Arcserve[®] Appliance Benutzerhandbuch

Version 7.0

arcserve

Arcserve[®] Appliance Onlinehilfe

Version 7.0

Liste der Inhalte wird im linken Fensterbereich angezeigt. Wenn Sie alle Themen anzeigen möchten, klicken Sie auf das oben verfügbare ^{\$TOC}-Symbol. CICSETVE^{*}

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 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.

© 2019 Arcserve und seine Schwestergesellschaften und Tochtergesellschaften. Alle Rechte vorbehalten. Drittanbieter-Marken oder Copyrights sind Eigentum der entsprechenden Rechtsinhaber.

Kontakt zum Arcserve-Support

Das Arcserve-Support

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.

Rückgaberichtlinie für die Arcserve Appliance

Um ein Produkt an Arcserve zurückzugeben, ist eine gültige RMA (Materialrückgabe-Autorisierung) erforderlich. Wenden Sie sich an den technischen Support von Arcserve, um eine RMA-Nummer zu erhalten. Kontaktieren Sie die Kundenbetreuung unter <u>Arcserve.com/support.</u> Support-Team kann Sie darüber informieren, wohin die RMS-Daten gesendet werden.

Rückgaben unterliegen einer Rücknahmegebühr von 10 %. Ausnahmen: 1) Wenn ein Auftrag nicht ordnungsgemäß abgewickelt wird, akzeptiert Arcserve eine RMA und gewährt den vollen Betrag als Gutschrift. 2) Wenn ein mangelhafter Artikel innerhalb von 30 Tagen zurückgegeben wird, akzeptiert Arcserve eine RMA und gewährt den vollen Betrag als Gutschrift. 3) Wenn technische Hardwareprobleme bestehen, die vom Support nach einem angemessenen Zeitraum nicht behoben werden, akzeptiert Arcserve eine RMA und ersetzt die Hardware durch eine Einheit mit gleichem Wert.

Für die RMA-Anforderung erforderliche Informationen:

- Seriennummer des Produkts (befindet sich auf der Rückseite der Appliance)
- Arcserve Bestellnummer
- Name des Ansprechpartners
- Telefonnummer des Ansprechpartners
- E-Mail-Adresse des Ansprechpartners
- Name des Ansprechpartners beim Kunden (falls verfügbar)
- Telefonnummer (falls verfügbar)
- E-Mail-Adresse (falls verfügbar)
- Beschreibung des Problems und alle Informationen zu bereits durchgeführter Fehlerbehebung.
- Angeforderter Versanddienst und Versandadresse.

Die RMA-Nummer muss deutlich sichtbar auf der Außenseite der Verpackung verzeichnet sein. Alle RMAs müssen in einer angemessenen Verpackung versandt werden. Alle RMAs sollten mit einem vertrauenswürdigen Beförderungsunternehmen versandt werden, der Paketverfolgung und -versicherung anbietet. Für Versandschäden oder verlorene RMAs trägt der Kunde die Verantwortung.

Inhalt

Kapitel 1: Informationen zu Arcserve Appliance Dokumentation .	1
Sprachenunterstützung	. 2
Produktdokumentation	. 3
Kapitel 2: Einführung in die Arcserve Appliance	5
Einführung	. 6
Arcserve Unified Data Protection	. 7
Arcserve Unified Data Protection Agent for Linux	8
Arcserve Backup	9
Arcserve Replication and High Availability (Arcserve RHA)	.10
Sicherheitsmaßnahmen	. 11
In der Box enthaltene Gegenstände	12
In der Box der Appliance 8000 Series enthaltene Gegenstände	. 13
In der Box der Appliance 9000 Series enthaltene Gegenstände	. 14
Nicht in der Box enthaltene Gegenstände	. 15
Verfügbare Modelle	. 16
Modelle 7100 - 7300v	17
Modelle 7400 - 7600v	19
Modelle 8100 - 8400	.21
Modelle 9012 - 9504DR	.22
Steuerelemente und Anzeigen	. 25
Vorderseite 7100 - 7300v	26
Vorderseite 7400 - 7600v	29
Vorderseite 8100 - 8200	.31
Vorderseite 8300 - 8400	.33
Vorderseite 9012 - 9048	.34
Vorderseite 9072DR - 9504DR	.36
Rückseite 7100 - 7300v	. 38
Rückseite 7400 - 7600v	. 40
Rückseite 8100 - 8200	42
Rückseite 8300 - 8400	44
Rückseite 9012 - 9048	45
Rückseite der 9072DR - 9504 DR	47
Von der Appliance verwendete Ports	.49

Arcserve UDP	
Unter Microsoft Windows installierte Komponenten	51
Unter Linux installierte Komponenten	55
Durch UDP Linux remote geschützter Knoten	57
Arcserve Backup	
Appliance für Linux-Unterstützung	
Hinzufügen von Ports zur CentOS 6.6 X64-Firewall	61
Kapitel 3: Installieren der Arcserve Appliance	63
So installieren Sie Arcserve Backup 18.0	64
So installieren Sie die 8100 - 8200 Series Appliance	66
So installieren Sie die 8300 - 8400 Series Appliance	67
So installieren Sie die 9012 - 9048 Series Appliance	67
So installieren Sie die 9072-9504DR Series Appliance	67
Kapitel 4: Aktualisieren von Arcserve UDP auf der Appliance	68
Anwenden einer Lizenz nach einem Upgrade der Arcserve-Software	69
Upgradesequenz aufArcserve Appliance	70
Aktualisieren der Arcserve Appliance als Arcserve UDP-Konsole und RPS	71
Aktualisieren der Arcserve Appliance als Arcserve UDP-RPS	
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance Aktualisieren von Arcserve UDP Linux Agent auf der Arcserve Appliance	ve App- 73 74
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance Aktualisieren von Arcserve UDP Linux Agent auf der Arcserve Appliance Aktualisieren von Arcserve Backup auf der Arcserve Appliance	ve App- 73 74 74
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance Aktualisieren von Arcserve UDP Linux Agent auf der Arcserve Appliance Aktualisieren von Arcserve Backup auf der Arcserve Appliance Upgradesequenz für UDP-Konsole, RPS und Agent	ve App- 73 74 75 76
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73 74 75 76 77
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73 74 75 76 77 78
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73 74 75 76 76 78 78
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73 74 75 76 77 78 78
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73 74 75 76 77 78 82 92 92 93
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73 74 75 76 77 78 82 92 92 93 94
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73 74 75 76 77 82 92 92 93 94 95
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73 74 75 76 77 78 82 92 92 93 94 95 96
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73 74 75 76 77 78 82 92 92 93 94 95 96 97
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance	ve App- 73 74 75 76 77 78 82 92 92 93 94 95 96 97 99
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser liance Aktualisieren von Arcserve UDP Linux Agent auf der Arcserve Appliance Aktualisieren von Arcserve Backup auf der Arcserve Appliance Upgradesequenz für UDP-Konsole, RPS und Agent Kapitel 5: Konfigurieren der Arcserve Appliance Konfigurieren der Netzwerkeinstellungen für Arcserve Appliance Einrichten derArcserve Appliance Konfigurieren der Arcserve Appliance Konfigurieren derArcserve Appliance Einrichten derArcserve Appliance Konfigurieren der Arcserve Appliance Konfigurieren der Arcserve Appliance Konfigurieren der Arcserve Appliance Kapitel 6: Arbeiten mit Arcserve Appliance Aktivieren eines Arcserve-Produkts auf der Appliance Erstellen eines Plans mithilfe des Arcserve Appliance-Assistenten Hinzufügen eines Knotens zu einem Plan Knoten nach Hostname/IP-Adresse hinzufügen Knoten nach Active Directory hinzufügen vCenter/ESX-Knoten hinzufügen	ve App- 73 74 75 76 77 78 82 92 92 93 94 95 96 97 99 91
Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcser Iiance Aktualisieren von Arcserve UDP Linux Agent auf der Arcserve Appliance Aktualisieren von Arcserve Backup auf der Arcserve Appliance Upgradesequenz für UDP-Konsole, RPS und Agent Kapitel 5: Konfigurieren der Arcserve Appliance Konfigurieren der Netzwerkeinstellungen für Arcserve Appliance Einrichten derArcserve Appliance Konfigurieren derArcserve Appliance Konfigurieren derArcserve Appliance Kapitel 6: Arbeiten mit Arcserve Appliance Aktivieren eines Arcserve-Produkts auf der Appliance Erstellen eines Plans mithilfe des Arcserve Appliance Hinzufügen eines Knotens zu einem Plan Knoten nach Hostname/IP-Adresse hinzufügen vCenter/ESX-Knoten hinzufügen Hyper-V-Knoten hinzufügen	ve App- 73 74 75 76 77 78 82 92 92 93 94 95 94 95 96 97 99 101 104

Sicherungsablaufplan für ein Bandgerät erstellen	107
Virtuellen On-Appliance-Standby-Plan erstellen	109
Erstellen eines Plans zur Sicherung von Linux-Sicherungsserver	110
Einrichten von Linux-Instant VM-Jobs im lokalen Appliance-Hyper-V	114
Migrieren der Arcserve UDP-Konsole mithilfe von ConsoleMigration.exe	115
Migrieren des vorinstallierte Linux-Sicherungsservers in CentOS 7.4	118
Durchführen der Migration zwischen Arcserve Appliances	120
Lösung 1	121
Lösung 2	126
Ändern der Eingabequelle des vorinstallierten Linux-Sicherungsservers	129
Kapitel 7: Überwachen des Appliance-Servers per Remote- Zugriff	133
Arbeiten mit IPMI	134
So ändern Sie das IPMI-Kennwort	135
So aktualisieren Sie die IPMI-Firmware	138
Arbeiten mit dem integrierten Dell Remote Access Controller (iDRAC)	139
Überwachung und Verwaltung des integrierten Dell Remote Access Controller (iDRA	4C) .140
Suchen der IP-Adresse des integrierten Dell Remote Access Controller (iDRAC)	142
Konfigurieren der DHCP- oder statischen IP-Adresse des iDRAC	144
Kapitel 8: Wiederherstellen oder Reparieren derArcserve Appliance	151
Debuggen und auf Werkseinstellungen zurücksetzen	152
Anwenden von Arcserve UDP-Werkseinstellungen unter Verwendung der Start- option in 7000-8000 Series Appliance	154
Anwenden von Arcserve UDP-Werkseinstellungen unter Verwendung der Start- option für Geräte der 9012-9504DR Serie	
Löschen der Konfiguration und Zurücksetzung der Appliance auf Werk- seinstellungen	160
Festplatte entfernen und ersetzen	164
Durchführen einer Bare Metal Recovery (BMR), ohne Daten beizubehalten	166
Durchführen einer Perform Bare Metal Recovery (BMR) und Beibehalten der Da	iten <mark>181</mark>
Kapitel 9: Durchführung einer Kapazitätserweiterung der App- liance	189
Arbeiten mit dem Erweiterungs-Kit in Arcserve Appliance 9012-9504 DR-Modelle	en <mark>190</mark>
Herstellen einer Verbindung zwischen dem Appliance-Server und dem Applianc Erweiterungs-Shelf	e- 197
Appliance-Infield-Erweiterung für alle verfügbaren Modelle	198
In der Box enthaltene Gegenstände	208

So stellen Sie eine Verbindung zwischen dem Appliance-Server und dem Appliance- Erweiterungs-Shelf her	211
So ändern Sie den Arcserve UDP-Datenspeicher	219
Hinzufügen eines Datenpfades auf dem Expansion Shelf zum Arcserve UDP-Datenspeicher $\ .$	220
Migrieren eines Hash-Ziels zur neuen SSD	221
Überprüfen die Gesamtkapazität des Datenspeichers auf der Arcserve UDP-Konsole	
Fortsetzen aller Pläne von der Arcserve UDP-Konsole	223
Kapitel 10: Arbeiten mit Netzwerkkonfiguration	225
Funktionsweise der Netzwerkkonfigurationsdetails	226
Konfiguration des NIC-Teaming-Prozesses	231
Deaktivieren des DHCP-Servers	233
Konfigurieren der IP-Adresse für den vorinstallierten Linux-Sicherungsserver	234
Aktivieren von Round-Robin auf dem DNS-Server zur Bereitstellung von Las- tenausgleich	236
So überprüfen Sie den Netzwerkstatus auf der Appliance	237
Kapitel 11: Sicherheitsmaßnahmen	238
Allgemeine Sicherheitsmaßnahmen	239
Sicherheitsmaßnahmen zur Elektrik	241
FCC-Konformität	243
Vorsichtsmaßnahmen gegen elektrostatische Entladungen (ESD)	244
Kapitel 12: Aktivieren von Sophos auf der Arcserve Appliance	. 245
Methode 1: Aktivieren von Sophos auf der Arcserve Appliance über die E-Mail	246
Methode 2: Aktivieren von Sophos auf der Arcserve Appliance mithilfe eines Skripts	247
Manuelle Installation von Sophos Intercept X Advanced for Server auf Arcserve Appliances	249
Kapitel 12: Aktualisieren der Firmware für Arcserve Appliance 9000 Series	. 254
Upgrade der BIOS-Firmware für Arcserve Appliance 9000 Series	254
Anzeigen der BIOS-Firmwareversion	254
Methode 1: BIOS-Firmware-Version von iDRAC Web Interface anzeigen	254
Methode 2: BIOS-Firmware-Version von BIOS Arcserve Appliance 9000 Series anzeigen	255
Herunterladen des aktualisierten Pakets für BIOS	256
BIOS aktualisieren	256
Überprüfen des aktualisierten BIOS	257
Überprüfen des aktualisierten BIOS mithilfe von Systemprotokollen	257
Überprüfen des aktualisierten BIOS über iDRAC Web Interface oder BIOS	258

Aktualisieren der iDRAC-Firmware für Arcserve Appliance 9000 Series	258
Anzeigen der iDRAC-Firmwareversion	258
iDRAC-Firmwareversion von iDRAC Web Interface anzeigen	259
Methode 2: iDRAC-Firmwareversion von BIOS Arcserve Appliance 9000 Series anzeigen	260
Herunterladen des aktualisierten Pakets für iDRAC	261
iDRAC aktualisieren	261
Überprüfen des aktualisierten BIOS	262
Überprüfen des aktualisierten iDRAC mithilfe von Systemprotokollen	262
Überprüfen des aktualisierten iDRAC von iDRAC Web Interface oder BIOS	263
Kapitel 13: Fehlerbehebung	
Linux-Sicherungsserver kann über die Konsole keine Verbindung herstellen	266
Sichern einer Arcserve Applianceaus duplizierten Knoten anderer Appliance- Berichte	268
Linux-Sicherungsserver kann nicht mit einem Knoten im Netzwerk kommunizie	ren <mark>269</mark>
Linux-Sicherungsserver kann das Netzwerk-DNS-Suffix nicht abrufen	271
Standardzeitzone auf der Appliance	272
Lizenzfehler, auch wenn Lizenzen verfügbar sind	
ARCserve UDP-Konsole zeigt beim Hinzufügen einer replizierten Remote-Konso zu einer remote verwalteten RPS-Task einen Fehler an	le 274
Die VSB-Task kann nicht mit einer anderen Appliance als Überwachungsserver durchgeführt werden	276
Kapitel 14: Best Practices	
Best Practices für die Netzwerkkonfiguration	279
Best Practices für Windows-Defender mit PowerShell-cmdlets	
Konfigurieren des vorinstallierten Linux-Sicherungsservers für externes Netzwei	rk282
Bewährte Methoden zum Ersetzen des Werkseinstellungs-Image wenn mit Sop gesichert	hos 283
Bewährte Verfahren zum Erstellen von Deduplizierungsdatenspeichern über Vo mes hinweg)lu- 293
Kapitel 15: Lizenzhinweise	296
PuTTY	297

Kapitel 1: Informationen zu Arcserve Appliance Dokumentation

Mithilfe des Arcserve Appliance Benutzerhandbuchs erfahren Sie, wie Sie Arcserve Appliance verwenden. Informationen zu Arcserve Appliance finden Sie in der Einführung. Im weiteren Verlauf des Abschnitts erhalten Sie Informationen zur Installation und Verwendung von Arcserve Appliance.

Dieser Abschnitt enthält folgende Themen:

Sprachenunterstützung	. 2
Produktdokumentation	. 3

Sprachenunterstützung

Die Dokumentation ist auf Englisch und in mehreren lokalen Sprachen verfügbar.

Ein übersetztes Produkt (manchmal auch als lokalisiertes Produkt bezeichnet) beinhaltet eine lokale Sprachenunterstützung für die Benutzeroberfläche, die Online-Hilfe und weitere Produktdokumentationen, sowie lokale Standardspracheneinstellungen für Datums-, Uhrzeit-, Währungs- und Zahlenformate.

Diese Version ist in den folgenden Sprachen verfügbar:

- Englisch
- Chinesisch (Vereinfacht)
- Chinesisch (Traditionell)
- Französisch
- Deutsch
- Italienisch
- Japanisch
- Koreanisch
- Portugiesisch (Brasilien)
- Spanisch

Produktdokumentation

Wenn Sie die Arcserve UDP-Dokumentation erhalten möchten, klicken Sie auf diesen Link zur <u>Arcserve-Dokumentation</u>.

Das Knowledge Center von Arcserve UDP umfasst die folgende Dokumentation:

Arcserve UDP Lösungshandbuch

Enthält ausführliche Informationen über die Verwendung der Arcserve UDP-Lösung in einer zentral verwalteten Konsolenumgebung. Dieses Handbuch enthält Informationen darüber, wie Sie die Lösung installieren und konfigurieren, wie Sie Ihre Daten schützen und wiederherstellen, wie Sie Berichte erstellen und wie Sie Arcserve High Availability verwalten. Die Vorgehensweisen sind konsolenorientiert und schließen Anleitungen zur Verwendung der verschiedenen Schutzpläne ein.

Arcserve UDP Versionshinweise

Enthält zusammenfassende Beschreibungen der wichtigsten Funktionen, Systemvoraussetzungen, bekannter Probleme oder Fehler in der Dokumentation sowie von Anwendungsgrenzen von Arcserve Unified Data Protection.

Arcserve UDP-Agent f ür Windows – Benutzerhandbuch

Enthält ausführliche Informationen über die Verwendung des Arcserve UDP-Agenten in einem Windows-Betriebssystem. Dieses Handbuch enthält Informationen z. B. zur Installation und Konfiguration des Agent und zum Schutz und zur Wiederherstellung der Windows-Knoten.

Arcserve UDP-Agent f ür Linux – Benutzerhandbuch

Enthält ausführliche Informationen über die Verwendung des Arcserve UDP-Agenten in einem Linux-Betriebssystem. Dieses Handbuch enthält Informationen z. B. zur Installation und Konfiguration des Agenten und zum Schutz und zur Wiederherstellung von Linux-Knoten.

Kapitel 2: Einführung in die Arcserve Appliance

Dieser Abschnitt enthält folgende Themen:

Einführung	6
Sicherheitsmaßnahmen	11
In der Box enthaltene Gegenstände	
Nicht in der Box enthaltene Gegenstände	15
Verfügbare Modelle	16
Steuerelemente und Anzeigen	
Von der Appliance verwendete Ports	49

Einführung

Arcserve Appliance ist die erste und kostengünstigste Datenschutz-Appliance mit Assured Recovery[™]. Jede Arcserve Appliance ist eine eigenständige Sicherungs- und Wiederherstellungslösung, die nur einmal eingerichtet werden muss. Die Architektur mit systemeigenen Cloud-Funktionen bietet eine unübertroffen einfache Bereitstellung und Benutzerfreundlichkeit, eine breite Palette von Funktionen wie globale quellbasierte Datendeduplizierung, Replikation an mehreren Standorten, Unterstützung für Bandlaufwerke und automatisierte

Datenwiederherstellungsfunktionen. Die Arcserve Appliance bietet unübertroffene Agilität und Effektivität sowie drastische Vereinfachungen von Disaster Recovery-Aktivitäten.

Arcserve Appliance ist vollständig mit der branchenführendenArcserve Unified Data Protection-Software integrierte, die auf modernen Hardware vorinstalliert ist. Die Appliance bietet eine vollständige und integrierte Datenschutzlösung für alle Benutzer, die nicht nur Ihren derzeitigen Anforderungen entspricht, sondern auch in Zukunft die sich stetig wandelnden Anforderungen für Sicherung, Archivierung und Notfallwiederherstellung erfüllt.

Folgende Software ist auf der Arcserve Appliance vorinstalliert:

- Arcserve UDP
- Arcserve Unified Data Protection Agent for Linux
- Arcserve Backup

Arcserve Appliance wird mit Hardware-Garantie definiert. Genauere Informationen zu dieser Garantie finden Sie unter <u>arcserve.com/arcserve-appliance-warranty</u>.

Arcserve Unified Data Protection

Die Arcserve UDP-Software ist eine umfassende Lösung für den Schutz komplexer IT-Umgebungen. Die Lösung schützt Ihre Daten auf verschiedenen Arten von Knoten wie Windows-Rechnern, Linux-Rechnern und virtuellen Rechnern auf VMware ESX-Servern oder Microsoft Hyper-V-Servern. 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.

Weitere Informationen zu den unterstützten Betriebssystemen finden Sie in der Kompatibilitätsmatrix.

Arcserve UDP bietet folgende Funktionen:

- Sichern von Daten in Datenspeichern mit/ohne Deduplizierung auf Recovery Point Servern
- Sichern von Wiederherstellungspunkten auf Band durch Integration in Arcserve Backup (ebenfalls in der Appliance enthalten)
- Erstellen von Virtual Standby-Rechnern aus Sicherungsdaten
- Replizieren von Sicherungsdaten auf Recovery Point Servern und Remote-Recovery Point Servern
- Wiederherstellen von Sicherungsdaten und Durchführen einer Bare-Metal-Recovery (BMR)
- Kopieren ausgewählter Datensicherungsdateien auf einen sekundären Sicherungsspeicherort
- Konfigurieren und Verwalten von Arcserve Full System High Availability (HA) f
 ür kritische Server in Ihrer Umgebung

Mit Arcserve UDP können Sie Sicherungsdaten, die als Wiederherstellungspunkte gespeichert wurden, von einem Server auf einen anderen Recovery Point Server replizieren. Sie können aus den Sicherungsdaten auch virtuelle Rechner erstellen, die bei Fehlern des Quellknotens als Standby-Rechner agieren können. Der virtuelle Standby-Rechner wird erstellt, indem Wiederherstellungspunkte in ein VMware ESX- oder Microsoft Hyper-V-Format für virtuelle Rechner konvertiert werden.

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

Weitere Informationen finden Sie im Arcserve UDP Lösungshandbuch.

Arcserve Unified Data Protection Agent for Linux

Arcserve Unified Data Protection Agent for Linux ist ein festplattenbasiertes Sicherungsprodukt, das für Linux-Betriebssysteme konzipiert wurde. Es bietet eine schnelle, einfache und zuverlässige Möglichkeit zum Schützen und Wiederherstellen von wichtigen Unternehmensdaten. Arcserve Unified Data Protection Agent for Linux verfolgt Änderungen in Knoten auf Blockebene und sichert nur die geänderten Blöcke in einem inkrementellen Vorgang. Dadurch ermöglicht die Software häufige Sicherungen. Die Größe der einzelnen Zuwachssicherungen reduziert sich (und damit auch das Zeitfenster für die Sicherung), und der Status der Sicherungen ist aktueller. Zusätzlich verfügt Arcserve Unified Data Protection Agent for Linux über eine Funktion zur Wiederherstellung von Dateien oder Ordnern sowie zur Bare-Metal-Recovery (BMR) einzelner Sicherungen. Sie können die Sicherungsinformationen auf einer NFS-Freigabe (Network File System) oder auf einer CIFS-Freigabe (Common Internet File System) im Sicherungsquellknoten speichern.

Die neueste Version von Arcserve Unified Data Protection Agent for Linux ist auf einem virtuellen Rechner in der Appliance vorinstalliert. Dieser virtuelle Rechner wird zum Linux-Sicherungsserver. Arcserve Unified Data Protection Agent for Linux ist im Standardinstallationspfade in der Arcserve Appliance installiert.

Wenn Sie die Konsole öffnen, ist der Linux-Sicherungsserver bereits zur Konsole hinzugefügt. Der systemeigene Hostname des Linux-Sicherungsserver lautet *Linux-BackupSvr*. Auf der Konsole übernimmt der Linux-Sicherungsserver jedoch den Hostnamen der Appliance mit der Konfiguration für Port 8018. Der Linux-Sicherungsserver arbeitet mittels Portdurchleitung hinter NAT. Der Linux-Sicherungsserver verwendet Port 8018 zur Kommunikation und zur Übertragung von Daten in der Arcserve Appliance.

Hinweis: Weitere Informationen zum Erstellen von Sicherungsplänen und zum Wiederherstellen von Linux-Rechnern finden Sie im Benutzerhandbuch zu Arcserve UDP Agent for Linux.

Der Linux-Sicherungsserver verwendet die folgenden Standard-Anmeldeinformationen:

- Benutzername: root
- Kennwort: Arcserve

Hinweis: Es wird empfohlen, das Standardkennwort zu ändern.

Arcserve Backup

Arcserve Backup ist eine hochleistungsfähige Lösung für die Datenschutzanforderungen von Unternehmen mit heterogenen Umgebungen. Sie bietet flexible Leistungsfähigkeit bei der Sicherung und Wiederherstellung, unkomplizierte Verwaltung, breite Geräteunterstützung und unübertroffene Zuverlässigkeit. Mit dieser Lösung können Sie Ihre Datenspeicherungsfähigkeiten optimieren, indem Sie Ihre Datenschutzstrategien an Ihre Speicheranforderungen anpassen. Darüber hinaus ermöglicht die flexible Benutzeroberfläche erweiterte Konfigurationen und bietet unabhängig von den technischen Vorkenntnissen der Benutzer ein kostengünstiges Mittel zur Implementierung und Verwaltung einer Vielzahl von Agenten und Optionen.

Arcserve Backup bietet umfassenden Datenschutz für verteilte Umgebungen und bietet virenfreie Sicherungs- und Wiederherstellungsvorgänge. Mit einer umfangreichen Palette an Optionen und Agenten bietet es besseren Datenschutz im gesamten Unternehmen. Zu den erweiterten Funktionen zählen Online-Sicherung und -Wiederherstellung bei laufendem Betrieb von Anwendungen und Datendateien, optimierte Geräte- und Datenträgerverwaltung sowie Systemwiederherstellung.

Arcserve ApplianceDie umfasst die Integration mit Arcserve Backup, um eine Sicherung auf Band vornehmen zu können. Arcserve Backup wird auf Ihrem Computer unter "C:\Programme (x86)\Arcserve" installiert, nachdem Sie "InstallASBU.bat" ausgeführt haben. Mithilfe der in der Arcserve Appliance installierten Komponenten können Sie das Ziel von Arcserve UDP auf einem Band sichern. Weitere Informationen zu den unterstützten Betriebssystemen finden Sie in der <u>Kom</u>patibilitätsmatrix.

Sie können das vollständige Installationspaket von Arcserve Backup von der Arcserve-Website herunterladen, um weitere Komponenten zu installieren. Weitere Informationen finden Sie in der <u>Arcserve Backup Dokumentation</u>.

Arcserve Backup Server verwendet die folgenden Standard-Anmeldeinformationen:

- Benutzername: caroot
- Kennwort: Arcserve

Arcserve Replication and High Availability (Arcserve RHA)

Arcserve RHA ist eine auf asynchroner Echtzeitreplikation sowie automatisiertem Switchover und Switchback für Anwendungen basierende Lösung, die es ermöglicht, kostengünstige Geschäftskontinuität für virtualisierte Umgebungen auf Windows-Servern zur Verfügung zu stellen. Weitere Informationen zu den unterstützten Betriebssystemen finden Sie in der <u>Kompatibilitätsmatrix</u>.

Arcserve RHA ermöglicht es Ihnen, Daten auf einen lokalen oder Remote-Server zu replizieren und somit jene Daten nach einem Serverabsturz oder Website-Disaster wiederherzustellen. Sie können Ihre Benutzer manuell oder automatisch auf den Replikatserver umschalten, wenn Sie über eine High Availability-Lizenz verfügen.

Hinweis: Arcserve RHA ist nicht in der Anwendung vorinstalliert. Weitere Informationen zum Installieren und Konfigurieren von Arcserve RHA finden Sie im <u>Instal-</u> <u>lationshandbuch</u>

Sicherheitsmaßnahmen

Aus Sicherheitsgründen müssen Sie alle Anweisungen durchlesen und befolgen, bevor Sie eine Arcserve Appliance auspacken, anschließen, installieren, einschalten oder in Betrieb nehmen. Wenn Sie die Sicherheitsmaßnahmen nicht einhalten, kann dies zu Verletzungen, zu Geräteschäden oder zu Fehlfunktionen führen.

Weitere Informationen zu den Sicherheitsmaßnahmen finden Sie im <u>Anhang</u> - <u>Sicherheitsmaßnahmen</u>.

In der Box enthaltene Gegenstände

In diesem Abschnitt sind die Gegenstände beschrieben, die in der Box folgender Appliance-Serien enthalten sind:

- 8000-Serie
- <u>9000-Serie</u>

In der Box der Appliance 8000 Series enthaltene Gegenstände

Folgende Gegenstände sind in der Box enthalten:

- Arcserve Appliance (Etikett mit der Seriennummer befindet sich auf der Rückseite der Appliance)
- Netzkabel: 1
- Netzwerkkabel: 1 rotes, 1 blaues (jeweils 1 m lang)
- IPMI-Portkabel: 1 (2 m lang)
- Montagekit Schiene/Rack enthält Folgendes:
 - 2 schnellmontierbare äußere Schienen
 - 2 innere Schienenerweiterungen
 - 3 Schienenadapter (nur Standardschienenmontage)
 - Weitere zugehörige Hardware nach Bedarf
- Arcserve-Abdeckplatte
- Microsoft Clientzugriffslizenz

Hinweis: Überprüfen Sie die Box, in der die Appliance geliefert wurde, und stellen Sie sicher, dass keine Gegenstände in der Box fehlen und keine sichtbaren Anzeichen von Beschädigungen vorliegen. Wenn Gegenstände fehlen oder beschädigt sind, bewahren Sie alle Verpackungsmaterialien auf, und wenden Sie sich an den Arcserve-Support.

In der Box der Appliance 9000 Series enthaltene Gegenstände

Arcserve Appliance9000 Serie enthält zwei Boxen: eine für 9012, 9024, 9048 und ein andere für 9072DR-9504 Disaster Recovery. Im Folgenden sind alle Gegenstände aufgeführt, die in den Boxen enthalten sind.

Die folgenden Elemente sind in der 9012, 9024, 9048 Zubehörbox enthalten:

- BLENDE, 1 E Box, 14G BLENDENBAUGRUPPE, LCD-Anzeige, AR (380-7406)
- SCHNELLSTARTHANDBUCH, ARCSERVE, INFODATEI ARCSERVE APPLIANCE
- HARDWARE-INSTALLATIONS HANDBUCH ARCSERVE DELL R440
- KABLE, FLEXBOOT, CAT6, NETZWERK, 3FT, ROT
- KABEL, FLEXBOOT, CAT6, NETZWERK, 3FT, BLAU
- KABEL, FLEXBOOT, CAT6, NETZWERK, 7FT, SCHWARZ
- Dell Handbuch Sicherheit, Umgebung, Vorschriften
- US-Netzkabel (2 X)a

Hinweis: Überprüfen Sie die Box, in der die Appliance geliefert wurde, und stellen Sie sicher, dass keine Gegenstände in der Box fehlen und keine sichtbaren Anzeichen von Beschädigungen vorliegen. Wenn Gegenstände fehlen oder beschädigt sind, bewahren Sie alle Verpackungsmaterialien auf, und wenden Sie sich an den Arcserve-Support.

