM

Problem

Wenn ich eine VMware-VM sichere, schlägt der Sicherungsjob mit einer der folgenden Fehlermeldungen im Aktivitätsprotokoll fehl:

Die Sicherung wurde abgebrochen, da Sicherungsjob für die Verwendung der Snapshot-Methode "Microsoft-VSS innerhalb der VM" konfiguriert wurde. Es ist jedoch nur die Snapshot-Methode "VMware Tools" anwendbar, da die hostbasierte VM-Sicherung die erforderlichen Tools auf der VM nicht bereitstellen konnte.

Oder

Die Sicherung wurde abgebrochen, da Sicherungsjob für die Verwendung der Snapshot-Methode "VMware Tools" konfiguriert wurde. Es ist jedoch nur die Snapshot-Methode "Microsoft-VSS innerhalb der VM" anwendbar, da die hostbasierte VM-Sicherung die Bereitstellung der Tools auf der VM nicht aufheben konnte.

Lösung

Der erste Fehler kann aufgrund mehrerer Ursachen auftreten. Sie haben die Option **Microsoft-VSS innerhalb der VM** ausgewählt, aber:

- Sie haben die VM nicht mit den erforderlichen Anmeldeinformationen aktualisiert.
- Die Anmeldeinformationen sind nicht korrekt.
- VMware Tools ist nicht installiert oder aktualisiert

In diesem Fall kann Arcserve UDP die Tools, die für die Verwendung der neuen Snapshot-Methode erforderlich sind, nicht auf dem virtuellen Rechner bereitstellen.

Um diesen Fehler zu beheben, aktualisieren Sie den virtuellen Rechner mit den richtigen Anmeldeinformationen. Stellen Sie sicher, dass VMware Tools aktualisiert ist und auf dem virtuellen Rechner ausgeführt wird. Übergeben Sie den Sicherungsjob nach der Überprüfung erneut.

Lösung

Der zweite Fehler kann in folgendem Szenario auftreten. Sie haben die Option **Microsoft-VSS innerhalb der VM** in den vorherigen Sicherungsjobs verwendet. Jetzt möchten Sie die Option **VMware Tools** verwenden, aber die Anmeldedaten des virtuellen Rechners wurden geändert (z. B. durch eine Änderung des Passworts

des Gastbetriebssystems ohne Aktualisierung des VM-Knotens in der Konsole) oder VMware Tools wird nicht ausgeführt. In solchen Fällen kann Arcserve UDP die Bereitstellung der Tools für die Verwendung der Snapshot-Methode (die vom vorherigen Sicherungsjob bereitgestellt wurden) auf dem virtuellen Rechner nicht aufheben.

Gehen Sie folgendermaßen vor, um diesen Fehler zu beheben:

- Aktualisieren Sie den virtuellen Rechner mit den richtigen Anmeldeinformationen. Stellen Sie sicher, dass VMware Tools aktualisiert ist und im Gastbetriebssystem des virtuellen Rechners ausgeführt wird. Übergeben Sie den Sicherungsjob nach der Überprüfung erneut.
- Heben Sie die Bereitstellung der Tools auf dem virtuellen Rechner manuell auf:
  a. Melden Sie sich beim virtuellen Rechner an.
  b. Navigieren Sie zum folgenden Ordner:

     C:\Programme\ARCServe\ASVMOperationTools\custom-freeze-vmware-snapshot\auto-deploy
  c. Klicken Sie mit der rechten Maustaste auf die Batch-Datei auto-undeploy.bat, und wählen Sie "Als Administrator ausführen" aus.
  d. Löschen Sie die folgenden Ordner:

     C:\Programme\ARCServe\as-hbbu-vmwarebackup

     C:\Programme\ARCServe\ASVMOperationTools
  e. Übergeben Sie den Sicherungsjob erneut.

Deaktivieren der erneuten Überprüfung des HBA während inkrementeller Sicherungen

Gilt für VMware ESX.

Gilt nur für UDP Version 6.5, nicht für Updates von Version 6.5.

Problem

Wenn der Quellknoten und der Proxy-Server sich in unterschiedlichen VMware ESX-Servern befinden, während ich eine inkrementelle Sicherung ausführe, nimmt die Sicherung mehr Zeit in Anspruch. Ich erhalte auch mehrere Meldungen zum erneuten Prüfen. Ich möchte die erneute Prüfung sämtlicher HBA (Host Bus Adapter) und sonstiger VMware ESX-Server bei inkrementellen Sicherungen deaktivieren.