Die folgenden Gegenstände sind in der 9072DR-9504DR Zubehörbox mit einem Rack-Schienenkit enthalten:

- BLENDE, 2E Box, CUS 14G BLENDENBAUGRUPPE, LCD, AR, (380-7405)
- SCHNELLSTARTHANDBUCH, ARCSERVE, INFODATEI ARCSERVE APPLIANCE
- HARDWARE-INSTALLATIONSHANDBUCH ARCSERVE DELL R740
- KABLE, FLEXBOOT, CAT6, NETZWERK, 3FT, ROT
- KABEL, FLEXBOOT, CAT6, NETZWERK, 3FT, BLAU
- KABEL, FLEXBOOT, CAT6, NETZWERK, 7FT, SCHWARZ
- KABELBAUGRUPPE, MINI-SAS, EXTERN, SFF-8088 ZU SFF-8644, 1M
- Dell Handbuch Sicherheit, Umgebung, Vorschriften
- US-Netzkabel (2 X)

Nicht in der Box enthaltene Gegenstände

Die folgenden Gegenstände sind nicht in der Box enthalten, aber eventuell für die Installation und Konfiguration der Appliance erforderlich:

- Überwachung
- Tastatur
- Externes Speichergerät (bei Bedarf)

Verfügbare Modelle

Die Serien Arcserve Appliance 7000, 8000 und 9000 sind je nach Ihren Anforderungen in unterschiedlichen Modellen verfügbar:

- Modelle 7100 7300v
- Modelle 7400 7600v
- Modelle 8100 8400
- Modelle 9012 9504 DR

Modelle 7100 - 7300v

Arcserve Appliance Modelle 7100 - 7300v

Arcserve Appliance Spezifikationen für die 7000-Serie						
Appliance-Modell	7100	7200	7200V	7300	7300V	
Sicherungsspeicherkapazität						
Reine Spei- cherkapazität*	3 TB	6 ТВ	6 TB	9 TB	9 TB	
Nutzbare Siche- rungskapazität**	2,8 TB	5,8 TB	5,8 TB	8,8 TB	8,8 TB	
Geschützte Kapazität (Quelldaten)***	Bis zu 8 TB	Bis zu 17 TB	Bis zu 17 TB	Bis zu 26 TB	Bis zu 26 TB	
Standardfunktionen						
Einheitliche Verwaltungs rungen auf Blockebene, erweiterte Virtualisierun Standby, Unterstützung Wiederherstellung, einh	Einheitliche Verwaltungskonsole, globale Deduplizierung, unbegrenzte inkrementelle Siche- rungen auf Blockebene, Komprimierung, Verschlüsselung, WAN-optimierte Replikation, erweiterte Virtualisierungsunterstützung, Sicherung ohne Agenten, Virtuelles Remote- Standby, Unterstützung für Bandlaufwerke, anwendungskonforme Sicherungen, granulare Wiederberstellung, einheitliche Berichte und Dasbhoard					
Virtuelles On-Appliance- Standby	N/V	N/V	Bis zu 3 vir- tuelle Maschinen	N/V	Bis zu 3 vir- tuelle Maschinen	
Gewährleistung und tech	nnische Daten					
Gewährleistung für das gesamte Systemdepot			3 Jahre			
Abmessungen (H x B x T in Zoll)	1.7" x 17,2	" x 25,6" (1HE -	mit rackmon	tierten 19 Zol	l-Schienen)	
Remoteverwaltungs- und Netz- werkschnittstellen- Ports		1 x IPMI und 2 x 1 GbE (RJ45)				
Festplattentyp und	4 x 1 TB SAS	4 x 2 TB SAS	4 x 2 TB SAS	4 x 3 TB SAS	4 x 3 TB SAS	
RAID-Konfiguration	(RAID 5)	(RAID 5)	(RAID 5)	(RAID 5)	(RAID 5)	
Konnektivität für externe Bandsicherung (SAS, SATA-Controller, FC)	1 x PASS					
System-RAM insgesamt	16 GB	16 GB	32 GB	32 GB	48 GB	
SSD-Laufwerk	120 GB SSD	120 GB SSD	120 GB SSD	240 GB SSD	240 GB SSD	

(Für Deduplizierungs-							
Hashtabellen)							
Maximalgewicht (lb)			41 lb				
Netzteile							
(einzeln oder red- undant)			1 x 600 W				
, Stromverbrauch							
(Wattzahl beim Leer- lauf/Laden/Starten)	93/116/143	122/164/143	125/167/145	125/167/145	129/188/152		
Wechselspannungs- und Frequenzbereich		100 - 240 V					
Amperewert			7,5 A max.				
1 TB = 1.000.000.000.000) Byte						
** Für V-Modelle wird der für die Sicherung verfügbare Speicherplatz um die Größe der Vir- tual Standby-VMs reduziert.							
***Geschätzte Kapazität unter Annahme eines normalen Deduplizierungs- und Kom- pressionsverhältnisses von 3:1. Die tatsächliche Sicherungskapazität kann je nach Daten- typ. Sicherungstyp. Ablaufplan usw. erheblich varijeren							
(1, p) Siener angstyp) Abit							

Modelle 7400 - 7600v

Arcserve Appliance Modelle 7400 - 7600v

Arcserve Appliance Spezifikationen für die 7000-Serie						
Appliance-Modell	7400	7400V	7500	7500V	7600	7600V
Sicherungsspeicherkapazität						
Reine Spei- cherkapazität*	16 TB	16 TB	20 TB	20 TB	30 TB	30 TB
Nutzbare Siche- rungskapazität**	15,8 TB	15,8 TB	19,8 TB	19,8 TB	29,8 TB	29,8 TB
Geschützte Kapazität (Quelldaten)***	Bis zu 46 TB	Bis zu 46 TB	Bis zu 58 TB	Bis zu 58 TB	Bis zu 90 TB	Bis zu 90 TB
Standardfunktionen						
Einheitliche Verwaltungs rungen auf Blockebene, erweiterte Virtualisierun Standby, Unterstützung Wiederherstellung, einh	konsole, g Komprimi gsuntersti für Bandla eitliche Be	globale Dedupl erung, Verschl ützung, Sicheru aufwerke, anw richte und Das	izierung, u üsselung, ung ohne i endungsk hboard.	unbegrenzte WAN-optim Agenten, Vi onforme Sie	e inkremei hierte Repl rtuelles Re cherunger	ntelle Siche- ikation, emote- n, granulare
Virtuelles On-Appliance- Standby	N/V	Bis zu 6 vir- tuelle Maschi- nen	N/V	Bis zu 9 vir- tuelle Maschinen	N/V	Bis zu 12 virtuelle Maschinen
Gewährleistung und tech	nische Dat	ten				
Gewährleistung für das gesamte Systemdepot			3 Ja	hre		
Abmessungen (H x B x T in Zoll)	3,5" x 1	7,2" x 25,6" (2ŀ	HE - mit ra	ckmontierte	en 19 Zoll-:	Schienen)
Remoteverwaltungs- und Netz- werkschnittstellen-Ports	1 x IPMI 8	& 2 x 1 GbE (RJ4	45) und 4 x	k 1 GbE (RJ4	5). Option	al 2 x 10 Gb
Festplattentyp und RAID-Konfiguration	10 x 2 TB SAS (RAID 6)	10 x 2 TB SAS (RAID 6)	12 x 2 TB SAS (RAID 6)	12 x 2 TB SAS (RAID 6)	12 x 3 TB SAS (RAID 6)	12 x 3 TB SAS (RAID 6)
Konnektivität für externe Bandsicherung (SAS, SATA-Controller, FC)	1 x PASS					
System-RAM insgesamt	64 GB	96 GB	64 GB	96 GB	128 GB	192 GB
SSD-Laufwerk	240 GB SSD	240 GB SSD	480 GB SSD	480 GB SSD	480 GB SSD	480 GB SSD

(Für Deduplizierungs-						
Hashtabellen)	<u> </u>					
Maximalgewicht (lb)			52	lb		
Netzteile						
(einzeln oder red-			2 x 92	20 W		
undant)						
Stromverbrauch	208/257/	208/257/	208/257/	208/257/	240/296/	240/296/
(Wattzahl beim Leer-		200, 200,			,,	,,
lauf/Laden/Starten)	358	358	358	358	369	369
Wechselspannungs-		100, 240)/				
und Frequenzbereich			100 - 2	240 V		
Amperewert			11 A ı	max.		
1 TB = 1.000.000.000) Byte					
** Für V-Modelle wird de	er für die S	icherung verfü	gbare Spe	eicherplatz u	ım die Grö	oße der Vir-
tual Standby-VMs reduziert.						
***Geschätzte Kapazität unter Annahme eines normalen Deduplizierungs- und Kom-						
pressionsverhältnisses von 3:1. Die tatsächliche Sicherungskapazität kann je nach Daten-						

typ, Sicherungstyp, Ablaufplan usw. erheblich variieren.

Modelle 8100 - 8400

Arcserve Appliance Modelle 8100 - 8400

Arcserve Appliance Spezifikationen für die 8000-Serie									
Appliance-Modell	UDP 8100	UDP 8200	UDP	UDP					
			8300	8400					
			48 TB	96 TB					
Quellensicherung*	12 TB bis 18 TB	24 TB bis 36 TB	bis 128	bis 240					
			ТВ	ТВ					
System-RAM	32 GB	32 GB	64 GB	128 GB					
			96	160					
May RAM **	64 GB/96 G	B/160 GB	GB/128	GB/192					
	04 00/30 0	ID/ 100 GB	GB/192	GB/256					
			GB	GB					
SSD Laufwork			480 GB	1,2 TB					
SSD-Laurwerk	120 GB 33D	200 GB 33D	SSD	SSD					
			E5-	E5-					
			2640	2650					
Drozoccor	E5-2609 V4, 8-CORE 1,7	E5-2620 V4, 8-CORE	V4, 10-	V4, 12-					
Prozessor	GHZ	2,1 GHZ	CORE	CORE,					
			2,4	2,2					
			GHZ	GHZ					
RAID-Karte	9361	L-4i	936	1-8i					
RAID-Kon-			RAID	6 mit					
figuration			BE	3U					
Laufwerkschächte	4		1	2					
			6 x 4	6 x 8					
			TB SAS	TB SAS					
			12G	12G					
			7 x 4	7 x 8					
			TB SAS	TB SAS					
Laufwerke	3 x 2 TB SAS 12G	3 x 4 TB SAS 12G	12G	12G					
	4 x 2 TB SAS 12G	4 x 4 TB SAS 12G	 Q v /	Q v Q					
			126	126					
			120	120					
			9 x 4	9 x 8					
			TB SAS	TB SAS					

		12G	12G			
		10 x 4	10 x 8			
		TB SAS	TB SAS			
		12G	12G			
		11 x 4	11 x 8			
		TB SAS	TB SAS			
		12G	12G			
		12 x 4	12 x 8			
		TB SAS	TB SAS			
		12G	12G			
		4 x 16	4 x 32			
		GB	GB			
DIMMs/Max. DIMMs	4 x 8 GB DDR4-2400/ 8	DDR4-	DDR4-			
		2400/	2400/			
		8	8			
Karten	LSI SAS9200-8E					
Netzteile		2 x, 920 W,				
		Hot-Swap-				
	2 x Hot Swan fähig, rodundant 500 W/ Woch	fähig, red-				
	solstrom Platinum	undant, hoch-				
		effizient,				
		Wechselstrom,				
		Platinum				

*Geschätzte Kapazität unter Annahme eines normalen Deduplizierungs- und Kompressionsverhältnisses von 3:1. Die tatsächliche Sicherungskapazität kann je nach Datentyp, Sicherungstyp, Sicherungsablaufplan usw. erheblich variieren.

**Arcserve Appliance verfügt über zusätzlichen Arbeitsspeicher, damit Virtual Standby / Instant VM-Recovery auf den Appliances gehostet werden können. Die Größe des zugeordneten VM-Speichers sollte von der Arbeitslast des Gast-BS abhängig gemacht werden. Arcserve bietet auch die Option, der standardmäßigen Appliance-Konfiguration je nach Kundenanforderungen zusätzlichen RAM hinzuzufügen.

Modelle 9012 - 9504DR

Arcserve Appliance Modelle 9012 - 9504DR

Arcserve Appliance Spezifikationen für die 9000-Serie											
Appliance-	901	902 [.]	904	9072-	9096-	9144-	<mark>9192</mark> -	9240-	9288-	9360-	
Modell	2	4	8	DR	DR	DR	DR	DR	DR	DR	9504DK

Nutzbare Kapa-	4	8	16	24 TD	э л тр	10 TD				120	1C0 TD		
zität	ТΒ	ΤВ	ΤВ	24 18	32 18	48 18	04 18	80 18	90 18	ТВ	109 18		
Quel-	12	24	48	72 TB		144	192	240	288	360	504 TB		
lensicherung	ΤВ	ΤВ	ТΒ	/210	90 16	ТВ	ТВ	ТВ	ТВ	ТВ	304 16		
											12 x 32		
System-RAM	6 x 8 GB (48				GB								
	GB)				(384								
Max. RAM /	176 GB / 10				768 GB								
DIMMS	DIMMS												
SSD Laufwork	190		<u>, ()</u>			2 v							
SSD-Laurwerk	400				2 X 1,9 IB SSD (RAID1)								
	her	4109	N 311- R 8-										
Prozessor)RF 1	.8		Intel Xeon Silber 4114, 10-CORE, 2,2 GHz								
		GHz	_,_										
Anzahl der Pro-													
zessoren	1			2									
	PERC H730P												
RAID Karta	Low-Profile												
NAID-Nai te	Adapter 2 GB			FERC 11/30F, WILLICALU, Z OD INV CAULE									
	NV Cache												
RAID-Kon-	RAID-5			RAID-6									
figuration													
Lauf-	4		16										
werkschachte					1		1		1	,			
Erweiterungs-		NA		11	10	8	6	4	6	4	NA		
Laufwerke	2		8	5 x 8	6 x 8	8 x 8	10 x	12 x	10 x	12 x	16 x 12		
Lauiweike	ТВ	ТВ	ТВ	ТВ	ТВ	ТВ	8 TB	8 TB	12 TB	12 TB	ТВ		
		. –			<u> </u>						Broad-		
	Integrierte Broadcom 5720 Dual- Port 1Gb LOM			com 5720									
				Broadcom 5720 QP 1Gb Network Toch- terkarte SAS 12Gbps externe HBA-Con-							QP 1Gb		
Base PCIe-Kar-											SAS		
ten					12Gbps								
											НВА		
											extern		
				Dual-									

			Port					
			10G					
			BaseT-					
			Kupfer					
	Externer SAS							
	12Gbps HBA-							
	Controller							
	Broadcom		Dual-					
	5719 Quad-		Port					
PCIe-Karten	Port 1G NIC	Dual-Port 10G (Kupfer)	10G					
(Work-		Dual-Port 10G SEP +	SFP +					
seinstellungen)	Dual-Port		Dual-					
	10G (Kupfer)	Dual-Port-FC 16G HBA	Port-FC					
	Dual-Port		16G					
	10G SFP +		НВА					
	100 511							
	Dual-Port-FC							
	16G HBA							
Netzteile	Dual, Hot-							
	Plug, red-							
	undante	Dual, Hot-Plug, redundante Stromversorgu	ng (1 +					
	Strom- 1), 750 W							
	versorgung (1							
	+ 1), 550 W							
iDRAC Enter-	1							
prise	-							

Steuerelemente und Anzeigen

Die Arcserve Appliance enthält verschiedene Steuerelemente und Anzeigen (LEDs) auf der Vorder- und Rückseite und auf jedem Datenträger. Diese Steuerelemente und Indikatoren ermöglichen die Steuerung verschiedener Funktionen und bieten eine schnelle Übersicht über den Status der Appliance und der Komponenten:

- Vorderseite 7100 7300v
- Vorderseite 7400 7600v
- Vorderseite 8100 8200
- Vorderseite 8300 8400
- Vorderseite 9012 9048
- Vorderseite 9072DR 9504 DR
- <u>Rückseite 7100 7300v</u>
- Rückseite 7400 7600v
- Rückseite 8100 8200
- Rückseite 8300 8400
- Rückseite 9012 9048
- Rückseite 9072DR 9504DR

Vorderseite 7100 - 7300v

Die Vorderseite des Arcserve Appliance enthält Schaltflächen des Bedienfeldes, LEDs des Bedienfeldes und LEDs des Datenträgers. In der folgenden Tabelle werden diese Elemente beschrieben.



Nummer	Steu- erelement/Anzeige	Beschreibung		
1	Netzschalter	Zum Ein- und Ausschalten der Stromversorgung für die Appliance-Komponenten. Beim Ausschalten wird die Haupt-Stromversorgung ausgeschaltet, die Appliance wird jedoch weiterhin mit Standby- Strom versorgt. Um sicherzustellen, dass die App- liance vollständig von der Stromversorgung getrennt ist, ziehen Sie vor Wartungsarbeiten das Netzkabel ab.		
2	Schaltfläche "Zurück- setzen"	Zum Neustart der Appliance.		
3	Netz-LED	Stetig grün: Zeigt an, dass das Netzteil der App- liance mit Strom versorgt wird. Diese LED sollte normalerweise leuchten, wenn die Appliance in Betrieb ist.		
4	Geräteaktivitäts-LED	Gelb blinkend: Zeigt Aktivität auf mindestens		
		einer der Festplatten an.		
----	-----------------------------------	---	--	--
-		Gelb blinkend: Zeigt Netzwerkaktivität im Netz-		
5	Netzwerkkarten-LED (NIC1)	werk 1 (Port ETH0) an.		
6	Notzworkkarton JED (NIC2)	Gelb blinkend: Zeigt Netzwerkaktivität im Netz-		
0		werk 2 (Port ETH1) an.		
		Stetig rot: Eine Überhitzungs-Bedingung ist auf-		
		getreten. (Dies kann durch eine Überlastung eines		
		Kabels verursacht werden.)		
		*Rot blinkend – schnell (1 Sekunde): Lüfterfehler.		
		Überprüfen Sie, ob der Lüfter nicht mehr betriebs-		
		bereit ist.		
		*Rot blinkend – langsam (4 Sekunden): Strom-		
7	Informations-LED	ausfall. Überprüfen Sie, ob die Stromversorgung		
		außer Betrieb ist.		
		Stetig blau: Lokale UID wurde aktiviert. Ver-		
		wenden Sie diese Funktion, um den Server in einer		
		Rack-Umgebung zu suchen.		
		Blau blinkend: Remote-UID wurde aktiviert. Ver-		
		wenden Sie diese Funktion, um den Server von		
		einem externen Standort aus zu suchen.		
	Schaltfläche "Geräte-ID (UID)"	Zum Ein- oder Ausschalten der Universal Infor-		
		mation-LED (blau) auf der Vorder- und Ruckseite		
8				
		Wenn die blaue LED aktiviert ist, kann die App-		
		liance problemios in einem Rack lokalisiert werden		
		(von vome oder ninten).		
9	Festplatten-LED	sprechenden Festplatte an		
		*Statig rat: Zeigt einen Ausfall der entsprechenden		
		Festplatte an.		
		Mit der Arcserve Appliance werden bei Ausfall einer		
	Festplatten-LED	Festplatte die restlichen Datenträger sofort akti-		
		viert. Damit wird sichergestellt, dass keine Daten		
10		verloren gehen und die Appliance normal wei-		
		terarbeitet. Daher ist es zum Schutz vor Pro-		
		blemen im Zusammenhang mit Ausfällen mehrerer		
		Festplatten wichtig, eine Festplatte schnellst-		
		möglich auszutauschen, um den potenziellen		
		Datenverlust zu minimieren.		
11	Verriegelung Festplatte	Zum Entriegeln und Entfernen der Festplatte.		
12	SSD (Solid State Drive)-LED	*Stetig rot: Zeigt einen Laufwerksausfall an.		
13	SSD (Solid State Drive)-LED	Stetig grün: Zeigt Laufwerkaktivität an.		

		Grün blinkend : Zeigt an, dass auf das Laufwerk zugegriffen wird.
14	Verriegelung SSD (Solid State Drive)	Zum Entriegeln und Entfernen des SSD-Laufwerks.

* Eine stetig rote oder rot blinkende LED weist auf irgendeine Art von Fehler hin. Um dieses Problem schnell zu lösen, wenden Sie sich an den <u>Arcserve-Support</u>.

Vorderseite 7400 - 7600v

Die Vorderseite des Arcserve Appliance enthält Schaltflächen des Bedienfeldes, LEDs des Bedienfeldes und LEDs des Datenträgers. In der folgenden Tabelle werden diese Elemente beschrieben.



Num- mer	Steu- erelement/Anzeige	Beschreibung	
		Zum Ein- und Ausschalten der Stromversorgung für	
		die Appliance-Komponenten. Beim Ausschalten wird	
		die Haupt-Stromversorgung ausgeschaltet, die App-	
1	Netzschalter	liance wird jedoch weiterhin mit Standby-Strom ver-	
		sorgt. Um sicherzustellen, dass die Appliance	
		vollständig von der Stromversorgung getrennt ist,	
		ziehen Sie vor Wartungsarbeiten das Netzkabel ab.	
2	Schaltfläche "Zurück-	Zum Neustart der Appliance.	
2	setzen"		
		Stetig grün: Zeigt an, dass das Netzteil der Appliance	
2	Netz-LED	mit Strom versorgt wird.	
5		Diese LED sollte normalerweise leuchten, wenn die	
		Appliance in Betrieb ist.	
4	Corätoaktivitäte LED	Gelb blinkend: Zeigt Aktivität auf mindestens einer	
4		der Festplatten an.	
5	Netzwerkkarten-LED (NIC1)	Gelb blinkend: Zeigt Netzwerkaktivität im Netzwerk	

		1 (Port ETH0) an.		
6	Netzwerkkarten-LED (NIC	2) Gelb blinkend: Zeigt Netzwerkaktivität im Netzwerk		
		Stetig rot: Eine Überhitzungs-Bedingung ist auf- getreten. (Dies kann durch eine Überlastung eines Kabels verursacht werden.)		
		*Rot blinkend – schnell (1 Sekunde): Lüfterfehler. Überprüfen Sie, ob der Lüfter nicht mehr betriebs- bereit ist.		
7	Informations-LED	*Rot blinkend – langsam (4 Sekunden): Strom- ausfall. Überprüfen Sie, ob die Stromversorgung außer Betrieb ist.		
		Stetig blau: Lokale UID wurde aktiviert. Verwenden Sie diese Funktion, um den Server in einer Rack- Umgebung zu suchen.		
		Blau blinkend: Remote-UID wurde aktiviert. Ver- wenden Sie diese Funktion, um den Server von einem externen Standort aus zu suchen.		
8	Stromausfall	Zeigt an, dass ein Netzteilmodul ausgefallen ist.		
9	Festplatten-LED	Grün blinkend : Zeigt Aktivität auf der ent- sprechenden Festplatte an.		
		*Stetig rot: Zeigt einen Ausfall der entsprechenden Festplatte an.		
10	Festplatten-LED	Festplatte die restlichen Datenträger sofort aktiviert. Damit wird sichergestellt, dass keine Daten verloren gehen und die Appliance normal weiterarbeitet. Daher ist es zum Schutz vor Problemen im Zusam- menhang mit Ausfällen mehrerer Festplatten wich-		
		tig, eine Festplatte schnellstmöglich auszutauschen, um den potenziellen Datenverlust zu minimieren.		
11	Verriegelung Festplatte	Zum Entriegeln und Entfernen der Festplatte.		

* Eine stetig rote oder rot blinkende LED weist auf irgendeine Art von Fehler hin. Um dieses Problem schnell zu lösen, wenden Sie sich an den <u>Arcserve-Support</u>.

Vorderseite 8100 - 8200

Arcserve ApplianceDie Vorderseite der 8100 - 8200 enthält Bedienfeldtasten, Bedienfeld-LEDs und Laufwerksträger-LEDs. In der folgenden Tabelle werden diese Elemente beschrieben.



Steuerelement/Anzeige	Beschreibung		
Netzschalter	Zum Ein- und Ausschalten der Stromversorgung für die App- liance-Komponenten. Beim Ausschalten wird die Haupt-Strom- versorgung ausgeschaltet, die Appliance wird jedoch weiterhin mit Standby-Strom versorgt. Um sicherzustellen, dass die App- liance vollständig von der Stromversorgung getrennt ist, zie- hen Sie vor Wartungsarbeiten das Netzkabel ab.		
Schaltfläche "Zurück- setzen" Zum Neustart der Appliance.			
Netz-LED	Stetig grün: Zeigt an, dass das Netzteil der Appliance mit Strom versorgt wird. Diese LED sollte normalerweise leuchten, wenn die Appliance in Betrieb ist.		
HDD-LED	Gelb blinkend: Zeigt Aktivität auf mindestens einer der Fest- platten an.		
Netzwerkkarten-LED (NIC1)	Gelb blinkend: Zeigt Netzwerkaktivität im Netzwerk 1 (Port ETH0) an.		

Netzwerkkarten-LED (NIC2)	Gelb blinkend: Zeigt Netzwerkaktivität im Netzwerk 2 (Port
	Stetig rot: Fine Überhitzungs-Bedingung ist aufgetreten.
	Hinweise Dies kann durch eine Überlastung eines Kahels vor
	ursacht werden.
	*Rot blinkend – schnell (1 Sekunde): Lüfterfehler, Übernrüfen
	Sie, ob der Lüfter nicht mehr betriebsbereit ist.
Informations-LED	*Rot blinkend – langsam (4 Sekunden): Stromausfall. Über- prüfen Sie, ob die Stromversorgung außer Betrieb ist.
	Stetig blau: Lokale UID ist aktiviert. Verwenden Sie diese Funk-
	tion, um den Server in einer Rack-Umgebung zu suchen.
	Blau blinkend: Remote-UID ist aktiviert. Verwenden Sie diese
	Funktion, um den Server von einem externen Standort aus zu
	suchen.
	Zum Ein- oder Ausschalten der Universal Information-LED
Schaltfläche "Geräte ID	(blau) auf der Vorder- und Rückseite der Appliance.
	Wenn die blaue LED aktiviert ist, kann die Appliance pro-
	blemlos in einem Rack lokalisiert werden (von vorne oder hin-
	ten).
Festplatten-I FD	Grün blinkend: Zeigt Aktivität auf der entsprechenden Fest-
	platte an.
	*Stetig rot: Zeigt einen Ausfall der entsprechenden Festplatte
	an.
	Mit der Arcserve Appliance werden bei Ausfall einer Festplatte
	die restlichen Datenträger sofort aktiviert. Damit wird sicher-
Festplatten-LED	gestellt, dass keine Daten verloren gehen und die Appliance
	normal weiterarbeitet. Daher ist es zum Schutz vor Problemen
	im Zusammenhang mit Ausfallen mehrerer Festplatten wichtig,
	eine Festplätte schnellstmöglich auszutauschen, um den poten-
Varriagalung Fastalatta	Zienen Datenvenust zu minneren.
verriegelung Festplatte Zum Entriegeln und Entrernen der Festplatte.	
SSD (Solid State Drive)-LED	"Stetig rot: Zeigt einen Lautwerksaustall an.
	Stetig grun: Zeigt Laufwerkaktivität an.
SSD (Solid State Drive)-LED	Grün blinkend : Zeigt an, dass auf das Laufwerk zugegriffen wird.
Verriegelung SSD (Solid	
State Drive)	Lan Entregen und Entremen des 550 Eddiwerks.

* Eine stetig rote oder rot blinkende LED weist auf irgendeine Art von Fehler hin. Um dieses Problem schnell zu lösen, wenden Sie sich an den <u>Arcserve-Support</u>.

Vorderseite 8300 - 8400

Die Vorderseite des Arcserve Appliance8300-8400 enthält Schaltflächen des Bedienfeldes, LEDs des Bedienfeldes und LEDs des Datenträgers. In der folgenden Tabelle werden diese Elemente beschrieben.



Steuerelement/Anzeige	Beschreibung		
Netzschalter	Zum Ein- und Ausschalten der Stromversorgung für die App- liance-Komponenten. Beim Ausschalten wird die Haupt-Strom- versorgung ausgeschaltet, die Appliance wird jedoch weiterhin mit Standby-Strom versorgt. Um sicherzustellen, dass die App- liance vollständig von der Stromversorgung getrennt ist, zie- hen Sie vor Wartungsarbeiten das Netzkabel ab.		
Schaltfläche "Zurück- setzen"	Zum Neustart der Appliance.		
Netz-LED	Stetig grün: Zeigt an, dass das Netzteil der Appliance mit Strom		

	versorgt wird.
	Diese LED sollte normalerweise leuchten, wenn die Appliance in
	Betrieb ist.
Netzwerkkarten-LED (NIC1)	Gelb blinkend: Zeigt Netzwerkaktivität im Netzwerk 1 (Port ETH0) an.
Netzwerkkarten-LED (NIC2)	Gelb blinkend: Zeigt Netzwerkaktivität im Netzwerk 2 (Port ETH1) an.
	Stetig rot: Eine Überhitzungs-Bedingung ist aufgetreten. (Dies kann durch eine Überlastung eines Kabels verursacht werden.)
	*Rot blinkend – schnell (1 Sekunde): Lüfterfehler. Überprüfen Sie, ob der Lüfter nicht mehr betriebsbereit ist.
Informations-LED	*Rot blinkend – langsam (4 Sekunden): Stromausfall. Über- prüfen Sie, ob die Stromversorgung außer Betrieb ist.
	Stetig blau: Lokale UID wurde aktiviert. Verwenden Sie diese Funktion, um den Server in einer Rack-Umgebung zu suchen.
	Blau blinkend: Remote-UID wurde aktiviert. Verwenden Sie
	diese Funktion, um den Server von einem externen Standort
	aus zu suchen.
Netz-LED	Zeigt an, dass ein Netzteilmodul ausgefallen ist.
Festplatten-LED	Grün blinkend : Zeigt Aktivität auf der entsprechenden Fest- platte an.
	*Stetig rot: Zeigt einen Ausfall der entsprechenden Festplatte
	an.
	Mit der Arcserve Appliance werden bei Ausfall einer Festplatte
	die restlichen Datenträger sofort aktiviert. Damit wird sicher-
Festplatten-LED	gestellt, dass keine Daten verloren gehen und die Appliance
	normal weiterarbeitet. Daher ist es zum Schutz vor Problemen
	im Zusammenhang mit Ausfällen mehrerer Festplatten wichtig,
	eine Festplatte schnellstmöglich auszutauschen, um den poten-
	ziellen Datenverlust zu minimieren.
Verriegelung Festplatte	Zum Entriegeln und Entfernen der Festplatte.

* Eine stetig rote oder rot blinkende LED weist auf irgendeine Art von Fehler hin. Um dieses Problem schnell zu lösen, wenden Sie sich an den <u>Arcserve-Support</u>.

Vorderseite 9012 - 9048

Die Vorderseite des Arcserve Appliance enthält Schaltflächen des Bedienfeldes, LEDs der Bedienfeldes und LEDs des Datenträgers. In der folgenden Tabelle werden diese Elemente beschrieben.



Num- mer	Steu- erelement/Anzeige	Symbol	Beschreibung
			Enthält den Systemstatus und die Sys- tem-ID, die Status-LED und die Anzeige für iDRAC Quick Sync 2 (drahtlos). Hinweis: Die Anzeige für iDRAC Quick Sync 2 steht nur bei bestimmten Kon- figurationen zur Verfügung.
			 LED-Status: Ermöglicht es Ihnen, die alle fehlgeschlagenen Hard- ware-Komponenten zu iden- tifizieren. Es gibt bis zu fünf Status-LEDs und eine allgemeine Systemzustands-LED-Leiste (Gehäusezustand und System- ID). Weitere Informationen fin- den Sie unter link
1	Linkes Bedienfeld	NA	 Quick Sync 2 (drahtlos): Zeigt an, dass das System für eine schnelle Synchronisierung aktiviert ist. Die Funktion "Quick Sync" (Schnelle Synchronisierung) ist optional. Diese Funktion ermöglicht die Ver- waltung des Systems mit mobilen Geräten. Diese Funktion liefert eine aggregierte Bestands- aufnahme der Hardware und Firmware sowie verschiedene auf Diagnosen und Informationen auf Systemebene, die bei der Feh- lerbehebung verwendet werden können. Weitere Informationen
2	Laufwerksteckplätze	NA	Hier können Sie Laufwerke installieren,

			die auf Ihrem System unterstützt wer- den. Weitere Informationen über Lauf- werke finden Sie unter Link.
3	Optisches Laufwerk (optio- nal)	NA	Ein optionales schlankes SATA DVD- ROM-Laufwerk oder ein DVD+/-RW-Lauf- werk.
4	VGA-Anschluss	101	Hier können Sie ein Anzeigegerät an das System anschließen. Weitere Infor- mationen finden Sie unter <u>link</u> .
5	USB-Port (optional)	ssæ	Der USB-Anschluss ist USB 2.0-kom- patibel.
6	Rechtes Bedienfeld	NA	Enthält den Netzschalter, USB-Port, iDRAC Direct micro-Port und die iDRAC- Direktstatus-LED.
7	Informationsetikett	NA	Das Informationsetikett ist ein aus- blendbarer Bereich mit Sys- teminformationen, wie Serviceetikett, NIC, MAC-Adresse und so weiter. Wenn Sie sicheren standardmäßigen Zugriff auf iDRAC haben, enthält das Etikett auch das sichere iDRAC-Stan- dardkennwort.

Vorderseite 9072DR - 9504DR

Die Vorderseite des Arcserve Appliance enthält Schaltflächen des Bedienfeldes, LEDs des Bedienfeldes und LEDs des Datenträgers. In der folgenden Tabelle werden diese Elemente beschrieben.



4

Nummer	Steu- erelement/Anzeige	Symbol	Beschreibung
1	Linkes Bedienfeld	NA	Enthält den Systemstatus und Sys- tem-ID, Status-LED und die Anzeige

			für iDRAC Quick Sync 2 (drahtlos).
			Hier können Sie Laufwerke instal-
2			lieren, die auf Ihrem System unter-
2	Lautwerksteckplatze	NA	stützt werden. Weitere
			Informationen finden Sie unter <u>link</u> .
	Rechtes Bedienfeld		Enthält den Netzschalter, VGA-Port,
3		NA	iDRAC Direct Micro USB-Anschluss
			und zwei USB 2.0-Ports.
	Informationsetikett	NA	Das Informationsetikett ist ein aus-
			blendbarer Bereich mit Sys-
			teminformationen, wie
4			Serviceetikett, NIC, MAC-Adresse
4			und so weiter. Wenn Sie sicheren
			standardmäßigen Zugriff auf iDRAC
			haben, enthält das Etikett auch das
			sichere iDRAC-Standardkennwort.

Rückseite 7100 - 7300v



	Name des Steu-			
Nummer	erelements bzw.	Beschreibung		
	der Anzeige			
1	Netzteil	Ermöglicht eine hocheffiziente Stromversorgung der Appliance.		
		Hinweis: Mithilfe des Hauptnetzschalters wird die App- liance mit der Stromversorgung verbunden oder von ihr getrennt. Beim Ausschalten über diesen Schalter wird die Haupt-Stromversorgung ausgeschaltet, die App- liance wird jedoch weiterhin mit Standby-Strom ver- sorgt. Um sicherzustellen, dass die Appliance vollständig von der Stromversorgung getrennt ist, ziehen Sie vor Wartungsarbeiten das Netzkabel ab.		
2	IPMI-Port (Remo- teverwaltung)	Der IPMI-Port (Intelligent Platform Management Inter- face) wird verwendet, um den physischen Zustand der Server, wie z. B. Temperatur, Spannung, Lüfter und Netz- teile, sowie der Appliance zu überwachen. Hinweis: Der standardmäßige Benutzername und das Kennwort für den IPMI-Zugriff lauten ADMIN/ARCADMIN (Groß-/Kleinschreibung). Es wird empfohlen, dass Sie das Kennwort so bald wie möglich ändern. Weitere Infor- mationen zum Ändern des IPMI-Kennworts finden Sie unter <u>So ändern Sie das IPMI-Kennwort</u> .		
3	Port für externes Spei- chergerät (SAS-Port für Band- laufwerk)	Zum Anschluss eines externen Speichergeräts (Fest- platte, Bandlaufwerk usw.) an die Appliance. Mit diesen tragbaren externen Speichergeräten können gesicherte Daten problemlos von einem Ort zum anderen trans- portiert werden.		
4	Seriennummerbereich	Eine eindeutige Seriennummer, die der Appliance zuge-		

		wiesen wurde.	
		Kommunikations-Port, der zum Anschluss eines seriellen	
5	Serieller COM1-Port	Geräts, wie z. B. einer Maus, an die Appliance verwendet wird.	
6	USB 2.0 (schwarz)	Zum Anschluss von USB 2.0-Geräten an die Appliance.	
7	USB 3.0 (blau)	Zum Anschluss von USB 3.0-Geräten an die Appliance.	
0	E/A-Port 1 für Netz-	Zur Übertragung von Netzwerkdaten zwischen dem	
0	werkdaten	Netzwerk und der Appliance. ((ETH0 für Netzwerk 1)	
9	E/A-Port 2 für Netz-	Zur Übertragung von Netzwerkdaten zwischen dem	
	werkdaten	Netzwerk und der Appliance. (ETH1 für Netzwerk 2)	
10	VGA-Anschluss	Zum Anschluss eines Monitors an die Appliance (bei	
		Bedarf).	

Rückseite 7400 - 7600v



Nummer	Name des Steu- erelements bzw. der Anzeige	Beschreibung
	Doppelnetzteil	Ermöglicht eine hocheffiziente Stromversorgung der Appliance.
1		Hinweis: Mithilfe des Hauptnetzschalters wird die Appliance mit der Stromversorgung verbunden oder von ihr getrennt. Der Vorteil eines Doppelnetzteils besteht darin, das beim Ausfall eines Netzteils das zweite Netzteil bereitsteht und genutzt werden kann. Beim Ausschalten über diesen Schalter wird die Haupt-Stromversorgung ausgeschaltet, die App- liance wird jedoch weiterhin mit Standby-Strom ver- sorgt. Um sicherzustellen, dass die Appliance vollständig von der Stromversorgung getrennt ist, ziehen Sie vor Wartungsarbeiten das Netzkabel ab.
2	IPMI-Port (Remo- teverwaltung)	Der IPMI-Port (Intelligent Platform Management Interface) wird verwendet, um den physischen Zustand der Server, wie z. B. Temperatur, Spannung, Lüfter und Netzteile, sowie der Appliance zu über- wachen. Hinweis: Der standardmäßige Benutzername und das Kennwort für den IPMI-Zugriff lauten ADMIN/ARCADMIN (Groß-/Kleinschreibung). Es wird empfohlen, dass Sie das Kennwort so bald wie mög- lich ändern. Weitere Informationen zum Ändern des

		IPMI-Kennworts finden Sie unter <u>So ändern Sie das</u>
		IPMI-Kennwort.
3	Port für externes Spei- chergerät (SAS-Port für Band- laufwerk)	Zum Anschluss eines externen Speichergeräts (Fest- platte, Bandlaufwerk usw.) an die Appliance. Mit die- sen tragbaren externen Speichergeräten können gesicherte Daten problemlos von einem Ort zum anderen transportiert werden.
4	Seriennummerbereich	Eine eindeutige Seriennummer, die der Appliance zugewiesen wurde.
5	Serieller COM1-Port	Kommunikations-Port, der zum Anschluss eines seri- ellen Geräts, wie z. B. einer Maus, an die Appliance verwendet wird.
6	USB 2.0 (schwarz)	Zum Anschluss von USB 2.0-Geräten an die App- liance.
7	USB 3.0 (blau)	Zum Anschluss von USB 3.0-Geräten an die App- liance.
8	E/A-Port 1 für Netz- werkdaten	Zur Übertragung von Netzwerkdaten zwischen dem Netzwerk und der Appliance. ((ETHO für Netzwerk 1)
9	E/A-Port 2 für Netz- werkdaten	Zur Übertragung von Netzwerkdaten zwischen dem Netzwerk und der Appliance. (ETH1 für Netzwerk 2)
10	VGA-Anschluss	Zum Anschluss eines Monitors an die Appliance (bei Bedarf).
11	Port für externes Spei- chergerät (Automatischer Band- wechsler/Bibliothek) LSI SAS 9212 - 4i4e	 Zum Anschluss eines externen Speichergeräts (Automatischer Bandwechsler/Bibliothek) an die Appliance. Mit diesen tragbaren externen Speichergeräten können gesicherte Daten problemlos von einem Ort zum anderen transportiert werden. Hinweis: Dieser Port ist unter dem Betriebssystem als LSI-Adapter SAS2 2008 Falcon vorhanden.