Lösung

Sie können die Suche deaktivieren, indem Sie einen Registrierungsschlüssel auf dem Proxy-Server erstellen und diesem einen Wert zuweisen.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Rechner an.
2. Navigieren Sie zum folgenden Ordner:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
   ```

3. Erstellen Sie den folgenden Registrierungsschlüssel (DWORD), wenn er nicht bereits vorhanden ist:

   ```
   DisableAllESXNodeRescan
   ```

4. Legen Sie den Wert des Registrierungsschlüssels auf 1 fest.

Deaktivieren der aufeinander folgenden Erstellung von Snapshots in VMware-VM für eine Sicherung

In der vorherigen Version von Arcserve UDP erstellten die Jobs Snapshots auf dem ESX-Host parallel zu Jobs, wenn mehrere VMware-VM-Sicherungsjobs gleichzeitig gestartet wurden. In manchen Fällen erhöhte die parallele Erstellung von Snapshots den Datenträger-E/A auf dem ESX-Host. Um diese Situation zu vermeiden, serialisiert Arcserve UDP Version 7.0 standardmäßig die Snapshot-Erstellung, wenn die Jobs auf dem gleichen Proxy-Server ausgeführt werden und die Snapshot-Erstellung für den gleichen ESX-Host erfolgt. Oder anders ausgedrückt: Die Snapshot-Erstellung erfolgt nacheinander, und idealerweise wird jeweils nur ein Snapshot erstellt. Aber dies ist nicht anwendbar, wenn die Sicherungsjobs auf verschiedenen Proxy-Servern ausgeführt werden oder die Sicherungsjobs für unterschiedliche ESX-Hosts erfolgen.

Um eine Situation zu vermeiden, in der die Snapshot-Erstellung eines Jobs hängt (oder sehr lange dauert) und die nächsten Jobs gesperrt werden, erfolgt die nächste Snapshot-Erstellung erst nach **fünf Minuten**. Nach fünf Minuten wird der nächste Snapshot erstellt.

Sie können dieses Verhalten durch folgende Schritte deaktivieren:

1. Melden Sie sich beim Proxy-Server an.
2. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

3. Erstellen Sie einen DWORD-Wert mit dem Namen **CreateSnapshotSequentially**.
4. Legen Sie den Wert auf 0 fest.

Sie können darüber hinaus auch das Standard-Zeitlimit (5 Minuten) ändern, indem Sie folgendermaßen vorgehen:

1. Melden Sie sich beim Proxy-Server an.
2. Öffnen Sie den Registrierungsschlüssel von folgendem Speicherort:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

3. Erstellen Sie einen DWORD-Wert mit dem Namen **CreateSnapshotTimeout**.
4. Legen Sie für den Wert eine Zahl fest.

   Die Einheit wird in Sekunden angegeben.

Nach Wiederherstellung von einem Host mit höherer ESXi-Version auf einen Host mit niedrigerer ESXi-Version hängt sich die VM beim Booten auf

Nach Wiederherstellung von einem Host mit höherer ESXi-Version auf einen Host mit niedrigerer ESXi-Version hängt sich die VM beim Booten auf, nachdem sie eingeschaltet wird.

Gilt für Windows-Plattformen Gilt nur für VMware-VMs.

Problem

Eine VM wird von einem Host mit höherer ESXi-Version auf einen Host mit niedrigerer ESXi-Version wiederhergestellt und danach eingeschaltet. Die VM hängt sich beim Booten auf.

Lösung

Die Gastbetriebssystem-Version dieser VM wird von der niedrigeren ESXi-Version möglicherweise nicht unterstützt. Zur Umgehung des Problems können Sie eine der folgenden Optionen verwenden:

- Stellen Sie die VM auf einem ESXi-Host wieder her, der diese Gastbetriebssystem-Version unterstützt oder
- Aktualisieren Sie den vorhandenen ESXi-Host auf die geeignete Version.

Beispiel: Eine Windows Server 2012 R2-VM wird von einem ESXi 5.5 gesichert und auf einem ESXi 5.0 Update 1 wiederhergestellt. Dieses Problem kann auftreten, weil ESXi 5.0 das Gastbetriebssystem Windows Server 2012 R2 erst ab Update 2 unterstützt.

Sie müssen ESXi 5.0 Update 1 auf Update 2 aktualisieren, damit das Gastbetriebssystem Windows Server 2012 R2 unterstützt wird. Um dieses Problem zu umgehen, können Sie auch die Gastbetriebssystem-Version der wiederhergestellten VM auf die Version wechseln, die von der aktuellen Version von ESXi unterstützt wird (im Beispiel oben: Wechsel zu Windows Server 2008 R2).

Hinweis: Durch diese Umgehung wird das Problem möglicherweise nicht behoben.

RAM-Auslastung erreicht 99 %, wenn Sicherungsjobs an die VM übergeben werden

RAM-Auslastung erreicht 99 %, wenn Sicherungsjobs unter Windows 2012 Hyper-V-CSV an VMs übergeben werden.

Problem

Während der Sicherung von VMs, die Teil des 2012 Hyper-V-Clusters sind, steigt die RAM-Auslastung schrittweise an und erreicht auf dem Hyper-V-Host des CSV-Besitzers 99 %. Dadurch funktionieren die virtuellen Rechner und der Hyper-V-Host während der Sicherung nicht mehr.

Lösung

Dieses Problem tritt aufgrund bekannter Fehler im Microsoft-Code auf.

Um dieses Problem zu beheben, laden Sie den von Microsoft bereitgestellten Hotfix unter folgendem Link herunter, und wenden Sie ihn auf alle Hyper-V-Hosts an:

https://support.microsoft.com/en-in/kb/2878635

Hyper-V-Auftrag schlägt fehl, es kann keine Verbindung zum Dienstprogramm auf dem Host hergestellt werden

Der Hyper-V-Wiederherstellungsauftrag schlägt fehl, und es wird eine Fehlermeldung angezeigt.

Problem

Beim Wiederherstellen eines virtuellen Hyper-V-Computers schlägt der Wiederherstellungsauftrag fehl, und der folgende Fehler wird im Aktivitätsprotokoll angezeigt;

Fehler beim Herstellen einer Verbindung mit dem Hyper-V-Wiederherstellungsprogramm auf Host xxxxx

Im Debugprotokoll des Wiederherstellungsauftrags werden die folgenden Fehlermeldungen angezeigt:

Fehler beim Herstellen einer Verbindung mit xxxxx:10218. Fehler: Zeitüberschreitung beim Verbindungsversuch, ohne eine Verbindung herzustellen (rc =-536805332)

Fehler beim Herstellen einer Verbindung mit xxxxx: 10218, Fehler-536805332

Lösung

Ein derartiges Problem wird in der Regel verursacht, wenn die Verbindung zwischen Sicherungsproxy und Hyper-V-Host von der Firewall blockiert wird. Deaktivieren Sie, wenn möglich, die Firewall, und versuchen Sie die Wiederherstellung erneut. Wenn Sie die Firewall nicht deaktivieren können, registrieren Sie den Port (oder Portbereich), der von dem Wiederherstellungsauftrag verwendet wird, bei der Firewallausnahme.

Standardmäßig wählt der Wiederherstellungsauftrag zufällig einen verfügbaren Port im Bereich zwischen 1024 und 65535 aus. Sie können den Bereich manuell anhand von festgelegten Registrierungswerten im Hyper-V-Host angeben.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Hyper-V-Host an.
2. Führen Sie den Befehl *regedit* aus, um den Registrierungseditor zu öffnen.
3. Navigieren Sie zu dem folgenden Registrierungsschlüssel (erstellen Sie Schlüssel, falls einer der Schlüssel nicht vorhanden ist):

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\HyperVRestoreStub

4. Erstellen Sie die folgenden beiden Registrierungswerte (DWORD):

   PortMin

   PortMax

5. Geben Sie Werte mit Anfang- und Endnummer des Portbereichs an.

   Hinweise:

   - Obligatorischer Bereich angegebener Werte: 1024-65535
   - Sie können für beide Registrierungswerte dieselbe Zahl angeben. In diesem Fall wird die feste Portnummer für den Wiederherstellungsauftrag verwendet. Wenn mehrere Wiederherstellungsaufträge gleichzeitig ausgeführt werden und sobald ein Wiederherstellungsauftrag diesen Port belegt, schlagen andere Wiederherstellungsaufträge fehl.

Automatischer Schutz erkennt und schützt virtuellen Computer nicht

Der virtuelle Computer wird im Rahmen des automatischen Schutzes nicht erkannt und automatisch geschützt.

Problem

Obwohl ein virtueller Computer zwar in Hypervisor (vCenter/ESX oder Hyper-V) von einer systemeigenen Clientanwendung (z. B. vSphere Client oder Hyper-V Manager) angezeigt werden kann, erkennt der automatische Schutz diesen Computer nicht, und folglich kann der virtuelle Computer nicht automatisch geschützt werden.

Ursachen

- Der virtuelle Computer weist im Hypervisor keinen gültigen Status auf. Der automatische Schutz überspringt beispielsweise virtuelle Computer, die in vCenter/ESX den Status "Getrennt", "Verwaist" oder "Zugriff nicht möglich" aufweisen.
- Der virtuelle Computer wird von Arcserve UDP-Aufgaben wie Virtual Standby (VSB), Instant VM (IVM) oder Assured Recovery (AR) erstellt (oder vom VSB/IVM/AR VM geklont). Arcserve UDP überspringt virtuelle Computer aufgrund der folgenden Überlegungen absichtlich:
  - Das Sichern von virtuellen Computern durch Arcserve UDP, die von VSB/IVM/AR erstellt wurden, ohne Einschränkung kann zu einer *Endlos-Sicherungsschleife* führen. Der automatische Schutz wird beispielsweise verwendet, um den gesamten ESX zu schützen. Im Sicherungsplan fügen Sie nach dem Hinzufügen einer Sicherungsaufgabe, eine VSB-Aufgabe hinzu, die den virtuellen VSB-Computer in demselben ESX erstellt. Nach der ersten Sicherung wird daher ein neuer virtueller VSB-Computer im ESX erstellt. Der neue virtuelle VSB-Computer wird vom automatischen Schutz erkannt und zum Sicherungsplan hinzugefügt. Bei der nächsten Sicherung wird dann ein neuer virtueller VSB-Computer aus einem früheren virtuellen VSB-Computer erstellt und zum Sicherungsplan hinzugefügt. Der Prozess wird fortgesetzt, bis der ESX-Speicher keinen freien Speicherplatz mehr aufweist.
  - Bei einem virtuellen Linux IVM/AR-Computer kann Arcserve UDP den virtuellen Computer nicht sichern, sofern die Speichermigration keine Konvertierung in einen normalen virtuellen Computer durchführt. Der Sicherungsauftrag kann abgeschlossen werden, der gesicherte

Wiederherstellungspunkt kann jedoch nicht wiederhergestellt werden. Dies geschieht aufgrund einer technischen Einschränkung der Linux IVM-Implementierung.

Lösung

Wenn Sie virtuelle VSB/IVM/AR-Computer sichern möchten oder die virtuellen Computer in durch Klonen oder Speichermigration in unabhängige virtuelle Computer konvertiert werden, befolgen Sie die nachfolgenden Schritte für virtuelle vSphere- und Hyper-V-Computer , damit diese vom automatischen Schutz erkannt werden können.

Virtueller vSphere-Computer

1. Melden Sie sich beim vSphere-Webclient an, und suchen Sie den virtuellen Computer.
2. Schalten Sie den virtuellen Computer aus.
3. Klicken Sie mit der rechten Maustaste auf den virtuellen Computer, und wählen Sie "Einstellungen bearbeiten" aus dem Menü aus.
4. Wählen Sie die Registerkarte für die **VM-Optionen** aus, und erweitern Sie "Erweitert".
5. Klicken Sie auf **Konfiguration bearbeiten**.
6. Suchen Sie im Dialogfeld der Konfigurationsparameter die Parameter mit einem der folgenden Namen:
   - VCM
   - UDP_IVM
   - UDP_ARVM
   - UDP_IVM_LINUX
   - UDP_VSBVM
   - UDP_ARVM_LINUX
   - UDP_ARIVM_LINUX
7. Löschen Sie den Wert des Parameters, und klicken Sie zum Speichern auf **OK**.

Für Hyper-V-VM

1. Melden Sie sich beim Hyper-V-Host an, und öffnen Sie Hyper-V Manager.
2. Suchen Sie den virtuellen Computer.

3. Klicken Sie mit der rechten Maustaste auf den virtuellen Computer, und wählen Sie "Einstellungen" aus dem Menü aus.
4. Wählen Sie im Dialogfeld "Einstellungen" die Option "Name" im linken Bereich aus.
5. Entfernen Sie alle Zeilen, die mit folgenden Zeichenfolgen beginnen:
   - VCM
   - UDP_IVM
   - UDP_ARVM
   - UDP_IVM_LINUX
   - UDP_VSBVM
   - UDP_ARVM_LINUX
   - UDP_ARIVM_LINUX
6. Klicken Sie zum Speichern auf **OK**.

Festlegen der Leseblockgröße beim Sichern einer VMDK-Datei

Problem

In einer bestimmten Umgebung wird der Sicherungsdurchsatz der VMware VM beim Sichern einer VMDK-Datei von der Leseblockgröße beeinträchtigt.

Lösung

Standardmäßig beträgt die VMDK-Leseblockgröße 2 MB. Sie können die Größe ändern.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Sicherungsproxy ohne Agent an.
2. Führen Sie den Befehl *regedit* aus, um den Registrierungseditor zu öffnen.
3. Navigieren Sie zu dem folgenden Registrierungsschlüssel:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll
4. Erstellen Sie die Registrierungswerte (DWORD) mit dem folgenden Namen:

   ReadVirtualDiskBlockSizeKB
5. Geben Sie den gewünschten Wert als Leseblockgröße an (Einheit ist KB).

Beim Klonen von LUNs wird die Reservierung von LUN Speicherplatz vererbt

Problem

Wenn während der Sicherung mithilfe eines Hardware-Snapshots ein LUN geklont wird, wird die Reservierung von Speicherplatz standardmäßig vom Quell-LUN vererbt.

Lösung

Sie müssen den Registrierungsschlüssel verwenden, den Arcserve UDP bereitstellt, um die Reservierung von Speicherplatz zu deaktivieren. Die Registrierungsschlüssel befinden sich am folgenden Speicherort:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

DisableLunSpaceReservation = 1

Gibt an, dass die Reservierungen von LUN-Speicherplatz deaktiviert werden.

Hinweis: Diese Option gilt nur, wenn eine FlexClone-Lizenz angewendet wird.

Weitere Informationen finden Sie unter Hinweise für den NetApp iSCSI/FC-Support für VMware.

Infos zu Virtual Standby

Dieser Abschnitt enthält die folgenden Fehlerbehebungsthemen im Zusammenhang mit Virtual Standby:

- Betriebssystem nicht gefunden
- Virtual Standby-Jobs schlagen aufgrund interner Fehler fehl
- Virtual Standby-Jobs im HotAdd-Transportmodus schlagen fehl
- Virtual Standby-Jobs an Hyper-V-Systeme schlagen fehl
- Problem durch doppelte Agent-UUID
- Option "Terminal-EC2-Ressourcen" wird nicht angezeigt

Operating System Not Found (Betriebssystem nicht gefunden)

Gültig auf Windows-Plattformen.

Problem:

Die folgende Meldung wird angezeigt, wenn das Einschalten des Virtual Standby-Rechners fehlschlägt:

Operating System Not Found (Betriebssystem nicht gefunden)

Lösung:

Das oben aufgeführte Verhalten kann auf virtuellen Rechner auftreten, die SCSI- und IDE-Geräte enthalten. Wenn dieses Problem auftritt, überprüfen Sie, wie die Datenträger auf Ihrem virtuellen Rechner konfiguriert sind, und stellen Sie sicher, dass die Startsequenz des wiederhergestellten virtuellen Rechners dieselbe ist, wie die der Quelle des virtuellen Rechners. Wenn die Startsequenz anders ist, aktualisieren Sie das BIOS auf dem wiederhergestellten virtuellen Rechner, damit sie mit der Startsequenz der Quelle übereinstimmt.

Hinweis: Hinweis: Verwenden Sie für die Darstellung des ersten IDE-Datenträgers (0:1).

Virtual Standby-Jobs schlagen aufgrund interner Fehler fehl

Gilt für Windows-Betriebssysteme.

Symptom 1:

Virtual Standby-Jobs schlagen fehl. Es wird eine der folgenden Meldungen im Aktivitätsprotokoll angezeigt:

Fehler beim Konvertieren des virtuellen Datenträgers.

Ein interner Fehler ist aufgetreten. Setzen Sie sich mit CA Support in Verbindung.

Außerdem wird im VDDK die folgende Fehlermeldung angezeigt:

Unbekannter Fehler.

Lösung 1:

Um dieses Problem zu beheben, beachten Sie folgende Lösungsmöglichkeiten:

- Konvertierungsvorgänge können fehlschlagen, wenn im Datenspeicher, der in der Virtual Standby-Richtlinie angegeben ist, nicht genügend freier Speicherplatz vorhanden ist. VDDK gibt die Meldung zurück, da die VDDK-API es (derzeit) nicht unterstützt, die Größe des freien Speicherplatzes im Datenspeicher zu erkennen. Um dieses Problem zu beheben, machen Sie im ursprünglichen Datenspeicher so viel Festplattenspeicher frei, wie für den Abschluss des Vorgangs erforderlich ist, und übergeben Sie den Job erneut.
- Netzwerkstörungen und starker Netzwerkverkehr können dazu führen, dass die Konvertierung fehlschlägt. Um dieses Problem zu beheben, stellen Sie sicher, dass der Quellknoten über das Netzwerk mit dem ESX Server- bzw. vCenter-System kommunizieren kann, und übergeben Sie den Job erneut.
- Wenn mehrere gleichzeitige Verbindungen vorliegen, die aus Jobs zur Sicherung oder Wiederherstellung von virtuellen Rechnern auf dem ESX Server- oder vCenter Server-System bestehen - wobei Verbindungen über den VMware vSphere Client stattfinden - schlagen diese Jobs möglicherweise fehl. Um dieses Problem zu beheben, beenden Sie alle unnötigen Verbindungen, und übergeben Sie den Job erneut.

  Dieses Problem hat seine Ursache in einer Verbindungsbeschränkung in VMware-VDDK. Folgende Protokollbeschränkungen der Netzwerkdateikopie (NFC) gelten für:

  ESXi 5: Von einem Übertragungspuffer für alle NFC-Verbindungen beschränkt und vom Host erzwungen; die Summe aller NFC-Verbindungpuffer zu einem

ESXi-Host darf 32 MB nicht überschreiten. 52 Verbindungen durch vCenter Server einschließlich der Grenze pro Host.

Hinweis: Verbindungen können nicht über Festplatten hinweg gemeinsam genutzt werden. Die Werte für "Maximale Beschränkungen" beziehen sich nicht auf SAN- oder HotAdd-Verbindungen. Wenn der NFC-Client nicht ordnungsgemäß heruntergefahren wird, können Verbindungen für zehn Minuten offen bleiben.

- Prüfen Sie die Abschnitte "Tasks" (Aufgaben) und "Events" (Ereignisse) des VMware vSphere Client-Protokolls, um interne Fehler beim spezifischen virtuellen Rechner zu entdecken. Beheben Sie die internen Fehler, und übergeben Sie den Job erneut.

  Beispiel: Eine andere Anwendung bzw. ein anderer Vorgang verwendet die VMDK-Datei. Um dieses Problem zu beheben, geben Sie die Datei frei, und übergeben Sie den Job erneut.

Symptom 2:

Virtual Standby-Jobs schlagen fehl. Es wird eine der folgenden Meldungen im Aktivitätsprotokoll angezeigt:

Fehler beim Konvertieren des virtuellen Datenträgers.

Ein interner Fehler ist aufgetreten. Setzen Sie sich mit CA Support in Verbindung.

Außerdem wird im VDDK die folgende Fehlermeldung angezeigt:

Open vmdk failed with error File not found. (Öffnen von vmdk fehlgeschlagen, Datei nicht gefunden)

Lösung 2:

Dieses Problem kann unter folgenden Umständen auftreten:

- In VDDK wurde ein Snapshot nicht richtig bearbeitet.
- In VDDK wurde ein Snapshot nicht manuell oder nicht vom virtuellen Rechner entfernt.

Um dieses Problem zu beheben, übergeben Sie den Job erneut. Wenn der Job erneut fehlschlägt, löschen Sie den wiederhergestellten virtuellen Rechner, und übergeben Sie den Job erneut.

Symptom 3:

Virtual Standby-Jobs schlagen fehl. Es wird eine der folgenden Meldungen im Aktivitätsprotokoll angezeigt:

'<Planname>' kann nicht auf den Knoten '<Knotenname>' angewendet werden. Der Arcserve UDP Agent-Webdienst auf dem Konverter "<Konvertername>" ist ausgelastet. Versuchen Sie es später erneut.

Außerdem wird in der Protokolldatei der UDP-Konsole (ARCApp.log) die folgende Fehlermeldung angezeigt:

[FEHLER] deployVsbTask: Fehler beim Aufrufen der D2D-Webdienst-API - Zeitüberschreitung. javax.xml.ws.WebServiceException: java.net.SocketTimeoutException: Zeitüberschreitung beim Lesen

Lösung 3:

Dieses Problem kann aufgrund einer Zeitüberschreitung auftreten. Gehen Sie folgendermaßen vor, um das Problem zu beheben:

1. Melden Sie sich bei der **UDP-Konsole** mit den entsprechenden Anmeldeinformationen an.
2. Öffnen Sie die Befehlszeilenschnittstelle und führen Sie den folgenden Befehl aus:

   regedit

   Die Registrierung wird angezeigt.
3. Navigieren Sie zu ***\SOFTWARE\Arcserve\Unified Data Protection\Engine\WebService***.
4. Stellen Sie sicher, dass der Schlüssel **timeoutValue** vorhanden ist. Wenn der Schlüssel nicht vorhanden ist, erstellen Sie ihn manuell.

   Sie können den neuen Schlüssel wie unten aufgeführt hinzufügen/ändern:

   - **Schlüsselname:** timeoutValue
   - **Wert:** <Geben Sie den Wert in Minuten ein>. Wenn Sie z. B. den Wert für die Zeitüberschreitung auf 20 Minuten festlegen möchten, geben Sie den Wert "20" an.
5. Beenden Sie **regedit**.
6. Navigieren Sie zum Installationsordner der **UDP-Konsole**. Beispiel: *C:\Programme\Arcserve\Unified Data Protection\Management\Configuration*.
7. Öffnen Sie die Datei **ConsoleConfiguration.xml** im Editor.
8. Suchen Sie im Abschnitt **<TimeoutConf>** den folgenden Text:

   <webServiceRequestTimeout>600</webServiceRequestTimeout>
9. Ändern Sie den Wert von **webServiceRequestTimeout** in Sekunden. Wenn Sie z. B. den Wert für die Zeitüberschreitung auf 20 Minuten festlegen möchten, geben Sie den Wert "1200" an.
10. **Speichern** Sie die Konfigurationsdatei und beenden Sie den Editor.

11. **Starten** Sie den **UDP-Konsolen-Verwaltungsdienst** neu, damit die Einstellungen wirksam werden.
12. Stellen Sie den Plan erneut bereit und überprüfen Sie die Ergebnisse.

Virtual Standby-Jobs im HotAdd-Transportmodus schlagen fehl

Gültig auf Windows-Plattformen.

Problem:

Wiederherstellungsvorgänge schlagen fehl, wenn Daten im HotAdd-Transportmodus wiederhergestellt werden. Folgende Meldung wird im Aktivitätsprotokoll angezeigt:

Ein unbekannter Fehler ist aufgetreten. Wenden Sie sich an den technischen Support.

Außerdem wird im VDDK die folgende Fehlermeldung angezeigt:

Unbekannter Fehler.

Lösung:

Wiederherstellungsvorgänge schlagen im HotAdd-Transportmodus fehl, wenn die Datenträgereinstellungen nicht ordnungsgemäß konfiguriert sind.

Gehen Sie wie folgt vor, um den Datenträger zu konfigurieren:

1. Melden Sie sich über ein Konto mit Administratorrechten beim Sicherungs-Proxy-System an.

   Öffnen Sie die Windows-Befehlszeile.

2. Geben Sie in der Befehlszeile folgenden Befehl ein:

   diskpart

   Drücken Sie die Eingabetaste.

   Gaben Sie "SAN" ein, und drücken Sie die Eingabetaste.

   Die aktuelle SAN-Richtlinie wird angezeigt.

3. Geben Sie folgenden Befehl ein:

   SAN POLICY = OnlineAll

   Drücken Sie die Eingabetaste.

   Die SAN-Richtlinie wird so konfiguriert, dass SAN-gehostete Volumes nicht automatisch geladen werden.

4. Um das schreibgeschützte Attribut des spezifischen SAN-Datenträgers zu löschen, wählen Sie den Datenträger aus der Datenträgerliste aus, und geben Sie den folgenden Befehl ein:

   attribute disk clear readonly

   Drücken Sie die Eingabetaste.

5. Gaben Sie "exit" ein, und drücken Sie die Eingabetaste.

   Der Datenträger ist nun konfiguriert, und Sie können den Job erneut übergeben. Wenn der Job erneut fehlschlägt, laden Sie die HotAdd-Datenträger manuell über die Datenträgerverwaltung des Proxysystems.

   Gehen Sie wie folgt vor, um die Datenträger manuell zu laden:

1. Melden Sie sich über ein Konto mit Administratorrechten beim Sicherungs-Proxy-System an.

   Öffnen Sie Windows-Systemsteuerung, und doppelklicken Sie auf "Verwaltung".

   Das Fenster "Verwaltung" wird geöffnet.

2. Doppelklicken Sie in der Liste "Favoriten" auf "Computerverwaltung".

   "Computerverwaltung" wird geöffnet.

3. Erweitern Sie den Bereich "Speicherung", und klicken Sie auf "Datenträgerverwaltung".

   Die Datenträger werden angezeigt.

4. Klicken Sie mit der rechten Maustaste auf den zu entfernenden Datenträger, und klicken Sie auf "Online".

   Der Datenträger ist nun geladen, und Sie können den Job erneut übergeben.

Virtual Standby-Jobs an Hyper-V-Systeme schlagen fehl

Gültig auf Windows-Betriebssystemen.

Problem:

Folgende Meldung wird im Aktivitätsprotokoll angezeigt:

Der Virtual Standby-Job konnte die Hyper-V-VM nicht abrufen.

Lösung:

Virtual Standby-Jobs schlagen unter folgenden Umständen fehl:

- Der Virtual Standby-Webservice kann aus dem Hyper-V-System keine Informationen zu den virtuellen Rechnern abzurufen. Kommunikationsprobleme zwischen dem Arcserve UDP- und dem Hyper-V-System treten auf, wenn die erforderlichen Hyper-V-Dienste nicht im Hyper-V-System ausgeführt werden.

  Lösung: Lösung: Stellen Sie sicher, dass alle erforderlichen Hyper-V-Dienste auf dem Hyper-V-System ausgeführt werden.

- Das Hyper-V-System enthält nicht den freien Speicherplatz, der für das Erstellen des virtuellen Virtual Standby-Rechners oder zum Erstellen eines Snapshots des virtuellen Virtual Standby-Rechners benötigt wird.

  Lösung: Lösung: Konfigurieren Sie das Hyper-V-System neu, um ausreichend freien Festplattenspeicher im Systemvolume zu schaffen.

Hinweis: Hinweis: Wenn Sie andere mögliche Ursachen entdecken, setzen Sie sich mit dem Arcserve-Support in Verbindung.

Problem durch doppelte Agent-UUID

Problem:

Ein Monitor in der Konsole, der dieselbe Agent-UUID hat, muss die Agent-UUID überschreiben.

Lösung:

1. Führen Sie von Ihrem Computer aus *regedit* aus.
2. Navigieren Sie zum Verzeichnis: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine*
3. Löschen Sie die Wertdaten der NodeID.
4. Starten Sie den Arcserve UDP Agent Service neu.

Änderungen an der Virtual Private Cloud im Virtual Standby-Task werden in Amazon EC2 wiedergegeben

Problem:

Wenn nach der Durchführung eines Virtual Standby-Tasks die Virtual Private Cloud (VPC) in den Netzwerkeinstellungen des Virtual Standby-Tasks geändert wird, um für die folgenden Aufgaben einen anderen Amazon-VPC zu verwenden, werden die Änderungen nicht in Amazon EC2 aktualisiert.

Lösung

In Amazon EC2 ist eine Änderung der VPC über die UDP-Konsole nicht zulässig, wenn mindestens ein Mal ein Virtual Standby-Task ausgeführt wurde. Als Übergangslösung können Sie in Arcserve UDP nun die alte Instanz beenden und mit Hilfe der Daten aus vorhergehenden Sitzungen eine neue Instanz erstellen.

Befolgen Sie diese Schritte:

1. Konfigurieren Sie einen Sicherungsplan mit VSB auf EC2 als sekundäre Aufgabe.
2. Führen Sie einige VSB auf AWS Aufgaben aus.
3. Ändern Sie die VPC-Einstellungen in der VSB-Aufgabe [Netzwerkeinstellungen].

   Die aktualisierten VPC-Einstellungen werden in der Instanz nach der nächsten erfolgreichen VSB-Aufgabe wiedergegeben.

Hinweise:

- Die alte Instanz, die in EC2 erstellt wurde, wird ignoriert und die neue Instanz mit aktualisiertem VPC wird in EC2 erstellt, um die Netzwerkänderungen wiederzugeben.
- Die neuen Einstellungen gelten auch für alte Snapshots.

Option "Terminal-EC2-Ressourcen" wird nicht angezeigt

Problem:

Wenn Knoten mit einem Plan mit der "Virtual Standby auf EC2"-Task in UDP 7.0 U1, UDP 7.0 oder UDP 6.5 U4 konfiguriert sind und Sie die Konsole auf UDP 7.0 U2 upgraden, wird die Option **Terminal-EC2-Ressourcen** nicht für diese spezifischen Knoten angezeigt.

Lösung:

Klicken Sie auf **Ändern** für den verknüpften Plan, und speichern Sie ihn.

Infos zum Kopieren von Wiederherstellungspunkten

Dieser Abschnitt enthält die folgenden Fehlerbehebungsthemen zum Kopieren von Wiederherstellungspunkten:

- Bandbreitenüberlastung bei Jobs zum Kopieren von Wiederherstellungspunkten in die Cloud
- Konfigurieren der Registrierung für das Kopieren von Wiederherstellungspunkten
- Merge-Auftrag übersprungen

Konfigurieren der Registrierung für das Kopieren von Wiederherstellungspunkten

Problem

Der Job zum Kopieren von Wiederherstellungspunkten wurde nicht ausgeführt.

Lösung

Sie können die Anzahl der Wiederholungsversuche und das Zeitintervall der wiederholten Jobs für den "Kopieren für Wiederherstellung"-Task mit den folgenden zwei Registrierungsschlüsseln steuern. Der Registrierungsschlüssel befindet sich auf dem Rechner, auf dem Sie den UDP-Agenten installiert haben:

Job für CRP wiederholen

Der Registrierungsschlüssel befindet sich auf dem Arcserve UDP-Agenten an folgendem Speicherort:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession\nodename1

Fügen Sie den neuen Schlüssel wie unten aufgeführt hinzu:

Schlüsselname: MaxRetryCount

Schlüsseltyp: REG_DWORD

Wert: 1 als Standardwert und Maximum (10)

Hinweis: Diese Aktualisierung gilt nur für einen einzigen Knoten "nodename1".

Für Jobs zum Kopieren von Wiederherstellungspunkten in die Cloud verwendet Arcserve UDP einen temporären Pfad, der mit den Registrierungsschlüsseln für temporäre Pfade konfiguriert werden kann.

Temporären Pfad konfigurieren

Der Registrierungsschlüssel befindet sich auf dem Arcserve Backup Server an folgendem Speicherort:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession

Schlüsselname: LocalTempPath

Schlüsseltyp: REG_SZ

Hinweis: Die Speicherung erfolgt standardmäßig unter dem Stammpfad für das Arcserve-Produkt.

Bandbreitenüberlastung bei Jobs zum Kopieren von Wiederherstellungspunkten in die Cloud

Problem

Das Ausführen von Jobs zum Kopieren von Wiederherstellungspunkten (Copy Recovery Points, CRP) hat oft eine Verlangsamung des Agentenrechners aufgrund von Bandbreitenüberlastung zur Folge.

Lösung

Arcserve ermöglicht es Ihnen, eine bestimmte Bandbreite für CRP-Jobs festzulegen. Das führt dazu, dass bei Ausführung mehrerer Jobs auf einem Rechner zusammen mit CRP-Jobs, die Bandbreite auf dem Agentenrechner automatisch kontrolliert wird, allerdings nur für die CRP-Jobs. Mit einem separaten Prozess für CRP-Jobs (AFCRPBackend.exe) können Sie die richtlinienbasierte QoS auf AFCRPBackend.exe festlegen und die Bandbreite für ausgehende Jobs drosseln.

Gehen Sie wie folgt vor:

1. Tippen Sie im Feld "Start" die Zeichenfolge "MMC" ein, und drücken Sie die Eingabetaste.

   Die Microsoft Management Console wird geöffnet.

2. Drücken Sie in der MMC-Konsole STRG+M.

   Das Dialogfeld "Snap-In hinzufügen/entfernen" wird geöffnet.

3. Wählen Sie im Dialogfeld "Snap-In hinzufügen/entfernen" unter den verfügbaren Snap-Ins die Option "Editor für Gruppenrichtlinien" aus, und klicken Sie auf "Hinzufügen".

4. Lassen Sie im Dialogfeld "Gruppenrichtlinienobjekt auswählen" die Standardeinstellung "Lokaler Computer", und klicken Sie auf "Fertig stellen".

5. Klicken Sie auf "OK".

   Das Dialogfeld "Snap-In hinzufügen/entfernen" wird geschlossen.

6. Erweitern Sie im linken Fensterbereich der MMC-Konsole "Lokaler Computer", "Computerkonfiguration", "Windows-Einstellungen", und klicken Sie mit der rechten Maustaste auf "Richtlinienbasierte QoS". Wählen Sie dann im Menü "Neue Richtlinie erstellen" aus.

7. Führen Sie in den Fenstern zur richtlinienbasierten QoS Folgendes durch, und klicken Sie dann auf "Weiter":

   – Geben Sie einen Namen für die neue Richtlinie ein.

– Legen Sie den DSCP-Wert auf 0 fest.

– Wählen Sie das Kontrollkästchen "Drosselungsrate für ausgehende Jobs festlegen" aus.

Hinweis: Es wird empfohlen, Mbit/s als Option auszuwählen.

8. Um festzulegen, wofür die QoS-Richtlinie gilt, wählen Sie das Kontrollkästchen "Nur Anwendungen mit dem Namen dieser ausführbaren Datei" aus, geben Sie den folgenden EXE-Pfad ein, und klicken Sie auf "Weiter":

   C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\AFCRPBackend.exe

   Hinweis: AFCRPBackend.exe hilft dabei, sicherzustellen, dass Bandbreitenbeschränkungen nur auf CRP-Jobs angewendet werden, auch wenn mehrere Jobs auf dem Agentenrechner ausgeführt werden.

9. Behalten Sie die Standardeinstellungen bis zum letzten Bildschirm bei, und klicken Sie auf "Fertig stellen".

Zusammenführungsjob übersprungen

Problem

- Der Zusammenführungsjob wurde übersprungen, da die Sitzung derzeit durch den Job zum Kopieren von Wiederherstellungspunkten gesperrt ist. Prüfen Sie, ob ein Job zum Kopieren von Wiederherstellungspunkten aussteht.
- Der Zusammenführungsjob wurde übersprungen, da die Sitzung derzeit durch den On-Demand-Job zum Kopieren von Wiederherstellungspunkten gesperrt ist. Der On-Demand-Job zum Kopieren von Wiederherstellungspunkten wird gerade ausgeführt oder wartet auf seine Ausführung.

Lösung

Um den Zusammenführungsjob fortzusetzen, müssen die Sperrdateien aus dem Sicherungsziel des Knotens entfernt werden.

Führen Sie das Tool "Sperre löschen" in *C:\Programme\Arcserve\Unified Data Protection\Engine\BIN>AFDeleteLockTool.exe* aus.

Hinweis: Dieses Tool löscht alle CRP-bezogenen Sperren (geplante CRPs und Ad-hoc-CRPs), und die Zusammenführung startet sofort. Zusammengeführte Sitzungen sind nicht für CRPs für das Kopieren in das Ziel verfügbar.

Verwendung:

AFDeleteLockTool.exe -path <BackupDestinationPath> -user <USERNAME> -password <PASSWORD> -type <crp/adhoccrp>

Bemerkungen:

-path: -Gibt den Pfad des Sicherungsziels an

-type: -Gibt den Task zum Löschen der Sperre an

crp: Löscht Sperren im Zusammenhang mit geplanten CRP-Jobs.

adhoccrp: Löscht Sperren im Zusammenhang mit ad-hoc-CRP-Jobs.

-user: -Gibt den Benutzernamen für das Sicherungsziel an

-password: -Gibt das Kennwort für das Sicherungsziel an

-path und -type sind obligatorisch

-user und -password sind optional. (beide Angaben müssen angegeben oder übersprungen werden)

Beispiele:

- Wenn Sie nur Sperren für geplante CRP-Tasks entfernen möchten, führen Sie das Tool bitte wie folgt aus:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -type crp

- Wenn Sie nur Sperren für Ad-hoc-CRP-Tasks entfernen möchten, führen Sie das Tool bitte wie folgt aus:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -user User123 -password "**********" -type crp

- Wenn Sie alle CRP-Sperren entfernen möchten, führen Sie das Tool bitte wie folgt aus:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -user User123 -password "**********" -type crp -type adhoccrp

Im Zusammenhang mit Arcserve UDP-Berichten

Dieser Abschnitt enthält das folgende Fehlerbehebungsthema im Zusammenhang mit Arcserve UDP-Berichten:

So zeigen Sie Diagramme zur Arcserve UDP-Berichtsanzeige an

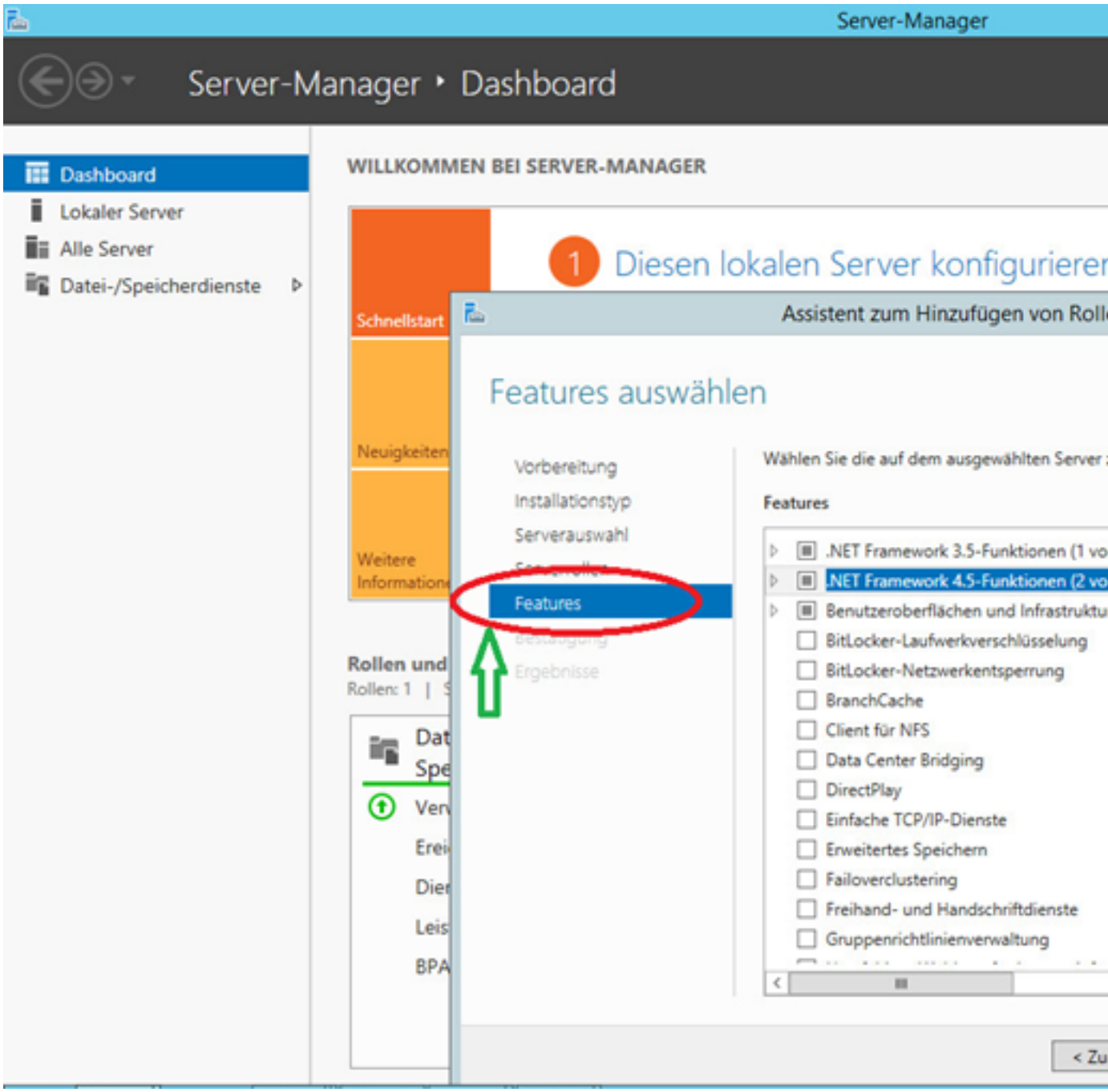
So zeigen Sie Diagramme zur Darstellung von Arcserve UDP-Berichten an

Es kann vorkommen, dass die Diagramme nicht angezeigt werden, wenn Sie sich Berichte ansehen möchten. Erfüllen Sie die folgende Voraussetzung, um das Problem für Windows 2012/2012r2 zu beheben.

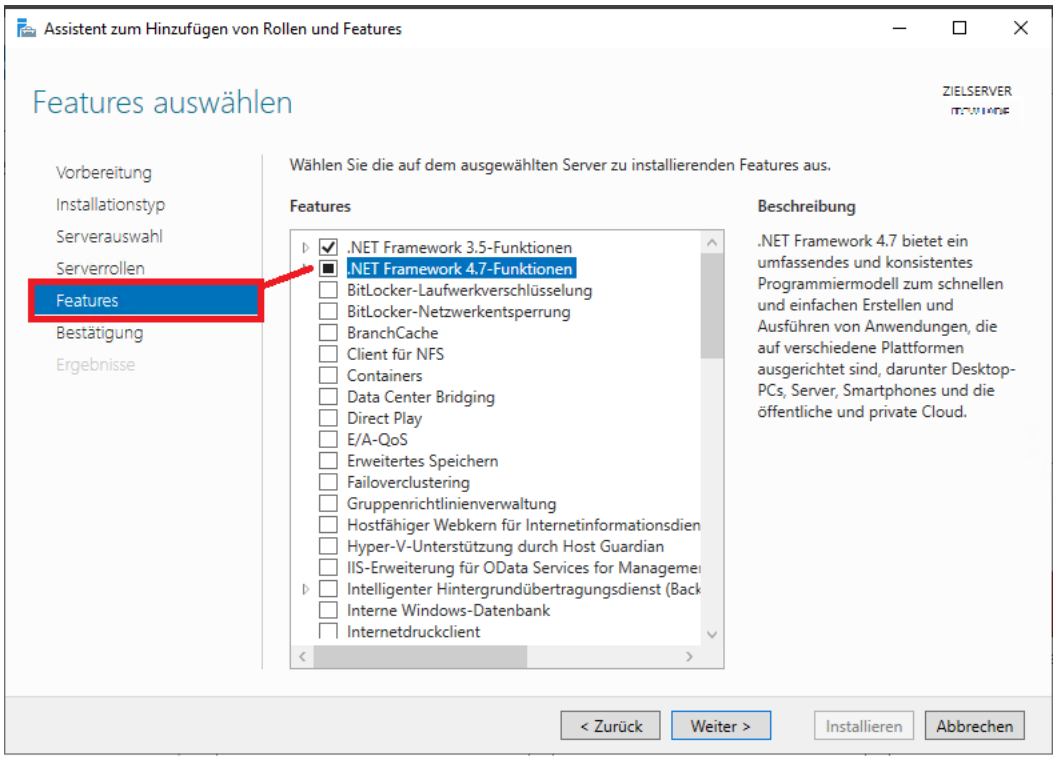
Um die Diagramme anzuzeigen, müssen Sie .NET 3.5 Framework oder eine höhere Version installieren.

Führen Sie zum Installieren von .NET Framework die folgenden Schritte aus:

1. Öffnen Sie den Server-Manager.
2. Klicken Sie im Dashboard in der oberen rechten Ecke auf **Verwalten**, und wählen Sie dann die Option **Rollen und Features hinzufügen** aus.



3. Führen Sie im Dialogfeld "Assistent zum Hinzufügen von Rollen und Features" die folgenden Schritte aus:
    a. Klicken Sie im linken Fensterbereich auf **Features**.
    b. Aktivieren Sie auf der Registerkarte **Features** das Kontrollkästchen **.NET Framework 3.5-Funktionen (installiert)**.
    c. Klicken Sie auf **Weiter**.



4. Klicken Sie im Fenster Installationsauswahl bestätigen auf **Installieren**.

   Die Installation von .NET Framework wird erfolgreich abgeschlossen.

   Wichtig! Wenn die Voraussetzung erfüllt ist und Diagramme mit den Optionen **Drucken/E-Mail/Speichern** dennoch nicht angezeigt werden, überprüfen Sie, ob die DLL-Datei "FCImgExportDll" im Registrierungs-Editor vorhanden ist. Um die DLL zu überprüfen, navigieren Sie zu folgendem Pfad:

   C:\Programme\Arcserve\Unified Data Protection\Management\BIN

   Gehen Sie folgendermaßen vor, um die Registrierung von "FCImgExportDLL.dll" aufzuheben und die Datei erneut zu registrieren:

   1. Navigieren Sie über die Eingabeaufforderung zu folgendem Pfad:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319

   2. Um die Registrierung der DLL aufzuheben, führen Sie den folgenden Befehl aus:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319>Regasm.exe /u "C:\Programme\Arcserve\Unified Data Protection\Management\BIN\FCImgExportDLL.dll"

   3. Um die DLL zu registrieren, führen Sie den folgenden Befehl aus:

C:\Windows\Microsoft.NET\Framework64\v4.0.30319>Regasm.exe "C:\Programme\Arcserve\Unified Data Protection\Management\BIN\FCImgExportDLL.dll" /codebase

Infos zu Microsoft Office 365 Exchange Online

Dieser Abschnitt enthält die folgenden Fehlerbehebungsthemen im Zusammenhang mit Microsoft Office 365 Exchange Online:

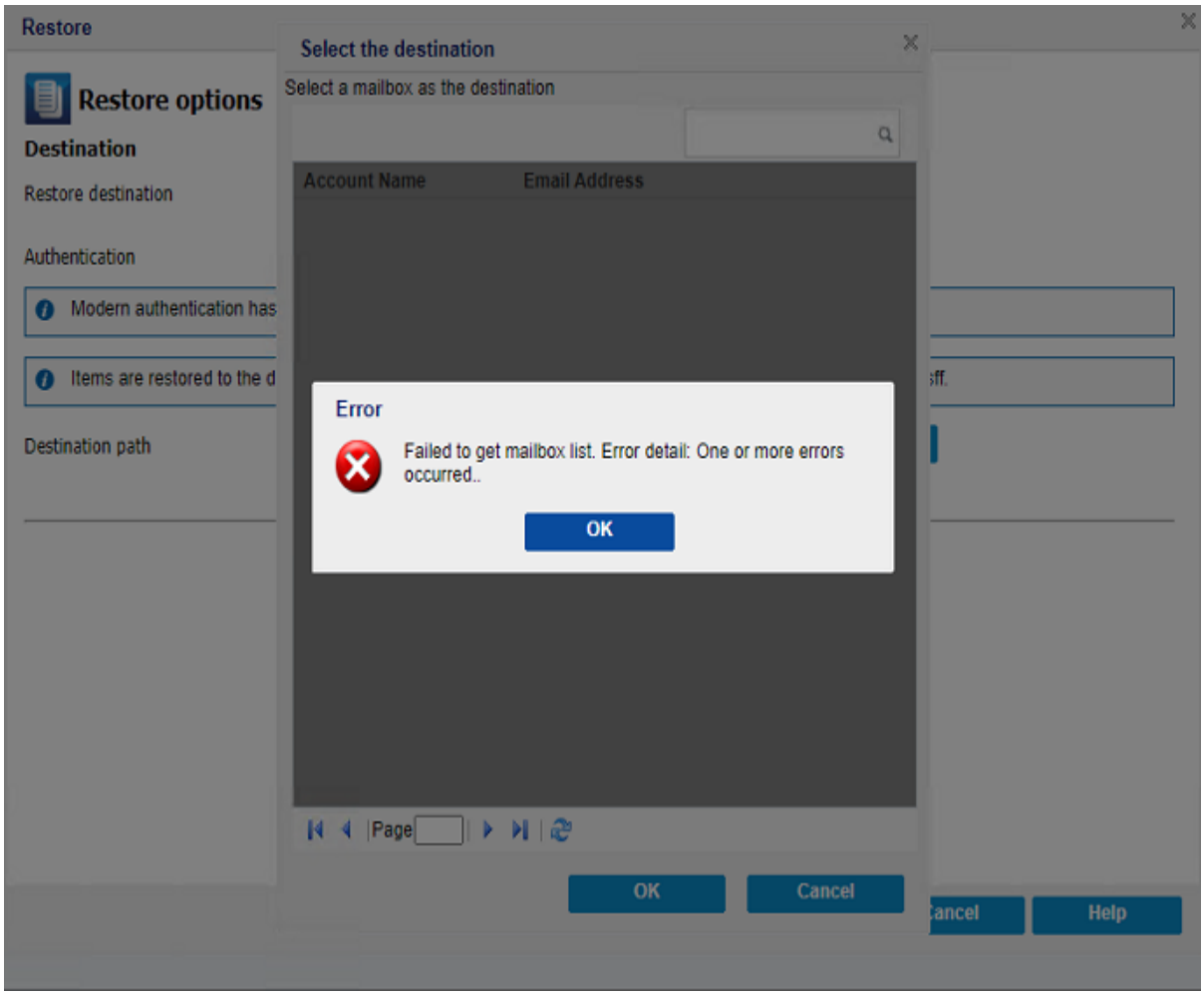
- Die Liste der Postfächer wird im Dialogfeld *Ziel auswählen* nicht angezeigt
- Zugriff oder Berechtigung für Exchange Online-Gruppe verweigert

Die Liste der Postfächer wird im Dialogfeld *Ziel auswählen* nicht angezeigt

Problem:

Beim Definieren der Wiederherstellungsoptionen wird im Dialogfeld "Ziel auswählen" die Liste der Postfächer nicht angezeigt. Wenn Sie die E-Mail-Daten mithilfe der vorhandenen Authentifizierung an einem alternativen Speicherort wiederherstellen und auf die Schaltfläche "Durchsuchen" klicken, um ein Ziel auszuwählen, wird die folgende Fehlermeldung angezeigt:

Die Postfachliste konnte nicht abgerufen werden. Fehlerdetails: Es ist mindestens ein Fehler aufgetreten.



Lösung:

Um diesen Fehler zu beheben, laden Sie ein gültiges Zertifikat unter der angegebenen Anwendungs-ID in das Azure-Portal hoch. Weitere Informationen finden Sie unter Verwenden eines selbstsignierten Zertifikats.

Zugriff oder Berechtigung für Exchange Online-Gruppe verweigert

Problem:

Wenn an die private Teams-Gruppe kein Postfach angehängt ist, wird die folgende Fehlermeldung angezeigt:

Fehler beim Sichern von Postfach [abcd-pvt-group]:Zugriff wurde verweigert

Lösung:

Führen Sie die folgenden Schritte aus, um dieses Problem zu vermeiden:

1. Erstellen Sie ein freigegebenes Postfach:
    a. Gehen Sie zur Microsoft-Anmeldeseite, und melden Sie sich dann beim Microsoft Office 365-Administratorkonto an.
    b. Navigieren Sie zur Seite "Exchange Online Admin Center".
    c. Gehen Sie im Dashboard zu **Empfänger** > **Freigegeben**.
    d. Klicken Sie auf die Schaltfläche **+**, um ein freigegebenes Postfach hinzuzufügen oder zu erstellen.
2. Legen Sie ein Kennwort fest, und weisen Sie die Office 365-Lizenz für das freigegebene Postfach zu:
    a. Kehren Sie zum Office 365-Administratorkonto zurück.
    b. Gehen Sie zu **Benutzer** > **Aktive Benutzer**, und wählen Sie dann das freigegebenes Postfach aus.
    c. Legen Sie das Kennwort fest, und weisen Sie die Office 365-Lizenz zu.
3. Fügen Sie das freigegebene Postfach als Mitglied der privaten Gruppe hinzu:
    a. Navigieren Sie zur Seite "Exchange Online Admin Center", und klicken Sie dann im Dashboard auf **Gruppen**.
    b. Wählen Sie das private Postfach aus, und klicken Sie dann auf **Bearbeiten**.
    c. Fügen Sie das freigegebene Postfach auf der Seite "Einstellungen bearbeiten" als Mitglied der Gruppe hinzu, und klicken Sie dann auf **Speichern**.
4. Fügen Sie das freigegebene Postfach für den globalen Administrator hinzu:
    a. Gehen Sie zum Azure-Portal.
    b. Navigieren Sie zum Abschnitt "Rollen", und wählen Sie dann die Rolle "Globaler Administrator" aus.
    c. Klicken Sie auf **Zuweisungen hinzufügen**, wählen Sie das freigegebene Postfach aus, und klicken Sie dann auf **Speichern**.
5. Aktualisieren Sie in der UDP-Konsole den Knoten mit der E-Mail-Adresse des freigegebenen Postfachs, und führen Sie dann den Sicherungsjob erneut aus.
6. Überprüfen Sie, ob der Sicherungsjob erfolgreich ausgeführt wird.

Kapitel 13: Anhang

In diesem Abschnitt werden die folgenden Themen behandelt:

Befehlszeilentool für Deduplizierungsdatenspeicher

Mit dem Befehlszeilen-Tool (as_gddmgr.exe) können Sie die Datenintegrität auf der Wiederherstellungspunktebene und auf der Datenspeicherebene für Deduplizierungsdatenspeicher überprüfen.

Sie können dieses Tool verwenden, um im Falle eines Hash-Datenbankfehlers eine Hash-Datenbank zu regenerieren. Sie können dieses Tool auch zum Abfragen und Verwalten der Backend-Bereinigung und Wiedergewinnung von Festplattenspeicherplatz für Deduplizierungsdatenspeicher verwenden.

Die Ausgabe des Befehls wird in der Windows-Befehlskonsole angezeigt. Das Tool generiert auch eine Protokolldatei im Ordner "Protokolle". Zum Beispiel ist "as_gddmgr_2014-9-4_11-14-22-655.log" eine Protokolldatei, die alle Details enthält.

Hinweis: Alle Befehle des Befehlszeilen-Tools (as_gddmgr.exe) unterstützen auch GUID-Datenträger. Beispiel: *-scan VerifyAll <Datenspeicher des GUID-Volumes> [-Password <Kennwort des Datenspeichers>]*

Speicherort:

Sie können "as_gddmgr.exe" im Ordner "Bin" des UDP-Installationspfads finden.

Syntax:

as_gddmgr.exe

-Scan CheckRecoveryPoint <data store name> -Node [<All> |<UDP agent node name>] -RecoveryPoint [<Latest>|<recovery point number>] [-LogLevel <n>]

-Scan VerifyRefCount <data store name> [-LogLevel <n>]

-Scan VerifyData <data store name> [-Password <data store password>] [-LogLevel <n>]

-Scan VerifyAll <data store name > [-Password < data store password >] [-LogLevel <n>]

-Scan RebuildHash <data store name> [-NewHashPath <new hash path>] [-LogLevel <n>]

-Scan RebuildHashWithIndexPath <index path> -NewHashPath <new hash path> [-LogLevel <n>]

-Purge Start <data store name>

-Purge Stop <data store name>

-Purge Status <data store name>

-Purge StartToReclaim <data store name>

-Purge StartToIdentifyObsoletedData <data store name>

Optionen:

CheckRecoveryPoint

Aktiviert die angegebenen Wiederherstellungspunkte vollständig und überprüft die Datenintegrität.

Node <All> | <UDP agent node name>

Gibt den Agentenknotennamen an.

RecoveryPoint <All> | <recovery point number>

Gibt den Wiederherstellungspunkt an, bei dem die Integrität überprüft werden soll.

Password <data store password>

Gibt das Datenspeicherkennwort an.

LogLevel <n>

Gibt die Zahl der Protokollebene an.

VerifyRefCount

Scannt Indexdateien und Referenzdateien, um die Referenzanzahl zu überprüfen, die in der Hash-Datenbank aufgezeichnet ist. Bevor Sie diese Option angeben, sollten Sie den Deduplizierungsdatenspeicher manuell anhalten.

VerifyData

Scannt Datendateien und regeneriert dann die Hash-Schlüssel, indem diese mit der Referenzdatei verglichen werden. Bevor Sie diese Option angeben, sollten Sie den Deduplizierungsdatenspeicher manuell anhalten.

VerifyAll

Führt die Vorgänge "VerifyRefCount" und "VerifyData" aus. Bevor Sie diese Option angeben, sollten Sie den Deduplizierungsdatenspeicher manuell anhalten.

RebuildHash

Legen Sie den Namen des Datenspeichers fest, und regenerieren Sie die Hash-Datenbank durch Scannen der Index- und Referenzdateien. Bevor Sie diese Option angeben, sollten Sie den Deduplizierungsdatenspeicher manuell anhalten.

RebuildHashWithIndexPath

Legen Sie den Deduplizierungsindexpfad fest, und regenerieren Sie die Hash-Datenbank durch Scannen der Index- und Referenzdateien. Die Option wird nur verwendet, wenn der Datenspeicher sich nicht auf einem Recovery Point Server befindet.

Start

Ermöglicht die Ausführung der Bereinigung und Wiedergewinnung von Festplattenspeicher parallel zu anderen regulären Arcserve UDP-Jobs. Durch die parallele Ausführung der Bereinigung kann es zu einer Durchsatzverschlechterung bei regulären Arcserve UDP-Jobs kommen.

Anhalten

Verhindert, dass die Bereinigung und die Wiedergewinnung von Festplattenspeicher parallel zu anderen regulären Arcserve UDP-Jobs ausgeführt werden.

Status

Fragt den Status der Bereinigung oder Wiedergewinnung von Festplattenspeicher ab.

StartToReclaim

Aktiviert die Ausführung der Bereinigung und Wiedergewinnung von Festplattenspeicher parallel mit anderen regulären Arcserve UDP-Jobs. Damit wird die Phase der Identifizierung veralteter Daten übersprungen, in der veraltete Datenblöcke lokalisiert werden. Es wird direkt die Phase der Wiedergewinnung von Festplattenspeicherplatz gestartet, in der Speicherplatz freigesetzt wird. Als Nebeneffekt kann diese Option die Effizienz des Prozesses der Wiedergewinnung von Festplattenspeicherplatz beeinträchtigen. Der Grund: Bei der Identifizierung veralteter Daten würden möglicherweise mehr veraltete Datenblöcke in den Datendateien lokalisiert werden, der Wiedergewinnungsprozess jedoch wartet nicht, bis die Identifizierung der veralteten Daten abgeschlossen ist. Durch die parallele Ausführung der Bereinigung kann es außerdem zu einer Durchsatzverschlechterung bei regulären Arcserve UDP-Jobs kommen.

StartToIdentifyObsoletedData

Ermöglicht die Ausführung der Bereinigung und Wiedergewinnung von Festplattenspeicher parallel zu anderen regulären Arcserve UDP-Jobs. Diese Option startet die Phase der Identifizierung veralteter Daten. Die Option ist hilfreich, wenn der Benutzer die Phase der Wiedergewinnung von Festplattenspeicherplatz während ihrer Ausführung überspringen möchte.

Hinweis: Beachten Sie, dass die Ausführung der folgenden Optionen lange dauern kann, da während des Vorgangs viele Dateien im Deduplizierungsdatenspeicher überprüft werden.

- VerifyRefCount
- VerifyData

- VerifyAll
- RebuildHash
- RebuildHashWithIndexPath

Beispiele:

as_gddmgr.exe -Scan CheckRecoveryPoint GDDDataStore1 -Node myComputer -RecoveryPoint 18

as_gddmgr.exe -Scan CheckRecoveryPoint GDDDataStore1 -Node All -RecoveryPoint Latest

as_gddmgr.exe -Scan VerifyRefCount GDDDataStore1

as_gddmgr.exe -Scan VerifyData GDDDataStore1 -Password 123

as_gddmgr.exe -Scan VerifyAll GDDDataStore1

as_gddmgr.exe -Scan RebuildHash GDDDataStore1

as_gddmgr.exe -Scan RebuildHash GDDDataStore1 -NewHashPath C:\NewHashPath

as_gddmgr.exe -Scan RebuildHashWithIndexPath D:\GDDDataStore\Index -NewHashPath D:\NewHashPath

as_gddmgr.exe -Purge Start GDDDataStore1

as_gddmgr.exe -Purge Stop GDDDataStore1

as_gddmgr.exe -Purge Status GDDDataStore1

as_gddmgr.exe -Purge StartToReclaim GDDDataStore1

as_gddmgr.exe -Purge StartToIdentifyObsoletedData GDDDataStore1

So zeigen Sie die Option "Überprüfung der Wiederherstellungspunkte" an

Ab der Version Arcserve UDP 7.0 ist die Funktion zur Überprüfung von Wiederherstellungspunkten standardmäßig im Planassistenten ausgeblendet. Es wird empfohlen, den Assure Recovery-Task zu verwenden, um mögliche Datenprobleme zu erkennen. Es wird empfohlen, den Assure Recovery-Task zu verwenden, um mögliche Datenprobleme zu erkennen. Weitere Informationen finden Sie unter Konfigurieren von Assured Recovery. Bei Bedarf können Sie diese Option weiterhin verwenden, um die Datenprüfung und -anzeige im Planassistenten durchzuführen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der UDP-Konsole an.
2. Navigieren Sie zum Installationsordner der UDP-Konsole. Beispiel: *C:\Programme\Arcserve\Unified Data Protection\Management\Configuration*.
3. Öffnen Sie die Datei ConsoleConfiguration.xml mit einem Texteditor.
4. Suchen Sie im Abschnitt <TimeoutConf> den folgenden Text:

   <recoveryPointCheck>FALSE</recoveryPointCheck>
5. Ändern Sie den Wert von False auf True.
6. Speichern Sie die Konfigurationsdatei und beenden Sie den Editor.
7. Starten Sie den Verwaltungsdienst der UDP-Konsole neu, damit die Einstellung wirksam wird.

   Hinweis: Die Arcserve UDP Version wurde von der Vorgängerversion aktualisiert und diese Option ist bereits in einem Plan ausgewählt und wird standardmäßig nicht ausgeblendet.

   Mithilfe dieser Option können Sie Datenbeschädigungsprobleme ermitteln, indem Sie das Dateisystem der Volumes überprüfen. Wenn der Sicherungsauftrag abgeschlossen ist, mountet Arcserve UDP den Wiederherstellungspunkt und führt den Befehl chkdsk Windows aus. Wenn der chkdsk-Befehl einen Fehler erkennt, wird der nächste Sicherungsjob in einen Überprüfungssicherungsjob konvertiert. Diese Option gilt sowohl für VMware- und Hyper-V-VMs mit Windows-Gastbetriebssystem. Beachten Sie folgende Hinweise, bevor Sie diese Option aktivieren:

   - Die folgenden Volume-Typen werden nicht unterstützt und werden beim **Recovery Point Check** übersprungen:
     - Das Volume mit einem anderen Dateisystem als NTFS
     - Das Volume vom Typ mit verteilter Parität

- Das Volume, das sich im Speicher-Pool befindet

- Der chkdsk-Befehl kann nicht alle Dateisystemprobleme erkennen. Die Überprüfung des Wiederherstellungspunktes ist möglicherweise erfolgreich, aber der Wiederherstellungspunkt kann dennoch beschädigt sein.
- Abhängig von der Größe des Dateisystems des Gastbetriebssystems kann die Ausführung des chkdsk-Befehls längere Zeit in Anspruch nehmen. Chkdsk nutzt eine große Menge des Systemspeichers des Sicherungs-Proxy-Servers und wirkt sich so auf die Performance des Proxy-Servers aus. Aus diesem Grund wird für den Abschluss des Sicherungsjobs mehr Zeit benötigt. *Im schlimmsten Fall wird der Systemspeicher des Sicherungs-Proxy-Servers überlastet, sodass der Server möglicherweise nicht mehr reagiert, vor allem dann, wenn viele Sicherungsjobs gleichzeitig ausgeführt werden.* Die Prüfung des Wiederherstellungspunkts selbst kann die Verwendung von Systemspeicher überwachen, und wenn die Speicherverwendung einen Schwellenwert erreicht, unterbricht sich die Prüfung des Wiederherstellungspunkts selbst für einige Zeit und gibt Systemspeicher frei. Es empfiehlt sich jedoch, diese Option zu deaktivieren, es sei denn, dies ist erforderlich oder Sie verfügen über einen leistungsstarken Sicherungs-Proxy-Server. Alternativ können Sie die Last auf mehrere Proxy-Servern verteilen, indem Sie mehrere Pläne erstellen und in jedem Plan verschiedene Proxyserver angeben.