Rückseite 8100 - 8200



Num- mer	Name des Steuerelements bzw. der Anzeige
1	Netzteilmodul Nr. 1
2	AC-Anschlussbuchse Nr. 1
3	Netzteil Nr. 2
4	AC-Anschlussbuchse Nr. 2
5	COM-Port
6	IPMI-Port (Remoteverwaltung)
7	Low-Profile PCI-Erweiterungssteckplatz
8	PCI-Erweiterungssteckplatz
9	Power Good-LED 1
10	Netzteilschalter 1
11	Power-Good-LED Nr. 2
12	Netzteilschalter Nr. 2
13	USB 2.0 Anschluss 1 (schwarz)
14	USB 2.0 Anschluss 2 (schwarz)
15	USB 3.0-Anschluss 3 (blau)
16	USB 3.0-Anschluss 4 (blau)
17	E/A-Port 1 für Netzwerkdaten (ETH0 für Netzwerk 1)
18	E/A-Port 2 für Netzwerkdaten (ETH1 für Netzwerk 2)

19	VGA-Anschluss	
20	Port für externes Speichergerät	
20	(SAS-Port für Bandlaufwerkoption)	

Rückseite 8300 - 8400



Name des Steuerelements bzw. der	
Anzeige	
Netzteilmodul Nr. 1 – Verriegelung	
Netzteilmodul Nr. 1 – Power-Good-LED	
Netzteilmodul 1 Steckdose	
Netzteilmodul 1 Lüfter	
Hintere SSDs (optional)	
IPMI-Port (Remoteverwaltung)	
Externe SAS HBA-Ports	
PCI-Erweiterungssteckplätze halber Länge	
Interner RAID-Controller	
PCI-Erweiterungssteckplätze voller Länge	
Netzteilmodul Nr. 2 – Verriegelung	
Netzteilmodul Nr. 2 – Power-Good-LED	
Netzteilmodul Nr. 2 – Wechselstrombuchse	
Netzteilmodul Nr. 2 – Lüfter	
COM-Port	
USB-Port 1 (2. Generation)	
USB-Port 2 (2. Generation)	
USB-Port 3 (3. Generation)	

19	USB-Port 4 (3. Generation)
20	ETH0 (Netzwerk 1)
21	ETH1 (Netzwerk 2)
22	VGA-Port (Monitor)
23	UID-LED

Rückseite 9012 - 9048

Die Rückseite der Arcserve Appliance enthält den Stromanschluss, die Kabelanschlüsse und die Ports für die Appliance. In der folgenden Tabelle werden diese Elemente beschrieben.



Nummer	Steu-	Sym-	Beschreibung
1	Serieller Port	10101	Über diesen Port können Sie ein Peri- pheriegerät an das System anschließen. Weitere Informationen finden Sie unter link.
2	Dedizierter iDRAC9-Netz- werkport		Verwenden Sie den iDRAC9 dedizierte Netz- werkport, um sicher auf den ein- gebetteten iDRAC auf einem separaten Management-Netzwerk zuzugreifen. Wei- tere Informationen finden Sie unter <u>link</u> .
3	Ethernet-Ports (2)	6 76	Verwenden Sie die Ethernet-Ports, um das Local Area Networks (LAN) mit dem Sys- tem zu verbinden. Weitere Informationen finden Sie unter <u>link</u> .
4	Riser-Steckplatz (volle Höhe)		Verwenden Sie Kartensteckplätze, um PCIe-Erweiterungskarten voller Höhe mit dem Riser voller Höhe zu verbinden.
5	Netzteil		Weitere Informationen zu den Netz- teilkonfigurationen finden Sie unter <u>Link</u> .
6	Netzteil		Weitere Informationen zu den Netz- teilkonfigurationen finden Sie unter <u>Link</u> .

	1		
7	LOM-Riserports (2)	동물	Weitere Informationen zu den Netz- teilkonfigurationen finden Sie unter <u>Link</u> .
8	USB 3.0-Port (2)	ss ~.	Verwenden Sie den USB 3.0-Port, um USB- Geräte mit dem System zu verbinden. Diese Ports sind 4-polig und USB 3.0-kom- patibel.
9	VGA-Anschluss		Über diesen Port können Sie ein Peri- pheriegerät an das System anschließen. Weitere Informationen finden Sie unter <u>link</u> .
10	CMA-Netzanschluss		Über den Cable Management Arm (CMA)- Netzanschluss stellen Sie eine Verbindung zum CMA her.
11	Schaltfläche "System-ID"	ē	 Klicken Sie auf die Schaltfläche "System- ID": Um ein bestimmtes System in einem Rack zu suchen. Um die System-ID zu aktivieren oder deaktivieren. Um iDRAC zurückzusetzen (halten Sie die Schaltfläche 15 Sekunden gedrückt). Hinweise: Um iDRAC mithilfe der System-ID zurückzusetzen, stellen Sie sicher, dass die Schaltfläche "System-ID" im iDRAC-Setup aktiviert ist. Wenn das System während des POST nicht reagiert, halten Sie die Schaltfläche "System-ID" (für mehr als fünf Sekunden) gedrückt, um den BIOS-Fortschrittsmodus auf- zurufen.

Rückseite der 9072DR - 9504 DR

Die Rückseite der Arcserve Appliance enthält den Stromanschluss, die Kabelanschlüsse und die Ports für die Appliance. In der folgenden Tabelle werden diese Elemente beschrieben.



Nummer	Steu- erelement/Anzeige	Symbol	Beschreibung
1	PCIe-Erwei- terungssteckplatz (3) (volle Höhe)	NA	Der PCIe-Erweiterungssteckplatz (Riser 1) verbindet bis zu drei PCIe-Erwei- terungskarten voller Höhe mit dem Sys- tem. Weitere Informationen finden Sie unter <u>link</u> .
2	PCIe-Erwei- terungssteckplatz (halbe Höhe)	NA	Der PCIe-Erweiterungssteckplatz (Riser 2) verbindet eine PCIe-Erwei- terungskarte halber Höhe mit dem Sys- tem. Weitere Informationen finden Sie unter <u>link</u> .
3	Rückwärtiges Handle	NA	Das rückwärtige Handle kann entfernt werden, um alle externe Kabel zu PCIe- Karten, die in der PCIe Erwei- terungssteckplatz 6 installiert sind, zu entfernen.
4	PCIe-Erwei- terungssteckplatz (2) (volle Höhe)	NA	Der PCIe-Erweiterungssteckplatz (Riser 2) verbindet bis zu zwei PCIe-Erwei- terungskarten voller Höhe mit dem Sys- tem. Weitere Informationen finden Sie unter <u>link</u> .
5	PCIe-Erwei- terungssteckplatz (2) (volle	NA	Der PCIe-Erweiterungssteckplatz (Riser

	Höhe)		3) verbindet bis zu zwei PCIe-Erwei- terungskarten voller Höhe mit dem Sys- tem. Weitere Informationen finden Sie unter <u>link</u> .
6	Netzteil (2)	NA	Weitere Informationen finden Sie unter <u>link</u> .
7	NIC-Ports	율	Die NIC-Ports, die auf der Netzwerk- Tochterkarte (NDC) integriert sind, stel- len die Verbindung zum Netzwerk her. Weitere Informationen zu den unter- stützten Konfigurationen finden Sie unter diesem Link.
8	USB-Port (2)	\$ \$ \$	Die USB-Ports sind 9-polig und 3.0-kom- patibel. Mit diesen Ports verbinden Sie USB-Geräte mit dem System.
9	VGA-Anschluss		Hier können Sie ein Anzeigegerät an das System anschließen. Weitere Infor- mationen finden Sie unter <u>link</u> .
10	Serieller Port	10101	Über diesen Port können Sie ein Peri- pheriegerät an das System anschlie- ßen. Weitere Informationen finden Sie unter <u>link</u> .
11	Dedizierter iDRAC9-Port	3 k	Dieser Port ermöglicht den Remote- Zugriff auf iDRAC. Weitere Infor- mationen finden Sie unter <u>link</u> .
12	Schaltfläche "System-ID"	٢	Die Schaltfläche "System-ID (ID)" steht auf der Vorder- und Rückseite der Sys- teme zur Verfügung Klicken Sie auf die Schaltfläche, um ein System in einem Rack zu identifizieren, indem Sie die Schaltfläche "System-ID" aktivieren. Mit der Schaltfläche "System-ID" kön- nen Sie auch iDRAC zurücksetzen und mithilfe des schrittweisen Modus auf das BIOS zugreifen.

Von der Appliance verwendete Ports

Folgende Themen enthalten Informationen zu den Ports, die in Arcserve UDP, Arcserve Backup und der Appliance für Linux-Support verwendet werden:

- Arcserve UDP
- Arcserve Backup
- Appliance f
 ür Linux-Unterst
 ützung

Arcserve UDP

Dieser Abschnitt enthält folgende Themen:

- Unter Microsoft Windows installierte Komponenten
- Unter Linux installierte Komponenten
- Per Remote-Zugriff durch UDP Linux geschützte Knoten

Unter Microsoft Windows installierte Komponenten

Die folgenden Ports sind für Sicherungs- und andere Aufträge in LAN-Umgebungen erforderlich:

Dor	Por-	Ini-		
POr-	t-	tiiert	Abhörprozess	Beschreibung
τ#	typ	von		
				Gibt den Standard-
				Kommunikations-Port
				zwischen der Arcserve
				UDP-Konsole und den
				Microsoft SQL Server-
				Datenbanken an,
				wenn diese sich auf
1433	тср	Remot	sqlsrvr.exe	unterschiedlichen
		e-Java		Computern befinden.
				Hinweis: Sie können
				den standardmäßigen
				Kommunikationsport
				während der Instal-
				lation von SQL Server
				ändern.
		Arc-		Überträgt Daten für
4090	тср	serve	HATransServer exe	Virtual Standby-Auf-
-050		UDP		gaben im Proxy-
		Agent		Modus.
				Reserviert für den Arc-
				serve-UDP den RPS
				Global Dedu-
				plizierungs-Daten-
				speicher-Dienst
				(GDD). Ein Arcserve
500-		Arc-		UDP-GDD-Daten-
0-	ТСР	serve	GDDServer.exe	speicher verwendet 3
5060		UDP-		freie Ports, die mit
		Server		5000 beginnen. Sie
				werden benötigt,
				wenn der Daten-
				speicher mit GDD akti-
				viert oder die
				WIE-
				aer-

				herstellungsaufgabe
				Verwendet wird.
				Kommunikation, uper
				die die Arcserve UDP-
		Arc-		Konsole und der Pri-
6052	ТСР	serve	CA.ARCserve.CommunicationFoundation.	märserver des glo-
		Backu-	WindowsService.exe	balen Arcserve
		p-GDB		Backup-Dashboards
				Daten syn-
				chronisieren können.
				Kommunikation, über
		Arc-		die die Arcserve UDP-
		CORVO	CA.ARC-	Konsole und der Arc-
6054	тср	Backu-	ser-	serve Backup-Pri-
		DdCKu-	ve.CommunicationFoundation.WindowsService.ex	enärserver Daten
		þ		synchronisieren kön-
				nen.
				Zum Herunterfahren
				von Tomcat, das von
8006				der Arcserve UDP-Kon-
				sole verwendet wird.
				Gibt den Standard-
				Port für HTTP/HTTPS-
				Kommunikation zwi-
				schen Remote-Ver-
				waltungskonsolen
				und dem Arcserve
				UDP-Server an.
				Gibt den Port der Stan
		Arc		
		AIC-		Vannunikation zwi-
0014	TOD	Serve	To	Kommunikation zwi-
8014	ICF	UDP	Iomcat/.exe	Schen Kemole-ver-
		Con-		Waltungskonsolen
		sole		und dem Arcserve
				UDP-Agent an.
				Hinweis: Sie können
				den standardmäßigen
				Kommunikationsport
				während der Instal-
				lation der Arcserve
				UDP-Komponenten
				ändern.
8014	тср	Arc-	httpd.exe	Gibt den Standard-

				Port für HTTP/HTTPS-
				Kommunikation zwi-
				schen dem Arcserve
				UDP-Server und den
				Arcserve UDP-Kon-
				solen an.
				* Gibt den frei-
				gegebenen Standard-
				Port und den einzigen
				Port an, den Sie öff-
				nen müssen, wenn
				Sie den Arcserve UDP-
		convo		Server als Repli-
				kationsziel ver-
		Sorvor		wenden. Öffnen Sie
		Server		nicht die Ports 5000 -
				5060, da diese von
				Datenspeichern mit
				aktivierter globaler
				Deduplizierung ver-
				wendet werden.
				Hinweis: Sie können
				den standardmäßigen
				Kommunikationsport
				während der Instal-
				lation der Arcserve
				UDP-Komponenten
				ändern.
				Gibt den Standard-
				Port für HTTP/HTTPS-
				Kommunikation zwi-
				schen Remote-Ver-
				waltungskonsolen
		Arc-		und dem Arcserve
		serve		UDP-Server an.
8015	тср	UDP	Tomcat7.exe	Gibt den Port der Stan
	_	Con-		dard-HTTP/HTTPS-
		sole		Kommunikation zwi-
				schen Remote-Ver-
				waltungskonsolen
				und dem Arcserve
				UDP-Agent an.
				Hinweis: Sie können

				den standardmäßigen
				Kommunikationsport
				während der Instal-
				lation der Arcserve
				UDP-Komponenten
				ändern.
				Reserviert für die Kom-
				munikation von Arc-
				serve UDP Server-
			Tomcat7.exe	Webdiensten mit
				dem RPS-Port-Frei-
		Arc-		gabedienst für Arc-
0010	TOD	serve		serve UDP auf dem
8010	TCP	UDP- Server		gleichen Server.
				Hinweis: Der Port
				kann nicht angepasst
				werden und kann für
				die Firewall-Ein-
				stellung ignoriert wer-
				den.
				Zum Herunterfahren
100	100		CA.ARCserve.CommunicationFoundation.	von Tomcat, das von
180-				Arcserve UDP Server
05			windowsService.exe	oder vom Agenten
				verwendet wird.

Unter Linux installierte Komponenten

Die folgenden Ports sind für Sicherungs- und andere Aufträge in LAN-Umgebungen erforderlich:

Port #	Porttyp	Initiiert von	Abhörprozess	Beschreibung
22	тср	SSH- Dienst		Arcserve UDP Linux – Abhängigkeit von Drit- tanbietern. Gibt den Stan- dard für den SSH-Dienst an. Sie können diesen Port allerdings ändern. Dieser Port ist für eingehende und ausgehende Kom- munikation erforderlich.
67	UDP	Arcserve UDP- Linux	bootpd	Wird für den PXE-Boot-Ser- ver verwendet. Nur erfor- derlich, wenn der Benutzer die PXE-Startfunktion ver- wenden möchte. Dieser Port ist für die eingehende Kommunikation erfor- derlich. Hinweis: Die Portnummer kann nicht angepasst wer- den.
69	UDP	Arcserve UDP- Linux	tffpd	Wird für den PXE-Boot-Ser- ver verwendet. Nur erfor- derlich, wenn der Benutzer die PXE-Startfunktion ver- wenden möchte. Dieser Port ist für die eingehende Kommunikation erfor- derlich. Hinweis: Die Portnummer kann nicht angepasst wer- den.
8014	тср	Arcserve UDP- Linux	Java	Gibt die Standard-Ports für HTTP/HTTPS-Kom- munikation zwischen den Remote-Konsolen und dem Arcserve UDP Agent

				für Linux an. Dieser Port ist
				für eingehende und aus-
				gehende Kommunikation
				erforderlich.
		Arcserve		Verwendet von Tomcat,
18005	ТСР	UDP-	Java	kann für die Firewall-Ein-
		Linux		stellung ignoriert werden.

Durch UDP Linux remote geschützter Knoten

Der folgende Port ist fü	r Sicherungs- und	andere Aufträge in I	LAN-Umgebungen	erforderlich:
--------------------------	-------------------	----------------------	----------------	---------------

Port #	Porttyp	Initiiert von	Abhörprozess	Beschreibung
22		SSH- Dienst		Arcserve UDP unter Linux von Drittanbieter. Gibt den Standard für den SSH-Dienst an. Sie können diesen Port allerdings ändern. Dieser Port ist für eingehende und ausgehende Kommunikation erforderlich.

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

Entsprechend muss der Remote-Administrator für Remote-Replikationen Port 8014 (für die Datenreplikation) und Port 8015 (Standard-Port für die Arcserve UDP-Konsole, der während der Installation geändert werden kann) öffnen oder weiterleiten, damit lokale Recovery Point Server den zugewiesenen Replikationsplan abrufen können.

Arcserve Backup

Die folgenden Ports sind für Sicherungs- und andere Aufträge in LAN-Umgebungen erforderlich:

Port #	Port- typ	lnitiiert von	Abhörprozess	Beschreibung
135	тср			Microsoft-Port- zuordnung
445	тср		MSRPC über Named Pipes	
6050	TCP/UD- P	CASU- niversalAgent	Univagent.exe	Arcserve Uni- versal Agent
6502	ТСР	Arcserve Com- munication Foun- dation	CA.ARC- serve.CommunicationFoundation. WindowsService.exe	Arcserve Com- munication Foun- dation
6502	тср	CASTapeEngine	Tapeng.exe	Arcserve-Band- prozess
6503	тср	CASJobEngine	Jobengine.exe	Arcserve-Job- prozess
6504	тср	CASDBEngine	DBEng.exe	Arcserve-Daten- bankprozess
7854	тср	CASportmapper	Catirpc.exe	Arcserve-Port- mapper
4152- 3	тср	CASDiscovery	CASDSCSVC.EXE	Arcserve-Dis- covery-Dienst
4152- 4	UDP	CASDiscovery	CASDSCSVC.EXE	Arcserve-Dis- covery-Dienst
9000- 9500	тср		Für andere Arcserve MS RPC-Dienste, die dynamische Ports verwenden	

Appliance für Linux-Unterstützung

Die folgenden Ports sind für Sicherungs- und andere Aufträge in LAN-Umgebungen erforderlich:

Port #	Porttyp	Initiiert von	Abhörprozess	Beschreibung
8017	ТСР			NAT -Port-Umleitung leitet 8017 auf der App- liance auf den Linux-Sicherungsserver um, damit ein anderer Linux-Knoten auf Amazon S3 gesichert werden kann.
8018	ТСР			NAT-Port-Umleitung leitet 8018 auf der App- liance auf den Port 8014 des Linux-Backup- Server-Agenten um.
8019	ТСР			NAT-Port-Umleitung leitet 8019 auf der App- liance auf den SSH-Port 22 des Linux-Siche- rungsservers um.
8021	ТСР			NAT -Port-Umleitung leitet 8021 auf der App- liance auf den Linux-Sicherungsserver um, damit ein anderer Linux-Knoten mit dem Port 8021 gesichert werden kann.
8036	ТСР			NAT-Port-Umleitung leitet 8036 auf der App- liance auf den Port 8036 des Linux-Siche- rungsservers um.
50000	ТСР			NAT -Port-Umleitung leitet 50000 auf der Appliance auf den Linux-Sicherungsserver um, damit ein anderer Linux-Knoten mit dem Port 50000 in die Cloud gesichert wer- den kann.
50001	ТСР			NAT -Port-Umleitung leitet 50001 auf der Appliance auf den Linux-Sicherungsserver um, damit ein anderer Linux-Knoten mit dem Port 50001 in die Cloud gesichert wer- den kann.
50002	ТСР			NAT -Port-Umleitung leitet 50002 auf der Appliance auf den Linux-Sicherungsserver um, damit ein anderer Linux-Knoten mit dem Port 50002 in die Cloud gesichert wer- den kann.
50003	ТСР			NAT -Port-Umleitung leitet 50003 auf der Appliance auf den Linux-Sicherungsserver

		um, damit ein a dem Port 50003 den kann.	nderer Linux-Knoten mit 3 in die Cloud gesichert wer-
50004	тср	NAT -Port-Umle Appliance auf d um, damit ein a dem Port 50004 den kann.	eitung leitet 50004 auf der en Linux-Sicherungsserver Inderer Linux-Knoten mit I in die Cloud gesichert wer-

Hinzufügen von Ports zur CentOS 6.6 X64-Firewall

Wenn Sie den vorinstallierten Arcserve Appliance Linux-Sicherungsserver auf v6.5 Update 2 aktualisieren, müssen Sie nach diesem Upgrade eine Ports manuell zu Linux hinzufügen, wenn es über eine CentOS 6.6 x64-Firewall verfügt.

Befolgen Sie diese Schritte:

- 1. Navigieren Sie zum folgenden Pfad:
 - vi /etc/sysconfig/iptables
- 2. Fügen Sie folgende fett markierte Zeilen manuell in der Datei *Iptables* hinzu, falls sie nicht bereits vorhanden sind:
 - # Firewall-Konfiguration wie von system-config-firewall geschrieben
 - # Die manuelle Anpassung dieser Datei wird nicht empfohlen.

*filter

:INPUT ACCEPT [0:0]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [0:0]

-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 67 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 69 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 8014 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 8016 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 8017 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 8021 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 8035 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 8036 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 50000 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 50001 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 50002 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 50003 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 50004 -j ACCEPT

-A INPUT -m state --state ESTABLISHED, RELATED -j ACCEPT

- -A INPUT -p icmp -j ACCEPT
- -A INPUT -i lo -j ACCEPT
- -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
- -A INPUT -j REJECT --reject-with icmp-host-prohibited
- -A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT

- 3. Speichern Sie die Datei *iptables*.
- Starten Sie den Service *iptables* mit folgendem Befehl erneut: /etc/init.d/iptables restart

Sie haben die Ports der CentOS 6.6 x64-Firewall erfolgreich hinzugefügt.
Kapitel 3: Installieren der Arcserve Appliance

Dieser Abschnitt enthält folgende Themen:

So installieren Sie Arcserve Backup 18.0	64
So installieren Sie die 8100 - 8200 Series Appliance	66
So installieren Sie die 8300 - 8400 Series Appliance	67
So installieren Sie die 9012 - 9048 Series Appliance	67
So installieren Sie die 9072-9504DR Series Appliance	67

So installieren Sie Arcserve Backup 18.0

Arcserve Backup 18.0 ist nicht auf der Appliance vorinstalliert. Sie können Arcserve Backup 18.0 mithilfe eines Skripts namens "InstallASBU.bat", das sich auf Ihrem Desktop befindet, installieren.

Befolgen Sie diese Schritte:

1. Suchen Sie auf Ihrem Desktop nach **InstallASBU.bat** und führen Sie die Datei aus.

Hinweis: Wenn Sie die .bat-Datei von einem nicht englischen Windows-System starten, wird der folgende Bildschirm angezeigt. Wählen Sie die Sprache für die Installation von Arcserve Backup 18.0 aus. Fahren Sie andernfalls mit Schritt 2 fort.



2. Geben Sie das Administratorkennwort ein, und starten Sie die Installation von Arcserve Backup 18.0.

Checking Arcserve Backup installation environment
Select language for Arcserve Backup Installation: 1. German (default) 2. English
Your choice [1]: You select "German". Are you sure? [y/n]:y
Enter Password for Administrator: *********
Starting to install Arcserve Backup r17 (German). This may take up to 25 minutes. Please do not close this window or shutdown the appliance.
Installing Arcserve Backup Completed.
Installing Arcserve Backup Patch Manager Completed.
Updating configurations of the Arcserve Backup server
Arcserve Backup r17 is installed successfully. UserName: caroot Password: Arcserve

Wenn die Installation abgeschlossen ist, wird das Symbol "Arcserve Backup" zu Ihrem Desktop hinzugefügt. Sie können sich nun mit den folgenden Anmeldeinformationen bei Arcserve Backup anmelden:

- Benutzername = caroot
- Kennwort = Arcserve

So installieren Sie die 8100 - 8200 Series Appliance

Die Appliance ist nur für die Installation in eingeschränkten Bereichen bestimmt. Nur entsprechend geschultes Personal sollte Setup und Wartung durchführen.

Vollständige Informationen zur Installation finden Sie unter <u>8100 - 8200 Appliance-</u> Installation.

So installieren Sie die 8300 - 8400 Series Appliance

Die Appliance ist nur für die Installation in eingeschränkten Bereichen bestimmt. Nur entsprechend geschultes Personal sollte Setup und Wartung durchführen.

Vollständige Informationen zur Installation finden Sie unter <u>8300 - 8400 Appliance-</u> Installation.

So installieren Sie die 9012 - 9048 Series Appliance

Die Appliance ist nur für die Installation in eingeschränkten Bereichen bestimmt. Nur entsprechend geschultes Personal sollte Setup und Wartung durchführen.

Vollständige Informationen zur Installation finden Sie unter <u>9012 - 9048 Appliance-</u> Installation.

So installieren Sie die 9072-9504DR Series Appliance

Die Appliance ist nur für die Installation in eingeschränkten Bereichen bestimmt. Nur entsprechend geschultes Personal sollte Setup und Wartung durchführen.

Vollständige Informationen zur Installation finden Sie unter <u>9072-9504DR App-</u> liance-Installation.

Kapitel 4: Aktualisieren von Arcserve UDP auf der Appliance

Dieser Abschnitt enthält folgende Themen:

Anwenden einer Lizenz nach einem Upgrade der Arcserve-Software	69
Upgradesequenz aufArcserve Appliance	70
Upgradesequenz für UDP-Konsole, RPS und Agent	76

Anwenden einer Lizenz nach einem Upgrade der Arcserve-Software

Nach der Aktualisierung von Arcserve UDP auf 7.0 oder der Aktualisierung von Arcserve Backup auf 18.0 ist der ursprüngliche Lizenzschlüssel auf der Arcserve Appliance nicht mehr funktionsfähig. Um die neuen Lizenzschlüssel für Arcserve Unified Data Protection 7.0 und Arcserve Backup 18.0 zu erhalten, wenden Sie sich an den für Sie zuständigen Mitarbeiter bzw. Vertreter.

Weitere Informationen zum Hinzufügen eines Lizenzschlüssels für Arcserve UDP finden Sie unter <u>Onlinehilfe für die Arcserve Produktlizenzierung</u>.

Upgradesequenz aufArcserve Appliance

Das Upgrade von Arcserve Appliance 5.0 auf Arcserve UDP v7.0 kann eine der folgenden Sequenzen umfassen:

- Aktualisieren von Arcserve UDP
 - Aktualisieren der Arcserve-Appliance als Arcserve-Konsole und RPS
 - Aktualisieren der Arcserve-Appliance als Arcserve UDP-RPS
 - 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
- Upgradesequenz f
 ür UDP-Konsole, RPS und Agent

Aktualisieren der Arcserve Appliance als Arcserve UDP-Konsole und RPS

Aktualisieren Sie diese Arcserve Appliance und beachten Sie anschließend die beschriebene <u>Aktualisierungssequenz</u>, um die Umgebung zu aktualisieren.

Aktualisieren der Arcserve Appliance als Arcserve UDP-RPS

Aktualisieren Sie die vollständige Produktionsumgebung. Details finden Sie unter Upgradesequenz.

Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcserve Appliance

- Aktualisieren Sie die gesamte Produktumgebung. Detaillierte Informationen finden Sie unter <u>Aktualisierungssequenz</u>.
- Wenn Sie nach der Aktualisierung eine Appliance als RPS aus der Arcserve UDP-Konsole hinzufügen und unten wird eine Warnung angezeigt, finden Sie weitere Informatinonen im Thema <u>Sichern der Arcserve Appliance aus duplizierten Knoten anderer Appliance-Berichte</u> im Abschnitt **Fehlerbehebung**.



Aktualisieren von Arcserve UDP Linux Agent auf der Arcserve Appliance

Befolgen Sie diese Schritte:

- 1. Aktualisieren Sie die Arcserve UDP-Konsole, in der die Umgebung des Linux-Sicherungsservers verwaltet wird.
- 2. Aktualisieren des Linux-Sicherungsservers auf der Arcserve Appliance.

Weitere Informationen finden Sie unter <u>Online-Hilfe zu Arcserve Unified Data Pro-</u> tection Agent für Linux.

Aktualisieren von Arcserve Backup auf der Arcserve Appliance

Im <u>Arcserve Backup-Implementierungshandbuch</u> erfahren Sie, wie Sie ein Upgrade für dieArcserve Appliance durchführen.

Upgradesequenz für UDP-Konsole, RPS und Agent

Planen Sie auf Grundlage der Support-Richtlinie zur Rückwärtskompatibilität Ihr Upgrade in folgender Abfolge, damit es reibungslos funktioniert:

- 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 Agenten im Rechenzentrum.
- 5. Aktualisieren Sie Arcserve UDP-RPS (Remote-Standort).
- 6. Aktualisieren Sie Arcserve UDP Agentless Proxy und einige Agenten am Remote-Standort.

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

7. Aktualisieren Sie den Arcserve UDP Virtual Standby Monitor.

Hinweis: Gemäß der Support-Richtline für die Rückwärtsreplikation muss die Ziel-RPS immer vor der Quell-RPS aktualisiert werden.

Kapitel 5: Konfigurieren der Arcserve Appliance

Dieser Abschnitt enthält folgende Themen:

Konfigurieren der Netzwerkeinstellungen für Arcserve Appliance	.78
Einrichten derArcserve Appliance	. 82
Konfigurieren derArcserve Appliance als Gateway	. 92

Konfigurieren der Netzwerkeinstellungen für Arcserve Appliance

Um die Arcserve Appliance zu verwalten, müssen Sie zuerst die Appliance an das Netzwerk anschließen. Dazu müssen Sie einen Hostnamen zur Appliance zuweisen und dann Netzwerkports konfigurieren.

Befolgen Sie diese Schritte:

 Nach dem Einschalten der Appliance wird das Fenster "Einstellungen" f
ür die Microsoft-Lizenzbedingungen ge
öffnet. Lesen und akzeptieren Sie die Bedingungen.

Das UDP-Dialogfeld Endbenutzer-Lizenzvereinbarung wird geöffnet.

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

Der Bildschirm "Willkommen im Arcserve Appliance -Konfigurationstool" wird angezeigt.

3. Geben Sie die folgenden Details ein:

Hostname

Geben Sie einen Hostnamen für die Appliance ein. Das Zuweisen eines Namens erleichtert die Identifizierung der Appliance im Netzwerk.

Fügen Sie diese Arcserve Appliance zu einer Domäne hinzu

Aktivieren Sie das Kontrollkästchen, um die Appliance als Mitglied einer Domäne in Ihrem Netzwerk aufzunehmen. Geben Sie die Werte in die Felder "Domäne", "Benutzername" und "Kennwort" an, die angezeigt werden, wenn die Option aktiviert ist.

Welcome to the	Arcserve® Appliance C	onfiguration Tool	
This tool will allow you can be performed on	to connect your Arcserve Ap the web-based console UI.	opliance to the LAN so that further co	nfiguration
Assign a hostname to network. Optionally, y	the Appliance. This will be up ou may add the Appliance to	ised to identify the Appliance on your a Domain.	r local
A new hostna on the configure	me will require a reboot to ta aration screen before rebooti	ke effect. You may configure the othe ng the Appliance.	er settings
Hostname	appliance	×	
Add this Arcs	erve Appliance to a doma	in	
			Save

Hinweis: Um einen neuen Hostnamen anzuwenden, müssen Sie die Appliance neu starten. Sie können die Appliance entweder jetzt oder erst nach der Konfiguration der Netzwerkeinstellungen starten. Nach dem Neustart der Appliance können Sie von jeder anderen Maschine aus über die URL *https://<Hostname>:8015* auf die Appliance zugreifen.

4. Klicken Sie auf **Speichern**.

Das folgende Dialogfeld wird geöffnet. Standardmäßig erkennt Arcserve UDP alle Netzwerkverbindungen in einem Netzwerk. Wenn einige Verbindungen nicht zugewiesen sind, bearbeiten Sie sie manuell, und geben Sie die Verbindungsdetails an.

erve Appliance				×
arcserve	Appliance Configuration	Ø	About the Appliance	
Your Arcserve Appliance m Reboot Appliance	nust be rebooted for the Hostname a	nd Domain settings to take effect.		
Hostname/ Domain	appliance (not assigned)	Edit		
UDP Console URL	https://appliance:8015			
Date and Time	1/24/2019 11:53:51 PM	Edit		
Network Connections				
Connection Name	IP Address	Description		
SLOT 3 Port 1 S Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	Edit	1
SLOT 3 Port 2 3 Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #2	Edit	
SLOT 3 Port 3 3 Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #3	Edit	
SLOT 3 Port 4 3 Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #4	Edit	
NIC1 Connected	10.57.25.39 Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #5	Edit	,

5. Um eine Netzwerkverbindung zu bearbeiten, klicken Sie im Feld **Netz**werkverbindungen auf **Bearbeiten**.

Das Dialogfeld Netzwerkverbindung wird geöffnet.

NIC1					
Status	Connected				
Description	Broadcom NetXtreme Giga	bit Ether	net #5		
Connection	Use DHCP to obtain I	P addres	s automa	atically.	
	IP Address	10	. 57	. 25	. 39
	Subnet Mask	255	. 255	. 255	. 0
	Default Gateway	10	. 57	. 25	. 1
	Obtain DNS server ad	dress au	itomatica	lly.	
	Preferred DNS Server	10	. 57	. 1	. 11
	Alternate DNS Server	10	. 64	. 1	. 11
			Sav	e	Cancel

6. Ändern Sie die Werte für die IP-Adresse, die Subnetzmaske und das Standard-Gateway nach Bedarf, und klicken Sie auf **Speichern**.

Hinweis: Optional können Sie Hostname, Domäne, Datum und Uhrzeit ändern.

7. Um die Änderungen zu übernehmen, klicken Sie auf **Appliance neu starten**, um die Appliance neu zu starten.

Die Appliance wird mit einem neuen Hostnamen neu gestartet. Nach dem Neustart öffnet sich das Fenster "Anmeldung".

8. Geben Sie den Benutzernamen und das Kennwort ein, und drücken Sie die Eingabetaste.

Der Bildschirm "Arcserve Appliance-Konfiguration" wird angezeigt.

9. Wenn das Fenster "Konfiguration" für die Appliance erneut geöffnet wird, klicken Sie auf **Assistenten starten**.



Einrichten derArcserve Appliance

Nach dem Neustart der Appliance mit dem neuen Hostnamen wird der Unified Data Protection-Assistent geöffnet. Der Assistent ermöglicht das Erstellen eines einfachen Sicherungsablaufplans. In dem Plan können Sie die Knoten festlegen, die Sie schützen möchten, und den Zeitplan für das Ausführen von Sicherungen angeben. Das Sicherungsziel ist der Appliance-Server.

Hinweis: Alle Schritte desArcserve Appliance-Konfigurationsassistenten sind optional. Sie können sie auch überspringen und direkt die UDP-Konsole öffnen und Pläne erstellen.

Befolgen Sie diese Schritte:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.

Der Unified Data Protection-Assistent öffnet sich zuerst und das Dialogfeld **Arc**serve ApplianceManagement wird angezeigt. Sie können die UDP-Konsole entweder als eine eigenständige Instanz oder per Remote-Zugriff über eine andere UDP-Konsole verwalten. Die Remoteverwaltungsfunktion der Konsolen ist nützlich, wenn Sie mehrere UDP-Konsolen verwalten.



- Wählen Sie aus, ob die Appliance lokal (Standard) oder über eine andere UDP-Konsole verwaltet werden soll. Wenn die Appliance von einer anderen UDP-Konsole verwaltet wird, geben Sie die URL der UDP-Konsole, den Benutzernamen und das Kennwort an.
- 3. Klicken Sie auf Weiter.

Das Dialogfeld **Datenspeicher** wird geöffnet. Ein Datenspeicher ist ein physischer Speicherbereich auf der Appliance und wird als Ziel für Ihre Sicherungen verwendet. Standardmäßig erstellt Arcserve UDP einen Datenspeicher mit dem Namen <hostname>_data_store. Für diesen Datenspeicher sind Deduplizierung und Verschlüsselung aktiviert. Weitere Informationen zu Deduplizierung und Verschlüsselung finden Sie unter <u>Datendeduplizierung</u> im Arcserve UDP-Lösungshandbuch.