- Wenn die Sicherung absturzkonsistent ist, erkennt chkdsk mit hoher Wahrscheinlichkeit Probleme (aufgrund der Gegebenheiten einer absturzkonsistenten Sicherung). Aktivieren Sie als Best Practice diese Option für eine absturzkonsistente Sicherung.
- Wenn Sie die Überprüfung des Wiederherstellungspunktes aktivieren möchten, jedoch den nächsten Sicherungsjob nicht in einen Überprüfungssicherungsjob konvertieren möchten, erstellen Sie einen DWORD-Wert mit dem Namen "CheckRecoveryPointIgnoreError" in der Registrierung des Proxyservers, und legen Sie den DWORD-Wert auf 1 fest. Erstellen Sie den DWORD-Wert an folgender Position:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

  Der DWORD-Wert gilt für alle Sicherungsjobs, die auf dem aktuellen Proxyserver ausgeführt werden. Wenn Sie das Verhalten eines bestimmten virtuellen Rechners steuern möchten, können Sie den Wert an folgender Position festlegen:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM-GUID>

Hinweis: Wenn Sie den Registry-Key zur Registry sowohl auf VM- als auch Proxy-Ebene hinzufügen, besitzt die Einstellung im Registry auf VM-Ebene Priorität über die Einstellung in der Registry auf Proxy-Ebene.

- Wenn der Sicherungsjob fehlschlagen soll, nachdem die Prüfung des Wiederherstellungspunkts ein Problem festgestellt hat (damit Sie sofort über das Problem informiert werden), erstellen Sie einen DWORD-Wert mit dem Namen "CheckRecoveryPointDontFailJob" in der Registrierung des Proxy-Servers und legen Sie den DWORD-Wert auf 0 fest. Erstellen Sie den DWORD-Wert an folgender Position:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

  Der DWORD-Wert gilt für alle Sicherungsjobs, die auf dem aktuellen Proxyserver ausgeführt werden. Wenn Sie das Verhalten eines bestimmten virtuellen Rechners steuern möchten, können Sie den Wert an folgender Position festlegen:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM GUID>.

  Hinweis: Wenn Sie den Registry-Key zur Registry sowohl auf VM- als auch Proxy-Ebene hinzufügen, besitzt die Einstellung im Registry auf VM-Ebene Priorität über die Einstellung in der Registry auf Proxy-Ebene.

So wenden Sie eine andere VDDK-Version als die in Arcserve UDP integrierte Version an

VMware Virtual Disk Development Kit (VDDK) 6.7.1 ist in Arcserve UDP 7.0 integriert. Gleichzeitig ist Arcserve UDP 7.0 mit VDDK 5.5 kompatibel. Wenn Sie VSB/Instant VM/Assured Recovery zu VMware 5.0 oder 5.1 durchführen möchten, verwenden Sie VDDK 5.5 anstelle von VDDK 6.7.1.

Wichtig! Arcserve ist nur für VDDK 6.7.1 und 5.5 zertifiziert. Andere Versionen von VDDK sind nicht sicher mitArcserve UDP Version 7.0 kompatibel.

Gehen Sie wie folgt vor, um das VDDK manuell zu ändern:

- Ändern des VDDK für eine Virtual Standby-Sicherung (VSB)
- Ändern des VDDK für eine hostbasierte Sicherung (HBBU)

Manuelles Ändern des VDDK für eine Virtual Standby-Sicherung (VSB)

Sie können die VDDK-Version manuell ändern oder mithilfe einer Windows-Batchdatei. In diesem Artikel finden Sie Anleitungen für beide Optionen.

Besondere Aspekte:

- Wenn Sie Instant VM oder einen Assured Recovery-Test ausführen, müssen Sie diese Schritte auf dem Wiederherstellungsserver/Proxy-Server durchführen.
- Bei VSB unter VMware müssen Sie einen dedizierten Agentenserver als VSB-Monitor verwenden und den VSB-Task im Proxy-Modus konfigurieren. Anschließend müssen Sie VDDK auf dem Hostserver des VSB-Monitors manuell auf Version 5.5 umstellen.
- Wenn Sie den VSB-Task in einem MSP-Plan oder einem standortübergreifenden Plan konfigurieren, müssen Sie VDDK auf dem RPS ändern, da es keinen Überwachungsserver gibt. Daher ist dieser RPS nicht als Proxy-Server für hostbasierte agentenlosen Sicherungstasks verfügbar.

Gehen Sie wie folgt vor, um das VDDK manuell zu ändern:

1. Melden Sie sich mit einem Administratorkonto oder einem Konto mit Administratorrechten bei dem Computer an, auf dem der Arcserve UDP-Agent installiert ist.
2. Benennen Sie den Ordner *VDDK* in "VDDK6.7" um.

3. Benennen Sie den Ordner *VDDK5.5* an folgendem Speicherort in "VDDK" um:

   C:\Programme\Arcserve\Unified Data Protection\engine\BIN

   Hinweis: Der Speicherort des Ordners "BIN" kann je nach dem Installationsort des Arcserve UDP-Agenten variieren.

4. Führen Sie den folgenden Befehl aus, um den Status des Diensts zu überprüfen:

   Hinweis: Sie dürfen den Dienst erst löschen, wenn er nicht mehr ausgeführt wird.

   sc query vstor2-mntapi20-shared

   Existiert der Dienst nicht, löschen Sie ihn wie im nächsten Schritt beschrieben. Wenn der Dienst ausgeführt wird, müssen Sie ihn vor dem Löschen zunächst mit dem folgenden Befehl anhalten:

   sc stop vstor2-mntapi20-shared

5. Führen Sie den folgenden Befehl aus, um den Dienst zu löschen:

   sc delete vstor2-mntapi20-shared

6. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Dienst gelöscht wurde:

   sc query vstor2-mntapi20-shared

   Hinweis: Sollte der Status des Diensts "STOP_PENDING" sein, müssen Sie den Rechner neu starten.

   Gehen Sie wie folgt vor, um die VDDK-Version mithilfe einer Windows-Batchdatei zu ändern:

1. Melden Sie sich mit einem Administratorkonto oder einem Konto mit Administratorrechten bei dem Computer an, auf dem der Arcserve UDP-Agent installiert ist.
2. Starten Sie das Hilfstool *ChangeToVDDK55.bat* an dem folgenden Standardspeicherort:

   C:\Programme\Arcserve\Unified Data Protection\engine\BIN

   Hinweis: Der Speicherort des Ordners "BIN" kann je nach dem Installationsort des Arcserve UDP-Agenten variieren.

   VDDK 5.5 wird installiert, nachdem ein neuer Job gestartet wurde.

Manuelles Ändern des VDDK für eine hostbasierte Sicherung (HBBU)

Sie können das VDDK für eine hostbasierte Sicherung (HBBU) manuell ändern.

Ändern von VDDK 6.7 für die Sicherung von vSphere 5.5 oder höher:

Gehen Sie wie folgt vor:

1. Laden Sie VDDK von der VMware-Website herunter.
2. Extrahieren Sie alle Dateien in einen temporären Ordner.
3. Suchen Sie den Ordner mit dem Namen ***bin*** unter dem folgenden Pfad und benennen Sie den Ordner um (z. B. *bin_alt*):

   <Arcserve UDP-Installationspfad>\Engine\BIN\VDDK\BIN\VDDK64\

   Beispiel: C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\VDDK\BIN\VDDK64\
4. Suchen Sie den Ordner mit dem Namen ***bin*** unter den extrahierten Dateien im temporären Ordner und kopieren Sie ihn in den folgenden Pfad:

   <Arcserve UDP-Installationspfad>\Engine\BIN\VDDK\BIN\VDDK64\.

   Das VDDK wird erfolgreich geändert.

Ändern von VDDK 5.5 für die Sicherung von vSphere 5.0 und 5.1:

Gehen Sie wie folgt vor:

1. Laden Sie VDDK von der VMware-Website herunter.
2. Extrahieren Sie alle Dateien in einen temporären Ordner.
3. Suchen Sie den Ordner mit dem Namen ***bin*** unter dem folgenden Pfad und benennen Sie den Ordner um (z. B. *bin_alt*):

   <Arcserve UDP-Installationspfad>\Engine\BIN\VDDK5.5\BIN\VDDK64\

   Beispiel: C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\VDDK5.5\BIN\VDDK64\
4. Suchen Sie den Ordner mit dem Namen ***bin*** unter den extrahierten Dateien im temporären Ordner und kopieren Sie ihn in den folgenden Pfad:

   <Arcserve UDP-Installationspfad>\Engine\BIN\VDDK5.5\BIN\VDDK64\.

   Das VDDK wird erfolgreich geändert.

So migrieren Sie Arcserve D2D r16.5-Sicherungsdaten von zwei Servern mit identischem Hostnamen zu RPS-Datenspeicher

Sie haben zwei Server mit identischem Hostnamen aber anderem FQDN-DNS-Namen, und Sie nutzen Arcserve D2D r16.5 zum Schutz. Wenn Sie die Daten zu einem Arcserve UDP-RPS-Datenspeicher migrieren möchten, gehen Sie folgendermaßen vor:

1. Beenden Sie den Arcserve D2D-Dienst auf Server 1.
2. Migrieren Sie Daten von Server 1 zum RPS-Datenspeicher unter Verwendung des Arcserve UDP-Jumpstart-Jobs.
3. Aktualisieren Sie den Arcserve UDP-Agenten auf Server 1.
4. Erstellen Sie einen Plan (oder verwenden Sie einen vorhandenen Plan) zum Schutz von Server 1, und wählen Sie den gleichen RPS-Datenspeicher als Sicherungsziel aus.
5. Stellen Sie den Plan bereit.
6. Beenden Sie den Arcserve D2D-Dienst auf Server 2.
7. Migrieren Sie Daten von Server 2 zum RPS-Datenspeicher unter Verwendung des Arcserve UDP-Jumpstart-Jobs.
8. Navigieren Sie auf dem RPS-Server zum Sicherungszielordner des Datenspeichers, und suchen Sie den Ordner für Server 2, indem Sie nach dem Hostnamen von Server 2 suchen.

   Beispiel: Wenn der Hostname des Server 2 "MyServer2" ist, ist der Ordnername "MyServer2".
9. Aktualisieren Sie den Arcserve UDP-Agenten auf Server 2.
10. Starten Sie den UDP-Agent auf Server 2, wenn er noch nicht läuft.
11. Öffnen Sie die Registrierung (auf einem bestimmten Server?), und suchen Sie nach folgendem Schlüssel:

    HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine"
12. Notieren Sie den Wert von "NodeID".

    Der Wert ist eine eindeutige ID im GUID-Format, wie z. B. "e856e0ba-66d7-4da5-8b98-2250173e349a".
13. Suchen Sie auf dem RPS-Server nach dem Ordner des Sicherungsziels von Server 2, und aktualisieren Sie die Knoten-ID mit **<folder_name>[NodeID value]**.

Beispiel: MyServer2[e856e0ba-66d7-4da5-8b98-2250173e349a]

14. Erstellen Sie einen Plan (oder verwenden Sie einen vorhandenen Plan) zum Schutz von Server 2, und wählen Sie den gleichen RPS-Datenspeicher als Sicherungsziel aus.
15. Stellen Sie den Plan bereit.

So stellen Sie Arcserve UDP in Microsoft Azure bereit

Sie können Arcserve UDP in Microsoft Azure bereitstellen, wenn Sie Arcserve Unified Data Protection v6.5 Update 2 oder höher verwenden. Die Funktion ist hilfreich, wenn Sie die Virtual Standby-Rechner in Microsoft Azure bereitstellen und Daten schützen möchten. Ein Virtual Standby-Rechner wird in Microsoft Azure erstellt und basiert auf mit Wiederherstellungspunkten zusammenhängenden Daten aus der lokalen Sicherung.

Virtual Standby konvertiert die Wiederherstellungspunkte in Formate für virtuelle Rechner in Microsoft Azure und bereitet einen Snapshot vor, damit die Daten bei Bedarf auf einfache Weise wiederhergestellt werden können.

Diese Funktion deckt auch die Hochverfügbarkeitsfunktion ab und stellt sicher, dass der virtuelle Rechner sofort übernehmen kann, wenn der Quellrechner ausfällt. Der Virtual Standby-Rechner wird erstellt, indem Wiederherstellungspunkte in das Azure-Format für virtuelle Rechner konvertiert werden.

Der nächste Schritt?

1. Grundlegendes zum Prozessablauf
2. Empfehlungen
3. Hinweise
4. Planen der Bereitstellung
5. Bereitstellen von Arcserve UDP in Microsoft Azure

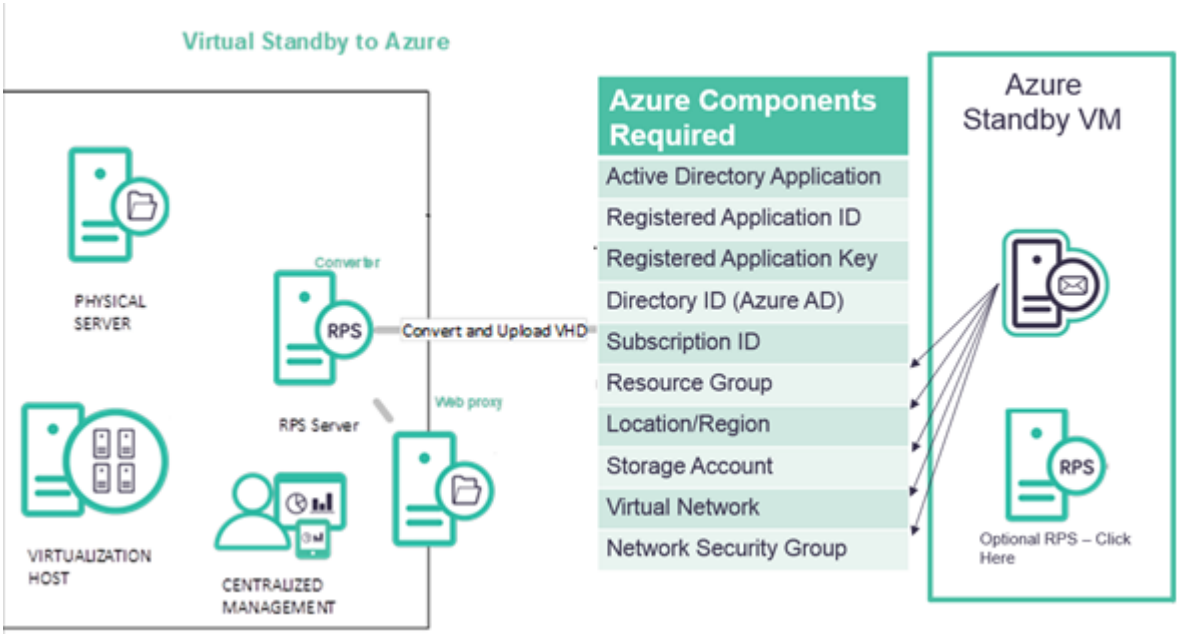
Grundlegendes zum Prozessablauf

Arcserve UDP unterstützt die Virtual Standby-VMs im Microsoft Azure. Wenn Sie die Datenschutzlösung bereits lokal bereitgestellt haben, können Sie Arcserve UDP in Microsoft Azure bereitstellen.

Die lokale Lösung besteht aus der Arcserve UDP-Konsole und Arcserve UDP-Recovery Point-Server (RPS). Sie können Windows-Systeme auf lokalen RPS sichern. Sie können einen Plan in der Arcserve UDP-Konsole erstellen, um eine Sicherung der Daten auf lokalem RPS und anschließend den Virtual Standby-Task durchzuführen.

Die Virtual Standby-Funktion überwacht das Heartbeat-Signal des Quellknotens. Wenn der Quellknoten ausfällt, übernimmt der virtuelle Rechner in Azure.

Das folgende Bild veranschaulicht den Prozessablauf für Arcserve UDP für Microsoft Azure:



Hinweise

Beachten Sie die folgenden Hinweise, bevor Sie Arcserve UDP in Microsoft Azure bereitstellen:

Hinweis: Weitere Informationen zu den Best Practices finden Sie unter Bereitstellen von Arcserve UDP für Microsoft Azure.

- Eine einzelne VHD-Datei darf in Microsoft Azure nicht einen Systemdatenträger aufweisen, der größer als 2048 GB ist, und darf nicht einen Datenträger aufweisen, der größer als 4095 GB ist. In Arcserve UDP Virtual Standby darf die Quelle nicht einen Systemdatenträger mit mehr als 2048 GB und darf nicht einen Datenträger mit mehr als 4095 GB aufweisen.
- Microsoft Azure VM und Arcserve UDP VSB unterstützt nur Windows 2008 R2 oder höher.
- Arcserve UDP unterstützt das Erstellen klassischer virtueller Computer als Standby-VM nicht.
- Bei Microsoft Azure VM müssen sich das System-Volume und das Start-Volume auf demselben Datenträger befinden.
- Microsoft Azure unterstützt keine Starts vom UEFI-System.

- Microsoft Azure unterstützt den Quellcomputer nicht als Hyper-V-Server.
- Arcserve UDP Virtual Standby unterstützt keine dynamischen Systemdatenträger für den Quellcomputer.
- Arcserve UDP in Microsoft Azure unterstützt nur Windows-Knoten.

Planen der Arcserve UDP-Bereitstellung in Microsoft Azure

Sie müssen die folgenden Tasks abschließen, bevor Sie Arcserve UDP in Microsoft Azure bereitstellen:

1. Überprüfen der Voraussetzungen
2. Vorbereiten eines Cloud-Kontos in Microsoft Azure
3. Vorbereiten von Microsoft Azure-Ressourcen

Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen für Arcserve UDP und Recovery Point-Server, bevor Sie Arcserve UDP in Microsoft Azure bereitstellen:

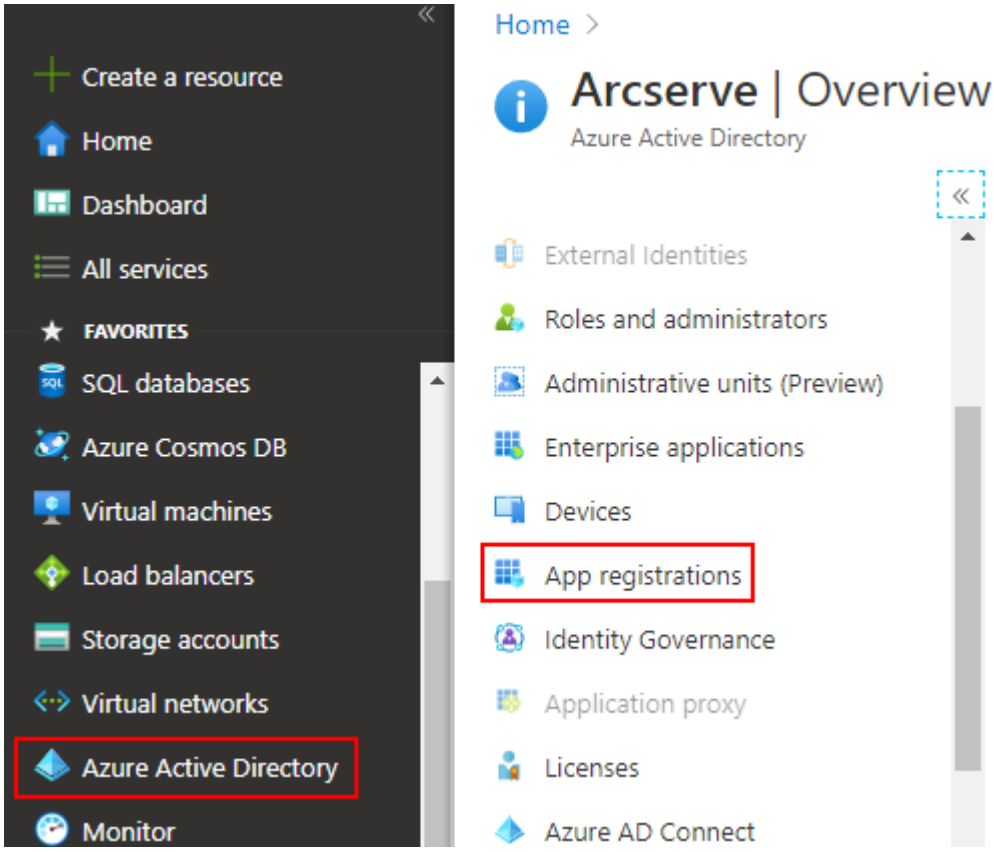
- Überprüfen Sie die Kompatibilitätsmatrix auf unterstützte Betriebssysteme, Datenbanken und Browser.
- Bereiten Sie die Server im Vorfeld auf die Bereitstellung als Arcserve UDP-Konsole und Recovery Point-Server vor.
- Die Server müssen die Systemanforderungen für die einzelnen Komponenten erfüllen:
  - **Server:** Windows 2008 R2 Server oder höher
  - **CPU:** Mindestens 4 Kerne und 2,7 GHz
  - **Speicherplatz:** 40 GB für die Installation des Betriebssystems
  - **RAM:** Mindestens 8 GB
  - **Sicherungsspeicher für Recovery Point-Server:** Je nach Größe der Quelldaten

Vorbereiten eines Cloud-Kontos in Microsoft Azure

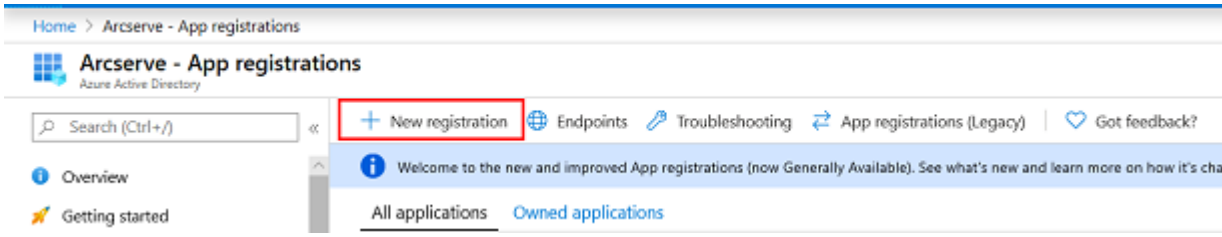
Dieser Abschnitt enthält Informationen zum Erstellen eines Cloud-Kontos in Microsoft Azure.

Gehen Sie wie folgt vor:

1. Gehen Sie folgendermaßen vor, um die Azure Active Directory-Anwendung zu registrieren, die Arcserve UDP für die Kommunikation mit Microsoft Azure verwendet:
   a. Melden Sie sich beim Azure-Portal an.
   b. Wählen Sie im linken Bereich **Azure Active Directory** aus, und klicken Sie dann auf **App-Registrierungen**.

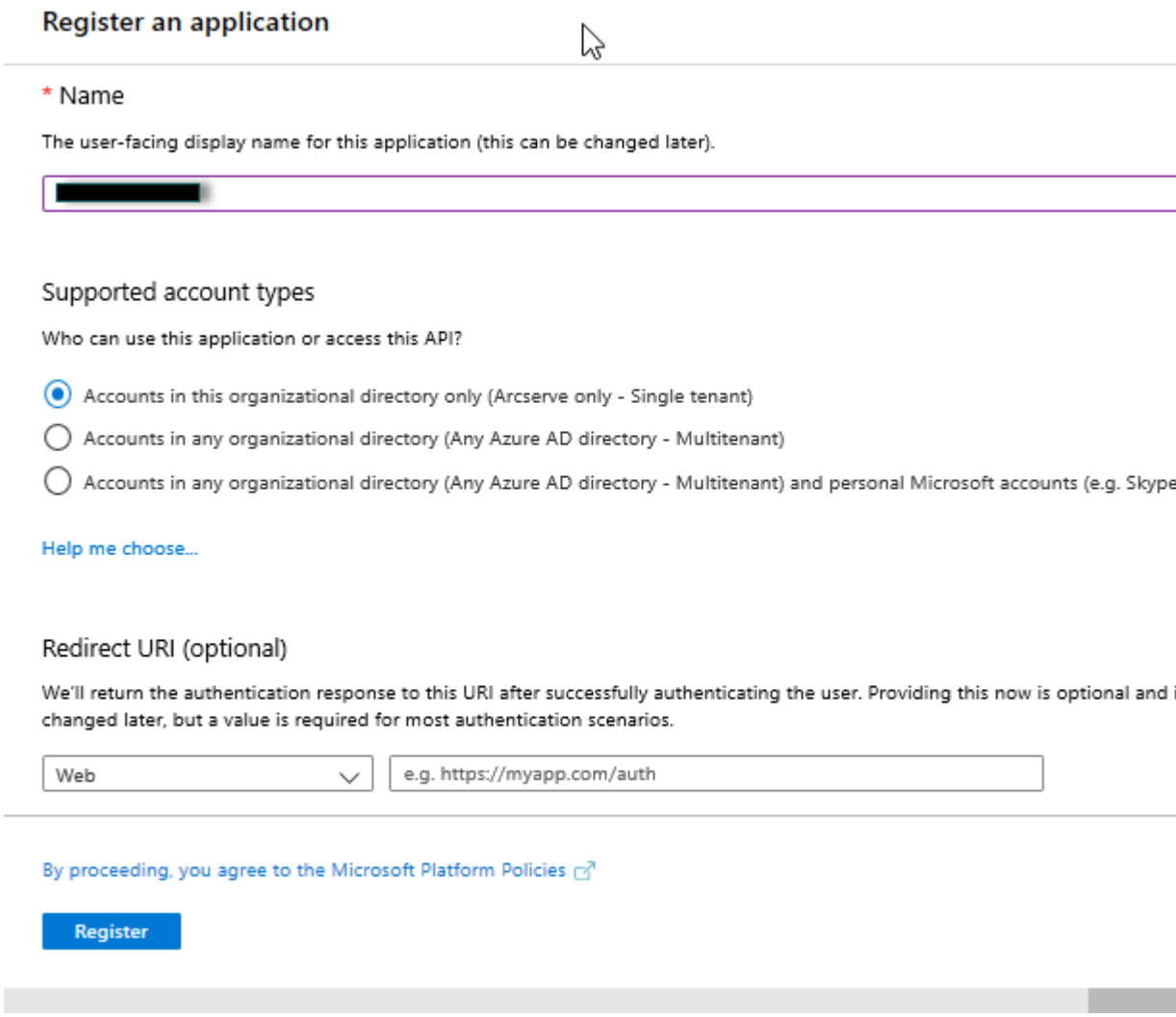


   c. Klicken Sie auf der Seite "Arcserve-App-Registrierungen" auf **Neue Registrierung**.

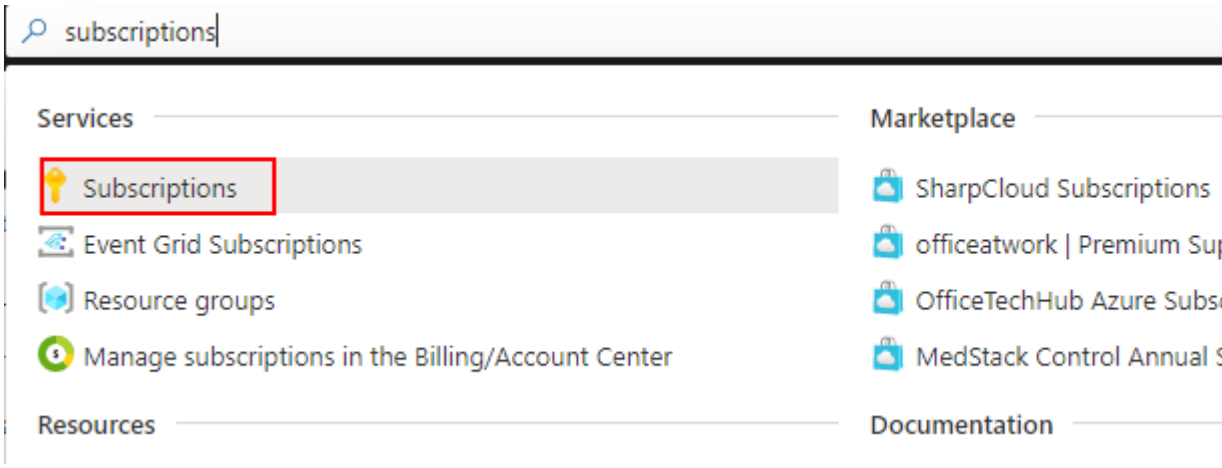


   d. Führen Sie auf der Seite Registrieren einer Anwendung die folgenden Schritte aus, und klicken Sie dann auf **Registrieren**:

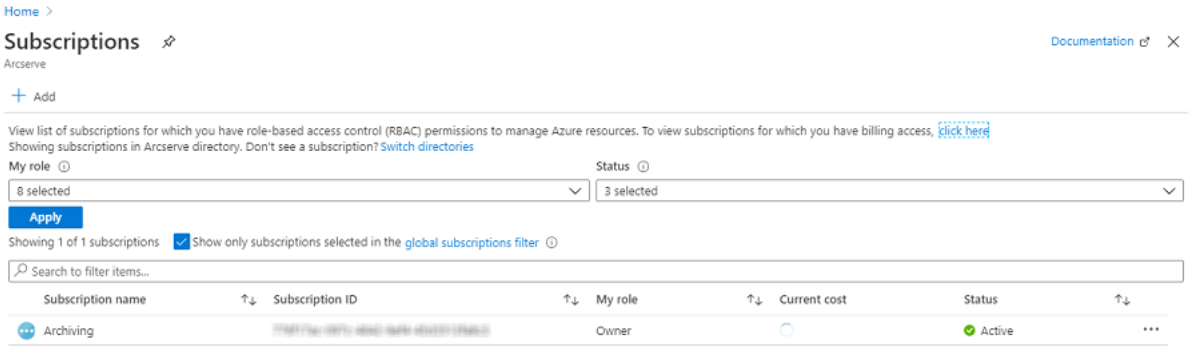
- Name: Geben Sie einen Namen für die Anwendung ein.
- Unterstützte Kontotypen: Wählen Sie einen unterstützten Kontotyp aus, um festzulegen, wer die Anwendung verwenden kann.
- Umleitungs-URI (optional): Wählen Sie **Web oder Öffentlicher Client (Mobilgerät und Desktop)** als Art der Anwendung aus, die Sie erstellen, und geben Sie dann den Umleitungs-URI für Ihre Anwendung ein.



e. Geben Sie in der Suchleiste Abonnements ein, und klicken Sie dann in der Liste auf **Abonnements**.

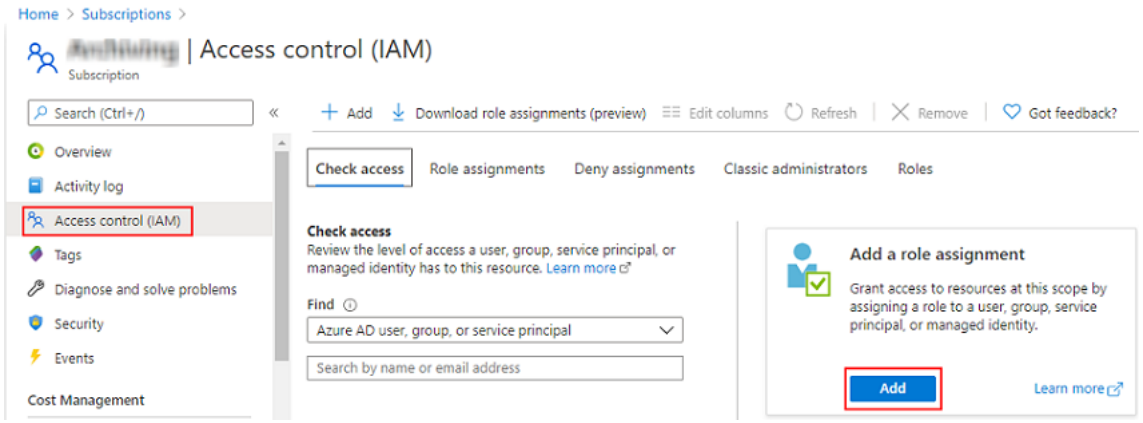


f. Wählen Sie auf den Abonnementseiten das Abonnement für Ihre Anwendung aus.



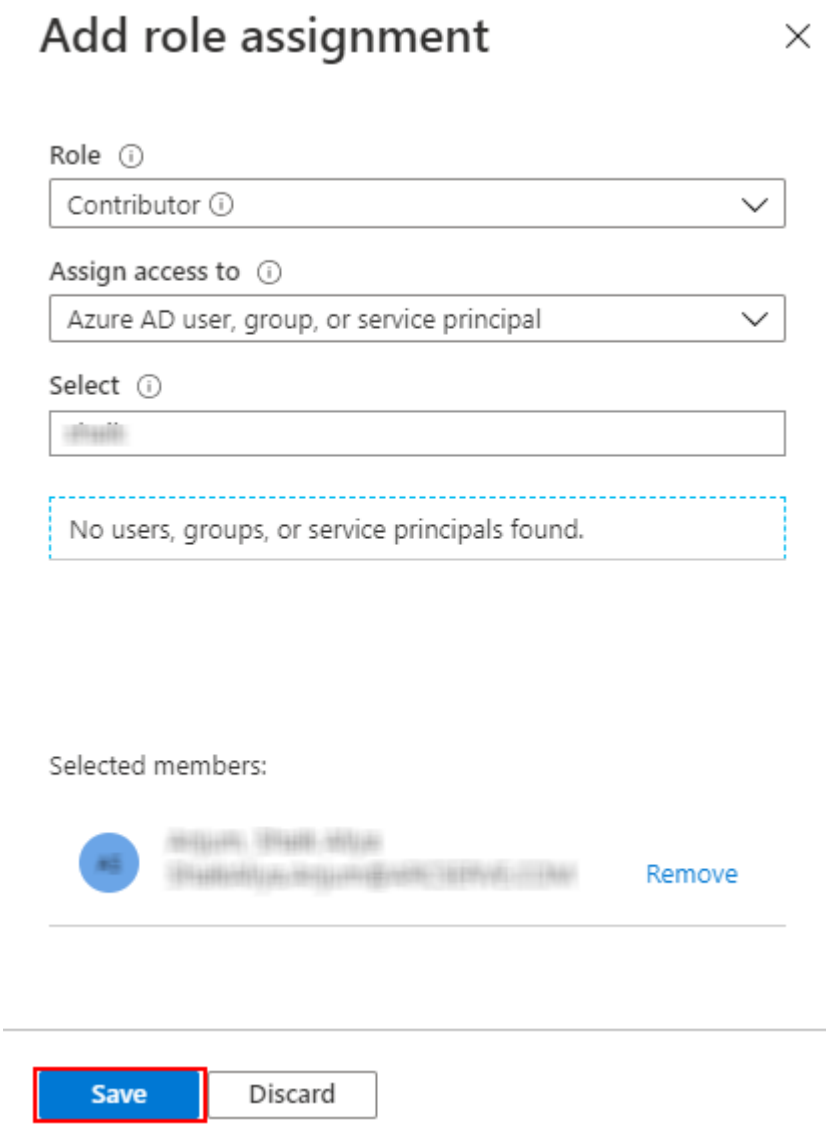
Hinweis: Wenn das erforderliche Abonnement nicht in der Abonnementliste angezeigt wird, wählen Sie den **globalen Filter für Abonnements** aus. Stellen Sie sicher, dass das gewünschte Abonnement für das Portal ausgewählt ist.

g. Gehen Sie von "Abonnements" zu **Zugriffskontrolle (IAM) > Zugriff prüfen**, und klicken Sie im Feld "Rollenzuweisung hinzufügen" auf **Hinzufügen**.



h. Führen Sie auf der Seite "Rollenzuweisung hinzufügen" die folgenden Schritte aus, und klicken Sie dann auf **Speichern**:

- Rolle: Wählen Sie die Rolle aus, die Sie der Anwendung zuweisen möchten.
- Zugriff zuweisen: Standardmäßig beibehalten.
- Auswählen: Standardmäßig werden Azure AD-Anwendungen nicht in den verfügbaren Optionen angezeigt. Um Ihre Anwendung zu suchen, suchen Sie nach dem Namen, und wählen Sie ihn anschließend aus.

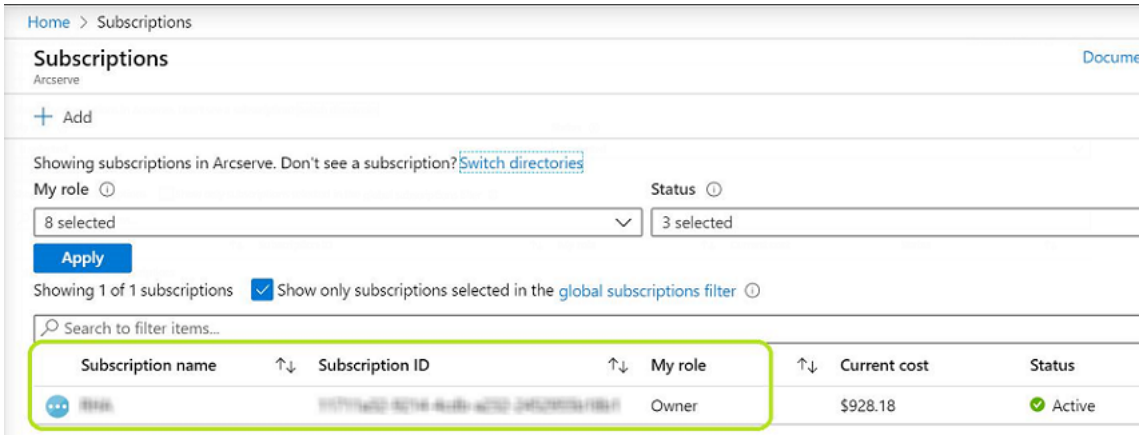


Die Azure Active Directory-Anwendung ist registriert und eine Rolle wurde erfolgreich zugewiesen.

Nun können Sie die nächsten Schritte mit der registrierten Anwendung durchführen, um die erforderlichen IDs und Schlüssel zu erhalten.

2. Um die Abonnement-ID[1] zu erhalten, führen Sie die folgenden Schritte aus:
   a. Klicken Sie im linken Navigationsbereich des Azure-Portals auf **Abonnements**.

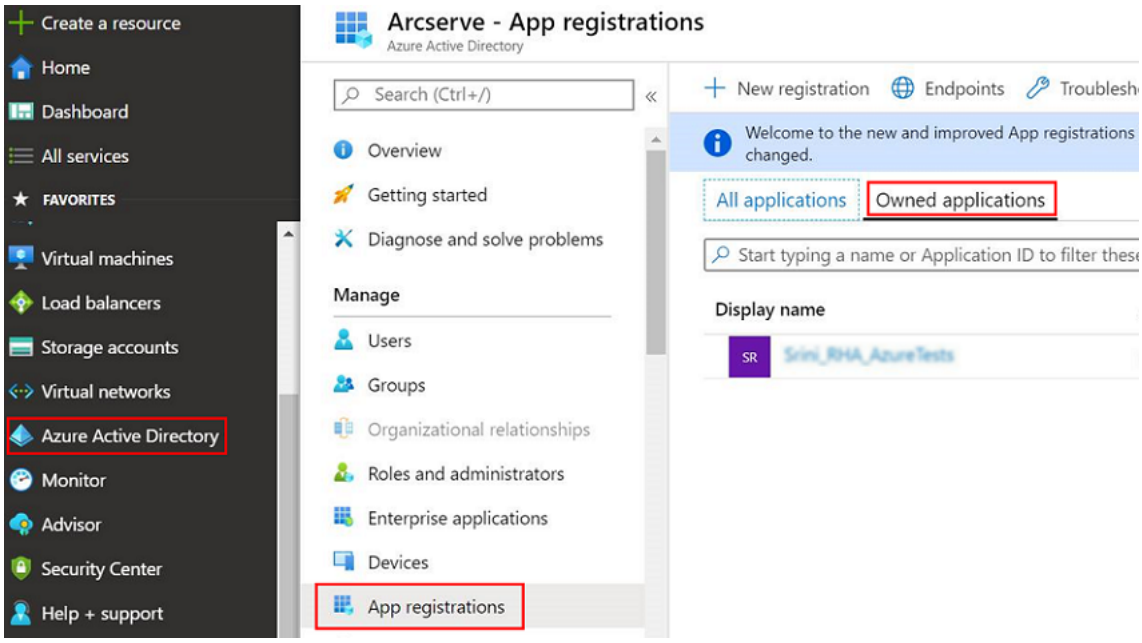
      Die Liste der Abonnements wird zusammen mit der Abonnement-ID angezeigt.



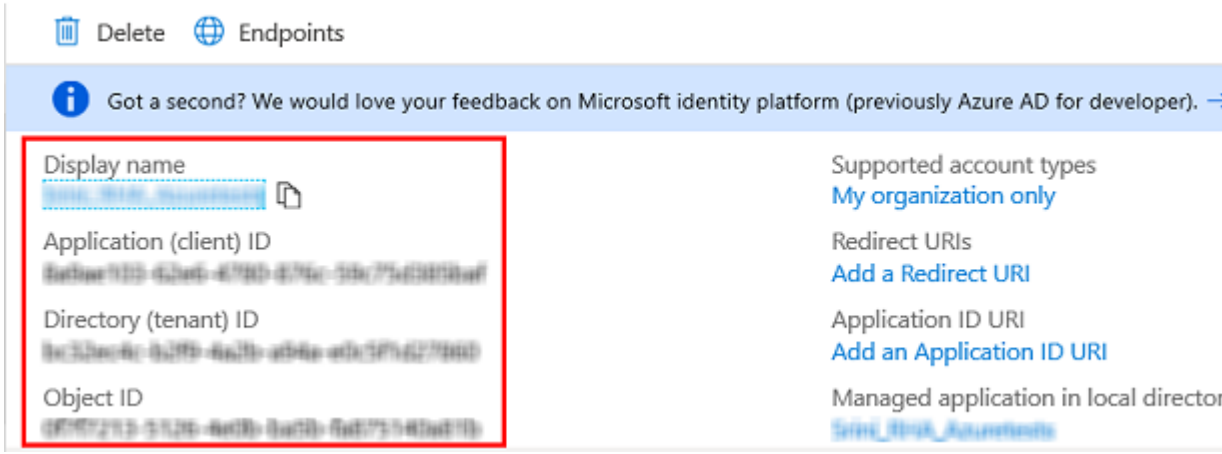
   b. Kopieren und speichern Sie die Abonnement-ID, die beim Hinzufügen des Microsoft Azure Cloud-Kontos in Arcserve UDP verwendet wird.

3. Um die Mandanten-ID[2] und Anwendungs-ID[3] zu erhalten, führen Sie die folgenden Schritte aus:
   a. Navigieren Sie zu **Azure Active Directory** > **App-Registrierungen** > **Anwendungen mit Besitzer**, und wählen Sie dann Ihre Anwendung aus.

[1]Die Abonnement-ID verweist auf eine GUID (Globally Unique Identifier), die Ihr Abonnement eindeutig für die Nutzung von Azure-Diensten identifiziert.
[2]Mandanten-ID verweist auf die ID des Azure Active Directory, wo Sie die Anwendungsregistrierung erstellt haben. Die Mandanten-ID wird in den Azure Active Directory-Eigenschaften als Verzeichnis-ID bezeichnet.
[3]Eine Anwendungs-ID bezieht sich auf eine GUID, die die Registrierung der Anwendung im Azure Active Directory-Mandanten eindeutig identifiziert. Manchmal wird sie auch als Client-ID bezeichnet.



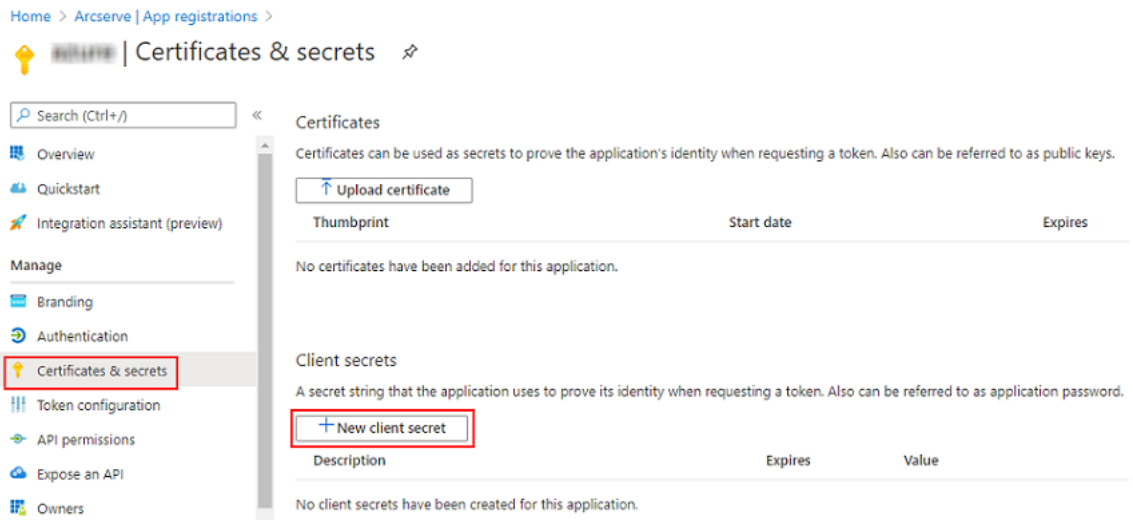
b. Kopieren Sie die ID für die Anwendung (Client) und die ID für das Verzeichnis (Mandant), und speichern Sie sie an einem sicheren Ort.



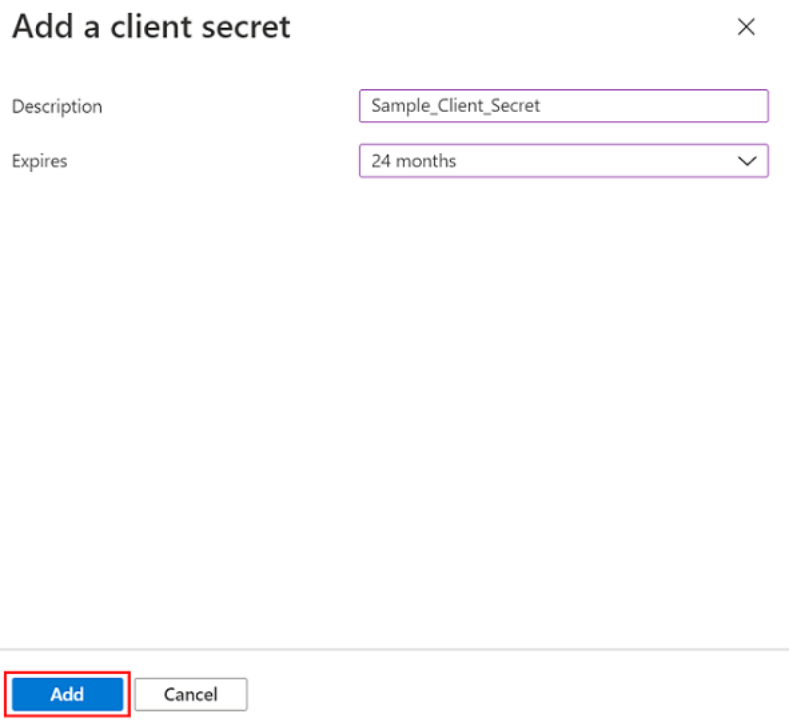
4. Um die Geheimer Client-Schlüssel[1]zu erhalten, führen Sie die folgenden Schritte aus:

   a. Wählen Sie auf der Seite "App-Registrierungen" die Anwendung aus, navigieren Sie im linken Fensterbereich zu **Zertifikate und Schlüssel**, und klicken Sie dann auf **Neuer Client-Schlüssel**, um einen Client-Schlüssel hinzuzufügen.

[1]Der geheime Client-Schlüssel wird in Azure als Authentifizierungsschlüssel bezeichnet.

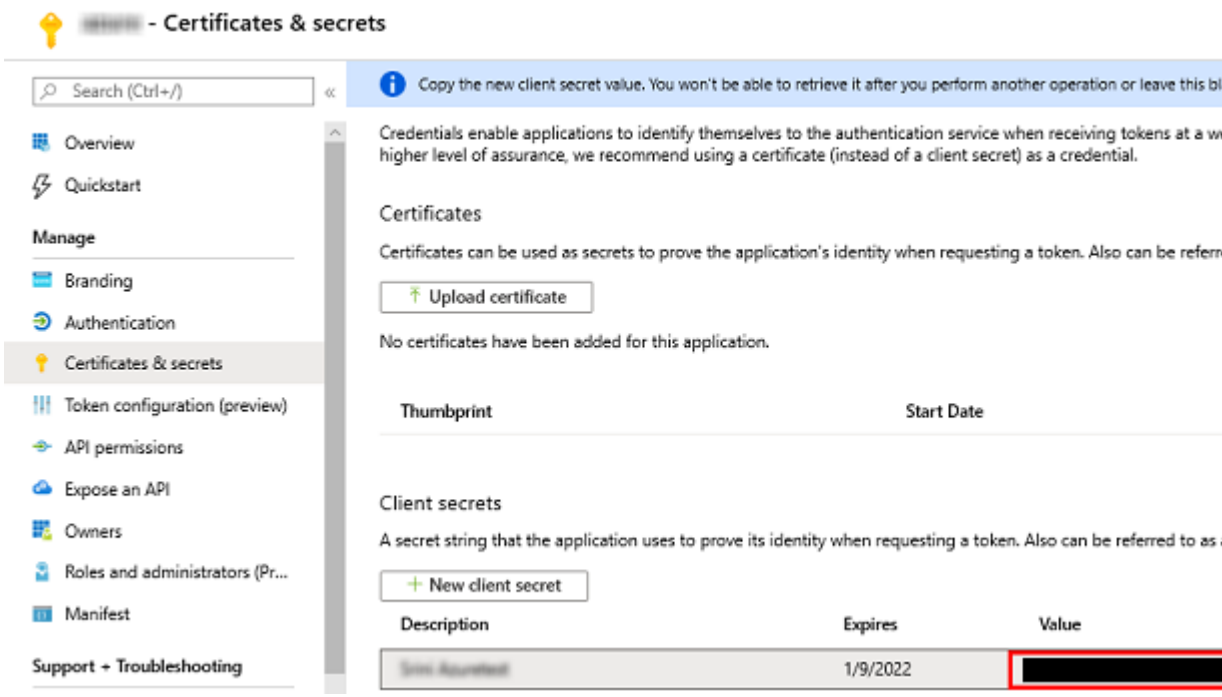


b. Geben Sie auf der Seite "Geheimer Client-Schlüssel" eine Beschreibung ein, wählen Sie bei Bedarf ein Ablaufintervall aus der Dropdown-Liste aus, und klicken Sie dann auf **Hinzufügen**.



Hinweis: Wir empfehlen, die Option **24 Monate** als Ablaufintervall auszuwählen, um zu vermeiden, dass der geheime Client-Schlüssel wiederholt generiert wird.

Der geheime Client-Wert wird angezeigt.



Wichtig! Kopieren und speichern Sie den Wert des geheimen Client-Schlüssels, da Sie ihn später nicht abrufen können. Wenn Sie vergessen haben, den Wert zu speichern, löschen Sie den bestehenden geheimen Client-Schlüssel, und erstellen Sie einen neuen Client-Schlüssel, wie in Schritt 4 erwähnt.

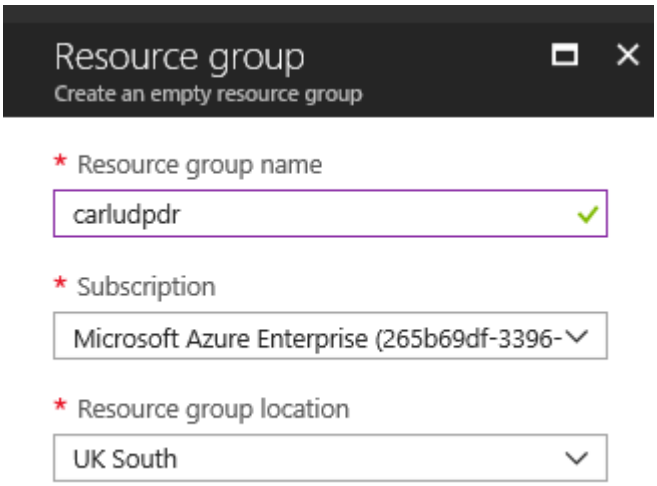
Das Cloud-Konto wurde erfolgreich in Microsoft Azure erstellt.

Vorbereiten von Microsoft Azure-Ressourcen

Bevor Sie ein Cloud-Konto für Microsoft Azure erstellen können, müssen Sie die folgenden Microsoft Azure-Ressourcen erstellen:

1. Gehen Sie wie folgt vor, um eine Ressourcengruppe zu erstellen:
    a. Melden Sie sich beim Azure-Portal mit gültigen Anmeldeinformationen an.
    b. Klicken Sie auf **Hinzufügen**, um eine leere Ressourcengruppe zu erstellen.
    c. Geben Sie einen Namen und Speicherort für die neue Res-

sourcengruppe an, und klicken Sie auf **Erstellen**.



2. Gehen Sie wie folgt vor, um ein Speicherkonto zu erstellen:
    a. Navigieren Sie zu **Speicherkonten**, und klicken Sie auf **Hinzufügen**.
    b. Geben Sie Folgendes an:

    Hinweis: Stellen Sie sicher, die sich das Speicherkonto, das virtuelle Netzwerk und die Netzwerk-Sicherheitsgruppe der Standby-VM am selben Standort befinden.

    Name

    Gibt den Namen des Speicherkontos an.

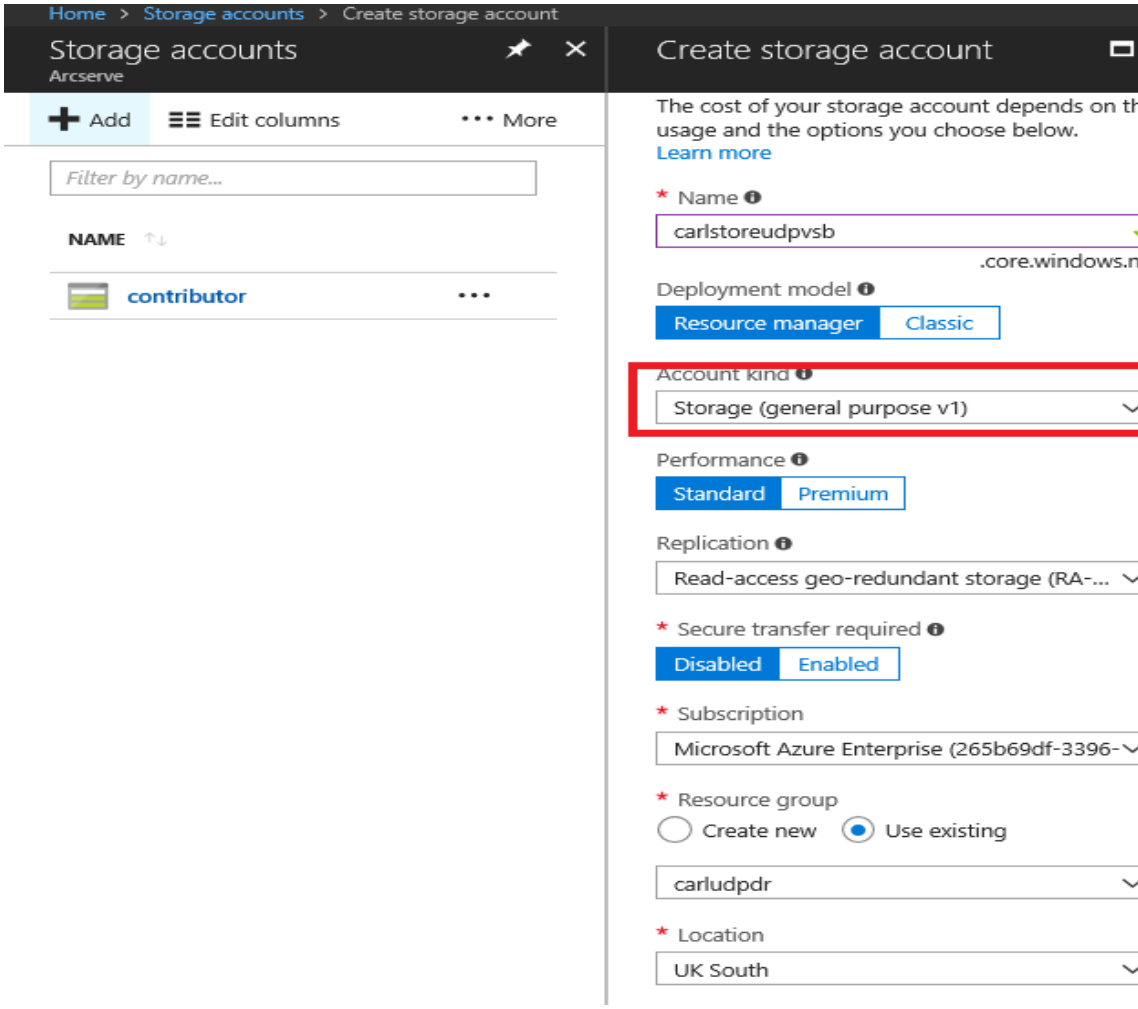
    Bereitstellungsmodell

    Wählen Sie das gewünschte Bereitstellungsmodell.

    Kontoart

    Geben Sie **Speicher (allgemein v1)** oder **SpeicherV2 (allgemein v2)** als Kontoart an.

c. Geben Sie bei Bedarf weitere Informationen an, und klicken Sie auf **Erstellen**:

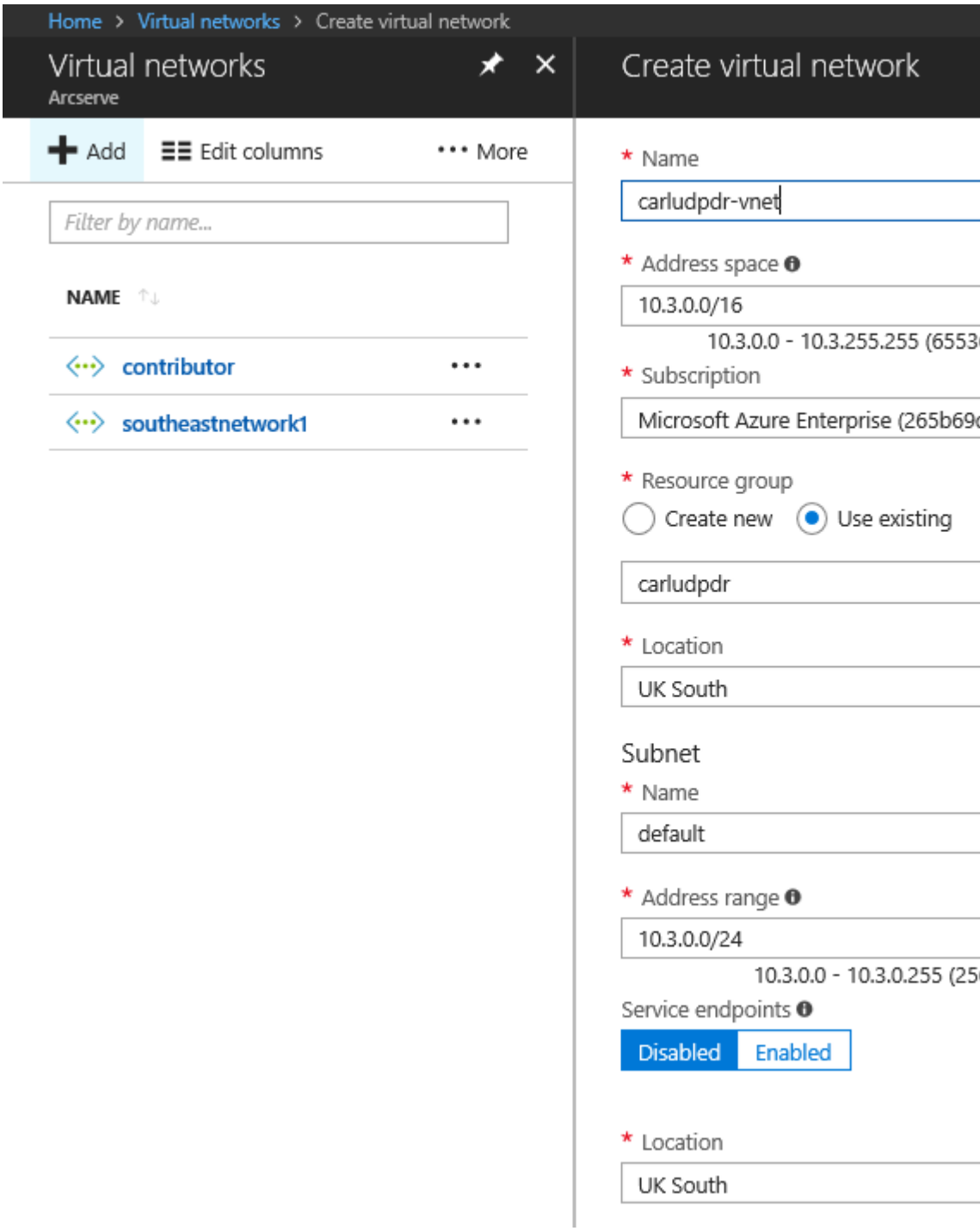


3. Gehen Sie wie folgt vor, um ein virtuelles Netzwerk und ein Subnetz zu erstellen:

   a. Navigieren Sie zur Startseite von Microsoft Azure, **Virtuelle Netzwerke**, und klicken Sie auf **Hinzufügen**.

   b. Geben Sie die erforderlichen Details ein, und klicken Sie auf

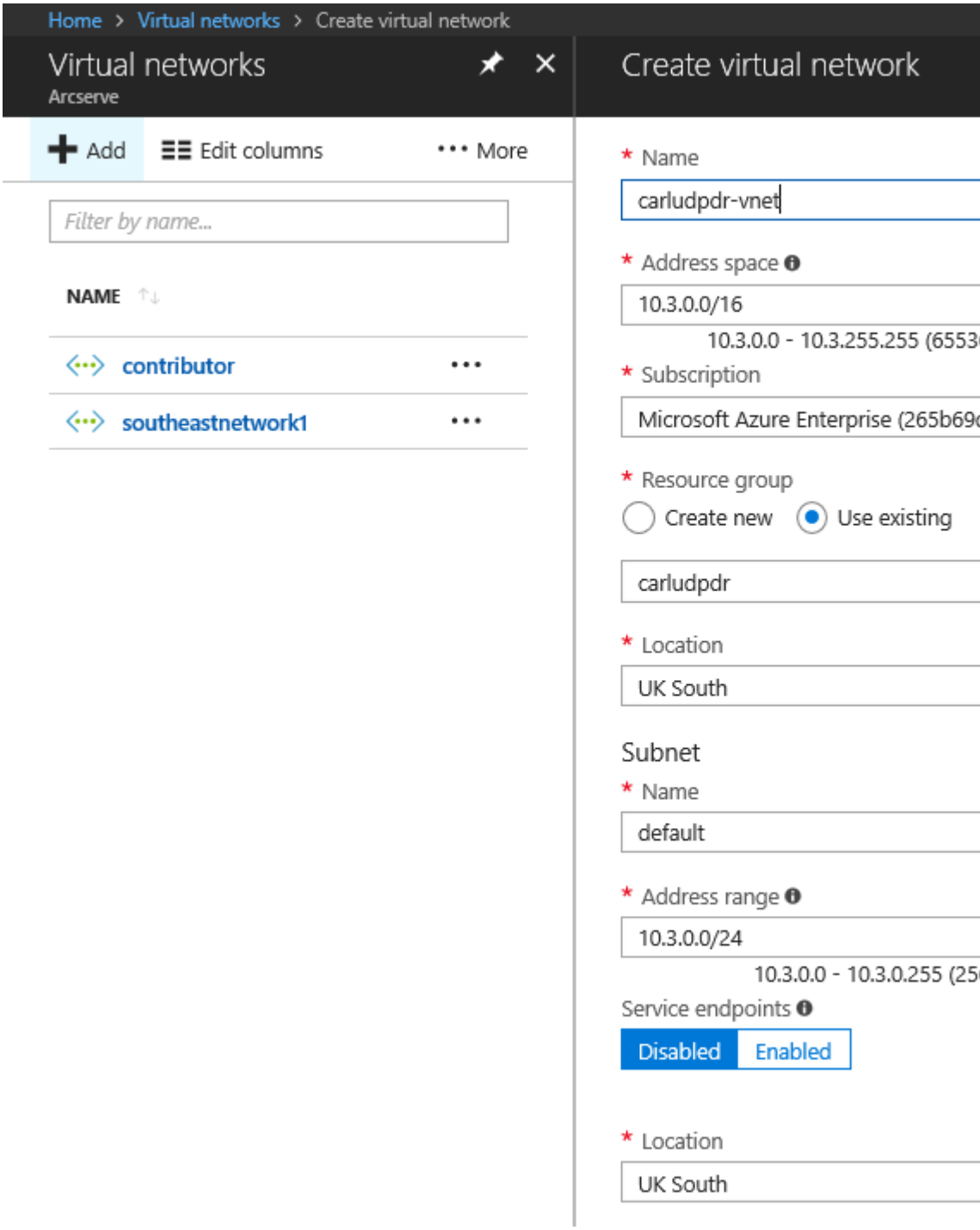
Erstellen.



4. Gehen Sie folgendermaßen vor, um eine Netzwerk-Sicherheitsgruppe zu erstellen:

    a. Navigieren Sie zur Startseite von Microsoft Azure, **Netzwerksicherheitsgruppen**, und klicken Sie auf **Hinzufügen**.

b. Geben Sie die erforderlichen Details ein, und klicken Sie auf **Erstellen**.



Microsoft Azure-Ressourcen wurden erfolgreich erstellt.

Bereitstellen von Arcserve UDP in Microsoft Azure

Nachdem Sie die erforderlichen Schritte abgeschlossen haben, können Sie nun Arcserve UDP in Microsoft Azure bereitstellen.

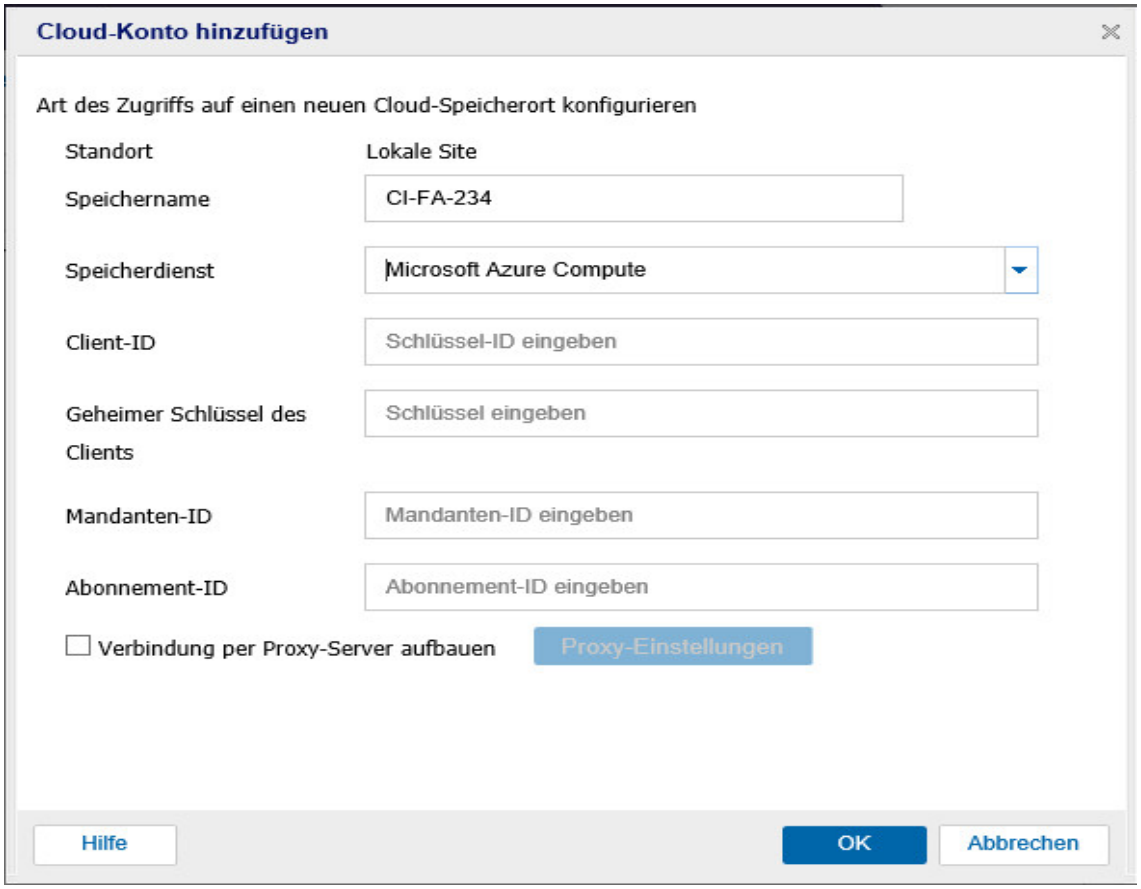
Der nächste Schritt?

1. Hinzufügen eines Azure Cloud-Kontos in Arcserve UDP
2. Erstellen eines Plans mit einem Sicherungstask
3. Hinzufügen eines Virtual Standby-Tasks zum Plan
4. Manuelles Ausführen des Virtual Standby-Jobs
5. Einschalten der Virtual Standby-VM in Azure
6. Überprüfen des Virtual Standby-VM-Status

Hinzufügen eines Azure Cloud-Kontos in Arcserve UDP

Fügen Sie ein Cloud-Konto für Windows Azure zum Kopieren von Dateien oder Wiederherstellungspunkten zu Cloud-Speichern hinzu. Sie können dieses Konto verwenden, wenn Sie Tasks für die Pläne Virtual Standby zu Cloud oder Instant Virtual Machine auf Microsoft Azure erstellen.

Hinweis: Um ein Cloud-Konto für Microsoft Azure hinzuzufügen, müssen Sie die erforderlichen Voraussetzungen erfüllen. Informationen finden Sie unter Komponenten.



Gehen Sie wie folgt vor:

1. Melden Sie sich an auf Arcserve Unified Data Protection und klicken Sie auf die Registerkarte **Ressourcen**.
2. Gehen Sie im linken Fensterbereich zu **Ziele** und klicken Sie auf **Cloud-Konten**.

   Die Seite **Ziele: Cloud-Konten** wird im mittleren Fensterbereich angezeigt.
3. Klicken Sie auf **Ein Cloud-Konto hinzufügen**.

   Die Seite **Ein Cloud-Konto hinzufügen** wird angezeigt.
4. Als **Kontonamen** geben Sie einen eindeutigen Namen an.

   Kontoname gibt den Namen des Cloud-Speichers an. Dieser Name wird zum Identifizieren des Cloud-Kontos zur Konsole hinzugefügt. Jedes Cloud-Konto muss einen eindeutigen Speichernamen haben.
5. Wählen Sie die Option aus der Dropdownliste **Konten**.

   Mehrere Felder erscheinen für die Konfiguration.
6. Geben Sie Informationen zur Konfiguration in die folgenden Felder ein und klicken Sie auf **OK**:

   Client-ID

   Bezieht sich auf die Anwendungs-ID der Anwendung Azure Active Directory. Kopieren Sie Ihre Client-ID im Text-Editor.

   Client-Geheimschlüssel

   Bezieht sich auf den Authentifizierungsschlüssel, der für die Active Directory Azure-Anwendung generiert wurde, die Sie als Client-ID eingeben. Kopieren Sie Ihren Client-Geheimschlüssel in den Texteditor.

   Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Speicherort aufbewahren. Betten Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

   Mandanten-ID

   Verweist auf die ID des Azure Active Directory, wo Sie die Active Directory Azure-Anwendung erstellt haben. Kopieren Sie die Mandanten-ID im Texteditor.

   Abonnement-ID

   Verweist auf einen Globally Unique Identifier (GUID), der Ihr Abonnement eindeutig für die Nutzung von Azure Services identifiziert. Kopieren Sie Ihre Abonnement-ID im Texteditor.

Proxy-Einstellungen

Legt die Proxy-Server-Einstellungen fest. Wählen Sie **Über einen Proxy-Server verbinden**, um diese Option zu aktivieren. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server eine Authentifizierung erfordert. Sie müssen die entsprechenden Authentifizierungsinformationen angeben, die für die Verwendung des Proxyservers erforderlich sind.

Das Cloud-Konto wird zur Konsole hinzugefügt.

Erstellen eines Plans mit einem Sicherungstask

Ein Plan umfasst verschiedene Arten von Tasks, die Sie ausführen möchten. Um einen Virtual Standby-Rechner zu erstellen, erstellen Sie einen Plan, der einen Sicherungstask und einen Virtual Standby-Task enthält. Ein Sicherungstask führt eine Sicherung der Quellknoten aus und speichert die Daten am angegebenen Ziel. Die Virtual Standby-Funktion verwendet die Sicherungsdaten und konvertiert sie in ein Format für virtuelle Rechner.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf die Registerkarte **Ressourcen**.
2. Navigieren Sie im linken Fensterbereich zu **Pläne**, und klicken Sie auf **Alle Pläne**.

   Wenn Sie zu einem früheren Zeitpunkt Pläne erstellt haben, werden diese Pläne im mittleren Fensterbereich angezeigt.
3. Klicken Sie im mittleren Fensterbereich auf **Plan hinzufügen**.

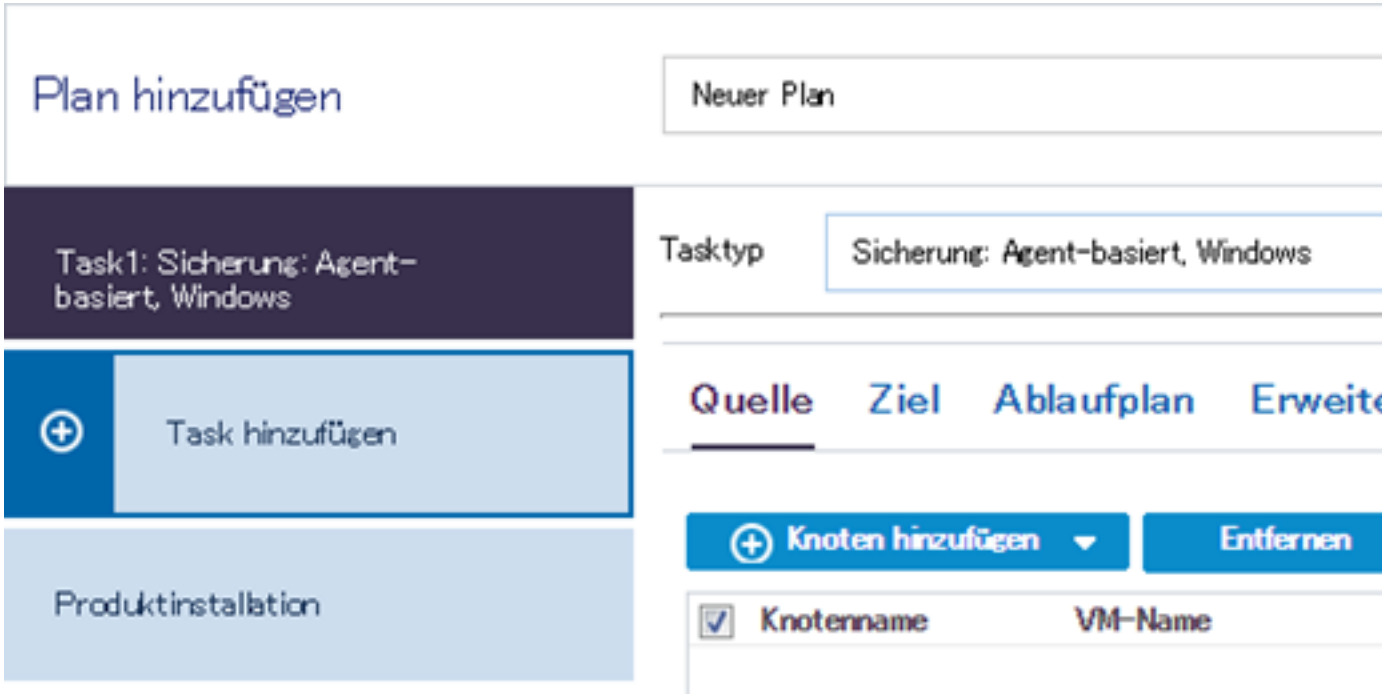
   Plan hinzufügen wird geöffnet.
4. Geben Sie einen Plannamen ein.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Diesen Plan unterbrechen**.

   Der Plan wird nicht ausgeführt, bis Sie das Kontrollkästchen deaktivieren, um den Plan fortzusetzen.

   Hinweis: Wenn ein Plan unterbrochen wird, werden die Jobs in Bearbeitung nicht unterbrochen, aber alle entsprechenden geplanten Jobs im Zusammenhang mit diesem Plan werden unterbrochen. Jobs können allerdings manuell ausgeführt werden. Sie können zum Beispiel manuell einen Sicherungsjob und einen Replikationsjob für einen Knoten ausführen, auch wenn der jeweilige Plan unterbrochen wurde. In diesem Fall wird der Folgetask, der für den (manuellen) On-

Demand-Job vorliegt, nicht ausgeführt. Wenn z. B. nach einem On-Demand-Sicherungsjob ein Replikationstask geplant ist, wird der Replikationsjob nicht für den On-Demand-Sicherungsjob ausgeführt. Der Replikationsjob muss manuell ausgeführt werden. Wenn Sie den Plan fortsetzen, werden die ausstehenden Jobs nicht sofort wiederaufgenommen. Nachdem Sie den Plan fortgesetzt haben, werden die ausstehenden Jobs zum nächsten geplanten Zeitpunkt ausgeführt.

6. Wählen Sie in der Drop-down-Liste **Tasktyp** die Option **Sicherung, Agent-basiertes Windows** aus.



Geben Sie nun Quelle, Ziel, Zeitplan und Erweitert-Details an.

Hinzufügen eines Virtual Standby-Tasks zum Plan

Erstellen Sie einen Virtual Standby to Azure-Task, sodass die Backup-Daten in ein VM-Format konvertiert werden und eine Virtual Machine erstellt wird. Die Virtual Standby-Funktion überwacht auch das Heartbeat-Signal des Quellknotens, damit der virtuelle Rechner umgehend übernimmt, wenn der Quellknoten ausfällt.

Hinweise:

- Virtual Standby kann die Wiederherstellungspunkt-Snapshots von host-basierten VM-Knoten und Knoten, die von einem Remote-Recovery Point Server repliziert wurden, nicht automatisch einschalten. Das automatische Einschalten ist auch nicht möglich, wenn die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird. Sie müssen Wiederherstellungspunkt-Snapshots für solche Knoten manuell einschalten.

- Wenn Sie den Plan unterbrechen und wieder aufnehmen, wird der Virtual Standby-Job nicht automatisch fortgesetzt. Sie müssen einen anderen Sicherungsjob manuell ausführen, damit der Virtual Standby-Job gestartet wird. Wenn Sie den Plan unterbrechen, steht auch die Option "Virtual Standby unterbrechen/wiederaufnehmen" nicht zur Verfügung. Wenn der virtuelle Rechner nach einer Unterbrechung des Plans nicht automatisch starten soll, müssen Sie das Heartbeat-Signal für die Knoten manuell unterbrechen.

Gehen Sie wie folgt vor:

1. Klicken Sie im linken Fensterbereich auf **Task hinzufügen**.

   Ein neuer Task wird im linken Fensterbereich hinzugefügt.

2. Wählen Sie im Drop-down-Menü **Tasktyp** die Option **Virtual Standby** aus.

   Der Virtual Standby-Task wird hinzugefügt.

3. Wählen Sie auf der Registerkarte **Quelle** eine Quelle für den Virtual Standby-Task aus.

4. Klicken Sie auf die Registerkarte **Virtualisierungsserver**, und geben Sie die Details für Virtualisierungsserver und Überwachungsserver ein.

   Virtualisierungstyp

   Geben Sie Azure als Virtualisierungstyp an.

   Kontoname

   Wählen Sie ein vorhandenes Azure-Konto aus, oder klicken Sie auf **Hinzufügen**, um ein Konto zu erstellen.

   Weitere Informationen finden Sie unter So fügen Sie ein Cloud-Konto hinzu.

   Ressourcengruppe

   Wählen Sie eine vorhandene Ressourcengruppe aus, oder klicken Sie auf **Hinzufügen**, um eine Ressourcengruppe zu erstellen.

   Weitere Informationen finden Sie unter Ressourcengruppe in Azure.

   Region

   Wählen Sie die Region aus, in der die Standby-VM in Azure betrieben werden soll. Weitere Informationen finden Sie unter Bereiche in Azure.

   Monitor

   Legen Sie den Hostnamen des Servers fest, der den Status des Quellservers überwacht.

   Hinweise:

- Sie können einem beliebigen physischen Computer oder virtuellen Rechner als Überwachungsserver verwenden.
- Sie können nicht den Sicherungsquellserver als Überwachungsserver verwenden.
- Der Überwachungsserver ist nicht erforderlich, wenn die Knoten von einem Remote-Recovery Point Server repliziert wurden oder die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird.
- Sie müssen den Überwachungsserver nicht konfigurieren, wenn die Virtual Standby-Quelle Replikationstask ist und sich der Replikationsziel-RPS-Server in Azure befindet.

Benutzername

Geben Sie den Benutzernamen für die Anmeldung beim Überwachungssystem an.

Kennwort

Geben Sie das Kennwort für den Benutzernamen für die Anmeldung beim Überwachungssystem an.

Protokoll

Geben Sie HTTP oder HTTPS als das Protokoll an, das Sie für die Kommunikation zwischen dem Arcserve UDP und dem Überwachungsserver verwenden möchten.

Port

Geben Sie den Port an, den Sie für die Datenübertragung zwischen Arcserve UDP und dem Überwachungsserver verwenden möchten.

5. Klicken Sie auf die Registerkarte **Virtueller Rechner**, und geben Sie die Details für VM-Grundeinstellungen, VM-Datenspeicher für VMware, VM-Pfad für Hyper-V und VM-Netzwerk ein.

Präfix des Namens des virtuellen Rechners

Geben Sie ein Präfix an, das Sie dem Anzeigenamen für den virtuellen Rechner in Azure hinzufügen möchten.

Standardwert: UDPVM_

Wiederherstellungspunkt-Snapshots

Geben Sie die Anzahl an Wiederherstellungspunkt-Snapshots (Wiederherstellungspunkten) für den virtuellen Standby-Rechner an. Die maximale Anzahl von Wiederherstellungspunkt-Snapshots beträgt 29.

Standardwert: 5

Kombinieren Sie alle unkonvertierten Sitzungen in Wiederherstellungspunkt-Snapshots.

Geben Sie an, ob alle unkonvertierten Sitzungen in einem einzigen Wiederherstellungspunkt-Snapshot kombiniert werden sollen, wenn der nächste geplante VSB-Job stattfindet.

Standard: Ausgewählt

Größe des virtuellen Rechners

Microsoft Azure bietet eine große Auswahl an Größen virtueller Rechner an, die für verschiedene Nutzungsfälle optimiert wurden. Sie haben unterschiedliche Kombinationen von CPU, Arbeitsspeicher, Speicher und Netzwerkkapazität. Weitere Informationen zu Größen virtueller Rechner und wie sie Ihren PC-Anforderungen entsprechen, finden Sie bei den Größen fürVirtuelle Windows-Rechner in Azure.

Speicherkontoname