Hinweis: Da dieser Datenspeicher verschlüsselt ist, müssen Sie ein Verschlüsselungskennwort angeben.

Orcserv Data Stores Your data store config	ORCSERVE* Appliance Configuration Data Stores Your data store configuration is shown below. More data stores can be added from the Arcserve UDP Console.				
appliance_data_st	tore				
Total Capacity 14.33 TB	Compression Deduplication Encryption Password Confirm Password	Standard Enabled Enabled			
Step 2 of 9		Previous	Next Cancel	-	

- 4. Geben Sie das Verschlüsselungskennwort für diesen Datenspeicher ein und bestätigen Sie es.
- 5. Klicken Sie auf Weiter.

Das Dialogfeld **E-Mail und Alert** wird geöffnet. Sie können den E-Mail-Server, mit dem Alerts gesendet werden, und die Empfänger definieren, die die Alerts erhalten. Sie können Optionen auswählen, mit denen festgelegt wird, ob die Empfänger die Warnmeldungen auf Basis von erfolgreichen Aufträgen, fehlgeschlagenen Aufträgen oder beidem erhalten.

CICSEIVE[®] Appliance Configuration

Email and Alert

Configure email notification settings and the types of alert notifications that you want to receive.

Enable email notifications					
Service	Other	¥			~
Email Server					
Port	25				
Email service requires	authentication.				
Subject	Arcserve Unified Data Protection Alert				
From					
Recipients	Separate email addresses with ;				
Options	Use SSL send STARTTLS Use HTML format				
■ Connect using a proxy	server				
Send a Test Email					
Send Alerts For	Successful Jobs				~
Step 3 of 9		Previous	Next	Cancel	'

6. Geben Sie die folgenden E-Mail- und Warnmeldungs-Details an:

Dienst

Gibt die E-Mail-Dienste an, z. B. Google Mail, Yahoo Mail, Live Mail oder andere.

E-Mail-Server

Gibt die Adresse des E-Mail-Servers an. Geben Sie zum Beispiel für den Google-E-Mail-Server "smtp.gmail.com" ein.

Port

Gibt die Portnummer des E-Mail-Servers an.

Authentifizierung erforderlich

Gibt an, ob der E-Mail-Server eine Authentifizierung verlangt. Wenn dies der Fall ist, geben Sie den Kontonamen und das Kennwort für die Authentifizierung an.

Betreff

Gibt den Betreff der E-Mail an, die an die Empfänger gesendet wird.

In

Gibt die E-Mail-ID des Senders an. Die Empfänger erhalten die E-Mail von diesem Absender.

Empfänger

Gibt die Empfänger an, die die Warnmeldungen erhalten sollen. Verwenden Sie ein Semikolon ";", um mehrere Empfänger zu trennen.

Optionen

Gibt die Verschlüsselungsmethode für den Kommunikationskanal an.

Verbindung per Proxy-Server aufbauen

Gibt den Benutzernamen und die Portnummer des-Proxy-Servers an, wenn Sie die Verbindung mit dem E-Mail-Server über einen Proxy-Server herstellen. Geben Sie außerdem einen Benutzernamen und ein Kennwort an, falls der Proxy-Server eine Authentifizierung verlangt.

Test-E-Mail senden

Sendet eine Test-E-Mail an die Empfänger. Durch Senden einer Test-E-Mail können Sie die Details überprüfen und bestätigen.

7. Klicken Sie auf Weiter.

8. Das Dialogfeld Replikation zum Remote-RPS wird geöffnet.

Replication to Remote RPS			
Configure the settings below if you want to replicate to a remote	v-managed Recove	erv Point Server des	stination.
 This appliance will replicate to a remotely-managed RPS. Arcserve UDP Console URL Username Password 			
Connect using a proxy server. Proxy Settings			
This appliance will not replicate to a remotely-managed RP	s.		
Stop 4 of 0	Destinue		Ganad

9. Geben Sie die folgenden Details an, wenn die Appliance auf einen remote verwalteten Recovery Point Server (RPS) replizieren soll. Weitere Informationen zu einem remote verwalteten RPS finden Sie im *Arcserve UDP-Lösungshandbuch*.

URL der Arcserve UDP-Konsole

Gibt die URL der Remote-Arcserve UDP-Konsole an.

Benutzername und Kennwort

Gibt den Benutzernamen und das Kennwort für die Verbindung mit der Remotekonsole an.

Verbindung per Proxy-Server aufbauen

Gibt die Details des Proxy-Servers an, falls die Remote-Konsole hinter einem Proxy-Server liegt.

- 10. Wenn die Appliance nicht auf einen remote verwalteten RPS repliziert werden soll, wählen Sie die Option **Diese Appliance wird nicht auf einen remote** verwalteten RPS repliziert aus.
- 11. Klicken Sie auf Weiter.

Das Dialogfeld **Plan erstellen** wird geöffnet. Sie können einen Basisplan erstellen, in dem Sie Knoten angeben, die geschützt werden sollen, und den Ablaufplan sichern.

arcserve	Appliance Configuration			
Create a Plan			? A	bout Creating a Plan
Next, you will need to create backup schedule. More than	a protection plan for your data. In th one protection plan can be created.	ne protection plan,	you will add nodes	and configure a
Skip Plan Creation				
Plan Name	Protection Plan 1			
Session Password				
Confirm Password Retain the Session Pa	ssword. You will need it to restore to	he data.		
How do you want to add n	odes to the plan?			
	Hostname/IP Address (for Windows mach	ines only)	*	
Step 5 of 9		Previous	Next	Cancel

Hinweis: Wenn Sie keine einfachen Pläne mit dem Assistenten erstellen möchten, gehen Sie wie folgt vor:

a. Klicken Sie auf Planerstellung abbrechen.

Das Dialogfeld Nächste Schritte wird geöffnet.

- b. Klicken Sie auf **Fertig stellen**, um die UDP-Konsole zu öffnen und Pläne zu erstellen.
- 12. Um einen Plan zu erstellen, geben Sie die folgenden Details an:

Name des Plans

Gibt den Namen des Plans an. Wenn Sie keinen Plannamen angeben, wird der Standardname "Schutzplan <n>" zugewiesen.

Sitzungskennwort

Gibt ein Sitzungskennwort an. Das Sitzungskennwort ist wichtig. Es wird bei der Wiederherstellung von Daten benötigt.

Wie möchten Sie Knoten zum Plan hinzufügen?

Gibt die Methode an, mit der Knoten zum Plan hinzugefügt werden. Wählen Sie eine der folgenden Methoden: Hostname/IP-Adresse

Bezieht sich auf die Methode zum manuellen Hinzufügen der Knoten mithilfe von Hostnamen oder IP-Adresse des Knotens. Sie können beliebig viele Knoten hinzufügen.

Knoten werden von Active Directory erkannt

Bezieht sich auf die Methode zum Hinzufügen von Knoten, die sich in einem Active Directory befinden. Sie können die Knoten zuerst mithilfe der Active Directory-Details ermitteln und dann die Knoten hinzufügen.

Von einem vCenter/ESX-Server importieren

Bezieht sich auf die Methode zum Importieren von VM-Knoten aus ESX- oder vCenter-Servern. Diese Option listet alle virtuellen Rechner auf, die anhand des hier angegebenen Hostnamens oder der IP-Adresse erkannt werden.

<u>Von einem Hyper-V-Server importieren</u>

Bezieht sich auf die Methode, mit der Sie die VM-Knoten von Microsoft Hyper-V-Servern importieren können.

Nachdem Sie eine Methode auswählt haben, geben Sie in den weiteren Dialogfeldern die Details an.

13. Nachdem die Knoten zu Ihrem Plan hinzugefügt wurden, klicken Sie auf **Wei**ter.

	ance Configuration			
Backup Schedule				
Enter criteria for the plan backup sche	dule.			
Install/upgrade and reboot on	Friday – at	9 👻 : 00	- PM -	
Run Incremental Backup daily at	10 - : 00 -	PM 👻		
Schedule Summary (Based)	upon your selections)			
On Friday at 9:00 PM, the lates does not have the latest version Agent installation will not occur On Friday at 10:00 PM, the firs On every day after the installat	st version of the Arcserve L n already installed. • on nodes imported from H t Full Backup will be perfor ion/upgrade is completed,	JDP Agent will be lyper-v or vCenter med. at 10:00 PM an In	installed on any sou /ESX. cremental Backup v	rrce node that vill be performed.
Cancel Plan Creation				
Step 7 of 9		Previous	Next	Cancel

Das Dialogfeld Sicherungsablaufplan wird geöffnet.

- 14. Geben Sie den folgenden Plan ein:
 - Ablaufplan für Installation oder Upgrade des Arcserve UDP-Agenten: Die aktuelle Version des Arcserve UDP-Agenten wird auf Quellknoten installiert, auf denen der Agent nicht installiert ist. Alle vorherigen Agenteninstallationen werden auf die aktuelle Version aktualisiert.
 - Ablaufplan für inkrementelle Sicherung: Zunächst wird eine vollständige Sicherung durchgeführt. Anschließend finden inkrementelle Sicherungen statt.

Hinweis: Wenn die Sicherung vor dem Zeitpunkt der Installation bzw. Aktualisierung geplant ist, wird die Sicherung automatisch für den nächsten Tag geplant. Wenn Sie beispielsweise die Agenteninstallation für Freitag 21:00 Uhr und die Sicherung für 20:00 Uhr planen, wird die Sicherung am Samstag um 20:00 Uhr durchgeführt.

 Planerstellung abbrechen: Um den Plan abzubrechen, den Sie gerade erstellt haben, klicken Sie auf Planerstellung abbrechen.

15. Klicken Sie auf Weiter.

Das Dialogfeld Bestätigung des Plans wird geöffnet.

CITCSETVE [®] And Plan Confirmation This is a confirmation of the plan	ppliance Configuration	ns or create a new plan.	
Protection Plan 1	Plan Name	Protection Plan 1	
⊕ Add a Plan	Nodes Protected Destination	1 app7600	
	Install/Upgrade	Friday, 9:00 PM	
	Backup Schedule	Daily Incremental, 10:00 PM	
	Edit Nodes Edit S	chedule Delete Plan	
Step 8 of 9		Previous Next	Cancel

16. Überprüfen Sie im Dialogfeld die Details des Plans. Sie können die Knoten oder den Ablaufplan ändern, indem Sie auf "Knoten bearbeiten" bzw. "Ablaufplan bearbeiten" klicken, oder Sie können einen Plan hinzufügen oder löschen.

Knoten bearbeiten

Fügen Sie die Quellknoten hinzu, die Sie schützen möchten.

Bearbeiten eines Ablaufplans

Ändert den Sicherungsablaufplan:

17. Klicken Sie nach der Überprüfung der Pläne auf Weiter.

Das Dialogfeld Nächste Schritte wird geöffnet.

Sie haben die Konfiguration erfolgreich abgeschlossen und sind nun bereit, mit der Arcserve UDP-Konsole zu arbeiten. Sie können weitere zu schützende Knoten hinzufügen, Pläne mit Funktionen wie Virtual Standby anpassen und weitere Ziele hinzufügen, indem Sie Recovery Point Server und Datenspeicher einschließen.

arcserve	Appliance Configuration						
Next Steps							
Configuration is complete and you are ready to open the Arcserve Unified Data Protection. With the Arcserve Unified Data Protection you can:							
Add more nodes to pro	otect						
Customize plans with features such as Virtual Standby.							
Add more destinations by including Recovery Point Servers and Data Stores.							
Click Finish to open Arcsei	rve Unified Data Protection.						
Step 9 of 9		Previous	Finish	Cancel			

18. Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden und dieArcserve UDP-Konsole zu öffnen.

Konfigurieren derArcserve Appliance als Gateway

Sie können Arcserve Appliance als Gateway konfigurieren.

Befolgen Sie diese Schritte:

- 1. Deinstallieren Sie die Arcserve UDP-Konsole aus der Arcserve Appliance.
- 2. Klicken Sie in der Arcserve UDP-Konsole auf die Registerkarte **Ressourcen**.
- 3. Navigieren Sie im linken Bereich der Arcserve UDP-Konsole zu Infrastrukturen, und klicken Sie auf Standorte.
- 4. Klicken Sie auf Standort hinzufügen.
- 5. Folgen Sie den Anweisungen des Assistenten zum **Hinzufügen eines Standorts**, um dasArcserve UDP Remote-Management-Gateway auf der Arcserve Appliance zu installieren.

Hinweis: Wenn Sie nach der Installation desArcserve UDP Remote-Management-Gateway auf der Arcserve Appliance auf **Assistenten starten** im Arcserve Appliance-Assistenten klicken, wird die Arcserve UDP-Konsole nicht gestartet. Geben Sie für den Zugriff auf die Arcserve UDP -Konsole direkt die URL der Arcserve UDP-Konsole ein.

Kapitel 6: Arbeiten mit Arcserve Appliance

Mit Arcserve Appliance können Sie Sicherungspläne für Windows, Linux und virtuelle Rechner erstellen. Sie können auch Daten auf ein Bandgerät schreiben und einen virtuellen Standby-Rechner erstellen.

Dieser Abschnitt enthält folgende Themen:

Aktivieren eines Arcserve-Produkts auf der Appliance	
Erstellen eines Plans mithilfe des Arcserve Appliance-Assistenten	95
Hinzufügen eines Knotens zu einem Plan	96
Sicherungsablaufplan für Linux-Knoten erstellen	
Sicherungsablaufplan für ein Bandgerät erstellen	107
Virtuellen On-Appliance-Standby-Plan erstellen	109
Erstellen eines Plans zur Sicherung von Linux-Sicherungsserver	110
Einrichten von Linux-Instant VM-Jobs im lokalen Appliance-Hyper-V	114
Migrieren der Arcserve UDP-Konsole mithilfe von ConsoleMigration.exe	115
Migrieren des vorinstallierte Linux-Sicherungsservers in CentOS 7.4	118
Durchführen der Migration zwischen Arcserve Appliances	
Ändern der Eingabequelle des vorinstallierten Linux-Sicherungsservers	

Aktivieren eines Arcserve-Produkts auf der Appliance

Informationen zum Aktivieren eines Arcserve-Produkts auf der Appliance finden Sie in der <u>Onlinehilfe zur Arcserve-Produktlizenzierung</u>.

Erstellen eines Plans mithilfe des Arcserve Appliance-Assistenten

Ein Plan ist eine Sammlung von Schritten, die definiert, welche Knoten wann gesichert werden sollen. Mit der Arcserve Appliance können Sie Basispläne erstellen. Mit dem Arcserve-Assistenten wird ein Plan in drei Schritten erstellt:

1. Fügen Sie die Knoten hinzu, die Sie schützen möchten.

Sie können Windows-Knoten oder virtuelle Rechner von vCenter/ESX-Servern oder Hyper-V-Servern auswählen.

- 2. Legen Sie den Sicherungsablaufplan fest.
- 3. Überprüfen und bestätigen Sie den Plan.



Neben einfachen Plänen können Sie mit Arcserve UDP auch komplexe Pläne erstellen und viele Parameter aus der UDP-Konsole steuern. Informationen zur Erstellung komplexer Pläne aus der UDP-Konsole finden Sie im *Arcserve UDP Lösungshandbuch*.

Hinzufügen eines Knotens zu einem Plan

Sie können einen Plan erstellen, um verschiedene Knoten zu schützen. Um Knoten zu schützen, müssen Sie Knoten zu einem Plan hinzufügen. Sie können Knoten im Arcserve Appliance-Assistenten hinzufügen. Im Assistenten können Sie Knoten mithilfe der folgenden Methoden hinzufügen:

- Manuelle Eingabe der IP-Adresse oder des Hostnamens f
 ür den Knoten (Knoten nach Hostname/IP-Adresse hinzuf
 ügen)
- Erkennen von Knoten aus einem Active Directory (Knoten nach Active Directory hinzufügen)
- Importieren von VM-Knoten von ESX/vCenter-Servern (vCenter/ESX-Knoten hinzufügen)
- Importieren von VM-Knoten von Microsoft Hyper-V-Servern (<u>Hyper-V-Knoten hinzufügen</u>)

Knoten nach Hostname/IP-Adresse hinzufügen

Um einen Knoten zu einem Plan hinzuzufügen, können Sie die IP-Adresse oder den Hostnamen zur Adresse manuell eingeben. Verwenden Sie diese Methode, wenn Sie nur wenige Knoten hinzufügen möchten. Sie können aber auch mehrere Knoten gleichzeitig hinzufügen. Auf diesen Knoten wird Arcserve Unified Data Protection Agent für Windows installiert.

Befolgen Sie diese Schritte:

1. Geben Sie im Dialogfeld **Knoten nach Hostname/IP-Adresse hinzufügen** die folgenden Details ein:

arcserve	Appliance Configuration					
Add Nodes by Hostna	ame/IP address			About Adding Node		
Enter the hostname/IP address information for the selected Windows nodes, to add to the plan.						
Hostname/IP Address	I	Noc	les Protected by	Plan		
Username			Node Name			
Password		Use	e the fields on the left to a	dd nodes to the plan.		
Description						
				Remove		
Cancel Plan Creation						
Step 6 of 9	Previo	ous	Next	Cancel		

Hostname/IP-Adresse

Gibt den Hostnamen oder die IP-Adresse des Quellknotens an.

Benutzername

Gibt den Benutzernamen des Knotens an, der über Administratorrechte verfügt.

Kennwort

Gibt das Benutzerkennwort an.

Beschreibung

Gibt eine Beschreibung an, um den Knoten identifizieren zu können.

Planerstellung abbrechen

Bricht den gerade erstellten Plan ab.

2. Klicken Sie auf Zur Liste hinzufügen.

Der Knoten wird im rechten Fensterbereich hinzugefügt. Um weitere Knoten hinzuzufügen, wiederholen die Schritte. Alle hinzugefügten Knoten werden im rechten Fensterbereich aufgelistet.

- 3. (Optional) Um die hinzugefügten Knoten aus der Liste im rechten Fensterbereich zu entfernen, wählen Sie die Knoten aus, und klicken Sie auf **Entfernen**.
- 4. Klicken Sie auf Weiter.

Die Knoten werden zum Plan hinzugefügt.
Knoten nach Active Directory hinzufügen

Um Knoten hinzuzufügen, die sich in einem Active Directory befinden, stellen Sie die Active Directory-Details zum Erkennen der Knoten bereit, und fügen Sie dann die Knoten zum Plan hinzu.

Befolgen Sie diese Schritte:

1. Geben Sie im Dialogfeld **Knoten nach Active Directory hinzufügen** die folgenden Details ein:

Benutzername

Gibt Domäne und Benutzernamen im Format Domäne\Benutzername an.

Kennwort

Gibt das Benutzerkennwort an.

Computernamenfilter

Gibt den Filter zum Erkennen der Knotennamen an.

Planerstellung abbrechen

Bricht den gerade erstellten Plan ab.

arcserve	Appliance Configuration			
Add Nodes by Active	Directory		•	About Adding Node
Enter the Active Directory inf	ormation to add nodes to the plan.			
Username	domain\username	Nod	es Protected by P	lan
Password			Node Name	
Computer Name Filter	*	Use	the fields on the left to valid entials and add the nodes to	date the node o the plan.
		_		
		_		
				Remove
Cancel Plan Creation				
Step 6 of 9		Previous	Next	Cancel

2. Klicken Sie auf Durchsuchen.

Die erkannten Knoten werden angezeigt.

OICSEIVE [®] Appliance Configuration												
٨dc	I N	odes by Active	e Direo	ctory						About Adding Nod		
Enter the Active Directory information to add nodes to the plan.												
Active Directory Results				Type node filter t	ext		×	Node	es Protected by F	lan		
		Name		Domain	Username	Verify			Node Name			
		applia8400.ARCSERVE.	СОМ	ARCSERVE.CO			~	Use	the fields on the left to vali	date the node		
	v	appliance1.ARCSERVE.	СОМ	ARCSERVE.CO				cicu		o die puik		
		appliance2511.ARCSER	VE.COM	ARCSERVE.CO			~	-				
	<				>			-				
I.	M	Page 3 of 61	► M	2				_				
l	Jsei	rname	administ	rator				_				
F	ass	sword	•••••	•••• •	•	Apply		-				
		Return			Add	to List				Remove		
Ċ	Car	ncel Plan Creation										
Step	60	of 9					P	Previous	Next	Cancel		

Um Knoten hinzuzufügen, wählen Sie die Knoten aus, und überprüfen Sie sie.

3. Wählen Sie zur Bestätigung die Knoten aus, geben Sie Benutzernamen und Kennwort ein, und klicken Sie auf **Übernehmen**.

Die Anmeldeinformationen werden überprüft und bestätigt. Bestätigte Knoten werden mit einem grünen Häkchen gekennzeichnet. Wenn die Überprüfung eines Knotens fehlschlägt, geben Sie die Anmeldeinformationen erneut ein, und klicken Sie auf noch einmal auf **Übernehmen**.

Hinweis: Sie müssen jeden Knoten überprüfen, bevor Sie ihn zur Liste hinzufügen können.

4. Klicken Sie auf Zur Liste hinzufügen.

Der ausgewählte Knoten wird zum rechten Fensterbereich hinzugefügt.

- 5. (Optional) Um die Knoten aus der Liste im rechten Fensterbereich zu entfernen, wählen Sie die Knoten aus, und klicken Sie auf **Entfernen**.
- 6. Klicken Sie auf Weiter.

Die Knoten werden zum Plan hinzugefügt.

vCenter/ESX-Knoten hinzufügen

Sie können VM-Knoten zu einem VMware vCenter/ESX-Server hinzufügen. Um diese Knoten hinzufügen zu können, müssen Sie die Knoten auf dem vCenter/ESX-Server erkennen und von dort importieren.

Befolgen Sie diese Schritte:

1. Geben Sie im Dialogfeld **Knoten nach vCenter/ESX hinzufügen** die folgenden vCenter/ESX-Serverdetails an:

Hostname/IP-Adresse

Gibt den Hostnamen oder die IP-Adresse des vCenter/ESX-Servers an.

Port

Gibt die Portnummer an, die verwendet werden soll.

Protokoll

Gibt das Protokoll an, das verwendet werden soll.

Benutzername

Gibt einen Benutzernamen auf dem Server an.

Kennwort

Gibt das Benutzerkennwort an.

Planerstellung abbrechen

Bricht den gerade erstellten Plan ab.

arcserve	Appliance Configuration			
Add Nodes by vCent	er/ESX		?	About Adding Nodes
Enter the vCenter/ESX inform	nation to add nodes to the plan.			
Hostname/IP Address		Nod	es Protected by Pla	an
Port	443		Node Name	
Protocol	HTTPS -	Use	the fields on the left to add r	nodes to the plan.
Username	root			
Password				
		_		
				Remove
Cancel Plan Creation				
Step 6 of 9		Previous	Next	Cancel

2. Klicken Sie auf Verbinden.

Die erkannten Hostnamen werden angezeigt.

3. Erweitern Sie einen Hostnamen, um die Knoten anzuzeigen.



4. Wählen Sie die Knoten aus, die Sie hinzufügen möchten, und klicken Sie auf **Zur Liste hinzufügen**.

Die ausgewählten Knoten werden im rechten Fensterbereich hinzugefügt.

- 5. (Optional) Um die Knoten aus der Liste im rechten Fensterbereich zu entfernen, wählen Sie die Knoten aus, und klicken Sie auf **Entfernen**.
- 6. Klicken Sie auf Weiter.

Die Knoten werden zum Plan hinzugefügt.

Hyper-V-Knoten hinzufügen

Mit dieser Methode können Sie VM-Knoten von einem Microsoft Hyper-V-Server importieren.

Befolgen Sie diese Schritte:

1. Geben Sie im Dialogfeld **Hyper-V-Knoten hinzufügen** die folgenden Details an.

arcserve	Appliance Configuration			
Add Hyper-v Nodes			3	About Adding Nodes
Enter Hyper-v information to	add nodes to the plan.			
Hostname/IP Address		Noc	les Protected by Pla	an
Username			Node Name	
Password		Use	the fields on the left to add n	odes to the plan.
				Remove
Cancel Plan Creation				
Step 6 of 9		Previous	Next	Cancel

Hostname/IP-Adresse

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.

Planerstellung abbrechen

Bricht den gerade erstellten Plan ab.

2. Klicken Sie auf Verbinden.

Die erkannten Hostnamen werden angezeigt. Erweitern Sie einen Hostnamen, um die Knoten anzuzeigen.

Add Hyper-v Nodes	Diance Configuration	n		About Adding Nod
Hyper-v Results	Type node filter text	×	Nodes Protect	ted by Plan
Name	Object Type		Node Name	
a 🔲 📑 👔 10.57.25.	Hyper-v Host		app-hyv-02	
Backup-agent	Virtual Machine			
🗐 🚪 Backup-hbbu	Virtual Machine			
UDPIVM_10.57.11	Virtual Machine			
UDPIVM_10.57.11.44725	Virtual Machine			
app-hyv-01	Virtual Machine			
app-hyv-02	Virtual Machine			
m 📄 appliance-test3	Virtual Machine	~		
Return	Add to	List		Remove
Cancel Plan Creation				
Step 6 of 9		Prev	ious Ne	xt Cancel

- 3. (Optional) Sie können den Knotennamen im Filterfeld eingeben, um den Knoten in der Struktur zu finden.
- 4. Wählen Sie den Knoten aus, und klicken Sie auf Zur Liste hinzufügen.

Die ausgewählten Knoten werden im rechten Fensterbereich hinzugefügt.

- 5. (Optional) Um die Knoten aus der Liste im rechten Fensterbereich zu entfernen, wählen Sie die Knoten aus, und klicken Sie auf **Entfernen**.
- 6. Klicken Sie auf Weiter.

Die Knoten werden zum Plan hinzugefügt.

Sicherungsablaufplan für Linux-Knoten erstellen

Sie können Linux-Knoten in der Arcserve Appliance-Konsole sichern. Der Linux-Sicherungsserver wurde bereits zur Konsole hinzugefügt.

Befolgen Sie diese Schritte:

- 1. Öffnen Sie die Arcserve Appliance-Konsole.
- 2. Klicken Sie auf "Ressourcen", "Pläne", "Alle Pläne".
- 3. Erstellen Sie einen Sicherungsablaufplan für Linux
- 4. Geben Sie "Quelle", "Ziel", "Ablaufplan" und "Erweiterte Konfigurationen" an.

Hinweis: Weitere Informationen zu den einzelnen Konfigurationen finden Sie unter Erstellen eines Sicherungsablaufplans für Linux im Lösungshandbuch.

5. Führen Sie den Sicherungsablaufplan aus.

Sicherungsablaufplan für ein Bandgerät erstellen

Arcserve Appliance ist in der Lage, Daten auf ein Bandgerät zu schreiben. Normalerweise entsprechen die Quelldaten dem Wiederherstellungspunkt, den Sie mithilfe des UDP-Sicherungsablaufplans in einen Datenspeicher gespeichert haben, und das Ziel ist ein Bandlaufwerk. Sie müssen Arcserve Backup Manager verwenden, um Ihre Bandsicherungsaufträge auf ein Band zu verwalten.

In der folgenden Prozessübersicht ist dargestellt, wie Sie mit der Arcserve Appliance auf ein Bandgerät schreiben können:

1. Schließen Sie das Bandgerät an dieArcserve Appliance an

Arcserve ApplianceAuf der Rückseite der befindet sich ein Port zum Anschluss eines Bandgeräts. Wenn das Bandgerät angeschlossen ist, wird es automatisch von der Arcserve Appliance erkannt.

2. Bandgerät mit Backup Manager konfigurieren

Öffnen Sie Backup Manager und fügen Sie das Bandgerät zu Backup Manager hinzu. Backup Manager ist die Schnittstelle, mit der Sie Arcserve Backup verwalten können. Nachdem Sie das Bandgerät zu Backup Manager hinzugefügt haben, konfigurieren Sie das Gerät.

Hinweis: Weitere Informationen zur Konfiguration und Verwaltung des Geräts finden sie unter <u>Verwalten von Geräten und Medien</u> im Arcserve Backup-Administrationsleitfaden.

3. Mit der UDP-Konsole mindestens einen Sicherungsauftrag erfolgreich durchführen

Sie benötigen mindestens eine erfolgreiche Sicherung, die Sie auf ein Bandgerät schreiben können. Um Daten zu sichern, erstellen Sie über die UDP-Konsole einen Plan und führen Sie eine Sicherung auf einen Datenspeicher durch.

Hinweis: Weitere Informationen zum Erstellen eines Sicherungsplan für unterschiedliche Knoten finden Sie unter <u>Erstellen von Plänen zum Schutz von</u> <u>Daten</u> im Lösungshandbuch.

4. Bandsicherungsauftrag über Backup Manager starten

Öffnen Sie Backup Manager und erstellen Sie einen Plan zur Sicherung von Daten auf das Bandgerät. Die Quelldaten sind das Ziel des UDP-Sicherungsplans und das Ziel des Bandgeräts. **Hinweis:** Weitere Informationen zum Erstellen eines Sicherungsplan finden Sie unter <u>Sichern und Wiederherstellen von D2D/UDP-Daten</u> im *Arcserve Backup-Administrationsleitfaden*.

Virtuellen On-Appliance-Standby-Plan erstellen

Die Arcserve Appliancekann als virtueller Standby-Rechner fungieren.

Befolgen Sie diese Schritte:

- 1. Überprüfen Sie, und stellen Sie sicher, dass Sie über einen erfolgreichen Sicherungsablaufplan verfügen.
- 2. Öffnen Sie die Arcserve Appliance-Konsole.
- 3. Navigieren Sie zu den Plänen, und ändern Sie den Sicherungsplan.
- 4. Fügen Sie eine Virtual Standby-Aufgabe hinzu.
- 5. Aktualisieren Sie die Quelle, das Ziel und virtuelle Rechnerkonfigurationen.

Hinweis: Weitere Informationen zu den Konfigurationen finden Sie im Thema zur <u>Erstellung eines Virtual Standby-Plans</u>Arcserve UDP im Lösungshandbuch.

6. Speichern Sie den Plan, und führen Sie ihn aus.

Erstellen eines Plans zur Sicherung von Linux-Sicherungsserver

In der Arcserve Appliance, können Sie den Linux-Sicherungsserver für die Sicherung konfigurieren.

Befolgen Sie diese Schritte:

- 1. Klicken Sie in der Arcserve UDP-Konsole auf die Registerkarte **Ressourcen**.
- 2. Klicken Sie im rechten Fensterbereich auf Alle Knoten.
- 3. Klicken Sie im mittleren Fensterbereich auf Knoten hinzufügen.

Das Dialogfeld Knoten zu Arcserve UDP-Konsole hinzufügen wird geöffnet.

- 4. Wählen Sie in der Dropdown-Liste **Hinzufügen von Knoten nach** die Option *Linux-Knoten hinzufügen*.
- 5. Geben Sie die Anmeldeinformationen für den Knoten ein, und klicken Sie auf **Zur Liste hinzufügen**.

Add Nodes to	Arcserve UDP Console					
Add nodes by	Add Linux Node	-				
				Node Name You have not added any node to the list	VM Name	Hypervisor
	Node Name/IP Address	Linux-BackupSvr				
1	SSH Key Authentication					
	User Name	root				
	Password	•••••				
(Non-root Credential					
	Password					
	Add Description					
		_				
		Ad	ld to List			Remove
Help						Save Cancel

6. Klicken Sie auf Speichern.

Der hinzugefügte Linux-Knoten wird in der Liste Alle Knoten angezeigt.

resources								
41	Nodes: /	All Node	s					≫
Nodes	Actions	- A	dd Nodes	Filter ×	(No filter applied)	-		Configuration Wizard
All Nodes								
Nodes without a Plan		Status	Node Name	VM N	ame	Plan		Select a node to view the related details
Plan Groups	E7.	0	linux-backupsvr					o o como :
Linux Backup Server Groups	-							
Linux Nodes								
Plans								
All Plans								
Destinations								
Recovery Point Servers								
Arcserve Backup Servers								
Shared Folders	1							
Cloud Accounts								
Remote Consoles								
Arcserve Cloud								
 Infrastructure 								
Storage Arrays								
Instant Virtual Machines								
Sites								
SLA Profiles								
	4						•	
	14 4 Pa	age 1	of 1 🗼 🕅 🧞			Displaying 1	- 1 of 1	

7. Navigieren Sie zu **Alle Pläne**, und erstellen Sie einen agentenbasierten Linux-Plan.

Die Registerkarte Quelle wird angezeigt.

resources					
Add a Plan	Agent-Based Linux Bac	kup Plan	Pause this plan	Save	Cancel Help
Task1: Backup: Agent-Based Linux	Task Type Backup	: Agent-Based Linux	¥		Delete Task
	Source De	stination Schedule	Advanced		
	Linux Backup Server	appliance	▼ Add		
		nove			
	Node Name	VM Name P	an	Site	
	Filter volumes for backu Files/folders to be exclu	P Exclude v			

8. Wählen Sie den Drop-down-Liste **Hinzufügen** die Option *In Arcserve UDP zu schützende Knoten* aus.

resources											
Add a Plan	Agent-Based Linux Backup	Plan	Pause this plan	Save	Cancel Help						
Task1: Backup: Agent-Based Linux	Task Type Backup: A	gent-Based Linux	Ŧ		Delete Task						
O Add a Task	Source Dest	ination Schedule	Advanced								
Linux Backup Server appliance v Add											
	Add Remo Select Nodes to Pro Add Linux Node	ve lect in Arcserve UDP	lan	Site							
	Eilter volumes for backup	Evaluate -									
	Files/folders to be exclude	d									

Das Dialogfeld "Zu schützende Knoten auswählen" wird geöffnet.

9. Schützen Sie den hinzugefügten Linux-Knoten, und klicken Sie auf **OK**.

Select	Nodes to Protect										ΘX
Available Nodes				-	Sel	ected Nodes					
	Node Name linux-backupsvr	VM Name	Plan	Site Local Site			Node Name linux-backupsvr	VM Name	Plan	Site Local Site	
					» > <						
					«						
H	4 Page 1] of 1 🕨 🕨	🖓 Dis	playing 1 - 1 of 1							
Hel	p									ОК Са	ncel

Die Registerkarte Ziel wird angezeigt.

10. Bei dem angezeigten Standardziel handelt es sich um den Datenspeicher, der mit dem Appliance-Assistenten erstellt wurde. Wählen Sie bei Bedarf die lokale Festplatte oder einen freigegebenen Ordner zum Sichern des Knotens aus.

resources						
Add a Plan Agent-Based Linux Backup Pla		Linux Backup Plan		Pause this plan	Save	Cancel Help
Task1: Backup: Agent-Based Linux	Task Type	Backup: Agent-Bas	ed Linux	T		Delete Task
	Source Destination Type	e Destination	O Local disk or s	Advanced	rver	
	Recovery Point	Server	appliance	v		
	Data Store		appliance_data	l_stor∈ ▼		
	Password Prote	ction	V 0			
	Session Passwo	brd				
	Confirm Session	Password				

11. Nach Angabe der auf den Plan bezogenen Einstellungen klicken Sie auf **Speichern**.

resources								
4	Plans: A	All Plans						≫
Nodes All Nodes	Actions	- Add a Plan	Configuration Wizard					
Nodes without a Plan		Plan Name		Nodes P	rotected		Status	Select a plan to view the related
vCenter/ESX Groups			Total	0	0	0		vetons.
Hyper-V Groups Linux Nodes	E	Agent-Based Linux Backup Plan	1	0	1	0	Deployment: Successful (1)	
Linux Backup Server Groups	_							
Plan Groups								
⊿ Plans								
All Plans								
 Destinations 								
Recovery Point Servers								
Arcserve Backup Servers								
Shared Folders								
Cloud Accounts	4							
Remote Consoles								
Arcserve Cloud								

Sie können nun erfolgreich eine Sicherung für den hinzugefügten Linux-Sicherungsserver ausführen.