Wählen Sie einen Namen für ein vorhandenes Speicherkonto aus, oder erstellen Sie ein Speicherkonto in Azure. Wenn Sie ein Speicherkonto in Azure erstellen, müssen Sie eine der folgenden Optionen als Kontoart angeben:

- Speicher (allgemein v1)
- SpeicherV2 (allgemein v2)

Weitere Informationen finden Sie unter Speicherkonto in Azure.

Virtuelles Netzwerk

Wählen Sie ein vorhandenes virtuelles Netzwerk aus, oder erstellen Sie ein virtuelles Netzwerk in Azure. Weitere Informationen finden Sie unter Virtuelles Netzwerk in Azure.

Subnetz

Wählen Sie ein vorhandenes virtuelles Subnetz basierend auf dem ausgewählten virtuellen Netzwerk aus, oder fügen Sie ein Subnetz in Azure hinzu. Weitere Informationen finden Sie unter Hinzufügen von Subnetzen in Azure.

Netzwerk-Sicherheitsgruppe

Wählen Sie eine vorhandene Netzwerk-Sicherheitsgruppe aus, oder erstellen Sie eine Netzwerk-Sicherheitsgruppe in Azure. Konfigurieren Sie die Regeln der Sicherheitsgruppe zum Öffnen der verknüpften Ports, darunter 3389 für Remote-Desktop, 8014, 8015 für Arcserve UDP Kommunikation. Weitere Informationen finden Sie unter Netzwerk-Sicherheitsgruppe.

Automatische Zuweisung einer öffentlichen IP-Adresse aktivieren

Wählen Sie diese Option aus, um eine öffentliche IP-Adresse der Standby-VM automatisch zuzuweisen, wenn die Standby-VM in Azure gestartet wird.

6. Klicken Sie auf die Registerkarte **Erweitert**, und geben Sie folgende Details an:

Virtuellen Rechner automatisch starten

Geben Sie an, ob Sie den virtuellen Rechner automatisch starten möchten.

Hinweis: Diese Option ist nicht verfügbar für hostbasierte VM-Knoten und Knoten, die von einem Remote-Wiederherstellungspunktserver repliziert werden und die Quelle des Virtual Standby-Tasks ist diejenige, die an einen anderen Standort repliziert wird. Die Virtual Standby-Quelle ist der Replikationstask und der Replikationsziel-RPS-Server in Azure.

Zeitlimit

Geben Sie die an, wie lange der Überwachungsserver auf ein Heartbeat-Signal warten muss, bevor ein Wiederherstellungspunkt-Snapshot eingeschaltet wird.

Häufigkeit

Legen Sie die Häufigkeit fest, mit der der Quellserver die Heartbeat-Signale an den Überwachungsserver sendet.

Beispiel: Der festgelegte Wert für das Zeitlimit ist 60. Der festgelegte Häufigkeitswert ist 10. Der Quellserver sendet Heartbeat-Signale in 10-Sekunden-Intervallen. Wenn der Überwachungsserver innerhalb von 60 Sekunden nach dem letzten erkannten Heartbeat-Signal kein Heartbeat-Signal erkennt, schaltet der Überwachungsserver unter Verwendung des letzten Wiederherstellungspunkt-Snapshot einen virtuellen Rechner ein.

Jobparameter anpassen

Sie können Jobparameter für die folgenden Optionen anpassen:

- *Anzahl der Threads, die für jeden Auftrag hochladen*: Standardwert: 4
- *Puffergröße für jeden Thread*: Standardwert: 4096 KB

E-Mail-Alerts aktivieren

Wählen Sie diese Option aus, um E-Mail-Alerts zu aktivieren. Sie erhalten E-Mail-Alerts abhängig von den Einstellungen, die Sie angeben.

- **Fehlendes Heartbeat-Signal für Quellrechner**: Virtual Standby sendet Alert-Benachrichtigungen, wenn der Überwachungsserver kein Heartbeat-Signal vom Quellserver erkennt.

  Hinweis: Diese Option ist nicht für Knoten verfügbar, die von einem Remote-Recovery Point Server repliziert wurden, oder wenn die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird.

- **VM eingeschaltet für Quellrechner, der mit automatischer Einschaltung konfiguriert ist**: Virtual Standby sendet Alert-Benachrichtigungen, wenn ein virtueller Rechner in Betrieb genommen wird, der so konfiguriert wurde, dass eine automatische Inbetriebnahme erfolgt, wenn kein Heartbeat-Signal entdeckt wird.

  Hinweis: Diese Option ist nicht verfügbar für hostbasierte VM-Knoten und die Knoten, die von einem Remote-Recovery Point Server repliziert werden, oder wenn die Quelle des Virtual Standby-Tasks diejenige ist, die an einen anderen Standort repliziert wird.

- **VM eingeschaltet für Quellrechner, der mit manueller Einschaltung konfiguriert ist**: Virtual Standby sendet Alert-Benachrichtigungen, wenn ein virtueller Rechner manuell eingeschaltet wird.
- **Virtual Standby-Fehler/-Ausfall/-Absturz**: Virtual Standby sendet Alert-Benachrichtigungen, wenn ein Fehler während des Konvertierungsprozesses festgestellt wird.
- **Virtual-Standby-Erfolg**: Virtual Standby sendet Alert-Benachrichtigungen, wenn ein virtueller Rechner erfolgreich eingeschaltet wurde.
- **Virtual Standby wurde nicht erfolgreich vom Wiederherstellungspunkt-Snapshot gestartet**: Virtual Standby sendet Alert-Benachrichtigungen, wenn die Option zur Aushilfswiederherstellung "Virtuellen Rechner automatisch starten" aktiviert ist, ein virtueller Rechner jedoch nicht automatisch eingeschaltet wird.

7. Klicken Sie auf **Speichern**.

   Die Änderungen werden gespeichert, und der Virtual Standby-Task wird automatisch auf dem Virtual Standby-Server bereitgestellt.

   Hinweis: Wenn der Virtual Standby-Task abgeschlossen ist, wird das VM-Standby-Volume erstellt. Der virtuelle Standby-Rechner wird erst erstellt, nachdem der virtuelle Rechner von Arcserve UDP eingeschaltet wurde.

   Sie haben den Virtual Standby to Azure-Plan erfolgreich erstellt und angewandt.

Manuelles Ausführen des Virtual Standby-Jobs

Um einen Virtual Standby-Job manuell auszuführen, müssen Sie zunächst eine manuelle Sicherung ausführen. Der Virtual Standby-Task wird mit einem Sicherungstask verknüpft. Wenn ein Plan einen Sicherungstask und einen Virtual Standby-Task enthält und Sie den Sicherungsjob manuell ausführen, wird der Virtual Standby-Job nach dem Abschluss des Sicherungsjobs automatisch ausgeführt.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte "**Ressourcen**".
2. Navigieren Sie im linken Fensterbereich zu **Knoten**, und klicken Sie auf **Alle Knoten**.

   Zeigt die Pläne an, die Sie hinzugefügt haben.
3. Wählen Sie die Knoten aus, die gesichert werden sollen. Dem ausgewählten Knoten muss ein Plan zugewiesen sein.
4. Klicken Sie im mittleren Fensterbereich auf **Aktionen**, **Jetzt sichern**.

   Das Dialogfeld **Sicherung jetzt ausführen** wird geöffnet.
5. Wählen Sie den Sicherungstyp aus, und geben Sie einen Namen für den Sicherungsjob an.
6. Klicken Sie auf **OK**.

   Der Sicherungsjob wird ausgeführt.

   Der Virtual Standby-Job wird sofort nach dem Sicherungsjob ausgeführt.

   Der Virtual Standby-Job wird manuell ausgeführt.

Einschalten der Virtual Standby-VM in Azure

Die Standby VM-Volumes werden in Azure nach Abschluss des Virtual Standby-Jobs erstellt. Die Standby-VM wird nur erstellt, wenn sie über Arcserve UDP eingeschaltet wird.

Virtual Standby kann so konfiguriert werden, dass Virtual Standby-Rechner aus Wiederherstellungspunkt-Snapshots automatisch in Betrieb genommen werden, wenn der Überwachungsserver kein Heartbeat-Signal vom Quellserver entdeckt. Optional können Sie Virtual Standby-Rechner aus Wiederherstellungspunkt-Snapshots manuell in Betrieb nehmen, falls ein Quellserver fehlschlägt, ein Notfall eintritt oder Sie einen Quellserver zur Wartung offline schalten wollen.

Befolgen Sie diese Schritte:

1. Navigieren Sie auf der Registerkarte "**Ressourcen**" zur Knotengruppe "**Virtual Standby**".

   Die Virtual Standby-Knoten werden im mittleren Fensterbereich angezeigt.
2. Wählen Sie im mittleren Fensterbereich den Knoten aus, und klicken Sie auf "**Standby-VM**".

   Das Dialogfeld "**Standby-VM**" wird geöffnet.
3. Führen Sie im Dialogfeld **Standby-VM** folgende Tasks aus:

   - Wählen Sie einen Datums-und Zeitbereich des Wiederherstellungspunkt-Snapshots aus, um den virtuellen Rechner einzuschalten.

- Klicken Sie auf **VM starten**.

  Der virtuelle Rechner wird unter Verwendung der im Wiederherstellungspunkt-Snapshot enthaltenen Daten eingeschaltet.

Sie können jetzt den Status überprüfen oder die Virtual Standby-VM herunterfahren. Weitere Informationen finden Sie in den folgenden Themen:

- Überprüfen des Virtual Standby-VM-Status
- Herunterfahren der Virtual Standby-VM in Azure

Herunterfahren der Virtual Standby-VM in Azure

Sie können die Virtual Standby-VM in Azure über die Arcserve UDP-Konsole herunterfahren.

Befolgen Sie diese Schritte:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie zu **Virtual Standby**.
3. Wählen Sie die Option aus, und klicken Sie im mittleren Fensterbereich mit der rechten Maustaste auf die **Virtual Standby-VM**.

   Das Dialogfeld "Standby-VM" mit den aktiven Snapshots wird geöffnet.
4. Wählen Sie einen aktiven Snapshot aus, und klicken Sie auf **VM herunterfahren**.
5. Klicken Sie auf **Löschen**.

   Ein Bestätigungsdialogfeld wird geöffnet.
6. Wenn Sie die an die Virtual Standby VM angehängten Festplatten löschen möchten, wählen Sie die Option **Löschen der angehängten Festplatte(n)**.
7. Klicken Sie auf **OK**.

   Die Virtual Standby-VM wurde erfolgreich heruntergefahren.

Überprüfen des Virtual Standby-VM-Status

Sie können den Status der Virtual Standby-VM über die Arcserve UDP-Konsole überprüfen.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Konsole auf **Ressourcen**.
2. Navigieren Sie zu **Virtual Standby**.
3. Wählen Sie im mittleren Fensterbereich die **Virtual Standby-VM**.

4. Der Status der Virtual Standby-VM wird im Feld "Konfigurations-Assistent" unter der Gruppe **Status des Virtual Standby** angezeigt.

   Der Status lautet **Wird ausgeführt**, wenn die Virtual Standby-VM eingeschaltet ist. Wenn sie nicht eingeschaltet ist, lautet der Status **N/V** oder **Ausgeschaltet**.

Arcserve UDP – Begriffe und Definitionen

Agentenbasierte Sicherung

Eine agentenbasierte Sicherung ist eine Methode zum Sichern von Daten unter Verwendung einer Agentenkomponente. Der Agent wird auf dem Quellknoten installiert.

Komprimierung

Komprimierung wird für Sicherungen verwendet. Eine Komprimierung wird oft ausgewählt, um den verwendeten Speicherplatz zu verringern, hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit der Sicherung.

Es sind folgende Optionen verfügbar:

Keine Komprimierung

Diese Option bedeutet niedrigste CPU-Auslastung (höchste Geschwindigkeit), aber auch höchste Speicherplatzverwendung für Ihr Sicherungs-Image.

Standard-Komprimierung

Es wird eine Komprimierung bis zu einem gewissen Grad ausgeführt. Diese Option bietet ein Gleichgewicht zwischen CPU-Auslastung und verwendetem Speicherplatz. Dies ist die Standardeinstellung.

Maximale Komprimierung

Es wird eine maximale Komprimierung durchgeführt. Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigste Speicherplatzverwendung für Ihr Sicherungs-Image.

Hinweise:

- Wenn Ihr Sicherungs-Image nicht komprimierbare Dateien (z. B. .jpg, .zip etc.) enthält, muss möglicherweise zusätzlicher Speicherplatz zugeordnet werden, um diese Daten zu verarbeiten. Die Aktivierung einer Komprimierungsoption kann in solchen Fällen eine erhöhte Speicherplatzverwendung zur Folge haben.
- Wenn Sie die Komprimierungsstufe von "Keine Komprimierung" auf entweder "Standard-Komprimierung" oder "Maximale Komprimierung" ändern, oder wenn Sie von "Standard-Komprimierung" bzw. "Maximale Komprimierung" auf "Keine Komprimierung" wechseln, ist die erste Sicherung nach der Änderung der Komprimierungsstufe automatisch eine vollständige Sicherung. Nachdem diese vollständige Sicherung durchgeführt wurde, werden alle weiteren

Sicherungen (vollständige Sicherung, Zuwachssicherung oder Überprüfungssicherung) gemäß dem Ablaufplan durchgeführt.

Diese Option ist nur für lokale oder Remote-Freigabeziele verfügbar. Sie können die Komprimierungseinstellung nicht ändern, wenn der Arcserve Unified Data Protection-Agent auf dem Datenspeicher gesichert ist.

- Wenn auf Ihrem Ziel nicht genügend freier Speicherplatz zur Verfügung steht, sollten Sie in Betracht ziehen, die Einstellung "Komprimierung" der Sicherung zu erhöhen. Diese Option ist nur für lokale oder Remote-Freigabeziele verfügbar. Sie können die Komprimierungseinstellung nicht ändern, wenn der Arcserve Unified Data Protection-Agent auf dem Datenspeicher gesichert ist.

Konfiguration

Eine Registerkarte in der Arcserve UDP-Konsole, auf der Konfigurationsparameter wie E-Mail-Alerts, Datenbankeinstellungen und Installationsvoreinstellungen definiert werden können

Dashboard

Eine Registerkarte der Arcserve UDP-Konsole, die den Status der letzten Sicherung und den Speicherstatus anzeigt. Hier können Sie die tatsächlich gespeicherten Daten, die Rohdaten und die wiederherstellbaren Daten sehen.

Datenspeicher

Ein Datenspeicher ist ein physischer Speicherbereich auf einem Datenträger. Sie können einen Datenspeicher unter einem beliebigen Windows-System erstellen, auf dem ein Recovery Point Server installiert ist. Datenspeicher können sich an einem lokalen Speicherort oder auf einer Remote-Freigabe, auf die das Windows-System zugreifen kann, befinden.

Ziel

Das Ziel ist ein Computer oder Server, auf dem Sie Sicherungsdaten speichern. Bei einem Ziel kann es sich um einen lokalen Ordner auf dem geschützten Knoten, einen freigegebenen Remote-Ordner oder einen Recovery Point Server (RPS) handeln.

Erkannte Knoten

Erkannte Knoten sind physische oder virtuelle Systeme, die zur Arcserve UDP-Konsole hinzugefügt werden, indem sie durch Discovery von Active Directory oder

vCenter/ESX-Server entdeckt, aus einer Datei importiert oder manuell mithilfe ihrer IP-Adressen hinzufügt werden.

Verschlüsselung

Die Arcserve Unified Data Protection-Lösung bietet eine Funktion für die Verschlüsselung von Daten.

Wenn das Sicherungsziel ein Recovery Point Server ist, sind die verfügbaren Verschlüsselungen "Keine Verschlüsselung" und "Datenverschlüsselung" mit AES-256. Sie können dies festlegen, um einen Datenspeicher zu erstellen. Wenn es sich beim Sicherungsziel um eine lokale Freigabe oder Remote-Freigabe handelt, sind die verfügbaren Optionen für das Verschlüsselungsformat "Keine Verschlüsselung", "AES-128", "AES-192" und "AES-256". Sie können diese Option während der Erstellung eines Ablaufplans für Sicherungen auf einer lokalen oder Remote-Freigabe oder über die Sicherungseinstellung für eine eigenständige Installation von Arcserve Unified Data Protection Agent festlegen.

Hauptfunktionen der Verschlüsselung

1. Die AES-256-Verschlüsselungsmethode wird angewendet auf:
   - Datenspeicher
   - Gespeicherte Kennwörter (in Schutzplänen, in der Registrierung, in Konfigurationsdateien usw.)
2. *Bei einem Sicherungsjob*: Wenn die Verschlüsselung aktiviert ist, werden die Daten verschlüsselt, bevor sie vom Server übertragen werden.
3. *Bei einem Replikationsjob:* Wenn die Verschlüsselung auf dem Replikationsziel aktiviert ist, werden die Daten verschlüsselt, bevor sie vom Server übertragen werden.

Verschlüsselungseinstellungen

a. Wählen Sie den Verschlüsselungsalgorithmus aus, den Sie für Sicherungen verwenden möchten.

   Bei der Datenverschlüsselung werden Daten in ein Format umgewandelt, das ohne den entsprechenden Entschlüsselungsmechanismus nicht verständlich ist. Die Arcserve Unified Data Protection-Lösung verwendet für Ihre Daten sichere AES-Verschlüsselungsalgorithmen (Advanced Encryption Standard) für größtmögliche Sicherheit und Datenschutz.

b. Wenn ein Verschlüsselungsalgorithmus ausgewählt wird, müssen Sie ein Verschlüsselungskennwort angeben (und es bestätigen).

- Das Verschlüsselungskennwort kann höchstens aus 23 Zeichen bestehen.
- Eine vollständige Sicherung und alle verknüpften Zuwachs- und Überprüfungssicherungen müssen das gleiche Kennwort zur Datenverschlüsselung verwenden.
- Wenn das Verschlüsselungskennwort für eine Zuwachs- oder Überprüfungssicherung geändert wird, muss eine vollständige Sicherung ausgeführt werden. Dies bedeutet, dass nach einer Änderung des Verschlüsselungskennworts die erste Sicherung trotz des ursprünglichen Sicherungstyps vollständig ist.

Wenn Sie zum Beispiel das Verschlüsselungskennwort ändern und eine angepasste Zuwachs- oder Überprüfungssicherung manuell übergeben, wird automatisch auf eine vollständige Sicherung gewechselt.