Einrichten von Linux-Instant VM-Jobs im lokalen Appliance-Hyper-V

Mit Arcserve Appliance können Sie Linux-Instant VM-Jobs im lokalen Appliance-Hyper-V einrichten

Befolgen Sie diese Schritte:

- 1. Öffnen Sie den Hyper-V-Manager.
- 2. Erstellen Sie einen neuen externen virtuellen Netzwerk-Switch.
- 3. Führen Sie den folgenden Befehl mit PowerShell aus, um Routing und RAS für den in Schritt 1 neu hinzugefügten virtuellen Netzwerk-Switch mithilfe der DOS -Befehlszeile neu zu konfigurieren:

C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance>powershell.\Rebuild-VMSwitch.ps1

Hinweis: Der Linux-Sicherungsserver *Linux-BackupSvr* wird während des Vorgangs neu gestartet.

4. Zum Ausführen eines Linux-Instant VM-Job zum lokalen Hyper-V wählen Sie den neu hinzugefügten virtuellen Netzwerk-Switch aus.

Jetzt können Sie den Linux-Instant VM-Job zu Hyper-V auf einer lokalen Appliance erfolgreich ausführen.

Migrieren der Arcserve UDP-Konsole mithilfe von ConsoleMigration.exe

Auf der Arcserve Appliance können Sie die Arcserve UDP-Konsole mit *ConsoleMigration.exe* auf eine andere Appliance migrieren. Ab Arcserve UDP 6.5 Update 2 oder höher können Sie die Arcserve UDP-Konsole zwischen zwei beliebigen Arcserve UDP-Konsolen migrieren, auch wenn sie nicht zur Appliance gehören.

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

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>Conso
leMigration.exe
Usage: ConsoleMigration.exe <-BackupDB¦-RecoverDB>
-BackupDB: Backup UDP Console database Arcserve_APP
-RecoverDB: Recover UDP Console database Arcserve_APP
```

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>ConsoleMig -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. Wenn die neue Arcserve UDP-Konsole eine Arcserve Appliance- ist, ändern Sie den Hostnamen, und starten Sie das System neu. Schließen Sie dann die Appliance-Konfiguration mithilfe des Appliance-Assistenten ab.

Hinweis: Wenn die Arcserve UDP-Konsole keineArcserve Appliance ist, überspringen Sie diesen Schritt. 4. Auf der neuen Arcserve UDP-Konsole führen Sie die im Bildschirm unten aufgeführten Schritte durch, um die Datenbank der Arcserve UDPKonsole wiederherzustellen. Wenn der Datenbank-Wiederherstellungsvorgang abgeschlossen ist, werden die Knoten für die neue Arcserve UDP-Konsole aktualisiert. Wenn die Aktualisierung von bestimmten Knoten fehlschlägt, werden die getrennten Knoten in der Datei DisconnectedNodesInfo-<MM-TT-JJJJ>.txt im Pfad C:\Programme\Arcserve\Unified Data Protection\Management\BIN\Appliance\logs aufgezeichnet. Sie können die getrennten Knoten über die Arcserve UDP-Konsole manuell aktualisieren.

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</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 Appliance-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: AbArcserve UDP v6.5 Update 4 wird die Option *-force* im Befehl *Con-soleMigration.exe* eingeführt, um die Migration der Sicherungsdatenbankdatei für die Wiederherstellung auf die Zielkonsole unter folgenden Bedingungen 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 möch-

ten. Beispiel: Eine Migration von einer Konsole mit SQL Server 2016 zu einer Konsole mit SQL Server 2014.

Migrieren des vorinstallierte Linux-Sicherungsservers in CentOS 7.4

Wichtig!Das Linux-Migrationstool Linux ist nur fürArcserve UDP V6.5 Update 4 oder höher verfügbar.

Das Linux-Migrationstool (Linux_migration.ps1) ist eine neue Funktion, die mit-Arcserve UDP v6.5 Update 4 eingeführt wurde und mit der Sie den vorinstallierten Linux-Sicherungsserver der Arcserve Appliance von der vorherigen CentOS-Version (z. B. CentOS 6.6) auf CentOS 7.4 migrieren können.

Befolgen Sie diese Schritte:

- 1. Melden Sie sich bei der Arcserve Appliance mit den Anmeldeinformationen des Administrators an.
- 2. Aktualisieren Sie die früheren Versionen von Arcserve UDP in Arcserve Appliance und Linux-Sicherungsserver auf Arcserve UDP V6.5 Update 4 oder höher. Der Linux-Agent auf dem Linux-Sicherungsserver muss auch auf die gleiche Version der Arcserve UDP-Konsole aktualisiert werden
- 3. Laden Sie *Linux-BackupSvr.zip* über den <u>Link</u> herunter (MD5 für diesen Download ist *OA51C1020CB8EA569B9DCEAF7BF226E0*), und extrahieren Sie die Dateien auf die lokale Festplatte. Beispiel: Wenn Sie die Dateien auf Laufwerk X: extrahieren, wird der Pfad wie unten angezeigt.



4. Öffnen Sie die PowerShell-Befehlszeile, und geben Sie folgenden Befehl ein, um den Verzeichnispfad in den Ordner zu ändern, der die Datei "Linux_ migration.ps1" enthält:

cd C:\Programme\Arcserve\Unified Data Protection\Engine\bin\Appliance\

5. Führen Sie den folgenden Befehl aus, um die Migration durchzuführen:

Linux_migration.ps1 -path X:\Linux-BackupSvr

Hinweis: X:\Linux-BackupSvr ist der Pfad, in den die Dateien aus Linux-BackupSvr.zip auf Ihrer lokalen Festplatte extrahiert werden.

Die Befehlszeile zeigt den Status der Migration an.

Nachdem die Migration erfolgreich abgeschlossen wurde, wird der alte Linux-Sicherungsserver ausgeschaltet und der Name des alten Linux-Sicherungsservers in *Linux-BackupSvr-CentOS<Versionsnummer>-<hhmm>* geändert. Der Import des neuen Linux-Sicherungsservers (CentOS 7.4) ist abgeschlossen, und der Name wurde im Hyper-V-Manager erfolgreich in *Linux-BackupSvr* geändert.

6. Aktualisieren Sie den Linux-Sicherungsserver in der Arcserve UDP-Konsole.

Nach der Migration des Linux-Sicherungsservers auf CentOS 7.4 sind alle Einstellungen des Linux-Sicherungsservers wie Linux-Sicherungspläne, Linux-Knoten und Linux-Jobs erfolgreich in der Arcserve Appliance-Konsole migriert und konfiguriert..

Durchführen der Migration zwischen Arcserve Appliances

In diesem Thema werden zwei Lösungen vorgestellt, mit denen Benutzer eine Migration von einer vorhandenen Arcserve Appliance auf eine neue Arcserve Appliance durchführen können.

Sie können zum Beispiel von Arcserve Appliance 8200 auf Arcserve Appliance 8400 migrieren. Es gelten die folgenden Voraussetzungen:

- Vergewissern Sie sich, dass eine Verbindung zu Appliance 8200 und zu Appliance 8400 hergestellt werden kann.
- Auf der neuen Appliance muss genügend Speicher für alle Daten auf der ursprünglichen Appliance frei sein.
- Vergewissern Sie sich, dass auf Arcserve Appliance- 8200 kein Job ausgeführt wird.

Weitere Informationen zur Migration der Konsole finden Sie im Thema Migrieren der Arcserve UDP-Konsole mit ConsoleMigration.exe.

Zum Migrieren von einer Appliance in eine andere stehen zwei Lösungen zur Verfügung, wie unten aufgeführt.

- Lösung 1
- Lösung 2

Lösung 1

Bare-Metal-Recovery (BMR)-Lösung

Gehen Sie wie folgt vor, um BMR aus der vorhandenen Arcserve Appliance auf einer anderen neuen Arcserve Appliance auszuführen:

1. Erstellen Sie einen Datenspeicher auf der neuen Arcserve Appliance 8400 und der Sicherungs-Arcserve Appliance 8200 für diesen Datenspeicher.

Hinweis: Die folgende Warnung können Sie einfach ignorieren:

Der Arcserve UDP Recovery Point Server-Datenspeicher ist konfiguriert auf Volume X:, Y:. Dieses Volume wird nicht gesichert.

2. Führen Sie nach der Sicherung eine BMR auf Appliance 8400 durch; verwenden Sie dabei den Wiederherstellungspunkt, den Sie im Schritt oben erhalten haben, und wählen Sie den Treiber *megasas.inf* manuell aus.

Mapufacturer	Version	Platform	Path
	10/00/2010 10 14 7 0	- Flationn	CAN (ND OV (CVINE) and 42 int
Intel	12/00/2016, 12.14.7.0	X04 C4	C:\\v(INDO\v(S\INE\com9.inf
MS HDC INTEL HDC	06/21/2006 10.014	v64	C.WINDOWSVINE\mshdc.inf
I SI	03/06/2015 6 707 0	- X04 EA	C.WINDOWS WIT WISHCCHI
INTEL	08/19/2016 10.1.2.80	v64	C:\w/NDOWS\INF\cem45 inf
AMD Section ACEB S	06/21/2006 10.0.14	x64	C:\WINDOWS\INE\usboottinf
INTEL	07/30/2013 94210	x64	C:\WINDOWS\INF\oem47 inf
GENDEV SYS. ACC	06/21/2006.10.0.14	x64	C:\WINDOWS\INF\machine.inf
Generic	10/08/2017, 10.0.14	x64	C:\WINDOWS\INF\usbxhci.inf

3. Starten Sie Appliance 8400 nach der BMR entsprechend der Systemeingabeaufforderung neu.

serve Appliance			
arcserve	Appliance Configuration		About the Appliance
Click Launch Wizard to con	tinue configuring your appliance with	n the Arcserve UDP Plan Configuration W	īzard.
Launch Wizard			
Hostname/ Domain	appliance	×	
UDP Console URL	You must restart your cor	nputer to apply these	
Date and Time	changes	Edit	
Network Connections	Before restarting, save any open f	iles and close all programs.	
Connection Name	IP Ad	Now Restart Later	
SLOT 3 Port 1 ONot Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	Edit
SLOT 3 Port 2 3 Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #	2 Edit
SLOT 3 Port 3 3 Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #	K3 Edit
SLOT 3 Port 4 Onnected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #	4 Edit
NIC1	10.57.25.39 Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #	5 Edit

4. Erstellen Sie jetzt den Netzwerk-Switch auf Appliance 8400 neu.

Führen Sie den folgenden Befehl mit PowerShell aus:

C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Rebuild-VMSwitch.ps1

🕌 « Program Files 🕨 Arcserve 🕨	Unified Data Protection Engine	 BIN + Appliance)	v C
Name	Date modified	Туре	Size	
setnat.ps1.log	5/10/2017 5:18 AM	Text Document	2 KB	
nat.log	5/10/2017 5:18 AM	Text Document	6 KB	
🚳 nat2.bat	5/10/2017 5:18 AM	Windows Batch File	2 KB	
dhcpdone.flag	5/10/2017 5:17 AM	FLAG File	0 KB	
resetdhcp.ps1.log	5/10/2017 5:17 AM	Text Document	2 KB	
linuxdone.flag	5/10/2017 4:52 AM	FLAG File	0 KB	
vmstarted.flag	5/10/2017 4:52 AM	FLAG File	0 KB	
adapterNameChanged.flag	5/10/2017 4:52 AM	FLAG File	0 KB	
📄 language.txt	5/10/2017 1:19 AM	Text Document	1 KB	
initstorage.ps1.log	5/9/2017 4:26 AM	Text Document	1 KB	
setos.flag	5/9/2017 1:42 AM	FLAG File	0 KB	
configuration_change.status	5/9/2017 1:39 AM	STATUS File	1 KB	
configuration_change.flag	5/9/2017 1:39 AM	FLAG File	0 KB	
ARCDiskCheck-Finish.tag	5/9/2017 1:39 AM	TAG File	0 KB	
Rebuild-VMSwitch.ps1	0000	Windows PowerS	3 KB	
resetdhcp.ps1	Proceeding Development	Windows PowerS	23 KB	
E ApplianceInformation.ex	Edia	Application	30 KB	
configuration_change.ps	Edit	Windows PowerS	19 KB	
🚳 arcrun.bat	Open with	Windows Batch File	1 KB	
initstorage.ps1	Restore previous versions	Windows PowerS	15 KB	
ARCDiskCheck.exe	Send to >	Application	130 KB	
setnat.ps1	Cut	Windows PowerS	4 KB	
	Сору			

- Führen Sie nun die folgenden Schritte aus, um die Daten auf Appliance 8200 nach Appliance 8400 zu kopieren und die Daten auf Appliance 8400 zu importieren:
 - a. Halten Sie alle UDP-Services auf der Arcserve Appliance 8200 mithilfe des folgenden Befehls aus der Befehlsauforderungszeile an:

C:\Programme\Arcserve\Unified Data Protection\Management\BIN> cmdutil.exe /stopall

b. Kopieren Sie alle Daten auf den Datenträgern X und Y von Arcserve Appliance- 8200 manuell nach Appliance 8400.



c. Starten Sie auf Appliance 8400 alle UDP-Dienste, und Importieren Sie dann die Daten, die Sie von Appliance 8200 kopiert haben.

resources			
Import a Data Store			
Recovery Point Server Data Store Folder Encryption Password	appliance X:\Arcserve\data_store\common • Next		Browse
		Save	Cancel Help

Lösung 2

Migrieren der Arcserve Appliance-Lösung

Wichtig! Wenn die vorhandene Appliance sowohl als Arcserve UDP-Konsole als auch als Arcserve UDP RPS fungiert, kann diese Lösung verwendet werden.

Voraussetzungen:

- Vergewissern Sie sich, dass auf Arcserve Appliance- 8200 kein Job ausgeführt wird.
- Sie haben die Arcserve UDP-Konsole von Arcserve Appliance 8200 auf 8400 migriert.

Hinweis: Weitere Informationen zur Migration der Arcserve UDP-Konsole von Appliance 8200 auf 8400 finden Sie unter <u>Migration der Arcserve UDP-Kon</u>-sole mit ConsoleMigration.exe.

Befolgen Sie diese Schritte:

1. Beenden Sie alle Arcserve UDP-Dienste auf Arcserve Appliance- 8200 mit dem folgenden Befehl in der Befehlszeile:

C:\Programme\Arcserve\Unified Data Protection\Management\BIN> cmdutil.exe /stopall

```
- 0 X
C-5.
                  Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>cmdut
il.exe /stopall
Start to kill process explorer.exe
Killing process explorer.exe
Process killed.
 tart to kill process D2DVDgc.exe
Stopping service 'Arcserve UDP Agent Service'...
Service Stopped.
 topping service 'Arcserve UDP RPS Data Store Service'...
ervice Stopped.
Stopping service 'Arcserve UDP RPS Port Sharing Service'...
Service Stopped.
Stopping service 'Arcserve UDP Identity Service'...
Service Stopped.
Stopping service 'Arcserve UDP Management Service'...
Service Stopped.
Stopping service 'Arcserve UDP Management Port Sharing Service'...
Service Stopped.
 topping service 'Arcserve UDP Agent Explorer Extension Service'...
ervice Stopped.
Stopping service 'Arcserve UDP Update Service'...
Service Stopped.
Stopping Arcserve UDP agent monitor...
Arcserve UDP agent monitor stopped.
Start to kill Arcserve UDP processes
Killing process sync_utl_d.exe
Process killed.
Killing process AFD2DMonitor.exe
Process killed.
Killing process GDDServer.exe
Process killed.
Killing process GDDServer.exe
Process killed.
Killing process GDDServer.exe
Process killed.
Killing process AStartup.exe
Process killed.
Killing process explorer.exe
Process killed.
Stopping mounting driver...
Mounting driver stopped.
 tart Windows Explorer.
```

- 2. Kopieren Sie alle Daten auf den Datenträgern X und Y von Arcserve Appliance- 8200 manuell nach Appliance 8400.
- 3. Starten Sie auf Appliance 8400 alle Arcserve UDP-Dienste, und importieren Sie dann die Datenspeicher, die Sie von Appliance 8200 kopiert haben.

resources		
Import a Data Store		
Recovery Point Server Data Store Folder Encryption Password	appliance X:\Arcserve\data_store\common Next	Browse
	Save	Cancel Help

Hinweis: Die Arcserve UDP-Protokolldateien werden nicht in die neue Appliance migriert.

Sie haben die vorhandene Arcserve Appliance- erfolgreich in eine andere neue Arcserve Appliance- migriert.

Ändern der Eingabequelle des vorinstallierten Linux-Sicherungsservers

Sie können die Tastatur des vorinstallierten Linux-Sicherungsservers ändern.

Befolgen Sie diese Schritte:

- 1. Melden Sie sich bei Arcserve Appliance als Administrator an.
- 2. Klicken Sie auf Einstellungen.



3. Klicken Sie auf Region & Sprache.



4. Klicken Sie auf +, um eine neue Eingabequelle auszuwählen.

🚸 Activities	🎋 Settings 🕶	Fri 00:14	.t •0 ⊕ -
		K Region & Language	×
		Language English (United States)	
		Formats United States (English)	
		Input Sources	Þ
		English (US)	
		+ - ^ ~ 🗉	
			7
			/ CENTOS

5. Wählen Sie die Sprache und das Tastaturlayout an aus.

Activities	¥ Settings ▼		Fri 00:20		∴ 40 O -
		Cancel	Add an Input Source	Add	_
	<	<	English (United States)		×
		Engli	sh (US)	25)	le le la companya de
		Fo Came	eroon Multilingual (gwerty)	ih)	
		Englis	sh (Australian)		
		Input	sh (Cameroon)		
		En Englis	sh (Canada)		
		+ Englis	sh (Colemak) sh (Dvorak alternativernational no s	dead keys)	
	_	Engli	sh (Dvorak)		_
					7
					CENTOS

6. Klicken Sie auf Hinzufügen.

Die Eingabequelle wurde erfolgreich hinzugefügt.

Kapitel 7: Überwachen des Appliance-Servers per Remote-Zugriff

Sie können Arcserve Appliance per Remote-Zugriff überwachen.

Dieser Abschnitt enthält folgende Themen:

Arbeiten mit IPMI	134
Arbeiten mit dem integrierten Dell Remote Access Controller (iDRAC)	

Arbeiten mit IPMI

Dieser Abschnitt enthält folgende Themen:
So ändern Sie das IPMI-Kennwort

Bevor Sie das IPMI-Kennwort ändern, müssen Sie auf den BIOS-Setup-Bildschirm zugreifen, um die IP-Adresse zu erhalten.

Befolgen Sie diese Schritte:

1. Starten Sie Ihr System.

Der Bildschirm "Bootup" wird angezeigt.

2. Drücken Sie den Schlüssel Löschen .

Der BIOS-Setup-Bildschirm wird angezeigt.

Hinweis: Verwenden Sie zum Navigieren die Pfeiltasten, und drücken Sie die **Eingabetaste**. Um zum vorherigen Fenster zurückzukehren, drücken Sie die **ESC**-Taste.

3. Wählen Sie oben im BIOS-Hauptbildschirm die Registerkarte IPMI aus.

Hinweis: Standardmäßig ist die Konfigurationsadressquelle auf DHCP eingestellt.

BMC Network Configuration		BIOS will set below setting
IPMI LAN Selection IPMI Network Link Status: Update IPMI LAN Configuration Configuration Address Source Station IP Address Subnet Mask Station MAC Address Gateway IP Address	[Failover] Shared LAN [No] [DHCP] 172.31.8.192 255.255.0.0 00-25-90-9c-46-eb 172.31.0.1	<pre>++: Select Screen f1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>

- Überprüfen Sie, ob die IP-Adresse korrekt ist. Sie können nur dann über den Webbrowser eine Verbindung mit der IPMI-Schnittstelle herstellen, wenn der Server sich im gleichen Netzwerk befindet.
- 5. Notieren Sie die IP-Adresse der Station.

6. Geben Sie die IP-Adresse für die Station in Ihren Webbrowser ein.

Nachdem über den IPMI-Port eine Verbindung mit dem Remoteserver hergestellt wurde, wird der IPMI-Anmeldebildschirm angezeigt.

PI	lease Login
Username	
Password	
	login

7. Geben Sie im Feld Benutzername Ihren Benutzernamen ein.

Standard: ADMIN

8. Geben Sie im Feld Kennwort Ihr Kennwort ein.

Standard: ARCADMIN

Die Startseite (IPMI-Hauptbildschirm) wird angezeigt.

System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	Help	
🔿 System	• I	\ominus Summa	ary					
System System FRU Reading Hardware Information	Firmware Revis	Firmware Revision : 03.27 IP address : 010.057.025.011						
Hardware Information		BIOS Version : BIOS Build Tim Redfish Version	Firmware Build Time : 01/18/2016 BMC MAC address : 00:25:90:fe:8c:b0 BIOS Version : 2.0 System LAN1 MAC address : 00:25:90:fc:70:48 BIOS Build Time : 12/17/2015 System LAN2 MAC address : 00:25:90:fc:70:49 Redfish Version : 1.0.0 Redfish Version : 1.0.0					
		€ - ∧ ~.	Remote Co Refresh Pr CrCServe Second	nsole Preview eview Image while (we prove on one) while (we prove one) while (we pro	Window principal principal water monotore			
			Power Con Host is c Power On Pow	ntrol via IPMI urrently on wer Down Rese	t			

9. Klicken Sie in der oberen Leiste auf die Option Konfiguration.

Der Bildschirm "Konfiguration" wird angezeigt.

System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	Help					
Configuration	ᅌ Configurat	Configuration										
Alerts	Use these page	Use these pages to configure various settings, such as alerts, users, or network etc.										
Date and Time	Alerts : Add, edit	Alerts : Add, edil or remove alert destinations Date and Time : Configure Date and Time Settings LDAP : Check the box below to enable LDAP authentication and enter the required information to access the LDAP server. Press the Save button to save your changes. Active Directory : Configure settings to authenticate and access the Active Directory server										
LDAP	Date and Time : LDAP : Check the optimum of the optimum o											
Active Directory	 Active Directory RADIUS : Config Mouse mode : C 	tive Directory : Configure settings to authenticate and access the Active Directory server ADIUS : Configure settings to authenticate and access the RADIUS server. Louse mode : Configure the mouse mode for remote conside										
RADIUS	Network : See th Dynamic DNS :	Mouse mode : Configure the mouse mode for remote console Network : See the MAC address or change network settings, including dynamic and static IP assignment Dynamic DNS : Configure dynamic update properties for Dynamic DNS SMTP : Configure the SMTP emails server SSL Certification : The dates for the default certificate and private key are shown below. To upload a new SSL certificate, use the Browse button to navigate to the certificate and press the Upload button. Name: Add-address in common servers.										
Mouse Mode	 SMTP : Configure SSL Certification Users : Add. edit 											
Network	Port : Configure IP Access Contro	the port number of the ser ol : Add, edit or remove IP	vices access rules									
Dynamic DNS	 SNMP : Configu Fan Mode : Con Web Section : Con 	ire SNMP setting ifigure the fan mode	unitere .									
SMTP	Toggle SUM Lice	insed Checking : Toggle o	n/off SUM license checking	1								
SSL Certification	1											
Users												
Port												

- 10. Klicken Sie in der Randleiste "Konfiguration" auf die Option Benutzer.
- 11. Wählen Sie den Benutzer (ADMN) aus der Benutzerliste aus.
- 12. Klicken Sie auf Benutzer ändern.

Das Fenster "Benutzer ändern" wird angezeigt.

System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	Help
Configu	iration	😌 Modify L	Jser				
Alerts		5.1					
Date an	d Time	Enter the n	ew information for the	user below and pres	is Modify. Press Car	icel to return to the user	list.
LDAP		User Name			_		
Active I	Directory	Change Pa	ssword 🕑				
RADIU:	s	Password: Confirm Pa	assword:				
Mouse	Mode	Network Pr	rivileges:	Ŧ			
Networ	k	Modify	Cancel				
Dynami	c DNS						
🔿 SMTP							
I SSL Ce	rtification						
Users							

- 13. Geben Sie Ihren Benutzernamen (ADMIN) ein.
- 14. Wählen Sie die Option Kennwort ändern aus.

Das Kennwortfeld wird aktiviert.

- 15. Geben Sie das neue Kennwort ein und bestätigen Sie es.
- 16. Klicken Sie auf Ändern, um die Änderungen zu speichern.

Ihr IPMI-Kennwort wurde erfolgreich geändert.

So aktualisieren Sie die IPMI-Firmware

Supermicro IPMI-Hilfsprogramme helfen Ihnen dabei, das IPMI entsprechend den Anforderungen Ihrer Organisation zu aktualisieren.

Befolgen Sie diese Schritte:

 Melden Sie sich bei IPMI an, navigieren Sie zur Registerkarte Maintenance, und klicken Sie auf Firmware Update.

Der Bildschirm "Firmware Update" wird angezeigt.

2. Klicken Sie auf Enter Update Mode.

Eine Meldung in einem Popup-Fenster der Webseite wird angezeigt.

3. Klicken Sie auf OK.

Der Bildschirm zum Herunterladen von BIOS und IPMI wird angezeigt.

4. Klicken Sie auf die .zip-Datei, die der Version des IPMI-Modells entspricht.

Die Datei wird heruntergeladen und der Bildschirm für das Hochladen der Firmware angezeigt.

- 5. Extrahieren Sie die Dateien aus der heruntergeladenen .zip-Datei.
- 6. Klicken Sie im Bildschirm "Firmware Upload" auf **Browse**, und wählen Sie die **.bin**-Datei aus den extrahierten Dateien aus.
- 7. Klicken Sie auf Upload Firmware.

Das Firmware-Image wird hochgeladen.

8. Klicken Sie auf Start Upgrade.

Die Firmware-Aktualisierung wird abgeschlossen und IPMI neu gestartet.

Sie können die aktualisierte Firmware-Version auf dem Bildschirm "Summary" anzeigen.

Arbeiten mit dem integrierten Dell Remote Access Controller (iDRAC)

Dieser Abschnitt enthält folgende Themen:

Überwachung und Verwaltung des integrierten Dell Remote Access Controller (iDRAC)

Arcserve Appliance9012-9504DR-Modelle sind mit einem integrierten Dell Remote Access Controller 9 (iDRAC9) installiert. Mit iDRAC9 können Serveradministratoren die allgemeine Verfügbarkeit von Arcserve Appliance verbessern. iDRAC bietet Administratoren Alerts zu Serverproblemen, ermöglicht die Remote-Server-Verwaltung kann. Außerdem ist weniger physischer Zugriff auf den Server erforderlich.

Sie müssen sich bei iDRAC anmelden, um den Systemstatus zu überwachen, Systeminformationen zu verwalten und die virtuelle Konsole zu starten.

Befolgen Sie diese Schritte:

So melden Sie sich bei iDRAC an:

1. Starten Sie einen Browser, und navigieren Sie zu https://<iDRAC-IP-Adresse.

Die Anmeldeseite von iDRAC wird angezeigt.

2. Geben Sie folgende Informationen ein:

Benutzername: Root

Kennwort: ARCADMIN

3. Klicken Sie auf Anmelden.

Überwachen des Systemstatus und Verwalten der Systeminformationen:

Sie können den iDRAC-Systemstatus überwachen und die folgenden Informationen verwalten:

- Systemstatus
- Systemeigenschaften
- Hardware- und Firmwarebestand
- Sensorzustand
- Speichergeräte
- Netzwerkgeräte
- Benutzersitzungen anzeigen und beenden

So Starten Sie die virtuelle Konsole:

- 1. Melden Sie sich bei https://<iDRAC-IP-Adresse> an.
- 2. Navigieren Sie zum Dashboard, und klicken Sie auf Virtuelle Konsole starten.

Die Seite "Virtuelle Konsole" wird angezeigt.

Die Anzeige der virtuellen Konsole zeigt den Remote-System-Desktop an. Sie können die Steuerung des Remote-Systems übernehmen und mithilfe der Tastatur und Maus Vorgänge ausführen.

Suchen der IP-Adresse des integrierten Dell Remote Access Controller (iDRAC)

Die Modelle der Arcserve Appliance 9012-9504DR-Serie sind für Verwendung von DHCP für iDRAC standardmäßig konfiguriert. Um iDRAC zugreifen zu können, stellen Sie sicher, dass Sie die Ethernet-Kabel an den dedizierten iDRAC9-Netzwerkport anschließen. Informationen zum Bedienfeld und dedizierten iDRAC9-Netzwerkport der Modelle der Arcserve Appliance 9012-9504DR-Serie finden Sie unter <u>Bedi</u>enfeld der 9012-9048, Bedienfeld der 9072DR-9504 DR.

Rückseite der 9012-9048 für iDRAC9 anzeigen



iDRAC9 dedicated network port on rear panel of Arcserve Appliance 9012-9048 series models

Rückseite der 9072DR-9504 DR für iDRAC9 anzeigen

iDRAC9 dedicated network port on rear panel of Arcserve Appliance 9072DR-9504DR series models

Sie finden die IP-Adresse des iDRAC auf der Appliance.

Befolgen Sie diese Schritte:

1. Notieren Sie iDRAC-IP beim Starten der Arcserve Appliance.

Initializing Firmware Int	terfaces Activate Windows	
F2 = System Setup F10 = Lifecycle Controller (Config iDRAC, Update FW, Install OS) F11 = Boot Manager F12 = PXE Boot	BIOS Version: 1.4.9 IDRAC IP: 10.57.25.	

2. Starten Sie einen Browser, und navigieren Sie zu https://<iDRAC-IP-Adresse.

\leftrightarrow > C	Not secure https://10.57.25/restgui/start.html?login		☆ 0
	Integrated Remote Ac	CCESS Controller 9	
	Type the User Name and Pass	word and click Log In.	
	Username: f	Password:	
	Domain:		
	This iDRAC 🔻		
	Security Notice: By accessing this computer, you confirm that su	ch access complies with your organization's security policy.	
	Log In		
			Windows.
	Online Help Supp	ort About	

Die Anmeldeseite von iDRAC wird angezeigt.

Konfigurieren der DHCP- oder statischen IP-Adresse des iDRAC

Sie können den DHCP-Netzwerk-Modus für iDRAC festlegen.

Befolgen Sie diese Schritte:

1. Drücken Sie F2 beim Starten der Arcserve-Appliance, und rufen Sie das System-Setup auf.

Entering System Setup F10 = Lifecycle Controller (Config iDRAC, Update FW, Install OS) F11 = Boot Manager F12 = PXE Boot	BIOS Version: 1.4.9 iDRAC IP: 10.57.25
Initializing Firmware Inte	arfaces Activate Windows

2. Klicken Sie im Bildschirm des Hauptmenüs des System-Setups auf i**DRAC Einstellungen**.

System Setup	Help About Exit
System Setup	
System Setup Main Menu	
System BIOS	
iDRAC Settings	
iDRAC Settings allows you to configure iDRAC.	
Samin Toutfol	Activate Windows Go to Action Center to a Finish Windo

3. Klicken Sie in den Optionen der iDRAC Einstellungen auf**Netzwerk**.

Die Felder für die Netzwerk-Einstellungen werden angezeigt.

System Setup		Help About	Exit
iDRAC Settings			
iDRAC Settings			
iDRAC Settings Version	3.00.00.32		•
iDRAC Firmware Version	3.21.21.21 (Build 30)		
System Summary			
System Event Log			
Network			
Alerts			
Front Panel Security			
Media and USB Port Settings			
Lifecycle Controller			
Power Configuration			
Use this page to configure the network properties, of properties, IPMI settings, and VLAN settings.	ommon iDRAC settings, IPv4 and IPv6		
Service Tag : 5Q6	T	Go to Action Center to a Finis	s h Windo

4. Wählen Sie Aktiviert für NIC-Einstellung aktivieren aus, und wählen Sie Dedizierte für NIC-Auswahl aus, um verwenden die dedizierte Netzwerkschnittstelle zu verwenden.

DRAC Settings	
RAC Settings • Network	
ETWORK SETTINGS	
Enable NIC	⊖ Disabled
NIC Selection	Dedicated
Failover Network	None
MAC Address	54:48
Auto Negotiation	O Off ⊚ On
Auto Dedicated NIC	Disabled O Enabled
Network Speed	O 10 Mbps O 100 Mbps ● 1000 Mbps
Active NIC Interface	Dedicated
Duplex Mode	Half Duplex I Full Duplex
OMMON SETTINGS	
Register DRAC on DNS	Disabled Denabled

5. Zum Einstellen des DHCP-Modus wählen Sie in den IPV4-Einstellungen die Option **Aktiviert** für **IPv4 aktivieren** und **DHCP aktivieren** aus.

RAC Settings				
RAC Settings • Network				
Auto Config Domain Name	Oisabled	O Enabled		
Static DNS Domain Name				
V4 SETTINGS				
Enable IPv4	O Disabled	Enabled		
Enable DHCP	O Disabled	Enabled		
IP Address	10.57.25			
Gateway	10.57.25			
Subnet Mask	255.255.255	v		
Use DHCP to obtain DNS server addresses	Disabled	 Enabled 		
Preferred DNS Server	0.0.0.0			
Alternate DNS Server	0.0.0			
V6 SETTINGS				
Colort Epoklad to proble N/C 10/her N/C is an	able dit anti-atan the		rala in	
Select Enabled to enable NIC, when NIC is enabled to enable NIC. when NIC is disabled, all community this group. When a NIC is disabled, all community of the second se	abled, it activates the ication to and (Pres	remaining cont is <f1> for more</f1>	rois in e help)	
 and group. When a file is disabled, all comman 			c noip)	

Hinweis: Wenn Sie die statische IP-Adresse für das dedizierte iDRAC-Netzwerk festlegen möchten, legen Sie für **IPv4 aktivieren** die Option **Aktiviert** und für **DHCP aktivieren Deaktiviert** aus. Legen Sie IP-Adresse, Gateway und Subnetzmaske entsprechend der Netzwerkkonfiguration fest.

System Setup		Help About Exit
iDRAC Settings		
iDRAC Settings • Network		
Auto Config Domain Name	O Enabled	
Static DNS Domain Name		
IPV4 SETTINGS		
Enable IPv4	○ Disabled	
Enable DHCP		
IP Address	10.57.25	
Gateway	10.57.25	
Subnet Mask	255.255.255	
Use DHCP to obtain DNS server addresses	O Enabled	
Preferred DNS Server	0.0.0.0	
Alternate DNS Server	0.0.0.0	
IPV6 SETTINGS		
Select Enabled to enable NIC. When NIC is enable this group. When a NIC is disabled, all communi	bled, it activates the remaining controls in cation to and (Press <f1> for more help)</f1>	
Service Tag : 5QL	Go to Activate W	indows Center to ac Back Wind

6. Klicken Sie auf **Zurück**, klicken Sie auf **Fertig stellen**, und klicken Sie dann auf **Ja** im Dialogfeld **Warnung**.

Die Netzwerkinformationen werden gespeichert.

System Setup		Help About Exit
iDRAC Settings		
iDRAC Settings		
iDRAC Settings Version	3.00.00.32 3.21.21.21 (Build 30)	
System Summary System Event Log Network Alerts	Warning Saving Changes Settings have changed. Do you want to save the changes?	
Front Panel Security Media and USB Port Settings Lifecycle Controller Power Configuration	Yes No	-
Service Tag 50		Activate Windows Go to Action Center <mark>to a Finish Win</mark> do

7. Klicken Sie im Dialogfeld Erfolg auf OK.

System Setup		Help About Exit
iDRAC Settings		
iDRAC Settings		
iDRAC Settings Version	3.00.00.32	-
iDRAC Firmware Version	3.21.21.21 (Build 30)	
System Summary	Success	
System Event Log	Saving Changes	
Network	The settings were saved	
Alerts	successfully.	
Front Panel Security		
Media and USB Port Settings	ок	
Lifecycle Controller		
Power Configuration		
		-
		Activate Windows
Service Tag: 5Q		Go to Action Center <mark>to a Finish Win</mark> do

Sie haben die Konfiguration der iDRAC DHCP abgeschlossen.

8. Klicken Sie auf **Fertig stellen**, und klicken Sie dann auf **Ja**, um das Setup zu beenden und das System neu zu starten.



Der DHCP-Netzwerk-Modus für iDRAC-Initialisierung ist nun konfiguriert.

Kapitel 8: Wiederherstellen oder Reparieren derArcserve Appliance

Dieser Abschnitt enthält folgende Themen:

Debuggen und auf Werkseinstellungen zurücksetzen	. 152
Anwenden von Arcserve UDP-Werkseinstellungen unter Verwendung der Start- option in 7000-8000 Series Appliance	154
Anwenden von Arcserve UDP-Werkseinstellungen unter Verwendung der Start- option für Geräte der 9012-9504DR Serie	. 157
Löschen der Konfiguration und Zurücksetzung der Appliance auf Werkseinstellunger	<u>160 160 1</u>
Festplatte entfernen und ersetzen	. 164
Durchführen einer Bare Metal Recovery (BMR), ohne Daten beizubehalten	.166
Durchführen einer Perform Bare Metal Recovery (BMR) und Beibehalten der Daten .	.181

Debuggen und auf Werkseinstellungen zurücksetzen

Das Thema beschreibt, wie Sie ein Debug für das System durchführen und es auf Werkseinstellungen zurücksetzen, wenn die folgende Fehlermeldung angezeigt wird:



Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

1. Klicken Sie in der angezeigten Fehlermeldung auf die Drop-Down-Option **Fehlerbehebung**.

Folgende Optionen werden angezeigt:

Befehlszeile

Über die Befehlszeile können Sie einige grundlegende Funktionsweise ausführen. Zum Beispiel können Sie überprüfen, ob eine Datei im Ordner vorhanden ist, Dateien kopieren und löschen Informationen zum Datenträgerlayout abrufen.

Anzeigen von Protokollen

Die Option "Protokolle anzeigen" zeigt die Protokolle in Notepad an. Sie können die Protokolle überprüfen und zur späteren Verwendung speichern, indem Sie auf *Datei, Speichern unter* klicken.

"Auf Werkseinstellungen zurücksetzen" erneut starten

Mit dieser Option können Sie erneut auf die Werkseinstellungen zurücksetzen, wenn das Problem behoben ist.

Hilfe

Das Dialogfenster "Hilfebibliothek" enthält Informationen zu Ursache, grundlegender Analyse und Lösungen für den Fehler. Gehen Sie wie folgt vor, um das Problem zu beheben. Tipps zu allgemeinen Operationen werden ebenfalls angezeigt. Zum Beispiel, wie das Datenträgerlayout abgerufen wird, wie Inhalt aus der Eigenschaftendatei zum Zurücksetzen der Werkseinstellungen abgerufen wird oder wie Sie die Protokolle speichern.

2. Klicken Sie in den angezeigten Optionen auf Hilfe.

Der Bildschirm zeigt mehrere Fehlercodes mit Details an.

0		Factory Reset Help
Category:		
Category: - Help - Error code 1001 - Error code 1002 - Error code 1003 - Error code 1003 - Error code 1005 - Error code 1005 - Error code 1007 - Error code 1007 - Error code 1010 - Error code 1010 - Error code 1011 - Error code 1011 - Error code 1013 - Error code 1013 - Error code 1016 - Error code 1018 - Error code 1019 - Error code 1020 - Error code 1020	Î	Cause: Program cannot find "post_factoryreset.ps1". Debug: Check if "post_factoryreset.ps1" exist at the path "x:\windows\system32\appliance". If existing, check the content, otherwise please collect the logs and contact Arcserve Support. Steps: 1. Open Command Prompt (cmd) from "Troubleshoot">"Command Prompt". 2. Type "cd x:\windows\system32\appliance\" and press Enter. 3. Type "dir" and press Enter. All the files and folders in the folder are displayed. Check if the file "post_factoryreset.ps1" is exist. 4. Also refer to ["Tip">"How to save the logs?"] for information on how to collect and save the logs for further analysis.
Error code 1022 Error code 1023 Error code 1031 Error code 1032 Error code 1032	~	
<	>	

0		Factory Rese	et Help						x
Category:									
Error code 1019 A	Steps:								^
Error code 1020		1. Open Comm	and Promp	ot (cmd)	from "Tr	oublesho	ot">"Commar	nd Prompt".	
- Error code 1022		2. Type "diskpar	t" and pre	ss Enter.					
- Error code 1023		Version of dis	coart is dis	played.					
- Error code 1031		3 Type DISKPAR	T> "list di	k" and n	ress Entr	er			
- Error code 1032		The dick list a		hown he	low The	bigger ci	ize dick is usually	our ourtern dick	
- Error code 1033		The disk list a	phears as a	nown be	iow. me	bigger si	ize uisk is usually	our system uisk	
Error code 1034		D'.1. 000	C 1.1	C			C		
Error code 1035		Disk ###	Status	Size	Free	Dyn	Gpt		
Error code 1036		Disk 0	Online	447G	0B				
Error code 1037		Disk 1	Online	3725G	0B				
Error code 1038									
Error code 1039		Here, the Disk 1	is the data	disk, the	e Disk 0 i	s the SSD	disk.		
Error code 1051									
Error code 1052		4. Type "select o	lisk <disk r<="" td=""><td>umber g</td><td>ot above</td><td>e>"and pr</td><td>ress Enter.</td><td></td><td></td></disk>	umber g	ot above	e>"and pr	ress Enter.		
Error code 1053		It will respond	with "Disk	<disk ni<="" td=""><td>umber a</td><td>ot above</td><td>> is now the sele</td><td>cted disk."</td><td></td></disk>	umber a	ot above	> is now the sele	cted disk."	
El Tin		5. Type DISKPAR	RT>"list pa	rtition" a	ind press	Enter.			
- How to get the diskla		The disk layou	t list will s	how as s	hown be	low			
How to get the conte		The disk by ou							
How to save the logs		Dartition ###	Turne		Size		Officat		
How to get IP address		Partition 1	Туре		2008 40		1024KP		
· · · · · · · · · · · · · · · · · · ·		Partition 1	Recover	У	SUUMB		102468		
< >		Partition 2	System		AAWR		SUIMB		~

Wenn Sie den richtigen Fehler auswählen und die im Tipp angezeigten Anweisungen befolgen, können Sie die Werkseinstellungen zurücksetzen und das Problem lösen.

Anwenden von Arcserve UDP-Werkseinstellungen unter Verwendung der Startoption in 7000-8000 Series Appliance

Sie können die UDP-Werkeinstellung auf dem Startmenü der Serie Arcserve Appliance anwenden. Mit den UDP-Werkeinstellungen können Sie dieArcserve Appliance in den ursprünglichen Zustand ohne Konfiguration zurücksetzen.

Hinweis: Sie können auch die Option **Sicherungsdaten beibehalten** auswählen, während Sie das Gerät auf die UDP-Werkeinstellungen zurücksetzen.

Befolgen Sie diese Schritte:



1. Drücken Sie F11, um das Startmenü aufzurufen.

2. Wählen Sie die Startoption zum Zurücksetzen von UDP auf die Werkseinstellungen.



Es wird eine Seite zum Zurücksetzen auf Werkseinstellungen angezeigt.



Hinweise:

- Die Option Vorhandene Sicherungsdaten erhalten ist standardmäßig aktiviert. Nur C:\ im ursprünglichen Betriebssystem wird neu erstellt. Daten unter X:\ volume und Y:\ volume bleiben unverändert.
- Wenn Sie die Option zum Erhalten vorhandener Sicherungsdaten deaktivieren, werden alle Daten auf den entsprechenden Volumes C:\, X:\ und Y:\ im ursprünglichen Betriebssystem neu erstellt.
- 1. Klicken Sie auf Zurücksetzen.

Ein Bestätigungsdialogfeld wird angezeigt.

onfir	m Factory Reset	
1	Are you sure you want to perform a factory reset on your Arcserve Appliance? Selecti result in returning all settings to their factory defaults.	ng Reset will
	All of your backup data will be preserved during the reset.	
	Pasat	Cancel

Sie können auf Abbrechen klicken, um die neu zu starten. Arcserve Appliance

- 2. Nachdem die Appliance auf die Werkseinstellungen zurückgesetzt wurde, können Sie eine der folgenden Aktionen durchführen:
 - Klicken Sie auf **Neustart**, um die Appliance neu zu starten.
 - Klicken Sie auf **Herunterfahren**, um die Appliance zu schließen.

arcserve [®] ,	Appliance			
Factory Reset Factory Reset is restoring all of the deleted. The Arcserve UDP software	settings on the Arcserve Appliance to their factory de is reverting to the version originally installed on the	faults. All resource: Appliance.	s, job history, reports, an	d logs are being
Reverting to Arcserve UDP V	ersion 7.0.4404.			
Existing backup data is being	g preserved.			
Factor	y Reset Is Complete			
0	Your Arcserve Appliance has been returned to its factory	defaults.	00000	
	Click Restart to restart the appliance and launch the Con shut down the appliance.	figuration Wizard or o	lick Shut Down to	
		Restart	Shut Down	
Factory reset is complete.				

Anwenden von Arcserve UDP-Werkseinstellungen unter Verwendung der Startoption für Geräte der 9012-9504DR Serie

Sie können die UDP-Werkeinstellung auf dem Startmenü der Serie Arcserve Appliance 9012-9504DR anwenden. Mit den UDP-Werkeinstellungen können Sie die Arcserve Appliance 9012-9504DR-Serie in den ursprünglichen Zustand ohne Konfiguration zurücksetzen.

Hinweis: Sie können auch die Option "Sicherungsdaten beibehalten" auswählen, während Sie das Gerät auf die UDP-Werkeinstellungen zurücksetzen.

Befolgen Sie diese Schritte:

1. Drücken Sie F11 auf der Tastatur, um das Startmenü aufzurufen.



2. Wählen Sie die Startoption Integrierter RAID-Controller 1: UDP auf Werkseinstellungen zurücksetzen.

Boot Manager
Boot Menu
Select UEFI Boot Option
Integrated RAID Controller 1: Windows Boot Manager
Integrated RAID Controller 1: UDP Factory Reset
UEFI Boot Option Maintenance
Boot From File
Add Boot Option
Delete Boot Option
Device Path : (Press <f1> for more help)</f1>
Go ^{co S} Finish ^{, Col}

Es wird eine Seite zum Zurücksetzen auf Werkseinstellungen angezeigt.

Factory Reset	
Performing a Factory Reset on your Arcserve Appliance will return all settings to their factory defaults. All resources, job hist be deleted. The Arcserve UDP software will revert from its current version to the version originally installed on the Appliance	tory, reports and log entries will e.
Reverting to Arcserve UDP Version 7.0.4399.	
Preserve existing backup data.	
Reset	Cancel

Hinweise:

- Die Option Vorhandene Sicherungsdaten erhalten ist standardmäßig aktiviert. Nur C:\ im ursprünglichen Betriebssystem wird neu erstellt. Daten auf Volume X:\ und Volume Y:\ bleiben unverändert.
- Wenn Sie die Option zum Erhalten vorhandener Sicherungsdaten deaktivieren, werden alle Daten auf den entsprechenden Volumes C:\, X:\ und Y:\ im ursprünglichen Betriebssystem neu erstellt.
- 3. Klicken Sie auf Zurücksetzen.

Ein Bestätigungsdialogfeld wird angezeigt.

•	Are you sure you want to perform a factory reset on	your Arcserve Appliance	e? Selecting Reset wil
:	result in returning all settings to their factory default	s.	170
	24 (JEA) (R		
	All of your backup data will be preserved during the	reset.	
		Contract of the second	10. 10. 10.
		Decot	Cancel

Sie können auf Abbrechen klicken, um die neu zu starten. Arcserve Appliance

- 4. Nachdem die Appliance auf die Werkseinstellungen zurückgesetzt wurde, können Sie eine der folgenden Aktionen durchführen:
 - Klicken Sie auf **Neustart**, um die Appliance neu zu starten.
 - Klicken Sie auf **Herunterfahren**, um die Appliance zu schließen.

arcserve",	Appliance
Factory Reset	
Factory Reset is restoring all of the deleted. The Arcserve UDP software	settings on the Arcserve Appliance to their factory defaults. All resources, job history, reports, and logs are being is reverting to the version originally installed on the Appliance.
Reverting to Arcserve UDP V	fersion 7.0.4404.
Existing backup data is bein	g preserved.
Factor	y Reset Is Complete
	Your Arcserve Appliance has been returned to its factory defaults.
	Click Restart to restart the appliance and launch the Configuration Wizard or click Shut Down to shut down the appliance.
	Restart Shut Down
Factory reset is complete.	

Löschen der Konfiguration und Zurücksetzung der Appliance auf Werkseinstellungen

Mit "Auf Werkseinstellungen zurücksetzen" können Sie dieArcserve Appliance in den ursprünglichen Zustand ohne Konfiguration zurücksetzen. Sie können die Zurücksetzung über die Arcserve UDP-Konsole durchführen.

Befolgen Sie diese Schritte:

1. Klicken Sie in der Arcserve UDP-Konsole auf der Registerkarte Einstellungen auf Auf Werkseinstellungen zurücksetzen.



Alle gesicherten Daten werden standardmäßig beibehalten.

Hinweise:

Arcserve UDP bietet die Option **Vorhandene Sicherungsdaten erhalten**, mit der Sie den vorhandenen Datenspeicher beibehalten können.

- Bei der Auswahl der Option Vorhandene Sicherungsdaten erhalten wird nur Volume C:\ neu erstellt. Daten auf Volume X:\ und Volume Y:\ bleiben unverändert.
- Wenn Sie die Option Vorhandene Sicherungsdaten erhalten nicht auswählen, werden alle Daten auf den entsprechenden Volumes C:\, X:\ und Y:\ neu erstellt.
- 2. Klicken Sie auf Auf Werkseinstellungen zurücksetzen.

Ein Bestätigungsdialog wird angezeigt.



3. Klicken Sie im Bestätigungsdialog auf **Zurücksetzen**, um die Zurücksetzung auf Werkseinstellungen zu starten.

Der Appliance-Rechner wird neu gestartet, und die Zurücksetzung wird folgt ausgeführt:

ORCSETVE[®] Unified Data Protection Appliance

Auf Werksvorgaben zurücksetzen

Durch Zurücksetzen auf die Werksvorgaben werden für alle Einstellungen auf der Arcserve UDP Appliance di wiederhergestellt. Alle Ressourcen, Berichte und Protokolle sowie die Jobübersicht werden gelöscht. Die Arcs zurückgesetzt, die ursprünglich auf der Appliance installiert wurde.

Arcserve UDP Version 6.0.3792 aktualisieren 1 wird wiederhergestellt.

Vorhandene Sicherungsdaten werden gelöscht.

Arcserve UDP wird neu installiert: 60% abgeschlossen

Nach Abschluss der Zurücksetzung wird ein Bestätigungsdialog angezeigt.

- 4. Wählen Sie im Bestätigungsdialog eine der folgenden Optionen aus:
 - Klicken Sie auf Neustart, um die Appliance neu zu starten.
 - Klicken Sie auf Herunterfahren, um die Appliance zu schließen.



Festplatte entfernen und ersetzen

Mit der Arcserve Appliance werden bei Ausfall einer Festplatte die restlichen Datenträger sofort aktiviert. Damit wird sichergestellt, dass keine Daten verloren gehen und die Appliance normal weiterarbeitet. Daher ist es zum Schutz vor Problemen im Zusammenhang mit Ausfällen mehrerer Festplatten wichtig, eine Festplatte schnellstmöglich auszutauschen, um den potenziellen Datenverlust zu minimieren.

Die Arcserve Appliance enthält vier Festplattenträger, die von links nach rechts mit 0, 1, 2 und 3 gekennzeichnet sind. Wenn Sie mehr als eine Festplatte ersetzen, sollten Sie die Ersatzfestplatten kennzeichnen, sodass Sie wissen, welche Festplatte in den einzelnen Festplattenträgern platziert werden muss. Sie sollten auch die Festplatten beschriften, die Sie aus der Appliance entfernen, damit Sie wissen, welche Laufwerkträgers sie belegt haben.

Wichtig! Ergreifen Sie beim Umgang mit den Festplatten geeignete Vorsichtsmaßnahmen, da die Geräte gegen statische Aufladung empfindlich sind und leicht beschädigt werden können.

- Tragen Sie eine Handschlaufe, um jegliche statische Entladung zu verhindern.
- Berühren Sie einen geerdeten Gegenstand, bevor Sie die Austausch-Festplatte aus der antistatischen Lieferverpackung nehmen.
- Fassen Sie eine Festplatte stets ausschließlich an den Rändern an und berühren Sie keine der sichtbaren Komponenten auf der Unterseite.

Befolgen Sie diese Schritte:

- 1. Um auf die Laufwerkshalter zugreifen zu können, müssen Sie zunächst die Abdeckplatte entfernen:
 - a. Lösen Sie die Verriegelung der Abdeckplatte.
 - b. Drücken Sie auf den Entriegelungsknopf, um die Stifte der Abdeckplatte einzuziehen.
 - c. Nehmen Sie vorsichtig die Abdeckplatte ab (mit beiden Händen).
- 2. Drücken Sie auf die Entriegelungstaste am Laufwerkträger. Daraufhin wird der Laufwerksgriff ausgefahren.



3. Ziehen Sie den Laufwerksträger am Griff vorne aus der Appliance. Die Festplatten sind in Laufwerk montiert, um ihren Ausbau und Austausch aus der Appliance zu vereinfachen. Diese Träger tragen außerdem zu einem ausreichenden Luftstrom für die Laufwerkschächte bei.

Wichtig! Mit Ausnahme kurzer Zeiträume (Swapping der Festplatten) sollte die Appliance nicht ohne vollständig belegte Laufwerksträger betrieben werden.

- 4. Entfernen Sie die alte Festplatte aus dem Laufwerkträger, und installieren Sie die neue Festplatte. Achten Sie dabei sorgfältig darauf, dass die Austausch-Festplatte richtig ausgerichtet sind: mit der Beschriftung nach oben und den sichtbaren Komponenten auf der Unterseite.
- 5. Schieben Sie den Laufwerksschacht in die Appliance, bis sie vollständig montiert ist, und fixieren Sie ihn durch Schließen des Laufwerksträger-Griffs.



6. Die Anweisungen zum Zurücksenden eines defekten Laufwerks erhalten Sie beim Arcserve-Support.

Durchführen einer Bare Metal Recovery (BMR), ohne Daten beizubehalten

In Arcserve Appliance können Sie eine Bare Metal Recovery mithilfe des Arcserve UDP-Bootkit durchführen.

Befolgen Sie diese Schritte:

1. Führen Sie die Anwendung *Arcserve UDP-Bootkit erstellen* in der Appliance aus, und erstellen Sie das startfähige BMR-ISO-Image oder einen USB-Stick für die x64-Plattform.

Hinweis: Sie müssen die lokalen Treiber für das ISO-Image mit einschließen. Um die lokalen Treiber einzuschließen, aktivieren Sie die Option **Lokale Treiber einschließen** im Fenster **Bootkit für Bare-Metal-Recovery erstellen**. Weitere Informationen zum Erstellen des Bootkits finden Sie unter diesem <u>Link</u>.

process is launched.		,	
Manufacturer	Version	Platform	Path
Intel	12/08/2016, 12.14.7.0	x64	C:\WINDOWS\INF\oem43.inf
Intel	07/30/2013, 9.4.2.10	x64	C:\WINDOWS\INF\oem9.inf
MS_HDC, INTEL_HDC	06/21/2006, 10.0.14	x64	U:\WINDUWS\INF\mshdc.inf
LSI	03/06/2015, 6.707.0	x64	L:\WINDUWS\INF\oem8.inf
INTEL ACCEDIC	08/19/2016, 10.1.2.80	x64	CIV/UD0WS\INF\oem45.inf
AMD.Section, ALER.S	05/21/2006, 10.0.14	X64	C:\WINDUWS\INF\usport.inf
GENDEV EVE ACC	0773072013, 3.4.2.10	x64	C: WINDOWS VINE Voem47. Inf
Generic	10/08/2017 10.0.14	v64	C:\WINDOWS\INF\usbyboilinf

2. Starten Sie die Arcserve Appliance mit dem BMR-ISO-Image oder dem USB-Stick.

Das Arcserve Bare-Metal-Recovery Setup wird angezeigt.

3. Wählen Sie die erforderliche Sprache aus, und klicken Sie auf Weiter.

arcs	erve	bare metal recovery
	English	
	Keyboard Layout:	
	US	~ <u>N</u> ext

4. Wählen Sie die Option Wiederherstellung von einer Arcserve Unified Data Protection-Sicherung aus, und klicken Sie auf Weiter.

arc	Serve [®] bare metal recovery
Bare Metal Re - <i>Select the</i>	L covery(BMR) type of backup for BMR
	Select type of restore source:
	Restore from a Arcserve Unified Data Protection backup Use this option to perform a restore from either a backup destination folder or a data store.
	○ Recover from a virtual machine
	Use this option to perform a virtual-to-physical (V2P) restore from a virtual machine created by Virtual Standby or Instant VM
	O Source is on a VMware machine
	O Source is on a Hyper-v machine

Das Fenster Assistent zum Auswählen eines Wiederherstellungspunkts wird angezeigt.

5. Klicken Sie auf **Durchsuchen**, und wählen Sie **Recovery Point Server durchsuchen** aus.

Bare Metal Recovery(BMR) - Select a Recovery Point	The following backed up machines are detected:			
The top pane displays all backed up machines and	Backed up Inf	formation		
their backup destinations. If you click on a machine, you can then see the associated recovery points on the bottom pane. Select a recovery point to continue.	Host Name:			
Note: By default, only the backed up machines	Operating S	ystem:		
that are detected from local volumes are listed here. After a new removable disk is attached or detached, you can click "Refresh" the mitchine list. You can also click "Browse" to add any baked up	DNS Suffix:			
machines from the remote shared folder or the data store.	Source:			
If you fail to browse the remote shared folder, it may be because the NIC driver is not installed or			_	
the IP address is incorrect. If necessary, you can perform the following:		Refresh	E.	Browse V
Click here to launch the load driver utility		Browse	from network/local po	ath
6 Network Adapter(s) Detected				
Intel(R) 1350 Gigabit Network Connection - IP Address: 10.10.255.255 - Status: Connected				
Intel(R) 1350 Gigabit Network Connection #2 - IP Address: 0.0.0.0 - Status: Disconnected				
▲ <u>U</u> tilities		Back	Next	Abort

Das Fenster Knoten auswählen wird angezeigt.

- 6. Geben Sie den Hostnamen des Recovery Point Servers, den Benutzernamen, das Kennwort, den Port und das Protokoll ein.
- 7. Klicken Sie auf Verbinden.
- 8. Sobald die Verbindung hergestellt ist, klicken Sie auf **OK**.

HUSt Name:	appliance7501 \checkmark		Port:	8014	
Jser Name:	administrator		Protocol:		HTTPS
Password:	••••••			Con	nect
		Node ID	095	1fd5c-3dd2-496	8-be64-5eaef

Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungspunkt auswählen** wird angezeigt.

9. Wählen Sie den gewünschten Wiederherstellungspunkt aus, und klicken Sie auf **Weiter**.
| Bare Metal Recovery(BMR)
- Select a Recovery Point | The following backed up machines are detected | d: | |
|--|--|---|---|
| The top pane displays all backed up machines and
heir backup destinations. If you dick on a
nachine, you can then see the associated
ecovery points on the bottom pane. Select a
ecovery point to continue.
Note: By default, only the backed up machines
hat are detected from local volumes are listed
on the program program back of the backed or | appkance7205 | Backed up Information
Host Name:
Operating System: | appliance7205
Windows Server 2016 X64 |
| Here, Article a new reinovable days is allocated of
relationed, you can click "Refresh" the machine list.
You can also click "Browse" to add any backed up
nachines from the remote shared folder or the
lata store. | | DNS Suffix:
Source: | arcserve.com Recovery Point Server |
| I you has to browse the remote shared toker, it
has be because the NIC driver is not installed or
he IP address is incorrect. If necessary, you can
erform the following:
<u>lick here</u> to launch the load driver utility | | | <u>R</u> efresh Bro <u>w</u> se v |
| <u>Click here</u> to launch the network configuration
utility | The following recovery points are detected fo | r the enerified machine. Select a recovery point a | nd continue. |
| <u>lick here</u> to launch the network configuration
blity | The following recovery points are detected fo
5/28/2018
10:00:15 PM
2:41:41 AM
5/26/2018
5/26/2018
5/26/2018
5/25/2018
5/25/2018
1:39:14 AM | r the specified machine. Select a recovery point a AR Status: | nd continue:
cted from current system):
iance7501
store: applance7501_data_store
68-be64-Seaefeeb079d |

10. (Optional) Geben Sie das Sitzungskennwort ein, wenn Sie dazu aufgefordert werden, und klicken Sie dann auf **OK**.

er Session Password	
•	ок
Current password length: 1 characters	Cancel

Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungsmodus auswählen** wird angezeigt.

11. Wählen Sie Erweiterter Modus aus, und klicken Sie auf Weiter.

Which reco	very mode do you want to use?		
OB	press Mode		
The	express mode will recover the system automatically with minimal user interaction by using the ine default settings.		
Ac	Ivanced Mode		
The a	advanced mode will assist you in customizing the restore process. Using this mode you will be to:		
Selec	t where to restore data on basic volumes or dynamic disks.		

Das Dialogfeld **Bare-Metal-Recovery (BMR) – Datenträgerpartitionen anpassen** wird angezeigt.

12. Klicken Sie mit der rechten Maustaste auf den größten verfügbaren Datenträger der GUID-Partitionstabelle (GPT), und klicken Sie auf **Datenträger reinigen**.

Current Destination Disk/Volume Layouts			
/b/s/d/ds/f/ /19627,59 Disk 1 (M 447,13 (Reset Commit	/stem Partiti C:\ (155.73 GB) \\1?\Volume(4dd 1 (18394.96 GB) (447.13 GB)	
Disk 2 (1 447.13	Map Disk From Clean Disk	(447.13 GB)	
	Convert to MBR * Convert to GPT		
	Convert to Basic Convert to Dynamic		
Original Source	Online Disk Disk Properties		
 Disk 0 (MBR) 111.79 GB 		Y:\ (111.79 G8)	
 Disk 1 (GPT) 7451.00 GB 	\\?\Volume[791b	FI System Partiti 👔 C:\ (155.73 GB) 👔 \\?\Volume(4dd 1 👔 X:\ (7218.46 GB) 👔	
	Current Destination I	Current Destination Disk/Volume Layouts	

13. Klicken Sie nach der Reinigung der Festplatte mit der rechten Maustaste auf denselben Datenträger, und klicken Sie auf **Commit**.

Adjust Disk Partitions You can adjust the disk/volume configuration on this screen. You can also select data to restore from the original source disk/volume. After selecting a disk/volume, you can then right-click the mouse button, and display the corresponding operation options. Note: If there is no mouse attached in your environment, you can select a disk/volume with TAB and Arrow keys, then press the Menu key to display the menu. The disk/volume changes you make will not take get into effect until you select "Commit" from the Operations menu or click "Next" to commit all changes.	Current Destination Disk/Volume Layouts			
		Reset	(18627.37 GB)	
	 Disk 1 (ME 447.13 G 	Commit	(447.13 GB)	
	 Disk 2 (MB. 447.13 GE 	Map Disk From Clean Disk	(447.13 GB)	
		Convert to MBR Convert to GPT		
		Convert to Basic Convert to Dynamic		
	Original Source Di	Online Disk		
	— Disk 0 (МВк) 111.79 GB	Disk Properties	Y:\ (111.79 GB)	
	 Disk 1 (GPT) 7451.00 GB 	\\?\Volume(791b	m Partiti C:\ (155.73 GB) 🔃 \\?\Volume[4dd 1 👔 X:\ (7218.46 GB) 👔	

Das Fenster Datenträgeränderungen übergeben wird angezeigt.

14. Klicken Sie auf Übergeben.

Operation	Details
Delete Volume	Volume Path[\\?\Volume{791b0915-1396-4e8d-8dfb-1fa02793003f}\
Delete Volume	Volume Path[\\?\Volume{821d05a8-3ecd-436f-a497-cc04fb3e4708}\
Delete Volume	Volume Path[C:\]
Delete Volume	Volume Path[F:\]
Delete Volume	Volume Path[D:\]
🕖 Clean Disk	Clean Disk [0]
	2

15. Wenn die Reinigung des Datenträgers abgeschlossen ist, klicken Sie auf **OK**.

Operation	Details
Delete Volume	Volume Path[\\?\Volume{791b0915-1396-4e8d-8dfb-1fa02793003f}\
Delete Volume	Volume Path[\\?\Volume{821d05a8-3ecd-436f-a497-cc04fb3e4708}\]
Delete Volume	Volume Path[C:\]
Delete Volume	Volume Path[F:\]
Delete Volume	Volume Path[D:\]

16. Klicken Sie im Dialogfeld Bare-Metal-Recovery (BMR) – Datenträgerpartitionen anpassen auf Zurück.

Bare Metal Recovery(BMR) - Adjust Disk Partitions	^	Current Destination Disk/Volu	@perations 👻
You can adjust the disk/volume configuration on this screen. You can also select data to restore from the original source disk/volume to the current destination disk/volume.		₩/blsklet,datt///	(18627.37 GB)
After selecting a disk/volume, you can then right-click the mouse button, and display the corresponding operation options.		- Disk 1 (MBR) 447.13 GB	(447.13 GB)
Note: If there is no mouse attached in your environment, you can select a disk/volume with TAB and Arrow keys, then press the Menu key to display the menu. The disk/volume changes you make will not take get into effect until you select "Commit" from the Operations menu or dick "Next" to commit all changes.		Disk 2 (MBR) 447,13 GB	(447. 13 GB)
		Original Source Disk/Volume Li Disk 0 (MBR) 111.79 GB	ayouts Y:\ (111.79 GB)
		Disk 1 (GPT) 7451.00 GB	XI dH/d4(1939// 👔 EFI System Partiti 😱 C:\ (155.73 GB) 👔 \\?\Volume[4dd 1 👔 X:\ (7218.46 GB) 👔
	~	Unallocated Primary	y
▲ <u>U</u> tilities			Back Next Abort

Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungsmodus auswählen** wird angezeigt.

17. Wählen Sie Express-Modus aus, und klicken Sie auf Weiter.

Express Mode	
The express mode will recover the system automatically with minimal user interaction by using the machine default settings.	
O Advanced Mode	
The advanced mode will assist you in customizing the restore process. Using this mode you will be able to: Select where to restore data on basic volumes or dynamic disks. Insert device driver before reboot.	
Note: After clicking Next, the BMR Wizard will create new partitions on the destination machine to match the existing partitions on the source machine. This may destroy any	

Das Dialogfeld **BMR** wird angezeigt.

18. Klicken Sie auf Ja.

BMR			8
?	The next step may result in comple you want to continue?	te loss of data on the	machine. Do
	R	Yes	No

Das Dialogfeld **Übersicht über die Wiederherstellungseinstellungen** wird angezeigt.

19. Klicken Sie auf Abbrechen.

Source Disk Destination	n Disk
ummary of Volume Restore Settings:	Destination Volume
<pre>Source volume V/?\Volume{791b0915-1396-4e8d-8dfb-1fa02793003f}\(300 MB) EFI System Partition (99 MB) C:\(155.73 GB) \/?\Volume{4dd1123f-0464-4cd6-9df0-1ab9b95c8901}\(76.29 GB) </pre>	\\?c06aa5e0-adb9-4849-8b15-20 \\?e3db4483-19ad-4550-8e0e-06 \\?257b3c2a-9cf1-44a0-a8b3-225) \\?98fb5326-630f-4842-82fa-48b
<	3

Das Dialogfeld **Bare-Metal-Recovery (BMR) – Datenträgerpartitionen anpassen** wird angezeigt.

20. Vergleichen und überprüfen Sie, ob die Kapazität der ersten vier Partitionen auf der Registerkarte Aktuelle Zieldatenträger/Volume-Layouts dem größten verfügbaren GPT-Datenträger auf der Registerkarte Ursprüngliche Quelldatenträger/Volume-Layouts entspricht, und klicken Sie aufWeiter.

Hinweis: Um die Größe der Partition anzuzeigen, halten Sie den Mauszeiger über den Datenträger, um die Datenträgereigenschaften anzuzeigen.

Bare Metal Recovery(BMR) ^ - Adjust Disk Partitions	Current Destination Disk/Volume Layouts	Operations v
You can adjust the disk/volume configuration on this screen. You can also select data to restore from the original source disk/volume to the current destination disk/volume.	Disk 0 (GPT) 18627.50 GB 117/Volume(791b EFI System Partiti C:\ (155.73 GB) 117/Volume(4dd 1 (1)	18394.96 GB)
After selecting a disk/volume, you can then right-click the mouse button, and display the corresponding operation options.	Disk 1 (MBR) Destination Volume: \\?\Volume(03331745-9734-4066-bd25-693087d5826b)\ File System Type : RAW	
Note: If there is no mouse attached in your environment, you can select a disk/volume with TAB and Arrow keys, then press the Menu key to display the menu. The disk/volume changes you make will not	Disk 2 (MBR) Copacity : 300MB Data on this volume will be restored from original volume `\\?\Volume[791b0915-1396- 8dfb-1fa02793003f]\`.	4e8d-
from the Operations menu or click "Next" to commit all changes.	Original Source Disk/Volume Layouts	
	- Disk 0 (MBR) 111.79 GB Y:\ (111.79 GB)	(1)
	Disk 1 (GPT) 7451.00 GB 117\Volume(791b) EFI System Partiti C:\ (155.73 GB) () 117\Volume(4dd 1) X:\ X:\	. (7218.46 GB) 🕕
	Unallocated Primary	
	Bock Next	Abort

Das Dialogfeld Übersicht über die Wiederherstellungseinstellungen wird angezeigt.

21. Klicken Sie auf OK.

ummary of Volume Restore Settings:	purce Disk Destination	n Disk
Source Volume Destination Volume	nmary of Volume Restore Settings:	Destination Volume
\\2\Volume/791b0915-1396-4e8d-8dfb-1f=02793003f\\ (300 MB) \\2\Volume/03331745-9734-4066-bd25-6	\\2\Wolume{791b0915-1396-4e8d-8dfb-1fa02793003f}\(300 MB)	\\203331745-9734-4066-bd25-69
EEI System Partition (99 MB)	EFI System Partition (99 MB)	\/?b9994f56-8c58-4bbf-bd7a-85a.
C:\(155.73 GB) \\?496da605-7066-442c-8ea2-c:	C:\(155.73 GB)	\\?496da605-7066-442c-8ea2-c3.
\\?\Volume{4dd1123f-0464-4cd6-9df0-1ab9b95c8901}\(76.29 GB) \\?59eaea46-103c-45e3-b0ed-5	\\?\Volume{4dd1123f-0464-4cd6-9df0-1ab9b95c8901}\ (76.29 GB)	\\?59eaea46-103c-45e3-b0ed-55.

Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungsprozess starten** wird angezeigt.

22. Deaktivieren Sie die Option Agent-Dienst nach Neustart nicht automatisch neu starten, und warten Sie, bis die Wiederherstellung abgeschlossen ist.

Bare Metal Recovery(BMR) - Start Restore Process	Summary of Restore Settings			
This page displays a summary of the disk/volume restore settings that you have made. Note: After the BMR process is complete and server has been rebooted, you may not want to perform backup jobs from this server. If you are just testing the BMR functionality, we recommend that you select the 'Do not start Agent service	Restore Item CRestore source volume '\?\Volume(791b0915-1396-4e8d-8dfb-1fa02793003f)\' Restore source volume 'EFI System Partition' to current destination disk 0 Restore source volume 'Cs\' to current destination disk 0 Restore source volume '\?\Volume(4dd1123f-0464-4cd6-9df0-1ab9b95c8901)\'	Status Completed Completed Restoring Not Started	Progress 100.0% 100.0% 0.8%	Throughput 367.44 MB/Minute 967.90 MB/Minute 2705:50 MB/Minute
Automotary and resolve option. When you select this option, you can manually start the Agent service (and the Recovery Point Server service, if installed) after reboot if you want to perform backup jobs. Enable Windows F8 boot option helps user perform further recovery or troubleshooting after BMR. For example, press F8 and boot into Active Directory Service Restore mode to perform Active Directory authoritative restore.	Automatically reboot your system after recovery.			
	Do not start Agent service automatically after reboot. Boot the system to Advanced Boot Options (F8) Menu on the next boot for Windows	s 8 / Windows Ser	ver 2012 and late	r OS.
	Elapsed Time: 00:00:24		0 2012 0 10 10 10	
	Estimated Time Remaining: 01:30:50			
	[0.8%] [576MB/76631MB] Restoring basic source volume 'C:\' to current destination dis	k 0		
▲ Utilities		Back	M	ext Abort

Das Dialogfeld **Bare-Metal-Recovery (BMR) – Gerätetreiber einfügen** wird angezeigt.

23. Wählen Sie den erforderlichen Treiber für RAID-Controller aus, und klicken Sie auf **Weiter**.

Fare Piecal Recovery(BFIR) ** Insert Device Driver An incompatibility problem has been detected and BMR is unable to find suitable driver for some device(s). The operating system of the host being recovered may be different than the operating system that was created on the BMR ISO image. Please select an appropriate driver for the device(s) or add a new driver by dicking "Add Driver" button.	Provide drivers for following devices:	Property Description Vendor LSI Logic / Symbios Logic Manufacturer AvagoTech Class SCSIAdapter Driver Description AVAGO MegaRAID SAS Adapter Hardware ID PCI\VEN_10008DEV_00SD&SUBSY
	Available Driver(s): Driver megasas2.inf megasas2.inf(1) megasas3.inf	Property Description Version 03/02/2015, 6.706.06.00 Manufacturer LSI, DELL Class SCSIAdapter Service megasas INF Path C:\WINDOWS\System32\driverStore\FileRepository\megasas.inf_a
	Insert Driver	< >>
▲ <u>U</u> tilities		Back Next Abort

Das Popup "Neustart" wird angezeigt, und die Arcserve Appliance wird automatisch neu gestartet.

Click Refloot to automatically reboot your system at this time. If you want to collect all BMR log files you can use the Activity log utility. <u>Click here</u> to launch the Activity Log utility.

Reboot	Cancel	

Der BMR-Prozess wurde erfolgreich abgeschlossen.

Durchführen einer Perform Bare Metal Recovery (BMR) und Beibehalten der Daten

In Arcserve Appliance können Sie eine Bare Metal Recovery mithilfe des Arcserve UDP-Bootkit durchführen.

Befolgen Sie diese Schritte:

1. Führen Sie die Anwendung *Arcserve UDP-Bootkit erstellen* in der Appliance aus, und erstellen Sie das startfähige BMR-ISO-Image oder einen USB-Stick für die x64-Plattform.

Hinweis: Sie müssen die lokalen Treiber für das ISO-Image mit einschließen. Um die lokalen Treiber einzuschließen, aktivieren Sie die Option Lokale Treiber einschließen im Fenster Bootkit für Bare-Metal-Recovery erstellen. Weitere Informationen zum Erstellen des Bootkits finden Sie unter diesem Link.

erson 2/08/2016, 12.14 7/30/2013, 9.4.2. 5/21/2006, 10.0.1 3/06/2015, 6.707 8/19/2016, 10.1.2 5/21/2006, 10.0.1	16, 12.14.7 13, 9.4.2.1 06, 10.0.14 15, 6.707.0 16, 10.1.2. 06, 10.0.14	.14.7.0 4.2.10 .0.14 707.0	x64 x64	C:\WINDOWS\INE\oem43 inf
2/08/2016, 12:14 7/30/2013, 9.4.2. 5/21/2006, 10.0.1 3/06/2015, 6.707 3/19/2016, 10.1.2 5/21/2006, 10.0.1	16, 12, 14,7 13, 9,4,2,1 06, 10,0,14 15, 6,707,0 16, 10,1,2,1 06, 10,0,14	.14.7.0 4.2.10 .0.14 707.0	x64 x64	L WINDOWSVINEVOEM43 Inf
7/30/2013, 3.4.2. 5/21/2006, 10.0.1 3/06/2015, 6.707 3/19/2016, 10.1.2 5/21/2006, 10.0.1	16, 10.0.14 15, 6.707.0 16, 10.1.2. 06, 10.0.14	.0.14 707.0	x04	C:\\r(INDO\r(S\INE\com9.inf
3/06/2015, 6.707. 3/19/2016, 10.1.2 5/21/2006, 10.0.1	15, 6.707.0 16, 10.1.2. 06, 10.0.14	707.0	- YD4	C:\WINDOWS\INF\00013.Ini
3/19/2016, 10.1.2 5/21/2006, 10.0.1	16, 10.1.2. 06, 10.0.14	1 2 00	v64	C:\WINDOWS\INE\oem8 inf
5/21/2006, 10.0.1	06, 10.0.14	. 1.2.00	x64	C:\WINDOWS\INF\oem45.inf
1 100 1001 0 0 1 0 I		.0.14	x64	C:\WINDOWS\INF\usbport.inf
//30/2013, 9.4.2.1	13, 9.4.2.1	4.2.10	x64	C:\WINDOWS\INF\oem47.inf
5/21/2006, 10.0.1	06, 10.0.14	.0.14	x64	C:\WINDOWS\INF\machine.inf
0/08/2017, 10.0.1	17, 10.0.14	.0.14	x64	C:\WINDOWS\INF\usbxhci.inf
0/08/2017, 10.0.1	17, 10.0.14	.0.14	x64	C:\\

2. Starten Sie die Arcserve Appliance mit dem BMR-ISO-Image oder dem USB-Stick.

Das Arcserve Bare-Metal-Recovery Setup wird angezeigt.

3. Wählen Sie die erforderliche Sprache aus, und klicken Sie auf Weiter.

arcse	erve	bare metal recovery
	English	
	Keyboard Layout:	
	US	Next

4. Wählen Sie die Option Wiederherstellung von einer Arcserve Unified Data Protection-Sicherung aus, und klicken Sie auf Weiter.

arc	Serve® bare metal recovery
Bare Metal Re - <i>Select the</i>	 ecovery(BMR) <i>type of backup for BMR</i>
	Select type of restore source:
	Restore from a Arcserve Unified Data Protection backup Use this option to perform a restore from either a backup destination folder or a data store.
	O Recover from a virtual machine
	Use this option to perform a virtual-to-physical (V2P) restore from a virtual machine created by Virtual Standby or Instant VM
	Source is on a VMware machine
	O Source is on a Hyper-v machine

Das Fenster Assistent zum Auswählen eines Wiederherstellungspunkts wird angezeigt.

5. Klicken Sie auf **Durchsuchen**, und wählen Sie **Recovery Point Server durchsuchen** aus.

Bare Metal Recovery (BHR) - Select a Recovery (BHR) The top pane displays all backed up machines and their backup destinations. If you click on a machine, you can then see the associated recovery points on the bottom pane. Select a recovery points on the bottom pane. Select a recovery point to continue. Note: By default, only the backed up machines that are detected from local volumes are listed mere. After a new removable disk is attached or detached, you can click "Refresh" the milytime list. for can also click "Browse" to add any balked up machines from the remote shared folder or the data store.	The following backed up machines are detected:	Backed up Information Host Name: Operating System: DNS Suffix: Source:			
If you fail to browse the remote shared folder, it may be because the NIC driver is not installed or the ID address is because 1 for a stalled or			Refrech		Browne
the IP address is incorrect. If necessary, you can perform the following: <u>Click here</u> to launch the load driver utility <u>Click here</u> to launch the network configuration utility	The following recovery points are detected for the specified r	nachine. Select a recovery point a	Browse fro	om network/local om Recovery Poin	t Server
6 Network Adapter(s) Detected Intel(R) 1350 Ggabit Network Connection -IP Address: 10.10.255.255 - Status: Connected Intel(R) 1350 Ggabit Network Connection #2 -IP Address: 0.0.0 - Status: Disconnected V					
▲ Utilities			<u>B</u> ack	Next	Abort

Das Fenster Knoten auswählen wird angezeigt.

- 6. Geben Sie den Hostnamen des Recovery Point Servers, den Benutzernamen, das Kennwort, den Port und das Protokoll ein.
- 7. Klicken Sie auf Verbinden.
- 8. Sobald die Verbindung hergestellt ist, klicken Sie auf **OK**.

Avst Name: appliance7501		~	Port:	8014
Jser Name:	administrator		Protocol:	
assword:	•••••	1		Connect
		Node ID	095	51fd5c-3dd2-4968-be64-5eaef

Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungspunkt auswählen** wird angezeigt.

9. Wählen Sie den gewünschten Wiederherstellungspunkt aus, und klicken Sie auf **Weiter**.

Bare Metal Recovery(BMR) - Select a Recovery Point	The following backed up machines are detec	ted:	
The top pane displays all backed up machines and their backup destinations. If you click on a machine, you can then see the associated recovery points on the bottom pane. Select a	appliance7205	Backed up Information Host Name:	appliance7205
recovery point to continue. Note: By default, only the backed up machines		Operating System:	Windows Server 2016 X64
that are detected from local volumes are listed here. After a new removable disk is attached or detached, you can dick "Refresh" the machine list. You can also click "Browse" to add any backed up		DNS Suffix:	arcserve.com
machines from the remote shared folder or the data store.		Source:	Recovery Point Server
he IP address is incorrect. If necessary, you can verform the following: <u>lick here</u> to launch the load driver utility <u>lick here</u> to launch the network configuration tility			Total and the second seco
tlity	The following recovery points are detected 5/28/2018 10:00:15 PM 2:41:41 AM 5/27/2018 2:41:41 AM 5/27/2018 2:41:41 AM	for the specified machine. Select a recovery point a AR Status: - Backup Type: - Incremental Backup	nd continue:
tbity	The following recovery points are detected 5/28/2018 10:00:15 PM 2:41:41 AM 5/27/2018 5/27/2018 5/25/20	for the specified machine. Select a recovery point a AR Status: - Backup Type: - Incremental Backup Backup Destination (Dete - Recovery Point Server: appl - Recovery Point Server: adpl -	nd continue: A cted from current system): lance7501 store: appliance7501_data_store 68-be64-Seaefeeb079d
6 Network Adapter(s) Detected	The following recovery points are detected 5/28/2018 10:00:15 PM 5/21/2018 5/27/2018 5/27/2018 5/25/2018 5/25/2018 5/25/2018 1:39:14 AM	for the specified machine. Select a recovery point a AR Status: - Backup Type: - Incremental Backup Backup Destination (Dete Recovery Point Server: appl - Recovery Point Server: appl - Recovery Point Server: appl Backup Description:	nd continue: ceted from current system): lance7501 store: appliance7501_data_store 68-be64-5eaefeeb079d
6 Network Adapter(s) Detected Intel(R) 1350 Ginabit Network Connection -IP Address: 10.10.255.255 - Status: Connected	The following recovery points are detected 5/28/2018 10:00:15 PM 2:41:41 AM 5/27/2018 5/27/2018 5/25/2018 5/25/2018 5/25/2018 10:00:11 PM 1:39:14 AM	for the specified machine. Select a recovery point a AR Status: - Backup Type: - Incremental Backup Backup Destination (Dete - Recovery Point Server: app - Recov	nd continue: A continue: A contract of the system of the

10. (Optional) Geben Sie das Sitzungskennwort ein, wenn Sie dazu aufgefordert werden, und klicken Sie dann auf **OK**.

er Session Password	
•	ок
Jurrent password length: 1 characters	Cancel

Das Dialogfeld Bare-Metal-Recovery (BMR) – Wiederherstellungsmodus auswählen wird angezeigt.

11. Wählen Sie Erweiterter Modus aus, und klicken Sie auf Weiter.

Which recovery mode do you want to use?			
O Express Mode			
The express mode will recover the system automatically with minimal use machine default settings.	er interaction by using the		
Advanced Mode			
The advanced mode will assist you in customizing the restore process. Us able to: Select where to restore data on basic volumes or dynamic disks.	sing this mode you will be		

12. Klicken Sie im Dialogfeld Bare Metal Recovery (BMR)-Datenträgerpartitionen anpassen auf Weiter.

You can adjust the disk/volume configuration on this screen. You can also select data to restore from the original source disk/volume to the current destination dick <i>kolume</i> .	 Disk 0 (GPT) 18616.32 GB 	Image: Non-State Image: Non-State<
After selecting a disk/volume, you can then right- click the mouse button, and display the corresponding operation options.	Disk 1 (MBR) 223.57 GB	(223.57 GB)
Note: If there is no mouse attached in your environment, you can select a disk/volume with TAB and Arrow keys, then press the Menu key to display the menu. The disk/volume changes you make will not take get into effect until you select "Commit" from the Operations menu or click "Next" to commit all changes.		
	Original Source Disk/Vo	Aume Layouts
	 Disk 0 (MBR) 223.57 GB 	Y:\ (223.57 GB)
	 Disk 1 (GPT) 18616.32 GB 	\\?\Volume(791b) EFI System Partiti) C:\ (155.73 GB) () \\?\Volume(4dd 1) X:\ (18383.77 GB)
	Primary	
▲ <u>U</u> tilities		Back Next Abort

13. Klicken Sie auf dem Bildschirm Übersicht über die Einstellungen zur Datenträgerwiederherstellung auf OK.

Source Disk	Destination Disk					
mmary of Volume Restore Settings:	Destination Volume	On Diale				
		On Disk				
C:\(155.73 GB)	C:\(155.73 GB)	Disk 0				
\\?4dd1123f-0464-4cd6-9df0-1	G:\ (76.29 GB)	Disk 0				
EFI System Partition (99 MB)	\\?821d05a8-3ecd-436f-a497-cc0	Disk 0				
onfirm your restore settings and dick OK to con	tinue. If you want to adjust restore settings ma	anually, dick Cancel				

 Deaktivieren Sie im Dialogfeld Bare-Metal-Recovery (BMR) – Wiederherstellungsprozess starten die Option Agent-Dienst nach Neustart nicht automatisch starten, und warten Sie, bis die Wiederherstellung abgeschlossen ist und der Rechner neu gestartet wird.

Bare Metal Recovery(BMR) - Start Restore Process	Summary of Restore Settings				
This page displays a summary of the disk/volume	Restore Item		Status	Progress	Throughput
estore settings that you have made.	Restore source volume 'C: \' to curr	ent destination disk 0	Restoring	1.8%	3115.69 MB/Minute
Note: After the BMR process is complete and perver has been rebooted, you may not want to beer form backup jobs from this server. If you are ust testing the BMR functionality, we recommend that you select the 'Do not start Agent service automatically after reboot' option. When you select this option, you can manually start the Agent service (and the Recovery Point server service, if installed) after reboot if you want to perform backup jobs.	Restore source volume '\/?\Volume: Restore source volume '\/?\Volume: Restore source volume 'EFI System	(791b0915-1396-4e8d-8dfb-1fa02793003f}\' (4dd1123f-0464-4cd6-9df0-1ab9b95c8901)\' Partition' to current destination disk 0	Not Started Not Started Not Started		
Enable Windows F8 boot option helps user perform further recovery or troubleshooting after BMR. For example, press F8 and boot into Active Directory Service Restore mode to perform Active Directory authoritative restore.	Automatically reboot your system af	ter recovery.			
	Boot the system to Advanced Boot (Dations (FB) Menu on the next boot for Windows	8 / Windows Serv	er 2012 and later	05
			07 11100113 361	CI 2012 GIG GUD	05.
	Elapsed Time:	00:00:33			
	Estimated Time Remaining:	00:52:55			
	[1.8%] [1632MB/90738MB] Restoring b	asic source volume 'C:\' to current destination di	sk 0		
▲ <u>U</u> tilities			Back	Ne	at <u>Abort</u>

Der BMR-Prozess wurde erfolgreich abgeschlossen.

Kapitel 9: Durchführung einer Kapazitätserweiterung der Appliance

Dieser Abschnitt enthält folgende Themen:

Arbeiten mit dem Erweiterungs-Kit in Arcserve Appliance 9012-9504 DR-Modellen 190

Arbeiten mit dem Erweiterungs-Kit in Arcserve Appliance 9012-9504 DR-Modellen

Mit dem ARCserve Erweiterungs-Kit können Sie die Kapazität der Arcserve Appliance 9012-9504DR Modelle erweitern.

Befolgen Sie diese Schritte:

- 1. Gehen Sie folgendermaßen vor, um die Festplatten in die leeren Datenträgersteckplätze einzufügen:
 - a. Überprüfen Sie in der Arcserve UDP-Konsole, dass keine Jobs auf dem Appliance-Server ausgeführt werden. Wenn Jobs ausgeführt werden, unterbrechen Sie die entsprechenden Pläne.
 - b. Legen Sie Festplatte in den leeren Datenträgersteckplatz ein.



- 2. Gehen Sie folgendermaßen vor, um Raid-6 in iDRAC zu konfigurieren:
 - a. Melden Sie sich in iDRAC an, und navigieren Sie zu "Konfiguration", "Speicherkonfiguration" und "Physische Festplattenkonfiguration".
 - b. Unter Physische Festplattenkonfiguration wählen Sie die Option RAID konvertieren in der Dropdown-Liste Aktionen f
 ür jede neue Festplatte aus.

Ein Dialogfeld wird mit der folgenden Fehlermeldung angezeigt:

RAC0516: Die Umwandlung physischer Laufwerke in RAID-kompatible Laufwerke überschreibt alle durch das BS erstellten RAID-Arrays.

Stellen Sie sicher, dass keine durch das BS konfigurierten RAID-Arrays vorhanden sind, und klicken Sie dann auf "OK".

c. Klicken Sie auf **OK**.

Unter Ausstehende Aktionen wird der Status In Raid konvertieren angezeigt.

Physic	al Disk Configuration 📀 6 Pending							🕏 Edit SSD Wear Three
Statu	s Name	State	Hotspare Status	Capacity	Media Type	Action		Pending Actions
	Physical Disk 0:1:10	Non-RAID	Unassigned	10949.00 GB	HDD	Action		Convert to RAID
	Physical Disk 0:1:11	Non-RAID	Unassigned	10949.00 GB	HDD	Action	•	Convert to RAID
	Physical Disk 0:1:14	Non-RAID	Unassigned	10949.00 GB	HDD	Action	•	Convert to RAID
	Physical Disk 0:1:15	Non-RAID	Unassigned	10949.00 GB	HDD	Action	•	Convert to RAID
	Physical Disk 0:1:16	Non-RAID	Unassigned	10949.00 GB	HDD	Action	•	Convert to RAID
2	Physical Disk 0:1:17	Non-RAID	Unassigned	10949.00 GB	HDD	Action	*	Convert to RAID

d. Klicken Sie auf eine der folgenden Optionen, um die ausstehenden Aktionen durchführen:

Jetzt anwenden

Die Aktion zur Konvertierung in Raid wird sofort gestartet.

Beim nächsten Neustart

Die Aktion zur Konvertierung in Raid wird beim nächsten Neustart gestartet.

Geplante Zeit

Die Aktion zur Konvertierung in Raid wird zum geplanten Zeitpunkt gestartet.

Alle ausstehenden verwerfen

Die Aktion zur Konvertierung in Raid wird für alle Laufwerke verworfen.

e. Navigieren Sie zu Wartung, Jobwarteschlange.

Die Liste der laufenden Jobs zur Konvertierung der Laufwerke in Raid wird angezeigt. Wenn der Job In RAID konvertieren abgeschlossen ist, ändern sich der Status in **Abgeschlossen (100 %)**.

- 3. Gehen Sie folgendermaßen vor, um einen virtuellen Datenträger zu erstellen:
 - a. Navigieren Sie zu "Konfiguration, "Speicherkonfiguration" und "Virtuelle Datenträgerkonfiguration".

- b. Klicken Sie unter Virtuelle Datenträgerkonfiguration auf Virtuellen Datenträger erstellen.
- c. Wählen Sie RAID-6 als Layout aus.
- d. Wählen Sie unter **Physischen Datenträger auswählen** den Datenträger aus, der in RAID konvertiert werden soll.
- e. Klicken Sie auf Zu ausstehende Vorgängen hinzufügen.

ate Virtual Disk	
Name	Enter or use auto-name
Layout	RAID-6 •
Media Type	HDD *
Stripe Element Size	64 KB 🔻
Capacity*	14.55 TB 🔻
Read Policy	Read Ahead
Write Policy	Write Back
Disk Cache Policy	Default 🔻
T10 PI Capability	Disabled •
Span Count	1 •

- f. Navigieren Sie zu "Konfiguration" und "Speicherkonfiguration".
- g. Klicken Sie auf eine der folgenden Optionen, um den ausstehenden Vorgang abzuschließen:

Jetzt anwenden

Der Vorgang zum Erstellen eines virtuellen Datenträgers wird sofort gestartet.

Beim nächsten Neustart

Der Vorgang zum Erstellen eines virtuellen Datenträgers wird beim nächsten Neustart gestartet.

Geplante Zeit

Der Vorgang zum Erstellen eines virtuellen Datenträgers wird zum geplanten Zeitpunkt gestartet.

Alle ausstehenden verwerfen

Der Vorgang zum Erstellen eines virtuellen Datenträgers wird für alle Datenträger verworfen.

h. Navigieren Sie zu Wartung, Jobwarteschlange.

Die Liste der laufenden Jobs zum Erstellen eines virtuellen Datenträgers wird angezeigt. Wenn der Job Virtuellen Datenträger erstellen abgeschlossen ist, ändern sich der Status in **Abgeschlossen** (100 %).

- i. Navigieren Sie zu Computerverwaltung und Datenträgerverwaltung.
- j. Doppelklicken Sie auf den neuen virtuellen Datenträger, den Sie hinzugefügt haben.

Das Fenster "Datenträger initialisieren" wird angezeigt.

- k. Wählen Sie die **GPT-Datenträger (GUID-Partitionstabelle)** aus, und klicken Sie auf **OK**.
- Wählen Sie im Fenster Datenträgerverwaltung den virtuellen Datenträger aus, und wenden Sie die folgenden Eigenschaften an:
 - Einen Laufwerksbuchstaben zuweisen
 - NTFS als Dateisystem angeben
 - Formatieren des Datenträgers

Somputer Management				- 🗆 X
File Action View Help				
Computer Management (Local System Tools On Task Scheduler	Volume	Layout Type File System Status Simple Basic Healthy (Recovery Partition) Simole Basic Healthy (FFI System Partition)	Capa 300 N 99 M	Actions Disk Management
Servert Viewer Servert Servert	 (C:) UDPData (X:) UDPHash (Y:) 	Simple Basic NTFS Healthy (Brown Partition) Simple Basic NTFS Healthy (Book, Page File, Crash Dump, Primary Partition) Simple Basic NTFS Healthy (Brimary Partition) Simple Basic NTFS Healthy (Primary Partition) Initialize Disk X You must initialize a disk before Logical Disk Manager can access it. Select disks: VDisk 0	76.29 155.7 1467i 1787.	More Actions >
	Olisk 0 Unknown 14903.00 GB Not Initialized	Use the following patition style for the selected disks: O MBR (Master Boot Record) (>	
	Disk 4 Basic 14902,88 GB Online	300 ME Healthy 99 M Healt IC-) 155.73 GB NTFS Healthy (Boot, Pag 76.29 GB Healthy (Recover Healthy (Primary Partition)	υ	
۲ ۲	Disk 5 Basic 1787.87 GB Online Unallocated	UDPHash (Y) 1787.87 GB NTFS Healthy (Primary Partition) Primary partition	v	

- 4. Gehen Sie folgendermaßen vor, um den Datenspeicher zu erweitern:
 - a. Navigieren Sie zu dem Datenträger, den Sie hinzugefügt haben, und erstellen Sie einen Ordner.
 - b. Starten Sie den **Arcserve Appliance**-Assistenten auf dem Arcserve Appliance-Desktop.

Die Seite Arcserve Appliance-Konfiguration wird geöffnet.

c. Klicken Sie auf UDP Konsole starten.

Die Anmeldeseite der Arcserve UDP-Konsole wird angezeigt.

- d. Melden Sie sich bei der UDP-Konsole als Administrator an.
- e. Navigieren Sie zu Ressourcen, Ziele und Recovery Point Server.
- f. Klicken Sie mit der rechten Maustaste auf den Datenspeicher, und klicken Sie auf **Beenden**.

arcserve [.]	ur	ified data	protectio	on	O Mes	sages (1) ad	dminis	strator •	Help •
dashboard resources	jobs	reports I	og settin	gs	high availab	oility			
	c Dest	inations: Reco	very Point S	erver				⇒ appliatest75	> appliat
▲ Nodes All Nodes	Actio	ms - Add	a Recovery Po	int Server				Configuration V	Mizard
Nodes without a Plan		Name		Status	Plan Count	Stored Data	D	Status	
 Plan Groups Linux Backup Server Groups 		appliatest75						Running	
All Plans		appliatest75	data store Modify		1	0 Byte	0	Backup Destination	TB free of
 Destinations 			Delete					Data	2 TB free
Recovery Point Servers			Stop					Destnation Index	
Arcserve Backup Servers			-0					Destination	TB free of
Shared Folders Cloud Accounts	4		RPS Jum	pstart	nts		1	Hash Destination	3.5 G8 free
Remote Consoles								Memory	# G8 free
 Infrastructure 								Allocation	_
Storage Arrays								 Settings 	
Sites								Compression Type	Standard
SLA Profiles								Encryption Algorithm	AES-256
						A	ctiva o to S	te Backupows Destination	X:\Arcserve \data_store \common

g. Navigieren Sie über die Befehlszeile zu c:\Programme\Arcserve\Unified Data Protection\Engine\BIN, und führen Sie folgenden Befehl aus:

as_gddmgr.exe –DataPath Add <Name des Datenspeichers> -NewDataPath <neue Datenordner>

Der folgende Beispielbildschirm zeigt die Details wie z. B. Volume-Kapazität, belegter Speicherplatz, freier Speicherplatz für die primären Datenpfad, erweiterter den Datenpfad und die Gesamtanzahl der Werte. Der Wert ist die Summe des primären Datenpfads und des Pfads für erweiterte Daten.

Um die Details zum Datenpfad anzuzeigen, können Sie auch den folgenden Befehl ausführen:

as_gddmgr.exe -DataPath Display <Name des Datenspeichers>

C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN>as_gddmgr.exe -Data path Add appliatest75_data_store -NewDataPath Y:\data Successfully load data store configuration information. Successfully added new expanded data path for the data store. The data store has 1 expanded data path(s) now: Volume capacity Used space Free space Primary data path : X:\Arcserve\data_store\data 18384 GB 1 GB 18383 GB Y:\data 224 GB Expanded data path1: 223 GB 1 GB Total 18608 GB 2 GB 18606 GB Success to add data path Y:\data. C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN>

Dem Datenspeicher wurde erfolgreich ein neuer erweiterter Datenpfad hinzugefügt.

- h. Navigieren Sie in der UDP-Konsole zu **Ressourcen**, **Ziele** und **Reco**very Point Server.
- i. Klicken Sie mit der rechten Maustaste auf den Datenspeicher, und klicken Sie auf **Starten**.
- j. Nehmen Sie die Pläne wieder auf, die Sie zuvor in der UDP-Konsole unterbrochen haben.

Die Datenkapazität von Arcserve Appliance wurde erfolgreich erweitert.

Herstellen einer Verbindung zwischen dem Appliance-Server und dem Appliance-Erweiterungs-Shelf

Dieser Abschnitt enthält folgende Themen:

Appliance-Infield-Erweiterung für alle verfügbaren Modelle

Mod ell	Aktuelle Kapa- zitäten\TB	Erwei- terungs- Shelf- Kapazität	Aktu- elle SSD – GB	Ne- ue SS- D RE- Q – GB	Freie Steck- plätze	Add-on- Karten	BES	CHREIBUNG
8100	4, 6	8 (6 x 2-TB- Fest- platten)	120	8 TB – 140	2, 3	LSI SAS 9200 – 8E HBA Qlogic Dual-Port HBA Quad- Port 1G Netz- werk- karte Dual-Port 10G SPF + Dual-Port 10G Kup- fer Infield- Erwei- terung – (MegaRAI- D SAS 9380-8e)	1. 2. 3.	Modell 8100 unterstützt nur 8-TB- Infield-Erwei- terung. 8100 - 8 TB Erweiterungs- Shelf mit inte- grierter und vor- konfigurierter SSD 240 GB. 8100 verfügt über 2 und 3 als optionale Steckplätze. Ein freier Steckplätze. Ein freier Steckplatz ist obligatorisch für die App- liance-Infield- Erwei- terung/Me- gaRAID SAS 9380-8e. Wenn beide optionalen Steckplätze

				mit Zusatz-
				karten befüllt
				sind, müssen
				Sie min-
				destens einen
				(vorzugsweise
				Steckplatz 3)
				Steckplatz frei
				geben, damit
				die Erwei-
				terung mög-
				lich ist.
			5.	Der SAS-
				Anschluss
				wird zwischen
				der Appliance
				und dem
				Erweiterungs-
				Shelf ver-
				wendet.
			6.	8100 – Erwei-
				terungs-Shelf
				enthält RAID
				6.
			7	Enwoitorupgs
			7.	Shelf onthält
				teile
			8.	Befolgen Sie
				nacn
				Anschluss der
				Erweiterungs-
				Sheit die
				Anweisungen
				zum Hin-
				Zurugen eines
				torupge
				terungs-

								leitfaden.
							9.	Wenn eine
								neue SSD
								erforderlich
								ist, folgen Sie
								den Anwei-
								sungen unter
								HASH-Ziel zu
								neuer SSD
								migrieren im
								Erwei-
								terungs-
								handbuch.
							1.	Modell 8200
								unterstützt 8-
						9200 – 8E		TB- oder 16-
						HBA		TB-Infield-
								Erweiterung.
						Qlogic		Clients kön-
						Dual-Port		nen jeweils
						НВА		nur ein Erwei-
		Q				Quad-		terungs-Shelf
		0		8		Port 1G		anschließen.
		(6 x 2-TB-		ТВ		Netz-	2.	8200 - 16 TB
		Fest-		-		werk-		Erweiterungs-
0200	0 1 2	platten)	220	NA	2.2	karte		Shelf mit inte-
8200	0, 12	ODER	220	16	2, 5	Dual-Port		grierter und
		_		ТВ		10G SPF +		vor-
		16 (6 x 4-		_				konfigurierter
		TB-Fest-		280		Dual-Port		SSD 480 GB.
		platten)				10G Kup-	3.	8200 verfügt
						Ter		über 2 und 3
						Infield-		als optionale
						Erwei-		Steckplätze.
						terung		Ein freier
						(MegaRAI	ł	Steckplatz ist
						D SAS		obligatorisch
						9380-8e)		für die App-
								liance-Infield-
						1		

				Erwei- terung/Me- gaRAID SAS 9380-8e.
			4.	Wenn beide optionalen Steckplätze mit Zusatz- karten befüllt sind, müssen Sie min- destens einen (vorzugsweise Steckplatz 3) Steckplatz frei- geben, damit die Erwei-
				terung mög- lich ist
			5.	Der SAS- Anschluss wird zwischen der Appliance und dem Erweiterungs- Shelf ver- wendet.
			6.	Shelf enthält RAID 6.
			7.	Erweiterungs- Shelf enthält zwei Netz- teile.
			8.	Befolgen Sie nach Anschluss der Erweiterungs-

								Shelt die
								Anweisungen
								zum Hin-
								zufügen eines
								Datenpfads
								im Erwei-
								terungs-
								leitfaden.
							9.	Wenn eine
								neue SSD
								erforderlich
								ist, folgen Sie
								den Anwei-
								sungen unter
								HASH-Ziel zu
								neuer SSD
								migrieren im
								Erwei-
								terungs-
								handbuch.
						LSI SAS 9200 – 8F	1.	Modell 8300
						HBA		unterstützt 8-
		8						тв-, 16-тв-
				8		Qlogic		oder 40-TB-
		(6 x 2-TB-		ΤВ		Dual-Port		Infield-Erwei-
		Fest-		-		НВА		terung. Cli-
		platten)		NA		Quad-		ents können
		ODER		16		Port 1G		jeweils nur
	16 20 24 28					Netz-		ein Erwei-
8300	32 36 40	16 (6 x 4-	480	_	2, 5, 6	werk-		terungs-Shelf
	52, 50, 40	TB-Fest-		560		karte		anschließen.
		platten)				Dual Part	2.	8300 – 16-TB-
		ODER		40				/40-TB-Erwei-
				ТВ		100 355 +		terungs-Shelf
		40 (12 x		-		Dual-Port		enthält ein-
		4-IB-Fest-		790		10G Kup-		gebaute und
		platten)				fer		vor-
						Infield		konfigurierte
						Frwei-		SSD 1,9 TB.
						LIWEI-		,

		,				
					3.	8300 verfügt
						über 2, 5 und
						6 als optio-
						nale Steck-
						plätze. Ein
						freier Steck-
						platz ist obli-
						gatorisch für
						die Appliance-
						Infield-Erwei-
						terung/Me-
						gaRAID SAS
						9380-8e.
					л	Wenn hoido
					4.	ontionalon
						Stockplätzo
						mit Add on
						Kartan gafüllt
				terung		sind müssen
						Sinu, mussen
				D SAS		Sie min-
				9380-8e)		destens einen
				,		Steckplatz frei
						macnen, um
						die Infield-
						Erweiterung
						verwenden zu
						können, vor-
						zugsweise
						Steckplatz 2.
					5.	Der SAS-
						Anschluss
						wird zwischen
						der Appliance
						und dem
						Erweiterungs-
						Shelf ver-
						wendet.
					6	Frwaiterungs
					υ.	Shalf onthalt
						Shen entitlatt

				RAID-6 (6 x 4- TB-Fest- platten).
			7.	Erweiterungs- Shelf enthält zwei Netz- teile.
			8.	Befolgen Sie nach Anschluss der Erweiterungs- Shelf die Anweisungen zum Hin- zufügen eines Datenpfads im Erwei- terungs- leitfe den
			0	leitfaden.
			9.	Wenn eine neue SSD erforderlich ist, folgen Sie den Anwei- sungen unter HASH-Ziel zu hasH-Ziel zu neuer SSD migrieren im Erwei- terungs- handbuch. (Nur für App-
				liance 8300:
				binder mit
				binden mit
				einem 40-1B-
				Appliance-
				Erweiterungs-

						LSI SAS	1.	Shelf bleibt eine 2-TB-SSD frei, die Sie in der Base-App- liance und nicht im Erweiterungs- Shelf plat- zieren müs- sen. Nähere Informationen hierzu finden Sie im Erwei- terungs- handbuch). Modell 8400 unterstützt 8-
8400	32,40,48,56,6- 4,72,80	8 (6 x 2-TB- Fest- platten) ODER 16 (6 x 4- TB-Fest- platten) ODER 40 (12 x 4-TB-Fest- platten)	1200	8 TB – NA 16 TB – NA 40 TB – NA	2, 5, 6	9200 – 8E HBA Qlogic Dual-Port HBA Quad- Port 1G Netz- werk- karte Dual-Port 10G SPF + Dual-Port 10G Kup- fer Infield- Erwei- terung (MegaRAI- D SAS 9380-8e)	2. 3.	unterstutzt 8- TB-, 16-TB- oder 40-TB- Infield-Erwei- terung. Cli- ents können jeweils nur ein Erwei- terungs-Shelf anschließen. 8400 – erfor- dert keine zusätzliche SSD. 8400 verfügt über 2, 5 und 6 als optio- nale Steck- plätze. Ein freier Steck- platz ist obli- gatorisch für die Appliance-

				Infield-Erwei- terung/Me- gaRAID SAS 9380-8e.
			4.	Wenn beide optionalen Steckplätze mit Zusatz- karten befüllt sind, müssen Sie min- destens einen (vorzugsweise Steckplatz 2) Steckplatz frei- geben, damit die Erwei- terung mög- lich ist.
			5.	Der SAS- Anschluss wird zwischen der Appliance und dem Erweiterungs- Shelf ver- wendet.
			6.	Erweiterungs- Shelf enthält RAID 6.
			7.	Erweiterungs- Shelf enthält zwei Netz- teile.
			8.	Befolgen Sie nach Anschluss der Erweiterungs-
			Shelf die	
--	--	--	-----------------	
			Anweisungen	
			zum Hin-	
			zufügen eines	
			Datenpfads	
			im Erwei-	
			terungs-	
			leitfaden.	

In der Box enthaltene Gegenstände

Folgende Gegenstände sind in der Box enthalten:

Hinweis: Wenn Sie feststellen, dass Gegenstände beschädigt sind, wenden Sie sich an den <u>Arcserve-Support</u>.

Appliance-Erweiterungs-Shelf

Hinweis: Die Anzahl der verfügbaren Datenträger im Erweiterungs-Shelf hängt von der Kapazität des Appliance-Erweiterungs-Shelf ab.



CVPM02-Modul (CacheVault Power Module02) und Kabel



MegaRAID SAS 9380-8e RAID-Controller



SAS-Kabel

Zwei SAS-Kabel, die verwendet werden, um den MegaRaid Controller im Appliance-Erweiterungs-Shelf und den Appliance-Server zu verbinden.



SSD (optional)

Hinweis: Für Appliance 8300 müssen Sie eine Verbindung mit der 40-TB-Appliance-Erweiterung herstellen, und Sie haben eine freie 2-TB-SSD.

So stellen Sie eine Verbindung zwischen dem Appliance-Server und dem Appliance-Erweiterungs-Shelf her

Befolgen Sie diese Schritte:

- 1. Bereiten Sie das Appliance-Erweiterungs-Shelf vor und platzieren Sie es in der Nähe des Appliance-Servers.
- 2. Verbinden Sie das *CacheVault Power Module02 (CVPM02)* mit dem *MegaRAID Controller 9380-8e*.



- 3. Halten Sie alle Prozesse der Arcserve UDP-Pläne an, und stellen Sie sicher, dass keine Jobs auf dem Appliance-Server ausgeführten werden.
- 4. Schalten Sie den Appliance-Server aus, und trennen Sie das Netzkabel vom Netzteil.

Hinweis: Trennen Sie den Computer von der Stromversorgung, um eine Beschädigung des System oder einen Stromschlag zu vermeiden.

- 5. Entfernen Sie die Abdeckung des Appliance-Server-Gehäuses.
- 6. Führen Sie folgende Schritte durch, um den *MegaRAID Controller 9380-8e* in einen verfügbaren PCI-e-Steckplatz des Appliance-Servers einzufügen:
 - a. Suchen Sie einen leeren PCI-e-Steckplatz.
 - b. Entfernen Sie die leere Halterungsplatte auf der Rückseite des Computers, die am PCIe-Steckplatz ausgerichtet ist.
 - c. Befestigen Sie die Klemmenschraube, falls vorhanden.
 - d. Richten Sie den MegaRAID Controller 9380-8e an einem PCIe-Steckplatz aus.
 - e. Drücken Sie den Raid-Controller vorsichtig, aber fest herunter, damit er richtig im Steckplatz sitzt.



- 7. Sichern Sie die *MegaRAID Controller 9380-8e*-Halterung am Gehäuse des Systems.
- 8. Ersetzen Sie die Abdeckung des Appliance-Server-Gehäuses.
- 9. Verbinden Sie den *MegaRAID Controller 9380-8e* auf dem Appliance-Server und den *MegaRAID Controller* in der Appliance-Erweiterungs-Shelf mit dem SAS-Kabel.



10. Fügen Sie die SSD ein (nur für Appliance 8300 + 40 TB Erweiterungs-Shelf).

Hinweis: Ist eine 40 TB Appliance-Erweiterungs-Shelf an die Appliance 8300 angeschlossen, stecken Sie die 2 TB SSD (im Lieferumfang der Appliance-Erweiterungs-Shelf enthalten) in den leeren SATA-Steckplatz auf der Rückseite der Appliance-Erweiterungs-Shelf 8300.



- 11. Schließen Sie die Netzkabel des Appliance-Erweiterungs-Shelf an, und schalten Sie das Appliance-Erweiterungs-Shelf ein.
- 12. Netzkabel des Appliance-Servers wieder anschließen und Appliance-Server einschalten.
- 13. Melden Sie sich beim Appliance-Server an um den MegaRAID Storage Manager zu öffnen, und melden Sie sich als Administrator an.

3	MegaRAID	Storage Manager 15.05.01.00 - Host View	x
			Avago
Server Details This page displays all the servers th You will be prompted for entering ho Use Configure Host to configure the	at were discovered. Choose ost credentials while logging hosts that you want to vier	a server and click on Login to start managing that server. n. v.	
Use LDAP Login	1	Enter User Name & Password	Configure Host
Remote servers:	Server :	10.: Use your Operating System's login username	
appliance-8400	User Name: Password:	administrator	
	Login Mode:	Full Access v	

- 14. Gehen Sie folgendermaßen vor, um den RAID-Controller über den MegaRAID Storage Manager zu überprüfen:
 - a. Navigieren Sie zur Registerkarte **Physisch**, auf der die beiden Controller aufgeführt sind.
 - b. Wählen Sie Controller 9380-8e aus, und stellen Sie sicher, dass alle an den Controller 9380-8e angeschlossenen Datenträger online und verfügbar sind.

Hinweis: Wenn es Datenträger gibt, die nicht online sind, klicken Sie mit der rechten Maustaste, und wählen Sie Scan Foreign Configuration.

udpu2verify	5 9380-8e(Bus 1 Dev 0 Domain 0)
SC826P (16), Connector: Pc Slot: 0, SAS, 1.819 TB, Slot: 1 SAS, 1.819 TB,	Disable Alarm Silence Alarm
 Slot: 2, SAS, 1.819 TB, Slot: 3, SAS, 1.819 TB, Slot: 3, SAS, 1.819 TB, 	Start Patrol Read Set Patrol Read Properties
Slot: 4, SAS, 1.819 IB, Slot: 5, SAS, 1.819 IB, Slot: 11, SSD (SATA), 2 BBU: Controller 1: AVAGO MegaRAID Backplane	Disable SSD Guard
	Scan Foreign Configuration
	Save Configuration
 Slot: 0, SAS, 3.639 TB, Slot: 1, SAS, 3.639 TB, Slot: 2, SAS, 3.639 TB, 	Set Consistency Check Properties Schedule Consistency Check
	Set Adjustable Task Rates
	Preserved Cache
	Manage Power Save Settings
	Update Controller Firmware Manage MegaRAID Advanced Software Options Manage Link Speed Save TTY Log

c. Wählen Sie die Option Importieren: Logische Konfiguration aus allen Fremddatenträgern importieren aus, und klicken Sie auf OK.



d. Klicken Sie auf Ja, um den Importprozess zu starten.



e. Klicken Sie auf OK.



Alle Laufwerke im Erweiterungs-Shelf sind nun online.

- 15. Navigieren Sie zur Registerkarte "Logisch", auf der Sie sehen, dass die folgenden Datenträger mit RAID-6 konfiguriert werden. Für andere Module der Erweiterungs-Shelf ist eine einzelne SSD als RAID-0 eingerichtet und unter *LSI MegaRAID SAS 9380-8e* aufgeführt.
 - Appliance-Server 8100 + Erweiterungs-Shelf mit 8 TB
 - Appliance-Server 8200 + Erweiterungs-Shelf mit 16 TB
 - Appliance-Server 8300 + Erweiterungs-Shelf mit 16 TB



- 16. Öffnen Sie die Computerverwaltung, und navigieren Sie zur Datenträgerverwaltung, und führen Sie folgende Schritte aus:
 - a. Formatieren Sie den als Appliance-Erweiterungs-Shelf montierten Datenträger als NTFS, und weisen Sie einen Laufwerksbuchstaben zu. Zum Beispiel "V:".
 - b. Formatieren Sie die SSD als NTFS , und weisen Sie einen Lauf-

a				Comp	outer Ma	nagement		
File Action View Help								
🗢 🧼 🙎 📅 📓 🛤								
🌆 Computer Management (Local	Volume	Layout	Туре	File System	Status			Capa ^
⊿ 👔 System Tools	0	Simple	Basic		Healthy (Recovery Partition)		300 N
D Task Scheduler	C.	Simple	Basic		Healthy (EFI System Partition)		99 M
Event Viewer	G	Simple	Basic		Healthy (Recovery Partition)		76.29
Shared Folders	🗇 (C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash	Dump, Primary Partition)	155.7 =
Local Users and Groups	📼 (V:)	Simple	Basic	NTFS	Healthy (Primary Partition)		7449.
Performance	📾 (X:)	Simple	Basic	NTFS	Healthy (Primary Partition)		7218.
📇 Device Manager	(Y:)	Simple	Basic	NTFS	Healthy (Primary Partition)		223.5
⊿ 🚝 Storage	Rew Volume (W:)	Simple	Basic	NTFS	Healthy (Primary Partition)	10	237.8 ~
Windows Server Backup	<			HI.				>
Disk Management								
Services and Applications	Disk 1	a la Craz						
	Basic	(V:)						
	/449.88 GB 7	449.87 GE	BNTFS	Destition				
	Chine F	Healthy (P	rimary	Partition)				
	Basic I	low Volu	mo (M	L)				
	237.84 GB	37.84 GB	NTES					
	Online	lealthy (P	rimary	Partition)				
			1	22				
				971	1.1	22	No. 19	_
	Disk 3							
	Basic			(C:)		Constraint	(X:)	
	7450.88 GB	00 MB	99 ME	155.73 GB	NTFS	76.29 GB	7218.46 GB NTFS	
	Unline	lealthy	Health	Healthy (B	oot, Page	Healthy (Recovery	Healthy (Primary Partiti	on)
						and an external dama data	The second se	2082 B

werksbuchstaben zu. Zum Beispiel "B:".

Sie haben erfolgreich eine Verbindung zwischen dem Appliance-Erweiterungs-Shelf und dem Appliance-Server hergestellt.

So ändern Sie den Arcserve UDP-Datenspeicher

Dieser Abschnitt enthält folgende Themen:

- Hinzufügen eines Datenpfads auf dem Erweiterungs-Shelf zum Arcserve UDP-Datenspeicher
- Migrieren eines Hash-Ziels zur neuen SSD
- <u>Überprüfen der Gesamtkapazität des Datenspeichers von der Arcserve UDP-Konsole aus</u>
- Fortsetzen aller Pläne von der Arcserve UDP-Konsole

Hinzufügen eines Datenpfades auf dem Expansion Shelf zum Arcserve UDP-Datenspeicher

Befolgen Sie diese Schritte:

- 1. Erstellen Sie einen Ordner im Volume auf dem Appliance-Erweiterungs-Shelf, zum Beispiel "V:\data".
- 2. Beenden Sie den Datenspeicher und verwenden Sie folgenden Befehl zum Erweitern des Datenspeichers auf das Appliance-Erweiterungs-Shelf:

as_gddmgr.exe -DataPath Add <Name des Datenspeichers> -NewDataPath <neue Datenordner>

as_gddmgr.exe -DataPath Display <Name des Datenspeichers>

Migrieren eines Hash-Ziels zur neuen SSD

Hinweis: Dieser Schritt ist nur erforderlich, wenn Sie eine neue SSD für die folgende Erweiterungs-Shelf verwenden:

- Appliance-Server 8100 + Erweiterungs-Shelf mit 8 TB;
- Appliance-Server 8200 + Erweiterungs-Shelf mit 16 TB;
- Appliance-Server 8300 + Erweiterungs-Shelf mit 16 TB;
- Appliance-Server 8300 + Erweiterungs-Shelf mit 40 TB;

Befolgen Sie diese Schritte:

- 1. Erstellen Sie einen Hash-Ordner auf der neuen SSD wie *W:\Arcserve\data_store\hash*.
- 2. Stellen Sie sicher, dass der Datenspeicher angehalten ist. Ist dies nicht der Fall, halten Sie den Datenspeicher in der Arcserve UDP-Konsole an.
- 3. Ändern Sie den Datenspeicher in der Arcserve UDP-Konsole, und setzen Sie das Hash-Ziel auf *W:\Arcserve\data_store\hash*.
- 4. Speichern Sie die Änderung des Datenspeichers.
- 5. Starten Sie den Datenspeicher in der Arcserve UDP-Konsole.

Überprüfen die Gesamtkapazität des Datenspeichers auf der Arcserve UDP-Konsole

Die Gesamtkapazität ist die Kapazität des Appliance-Servers plus die Kapazität des Appliance-Erweiterungs-Shelfs.

Fortsetzen aller Pläne von der Arcserve UDP-Konsole

Setzen Sie alle angehaltenen Pläne über die Arcserve UDP-Konsole fort.

Kapitel 10: Arbeiten mit Netzwerkkonfiguration

Dieser Abschnitt enthält folgende Themen:

Funktionsweise der Netzwerkkonfigurationsdetails	
Konfiguration des NIC-Teaming-Prozesses	231
Deaktivieren des DHCP-Servers	
Konfigurieren der IP-Adresse für den vorinstallierten Linux-Sicherungsserver	234
Aktivieren von Round-Robin auf dem DNS-Server zur Bereitstellung von Las- tenausgleich	236
So überprüfen Sie den Netzwerkstatus auf der Appliance	

Funktionsweise der Netzwerkkonfigurationsdetails

Dank der Netzwerkkonfiguration auf der Appliance kann der integrierte Linux-Sicherungsserver (virtueller Name in Hyper-V-Manager: Linux-BackupSvr) hinter NAT-Gerät funktionieren. Dies bietet folgende Vorteile:

- Der Benutzer muss den Hostnamen des integrierten Linux nicht ändern.
- Der Benutzer speichert eine IP-Adresse f
 ür den Linux-Sicherungsserver im Netzwerk.
- Der Linux-Sicherungsserver kann eine Verbindung zu jedem beliebigen Rechner im öffentlichen Netzwerk herstellen.
- Jeder Rechner im öffentlichen Netzwerk kann mit dem Linux-Sicherungsserver nur über den speziellen Port des Appliance-Servers eine Verbindung herstellen.

Netzwerkkonfigurationsdetails:

Auf dem Hyper-V-Manager gibt es einen rein internen virtuellen Switch (*Linux-BkpSvr-Switch*), der nur von Linux-BackupSvr verwendet wird.

Virtual Machin	nes				
Name	~	State	CPU Usage	Assigned Memory	Uptime
Linux-Backu	pSvr	Running	0 %	4096 MB	00:07:26
<	Virtual Sw Virtual Sw Virtual Sw New Linux Inte	vitch Manager for Switches virtual network swi (-BkpSvr-Switch rnal only	APPLIANCE	Virtual Switch Prope Name: Linux-BkpSvr-Switch	erties —
Checkpoint	★ Global I	letwork Setting: Address Range .5-5D-0A-01-00 to	s 00-15-5D-0	Notes:	
Linux-Backı				Connection type What do you want to O External network Broadcom NetXth Allow manage	connect this virtual reme Gigabit Etherne ment operating systemet 10 victoria
2034				Internal network Private network	root 1/0 virtualizado

 Unter Systemsteuerung\Netzwerk und Internet\Netzwerkverbindungen wird ein "Hyper-V-Adapter für virtuelles Ethernet" namens "LinuxBkpSvr" angezeigt. Die IPv4-Adresse für diesen Switch wurde standardmäßig auf "192.168.10.1" festgelegt, wie unten gezeigt.

LinuxBkpSvr	Unidentified network	Hyper-V Virtual Ethernet Adap	pter No network acc
LinuxBkpSvr Properties	× Internet Prot	tocol Version 4 (TCP/IPv4) Properties	×
Networking Sharing	General		
Connect using:	You can ge	t IP settings assigned automatically if your	network supports
👳 Hyper-V Vitual Ethemet Adapter	this capabil for the app	lity. Otherwise, you need to ask your netw propriate IP settings.	ork administrator
Config	ure Obtai	n an IP address automatically	
This connection uses the following items:	Use t	he following IP address:	
Client for Microsoft Networks	^ IP addre	192 . 168 .	10 . 1
Cos Packet Scheduler	Subnet r	mask: 255 . 255 .	255.0
Internet Protocol Version 4 (TCP/IPv4) Microsoft Network Adapter Multiplexor Protocol	Default	gateway:	
Microsoft LLDP Protocol Driver Internet Protocol Version 6 (TCP/IPv6)	↓ Obtai	n DNS server address automatically	
<	> Ose t	he following DNS server addresses:	
Instal Uninstal Proper	ties Preferre	d DNS server:	
Description	Alternat	e DNS server:	
Transmission Control Protocol/Internet Protocol. The def wide area network protocol that provides communication across diverse interconnected networks.	auit Valid	ate settings upon exit	Advanced
ок	Cancel	0	Cancel

 Sie haben in der Standardeinstellung DHCP-Server auf dem Appliance-Rechner konfiguriert. Der DHCP-Server funktioniert nur auf dem virtuellen Hyper-V-Adapter.



Standardmäßig stellt nur eine 192.168.10.2 im Adresspool sicher, dass der integrierte Linux-Sicherungsserver die IP 192.168.10.2 erhält.

👰 DHCP									
File Action View Help									
🗢 🔶 🔟 🖬 💷 💷	💠 🔿 📷 🔒 📓 📷 🖳								
9 DHCP	Start IP Address	End IP Address	Description						
 appliance appliance Server Options Scope [192.168.10.0] nat Address Pool Address Leases Address Leases Reservations Scope Options Policies Policies Filters IPv6 	2 ⊞ 192.168.10.2	192.168.10.2	Address range for distribution						

NAT wurde auf dem Appliance-Rechner konfiguriert.

Narr	ne	Status	Device Name	Connectivity	Network Category
Q 1	NIC1	Disabled	Broadcom NetXtreme Gigabit Et		
<u>्</u> व ।	NIC2	Disabled	Broadcom NetXtreme Gigabit Et		
- Q I	NIC3	Disabled	Broadcom NetXtreme Gigabit Et		
- Q I	NIC4	ARCSERVE.COM	Broadcom NetXtreme Gigabit Et	Internet access	Public network
Q I	LinuxBkpSvr	Unidentified network	Hyper-V Virtual Ethernet Adapter	No network access	Public network



 Die Port-Umleitung auf der Appliance wurde f
ür den Linux-Sicherungsserver konfiguriert.

Administrator: Command Prompt					
c:\Windows\Syst	em32>netsh i	nterface portprox	xy show all		
Listen on ipv4:		Connect to ipv4	:		
Address	Port	Address	Port		
*	8018	192.168.10.2	8014		
*	8019	192.168.10.2	22		
*	8035	192.168.10.2	8035		
*	8017	192.168.10.2	8017		
*	8021	192.168.10.2	8021		
*	50000	192.168.10.2	50000		
*	50001	192.168.10.2	50001		
*	50002	192.168.10.2	50002		
*	50003	192.168.10.2	50003		
*	50004	192.168.10.2	50004		

Der Linux-Sicherungsserver ruft die IP-Adresse 192.168.10.2 vom DHCP-Server ab. Nachdem die IP-Adresse abgerufen wurde, kommuniziert das Back-End-Skript (C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\resetdhcp.ps1) mit Linux, um das Systemgebietsschema des Linux-Sicherungsservers zu ändern und mit dem Systemgebietsschema des Appliance-Windows-BS konsistent zu machen.