Hinweis: Diese Option ist nur für die lokale oder Remote-Freigabeziele verfügbar. Sie können die Verschlüsselungseinstellung nicht deaktivieren, wenn der Arcserve Unified Data Protection-Agent im Datenspeicher gesichert wird.

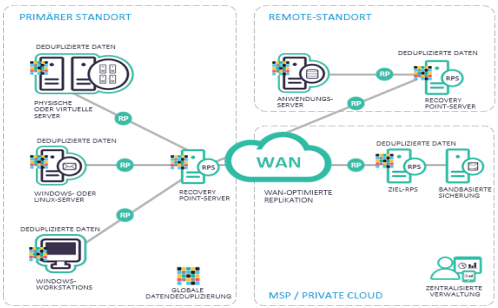
c. Die Arcserve Unified Data Protection-Lösung verwendet ein Verschlüsselungskennwort und ein Sitzungskennwort.

- Das Verschlüsselungskennwort ist für den Datenspeicher erforderlich.
- Das Sitzungskennwort ist für den Knoten erforderlich.
- Wenn der Datenspeicher verschlüsselt ist, ist das Sitzungskennwort obligatorisch. Wenn der Datenspeicher nicht verschlüsselt ist, ist das Kennwort optional.

Ein Kennwort ist nicht erforderlich, wenn Sie versuchen, die Wiederherstellung auf dem gleichen Rechner durchzuführen, auf dem die Sicherung ausgeführt wurde. Wenn Sie jedoch versuchen, die Wiederherstellung auf einem anderen Rechner durchzuführen, ist ein Kennwort erforderlich. Standardmäßig ist nur für die erste Anmeldung ein Kennwort erforderlich. Um das Kennwort auch nach der ersten Anmeldung einzugeben, muss der Administrator Arcserve den Erweiterungsdienst des UDP Agent-Explorers manuell anhalten.

Globale Deduplizierung

Die globale Deduplizierung von Arcserve UDP reduziert die Menge der tatsächlich während Sicherungszyklen übertragenen Daten deutlich. Die Möglichkeit der Deduplizierung über alle Clients in der Umgebung hinweg begrenzt die unnötige Speicherung und Übertragung existierender Daten – und dies erfolgt auf globaler Ebene, da Daten über Knoten, Jobs und Standorte hinweg dedupliziert werden.



Hostbasierte agentenlose Sicherung

Eine hostbasierte agentenlose Sicherung ist eine Methode zum Sichern von Daten ohne Verwendung einer Agentenkomponente auf dem Quellrechner.

HOTADD-Transportmodus

Der HOTADD-Transportmodus ist eine Methode zum Datentransport, mit der Sie mit SCSI-Datenträgern konfigurierte virtuelle Rechner sichern können. Weitere Informationen finden Sie im "Virtual Disk API Programming Guide" auf der VMware-Website.

Job

Ein Job ist eine Arcserve UDP-Aktion zum Sichern, Wiederherstellen, Erstellen von Virtual Standby oder Replizieren von Knoten.

Jobs

Eine Registerkarte in der Arcserve UDP-Konsole, auf der Sie den Status aller Aufträge wie Sicherung, Replikation und Wiederherstellung überwachen können. Die Details umfassen Jobs, Tasktypen, Knoten-IDs, Wiederherstellungspunkte und Plannamen.

NBD-Transportmodus

Der NBD-Transportmodus (Network Block Device), auch LAN-Transportmodus genannt, verwendet das NFC-Protokoll (Network File Copy) zum Kommunizieren. Verschiedene VDDK- und VCB-Vorgänge verwenden eine Verbindung für jeden virtuellen Datenträger, auf den bei der Verwendung von NBD auf jedem ESX-/ESXi-Server-Host zugegriffen wird.

NBDSSL-Transportmodus

Der Transportmodus Network Block Device Secure Sockets Layer (NBDSSL) verwendet das NFC-Protokoll (Network File Copy) zur Kommunikation. NBDSSL überträgt verschlüsselte Daten über TCP/IP-Kommunikationsnetzwerke.

Knoten

Ein Knoten ist ein physisches oder virtuelles System, das von Arcserve UDP geschützt wird. Arcserve UDP kann physische Knoten und virtuelle Rechner auf vCenter/ESX-Servern und Microsoft Hyper-V-Servern schützen.

Plan

Ein Plan ist eine Gruppe von Tasks zum Verwalten der Sicherung, Replikation und Erstellung von Virtual Standby-Rechnern. Ein Plan besteht aus einem einzelnen oder mehreren Tasks. Tasks sind eine Reihe von Aktivitäten zum Definieren von Quelle, Ziel, Ablaufplan und erweiterten Parametern.

Geschützte Knoten

Geschützte Knoten sind die Knoten, für die Sicherungspläne zum Sichern von Daten in regelmäßigen Intervallen vorliegen.

Aktuelle Ereignisse

Aktuelle Ereignisse sind Jobs, die sich in Ausführung befinden oder vor Kurzem abgeschlossen wurden.

Wiederherstellungspunkt

Ein Wiederherstellungspunkt ist ein Snapshot eines Sicherungsknotens zu einem bestimmten Zeitpunkt. Ein Wiederherstellungspunkt wird erstellt, wenn Sie einen

Knoten sichern. Wiederherstellungspunkte werden auf dem Sicherungsziel gespeichert.

Recovery Point Server

Ein Recovery Point Server ist ein Zielknoten, auf dem Sie den Server installieren. Sie können Datenspeicher auf einem Recovery Point Server erstellen. Der Recovery Point Server (RPS) fungiert als Sicherungs-Repository für Datenträger-Images und bietet eine einmalige Reihe von Technologien, die die Grundbausteine für die Arcserve UDP-Lösung bilden. Zu den Hauptfunktionen von RPS zählen wahre quellseitige Deduplizierung, sichere integrierte Replikation von Datenträger-Images, RPS-Jumpstart und "Offline"-Synchronisierung sowie mandantenfähige Speicherung.

Replizieren

"Replizieren" ist ein Task, der Wiederherstellungspunkte von einem Server auf einem anderen Server dupliziert.

Ressourcen

Ressourcen ist eine Registerkarte in der Arcserve UDP-Konsole. Auf der Registerkarte **Ressourcen** können Sie Quellknoten, Ziele und Pläne verwalten.

SAN-Transportmodus

Der SAN-Transportmodus (Storage Area Network) ermöglicht es Ihnen, Sicherungsdaten von Proxy-Systemen, die mit dem SAN verbunden sind, auf Speichergeräte zu übertragen.

Systeme

Systeme sind alle Arten von Knoten, Geräten und virtuellen Rechnern, die von Arcserve Unified Data Protection verwaltet werden können. Dies umfasst physische Rechner, Linux-Rechner, virtuelle Rechner und Virtual Standby-Rechner.

Tasks

Ein Task besteht aus einer Reihe von Aktivitäten zum Definieren verschiedener Parameter für das Sichern, Replizieren und Erstellen von Virtual Standby-Rechnern. Diese Parameter umfassen Quelle, Ziel, Ablaufplan und bestimmte erweiterte Parameter. Jeder Task ist mit einem Plan verknüpft. Ein Plan kann mehr als einen Task haben.

Ungeschützte Knoten

Ungeschützte Knoten sind Knoten, die zu Arcserve Unified Data Protection hinzugefügt werden, denen jedoch kein Plan zugewiesen ist. Wenn kein Plan zugewiesen ist, können Sie keine Daten sichern, und der Knoten bleibt ungeschützt.

Datendeduplizierung

Datendeduplizierung ist eine Technologie, die Duplikate von identischen Daten beseitigt, was den erforderlichen Speicherplatz reduziert. Organisationen können aus verschiedenen Gründen über duplizierte Daten verfügen. Ein Beispiel ist ein E-Mail-Anhang, der an mehrere Benutzer weitergeleitet wird. Wenn Sie diese Daten speichern, speichern Sie im Sicherungs-Speicherdatenträger mehrere Kopien derselben Daten.

Datendeduplizierung beseitigt redundante Daten und speichert nur eine Instanz der Daten. Alle weiteren Instanzen werden durch einen Verweis auf diese Instanz ersetzt. Diese Methode kann den Speicherplatz, der für das Speichern von Sicherungsdaten erforderlich ist, erheblich reduzieren.

Zum Beispiel können 100 Benutzer dieselbe Datei mit einer Größe von 10 MB auf ihrem jeweiligen lokalen System gespeichert haben. Um all diese lokalen Systeme oder Knoten zu sichern, benötigen Sie einen Speicherplatz von 1000 MB. Durch Datendeduplizierung können Sie den Speicherplatz auf ungefähr 10 MB reduzieren, da nur eine Instanz der Datei auf dem Datenträger gespeichert wird. Die verbleibenden 99 Instanzen verweisen auf diese Instanz.

Vorteile der Datendeduplizierung

- speichert mehr Sicherungsdaten in einem Speicherplatz
- reduziert die Datenmenge, die über das Netzwerk gesendet wird
- beschleunigt die Sicherungen, da Verweise anstelle von tatsächlichen Daten gespeichert werden
- reduziert die Kosten für Netzwerkbandbreite und Speicherdatenträger

Arten der Datendeduplizierung

Arcserve UDP unterstützt folgende zwei Arten der Datendeduplizierung.

Quellseitige Datendeduplizierung

Stellt sicher, dass für die Datensicherung nur eindeutige Daten vom Agent zum Recovery Point Server gesendet werden.

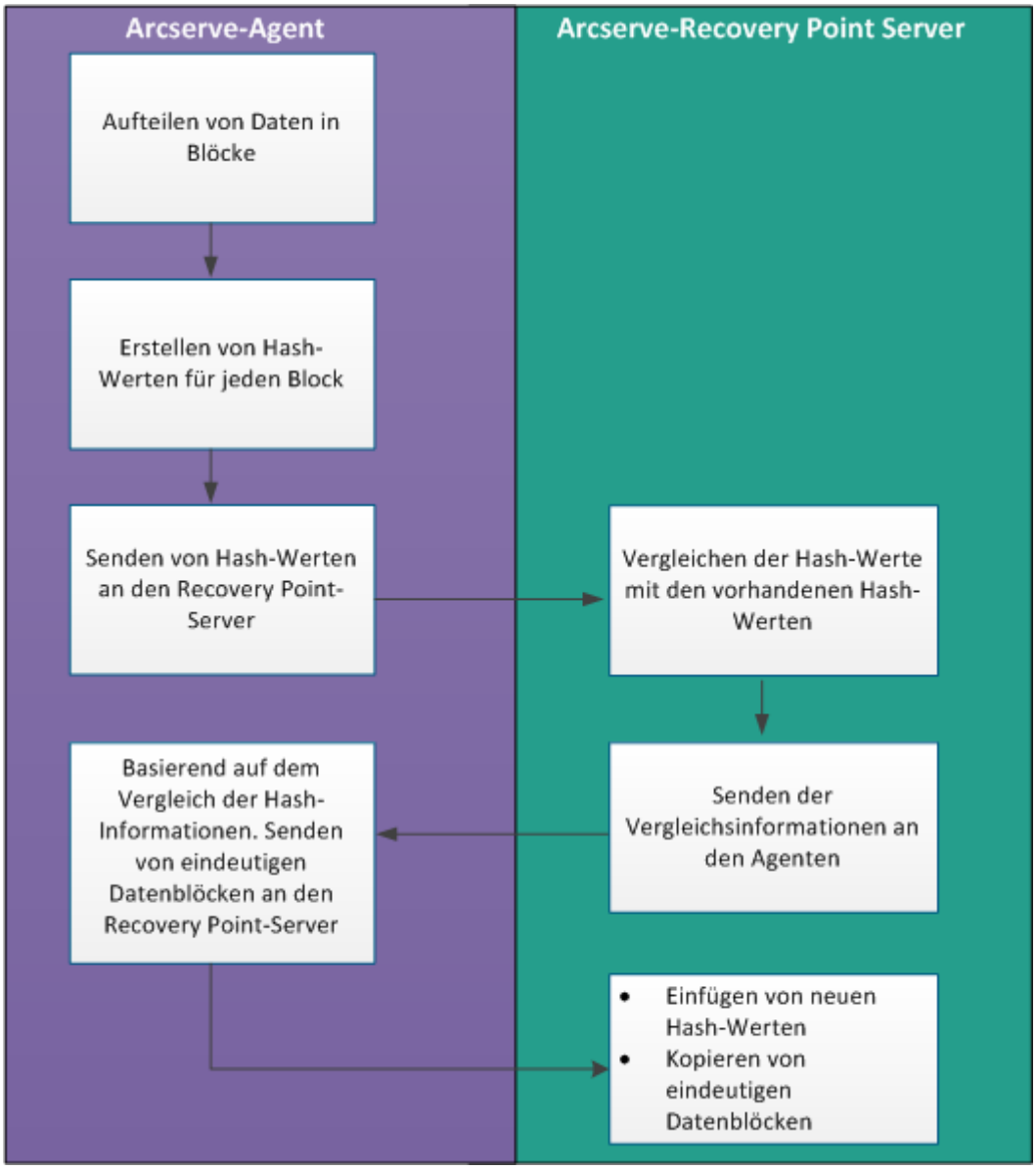
Globale Deduplizierung

Stellt sicher, dass auf einem Recovery Point Server nur eindeutige Daten von unterschiedlichen Agenten gesichert werden. Wenn auf verschiedenen Knoten ähnliche Datenblöcke vorliegen, wird am Recovery Point Server nur eine Kopie gesichert.

Funktionsweise der Datendeduplizierung

Der Arcserve UDP-Deduplizierungsprozess unterteilt Daten in Datenblöcke. Jeder Block erhält eine eindeutige Kennung, die als Hash bezeichnet wird. Der Hash-Wert wird basierend auf dem Volume-Cluster berechnet. Die standardmäßige Größe von Deduplizierungsblöcken beträgt 4 KB (die standardmäßige Größe von Volume-Clustern beträgt auf den meisten Knoten 4 KB). Diese Hash-Werte werden mit den Hash-Werten der vorhandenen Sicherungsdaten verglichen. Wenn doppelte Verweise gefunden werden, werden die entsprechenden Datenblöcke nicht gesichert. Es werden nur Datenblöcke mit eindeutigen Verweisen gesichert.

Das folgende Diagramm veranschaulicht die Funktionsweise der Deduplizierung in Arcserve UDP.



Wenn eine Sicherung ausgelöst wird, unterteilt der Deduplizierungsprozess auf dem Agenten die Daten zunächst in Blöcke und weist jedem Block einen eindeutigen Hash-Schlüssel bzw. Hash-Wert zu. Anschließend werden die Hash-Werte an den Recovery Point Server gesendet. Auf dem Recovery Point Server werden diese Hash-Werte mit den vorhandenen Hash-Werten verglichen, und duplizierte Hash-Werte werden herausgefiltert. Die Ergebnisse dieses Vergleichs werden an den Agenten zurückgesendet. Auf der Grundlage dieser Information zu duplizierten Hash-Werten sendet der Agent die eindeutigen Datenblöcke an den Recovery Point Server, um sie zu sichern. Die neuen Hash-Werte für diese Datenblöcke werden auch in die Liste der vorhandenen Hash-Werte auf dem Recovery Point Server aufgenommen.

Wenn mehrere Agenten verwendet werden, ist der Deduplizierungsprozess derselbe, allerdings werden duplizierte Daten für mehrere Agenten herausgefiltert. Dadurch werden auch bei Verwendung mehrerer Agenten Datenduplikate vermieden.

Der Einsatz von Datendeduplizierung in Arcserve UDP bietet folgende Vorteile:

- **schnellere vollständige Sicherungen**
- **schnellere Zusammenführungsjobs**
- **Unterstützung von globaler Deduplizierung**
- **optimierte Replikation**

Wann sollten Sie Deduplizierung verwenden?

Folgende Szenarien sind Beispiele für Situationen, in denen ein Deduplizierungsdatenspeicher zu einer gesteigerten Effizienz führen kann:

- Wenn mehrere Knoten mit ähnlichen Daten vorliegen: Wenn Sie in diesem Szenario Daten von allen Knoten in einem Datenspeicher sichern, könnte die Menge der Daten, die tatsächlich im Recovery Point Server gespeichert werden, erheblich reduziert werden. Der benötigte Speicherplatz könnte merkbar kleiner ausfallen.
- Wenn Sie häufig eine vollständige Sicherung eines Knotens durchführen müssen: In diesem Szenario ist der Großteil Ihrer Sicherungsdaten bereits vorhanden, sodass die Sicherungsdauer deutlich kürzer ausfallen könnte.
- Wenn die Netzwerkbandbreite beschränkt ist: Die Netzwerkauslastung kann reduziert werden, da nur eindeutige Datenblöcke über das Netzwerk versendet werden.
- Wenn gesicherte Daten häufig auf unterschiedliche Knoten verschoben werden: Wenn Sie versuchen, den neuen Knoten (auf den die Daten vom ursprünglichen Knoten verschoben werden) zu sichern, ist in diesem Szenario die Kopie bereits auf dem Ziel vorhanden, und es werden nur Verweisinformationen gesichert.

Konfigurieren von Datenspeichern mit Deduplizierung in Arcserve UDP

Folgende Parameter sind für die Konfiguration eines Datenspeichers mit Deduplizierung relevant:

Datenziel

Im Datenziel werden die geschützten Daten gespeichert. Es empfiehlt sich, für das Datenziel einen großen Datenträger zu verwenden, da es die ursprünglichen Datenblöcke der Quelle enthält.

Indexziel

Im Indexziel werden die Indexdateien gespeichert. Es empfiehlt sich, einen anderen Datenträger zu verwenden, um den Durchsatz der Deduplizierung zu verbessern.

Hash-Ziel

Im Hash-Ziel werden die Hash-Dateien gespeichert. Es empfiehlt sich, ein SSD-Laufwerk mit hoher Geschwindigkeit zu verwenden, da die Deduplizierungskapazität auf diese Weise bei geringem Bedarf an zugeordnetem Arbeitsspeicher verbessert werden kann.

Wenn das Hash-Ziel auf einem Hochgeschwindigkeits-SSD konfiguriert ist, kann es verwendet werden, um die Deduplizierungskapazität bei geringem Bedarf an zugeordnetem Arbeitsspeicher zu steigern.

Ordner des Sicherungsziels

Der Zielordner, in dem sich die D2D-Dateien und Katalogdateien befinden.

Blockgröße

Die "Blockgröße der Deduplizierung" wirkt sich auch auf die "Schätzung der Deduplizierungskapazität" aus. Der Standardwert für "Blockgröße der Deduplizierung" beträgt 16 KB. Wenn Sie ihn auf 32 KB setzen, verdoppelt sich der Wert für "Schätzung der Deduplizierungskapazität". Die Vergrößerung der Deduplizierungsblockgröße kann dazu führen, dass der Deduplizierungsprozentsatz verkleinert wird. Gleichzeitig werden die Speicheranforderungen verkleinert.

Arbeitsspeicherzuordnung

Verwenden Sie das Tool "Geschätzte Arbeitsspeicher- und Datenspeichererfordernisse", um die Speicheranforderungen einzuschätzen. Wenn der zugeordnete Speicher nicht ausreicht und der Speicher vollständig ausgelastet ist, dann können die neuen Daten das neue Hash nicht in die Hash-DB einfügen. Dadurch können Daten, die danach gesichert werden, nicht

dedupliziert werden, was dazu führt, dass das Deduplizierungsverhältnis abnimmt. Wenn Sie aus irgendeinem Grund den Speicher nicht vergrößern können, dann versuchen Sie, die Deduplizierungsblockgröße zu vergrößern, da dadurch die Speicheranforderung verkleinert wird.

Hinweis: Die Blockgröße kann für einen vorhandenen Datenspeicher nicht geändert werden.

Beachten Sie, dass ein neuer Sicherungsjob nicht gestartet werden kann, sobald der Hash-Speicher voll ist. Der aktuelle Sicherungsjob (der gestartet wurde, bevor der Hash-Speicher voll war) kann jedoch fortgeführt und abgeschlossen werden. In diesem Fall werden keine neuen Hash-Schlüssel in die Hash-Datenbank eingefügt. Dies wirkt sich auf den Deduplizierungsprozentsatz aus.

Der Grund dafür ist, dass alle Datenblöcke im aktuellen Sicherungsjob noch mit den vorhandenen Hash-Schlüsseln in der Hash-Datenbank verglichen werden.

• Wenn er mit dem vorhandenen Hash-Schlüssel dupliziert wird, dann wird er nicht mehr auf den Datenträger geschrieben.

• Wenn er nicht mit dem vorhandenen Hash-Schlüssel dupliziert wird, dann wird er auf den Datenträger geschrieben. Der neue Hash-Schlüssel wird jedoch nicht in die Hash-Datenbank eingefügt, da die Hash-Datenbank voll ist. Dadurch können die daraus folgenden Datenblöcke nicht mit diesen neuen Hash-Schlüsseln verglichen werden.

Deduplizierung, Verschlüsselung und Komprimierung

Zusätzlich zur Datendeduplizierung können für Datenspeicher auch Komprimierung und Verschlüsselung angewendet werden.

Wenn Sie Verschlüsselung aktivieren, verwendet Arcserve Unified Data Protection Agent für Windows CPU-Ressourcen, um die Daten zu verschlüsseln. Da die Verschlüsselung nur für die eindeutigen Daten eingesetzt wird, können die für die Verschlüsselung erforderlichen CPU-Ressourcen minimal ausfallen, wenn der Deduplizierungsprozentsatz hoch ist.

- Ohne Komprimierung und Deduplizierung ist die CPU-Auslastung für den Komprimierungstask niedriger, und die gespeicherten Daten verwenden ein nicht komprimiertes Format.
- Bei standardmäßiger Komprimierung und Deduplizierung ist die CPU-Auslastung für den Komprimierungstask optimal, die gespeicherten Daten verwenden ein komprimiertes Format, und die Speicherplatzanforderung ist niedrig.
- Bei maximaler Komprimierung und Deduplizierung ist die CPU-Auslastung für den Komprimierungstask maximal, die gespeicherten Daten betragen 2 bis 3 % mehr, und die Speicherplatzanforderung ist niedrig.

Einschränkungen bei der Deduplizierung

Wenn Sie einen Deduplizierungsdatenspeicher erstellt haben, können Sie Komprimierungstyp, Verschlüsselungseinstellung und Deduplizierungsblockgröße ändern.