```
[root@Linux-BackupSvr network-scripts]# cat ifcfg-eth0
TYPE=Ethernet
B00TPR0T0=dhcp
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4 FAILURE FATAL=no
IPV6INIT=yes
IPV6 AUTOCONF=yes
IPV6 DEFROUTE=yes
IPV6 PEERDNS=yes
IPV6 PEERROUTES=yes
IPV6 FAILURE FATAL=no
IPV6 ADDR GEN MODE=stable-privacy
NAME=eth0
UUID=9ae68090-5e77-4396-b6c4-a5d6d83ab62f
DEVICE=eth0
ONB00T=yes
ZONE=
[root@Linux-BackupSvr network-scripts]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
       inet 192.168.10.2 netmask 255.255.255.0 broadcast 192.168.10.255
       inet6 fe80::c08c:d0dc:bf67:8afa prefixlen 64 scopeid 0x20<link>
       ether 00:15:5d:0a:01:00 txqueuelen 1000 (Ethernet)
       RX packets 20955 bytes 28503433 (27.1 MiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 19202 bytes 1534457 (1.4 MiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
       inet 127.0.0.1 netmask 255.0.0.0
       inet6 ::1 prefixlen 128 scopeid 0x10<host>
       loop txqueuelen 1 (Local Loopback)
RX packets 14 bytes 1600 (1.5 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 14 bytes 1600 (1.5 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Konfiguration des NIC-Teaming-Prozesses

Die Arcserve Appliance enthält integrierte Ethernet-Ports. Um diese Ports verwenden zu können, muss das Ethernet-NIC-Teaming konfiguriert werden. NIC-Teaming ermöglicht die Platzierung mehrerer Netzwerkadapter in einem Team für Bandbreitenaggregation und Netzwerkverkehr-Failover, um im Falle eines Netzwerkkomponentenausfalls Konnektivität sicherzustellen.

Um ein funktionierendes NIC-Team zu konfigurieren, ist ein Netzwerk-Switch erforderlich, der die Verbindungsbündelung unterstützt. Informationen zur richtigen Konfiguration des NIC-Teams erhalten Sie beim Hersteller Ihres Netzwerk-Switches und in der Dokumentation zur Microsoft Windows-Konfiguration.

Gehen Sie folgendermaßen vor, wenn der Netzwerk-Switch konfiguriert ist:

1. Starten Sie über Windows-Desktop den Arcserve Appliance-Assistenten.

Hinweis: Wenn eine DHCP- oder statische IP-Adresse verwendet wird, können Sie die IP-Adresse für das NIC-Team im Fenster "Netzwerkverbindungen" konfigurieren. Stellen Sie sicher, dass dem NIC-Team eine gültige IP-Adresse zugewiesen wurde und dass es in Ihrem Netzwerk verfügbar ist.

Network Connections					
Connection Name	IP Address	Description			
Ethernet 2 Connected	10.57.25 Automatic via DHCP	Intel(R) I350 Gigabit Network Connection #2	Edit		
-					
		Activate	Windows		

2. Führen Sie folgenden Befehl aus:

C:\\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\resetnic.bat

Die Konfiguration wird abgeschlossen und die folgende Meldung wird angezeigt.



Um zu verifizieren, dass die Konfiguration funktioniert, melden Sie sich beim Linux-Sicherungsserver im Hyper-V-Manager an, und pingen Sie die IP-Adresse für die spezifischen Computer in Ihrem Intranet. Wenn dies fehlschlägt, nehmen Sie eine Überprüfung vor und wiederholen Sie diesen Vorgang.

Deaktivieren des DHCP-Servers

Der DHCP-Server ist auf der Appliance standardmäßig aktiviert. Der DHCP-Server funktioniert nur auf dem Hyper-V-Adapter für virtuelles Ethernet (*LinuxBkpSvr*) auf der Appliance, um sicherzustellen, dass der vorinstallierte Linux-Sicherungsserver die IP-Adresse der Appliance abrufen und mit der Appliance kommunizieren kann, ohne dass sich dies auf die Produktionsnetzwerkumgebung auswirkt.

Gehen Sie folgendermaßen vor, um den DHCP-Server zu deaktivieren:

- 1. Öffnen Sie die Datei C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Configuration\Appliance.properties.
- 2. Ändern Sie die Datei in *DHCP_ENABLE=false*. Die Datei *App-liance.properties* sieht wie unten dargestellt aus:

DHCP_ENABLE=false AdapterName=LinuxBkpSvr Appliance_IPAddress=192.168.10.1 Linux IPAddress=192.168.10.2

- 3. Speichern Sie die Datei.
- 4. Löschen Sie die Datei C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\dhcpdone.flag.
- 5. Führen Sie C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\resetdhcp.ps1 wie unten dargestellt in der DOS-Befehlszeile aus, um den DHCP-Server-Dienst zu deaktivieren:

C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance>powershell .\resetdhcp.ps1

Konfigurieren der IP-Adresse für den vorinstallierten Linux-Sicherungsserver

Für den vorinstallierten Linux-Sicherungsserver verwendet der Sicherungsserver standardmäßig die IP-Adresse 192.168.10.2 zur Kommunikation mit dem Appliance-Server. In der Einführung zur Netzwerkkonfiguration finden Sie weitere Informationen zum vorinstallierten Linux-Sicherungsserver, anhand derer Sie erkennen können, wie der vorinstallierte Linux-Sicherungsserver mit dem Appliance-Server kommuniziert.

Befolgen Sie diese Schritte, um die IP-Adresse für den vorinstallierten Linux-Sicherungsserver anzugeben:

- 1. Öffnen Sie die Datei C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Configuration\Appliance.properties.
- Ändern Sie die IP-Adresse f
 ür Appliance_IPAddress und Linux_IPAddress. Legen Sie z. B. "Appliance_IPAddress" auf 192.168.100.1 und "Linux_IPAddress" auf 192.168.100.2 fest.

Hinweis:

- Die IP-Adresse f
 ür "Appliance_IPAddress" ist auf die Netzwerkschnittstelle LinuxBkpSvr (Hyper-V-Adapter f
 ür virtuelles Ethernet) festgelegt, die zur Kommunikation mit diesem vorinstallierten Linux-Sicherungsserver verwendet wird.
- Die IP-Adresse f
 ür "Linux_IPAddress" ist auf den vorinstallierten Linux-Sicherungsserver festgelegt.
- Stellen Sie sicher, dass "Appliance_IPAddress" und "Linux_IPAddress" die IP-Adresse desselben Subnetzwerks verwenden.

Nach den Änderungen sieht der Inhalt der Datei wie folgt aus:

DHCP_ENABLE=true

AdapterName=LinuxBkpSvr

Appliance_IPAddress=192.168.100.1

Linux_IPAddress=192.168.100.2

- 3. Speichern Sie die Datei.
- 4. Löschen Sie die Datei C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\dhcpdone.flag.

5. Führen Sie C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\resetdhcp.ps1 aus, um die IP-Adresse für die Netzwerkschnittstelle LinuxBkpSvr und den vorinstallierten Linux-Sicherungsserver zurückzusetzen.

Hinweis:

Der vorinstallierte Linux-Sicherungsserver wird während des Vorgangs heruntergefahren und neu gestartet, wenn Sie die Einstellung für "Linux_IPAddress" geändert haben.

6. Führen Sie folgenden Befehl über die Befehlseingabeaufforderung aus:

C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance>powershell .\resetdhcp.ps1

Aktivieren von Round-Robin auf dem DNS-Server zur Bereitstellung von Lastenausgleich

Der Microsoft-DNS-Server unterstützt das Round-Robin-Verfahren, mit dem ein Lastenausgleich zwischen Servern bewirkt werden kann. Diese Funktion ermöglicht DNS das Senden beider IP-Adressen, wenn eine Abfrage für *myServer.mydomain.com* empfangen wird. Der Client (bzw. Resolver oder Konfliktlöser) verwendet immer die erste Adresse. Wenn DNS das nächste Mal eine Abfrage für diesen Namen empfängt, wird die Reihenfolge der Liste von IP-Adressen in Round-Robin-Manier geändert (d. h. die Adresse, die in der vorherigen Liste an erster Stelle stand, steht in der neuen Liste an letzter Stelle). Round-Robin von Namensdatensätzen wird nicht unterstützt, da für jeden Alias jeweils nur ein kanonischer Name vorhanden sein darf.

In der Appliance können Sie Datensätze für alle IPv4-Adressen zum Domain Name Service(DNS)-Server hinzufügen, um einen Lastenausgleich zwischen den Netzwerkschnittstellen zu bewirken.

Weitere Informationen zum Lastenausgleich zwischen Servern finden Sie unter <u>RFC</u> <u>1794</u>.

So fügen Sie einen Datensatz für zusätzliche IP-Adressen zum Domain Name Service-Server hinzu

Wenn ein Server über zwei oder mehr Netzwerkkarten (NICs) oder über mehr als eine IP-Adresse für eine Netzwerkkarte verfügt, können Sie einen Eintrag für die zusätzlichen IP-Adressen auf dem DNS-Server hinzufügen, indem Sie einen "A"-Datensatz für jede IP-Adresse erstellen.

Beispiel:

Angenommen, der DNS-Hostname eines Servers lautet <myserver> und die DNS-Domäne <mydomain.com>. Diesem Server sind die beiden folgenden IP-Adressen zugewiesen:

- IPAddress1
- IPAddress2

Um diese IP-Adressen dem DNS-Server hinzuzufügen, erstellen Sie zwei "A"-Datensätze in der Zone <mydomain.com>, wie unten angegeben:

- Myserver A <IPAddress1>
- Myserver A <IPAddress2>

Damit der Resolver jedes Mal die gleiche IP-Adresse erhält, erstellen Sie zwei weitere "A"-Datensätze, die jeder Adresse einen eindeutigen Namen zuweisen, wie unten angegeben:

- Altname1 A <IPAddress1>
- Altname2 A <IPAddress2>

Mit dieser Methode erhält ein Resolver immer IPAddress1, wenn eine Anfrage für Altname1 gesendet wird, und immer IPAddress2, wenn eine Anfrage für Altname2 gesendet wird.

So überprüfen Sie den Netzwerkstatus auf der Appliance

Das Tool ApplianceNetworkStatusCheck.ps1 wird verwendet, um Informationen über den aktuellen Gesamtnetzwerkstatus des Arcserve Appliance Servers zu sammeln und einen Bericht im XML-Format zu generieren. Der Bericht enthält Informationen über den Netzwerkadapter, den Netzwerkswitch, den virtuellen Hyper-V-Switch, DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), RRAS (Route and Remote Access Service) und andere wichtige Konfigurationen auf dem Server.

Das Tool ApplianceNetworkStatusCheck.ps1 ist in Arcserve Appliance Server UDP V7.0 Update1 verfügbar.

Gehen Sie wie folgt vor, um den Netzwerkstatusbericht des Appliance-Servers mithilfe dieses Tools zu generieren:

- 1. Melden Sie sich beim Arcserve Appliance-Server als Administrator an.
- 2. Öffnen Sie die Eingabeaufforderung, und geben Sie den Ordnerspeicherort ein:

C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance

3. Führen Sie ApplianceNetworkStatusCheck.ps1 aus, um einen Bericht zu generieren:

#Powershell.\ ApplianceNetworkStatusCheck.ps1

```
c:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance>powershell .\ApplianceNetworkStatusCheck.psl
1. Check network switch
2. Check HyperV virvual switch
3. Check DHCP service and properties
4. Check ipv4 to ipv4 tcp netsh interface portproxy
5. Check RRAS NAT interface
CHECK FINISH
Start create html report
```

Der Browser wird geöffnet und zeigt den gesamten Netzwerkstatusbericht des Appliance-Servers an.

Kapitel 11: Sicherheitsmaßnahmen

Dieser Abschnitt enthält folgende Themen:

Allgemeine Sicherheitsmaßnahmen	2 39
Sicherheitsmaßnahmen zur Elektrik	241
FCC-Konformität	243
Vorsichtsmaßnahmen gegen elektrostatische Entladungen (ESD)	

Allgemeine Sicherheitsmaßnahmen

Sie müssen die folgenden allgemeine Sicherheitsmaßnahmen ergreifen, um sich selbst zu schützen und die Appliance vor Schäden oder Fehlfunktionen zu schützen:

 Geräte der EMI-Klasse A (Unternehmensgeräte) sind hinsichtlich der elektromagnetischen Konformität als Unternehmensgeräte (A) und nicht als Heimgeräte registriert. Verkäufer und Benutzer diesbezüglich Sorgfalt walten lassen.

A급기기(업무용방송통신기자재)

이 기 기 는 업 무 용 (A급)으로 전 자 파 적 합 기 기 로 서 판 매 자 또 는 사 용 자 는 이 점 을 주 의 하 시 기 바 라 며,가 정 외 의 지 역 에 서 사 용 하 는 것 을 목 적 으 로 합 니 다

Hinweis: Diese Sicherheitsmaßnahme bezieht sich nur auf Südkorea. Weitere Informationen erhalten Sie beim Arcserve-Support auf <u>htt</u>-<u>ps://www.arcserve.com/support</u> oder telefonisch unter 0079885215375 (Südkorea).

- Überprüfen Sie den Kasten, in dem die Appliance ausgeliefert wurde, und stellen Sie sicher, dass keine sichtbaren Anzeichen von Beschädigungen zu erkennen sind. Wenn Beschädigungen erkennbar sind, bewahren Sie das gesamte Verpackungsmaterial auf und wenden Sie sich sofort an den Arcserve-Support unter https://www.arcserve.com/support.
- Suchen Sie einen geeigneten Aufstellungsort für das Rackelement, in dem die Appliance installiert wird. Er sollte sich in einem sauberen, staubfreien Bereich befinden, der gut gelüftet und aufgeräumt ist. Vermeiden Sie Bereiche, in denen Wärme, Elektrorauschen oder elektromagnetische Felder generiert werden.
- Das Rack muss auch in der N\u00e4he von mindestens einer geerdeten Steckdose platziert werden. Je nach Modell enth\u00e4lt die Appliance entweder ein einzelnes Netzteil oder ein redundantes Netzteil und ben\u00f6tigt im letzten Fall zwei geerdete Steckdosen.
- Diese Appliance ist nur für die Verwendung an einem sicheren Ort vorgesehen.
 - Ein Zugriff darf nur durch Wartungspersonal oder durch Benutzer erfolgen, die über die Gründe für den Einschränkungen am Aufstellungsort und über alle Vorsichtsmaßnahmen informiert sind, die ergriffen werden müssen; und

- Der Zugriff erfolgt mithilfe eines Werkzeugs, mit einem Schloss und einem Schlüssel oder mit einer anderen Sicherheitsvorkehrung und wird von der für den Standort zuständigen Stelle kontrolliert.
- Platzieren Sie die obere Abdeckung der Appliance und alle Komponenten, die von der Appliance entfernt werden, auf einem Tisch, damit Sie nicht versehentlich auf die Komponenten treten.
- Tragen Sie während der Arbeit an der Appliance keine losen Kleidungsstücke wie Krawatten oder Ärmel ohne Knöpfe, die mit elektrischen Stromkreisen in Kontakt kommen oder in einen Lüfter gezogen werden können.
- Entfernen Sie jeglichen Schmuck und alle Gegenstände aus Metall vom Körper, da es sich um ausgezeichnete metallische Leiter handelt, die zu Kurzschlüssen führen und Sie verletzen können, wenn Sie in Kontakt mit Leiterplatten (PCBs) oder mit stromführenden Bereichen kommen.
- Nach dem Zugriff auf das Innere der Appliance schließen Sie die Appliance und fixieren sie mit den Halteschrauben am Rack, nachdem Sie sichergestellt haben, dass alle Verbindungen hergestellt wurden.

Sicherheitsmaßnahmen zur Elektrik

Sie müssen die folgenden allgemeine Sicherheitsmaßnahmen zur Elektrosicherheit ergreifen, um sich selbst zu schützen und die Appliance vor Schäden oder Fehlfunktionen zu schützen:

- Sie müssen die Position des Netzschalters der Appliance sowie die Positionen des Not-Aus-Schalters für den Raum, des Trennschalters und der Steckdose kennen. Bei einem Unfall im Zusammenhang mit der Elektrik können Sie dann die Appliance schnell von der Stromversorgung trennen.
- Arbeiten Sie bei der Arbeit mit Hochspannungskomponenten nicht allein.
- Die Appliance sollte stets von der Stromversorgung getrennt sein, wenn wichtige Systemkomponenten, wie z. B. das Serverboard, Arbeitsspeichermodule, das DVD-ROM-Laufwerk und das Diskettenlaufwerk ausgebaut oder eingebaut werden (nicht erforderlich für hot-swap-fähige Laufwerke). Beim Trennen der Stromversorgung sollten Sie zuerst die Appliance über das Betriebssystem ausschalten und dann die Netzkabel von allen Netzteilmodulen in der Appliance abziehen.
- Beim Arbeiten in der N\u00e4he frei liegender elektrischer Stromkreise sollte eine andere Person, die mit den Ausschalt-Bedienelementen vertraut ist, in der N\u00e4he sein, um gegebenenfalls die Stromversorgung auszuschalten.
- Benutzen Sie beim Arbeiten mit Elektrogeräten nur eine Hand. Auf diese Weise vermeiden Sie einen geschlossenen Stromkreis, der zu einem Stromschlag führt. Verwenden Sie Metallwerkzeuge mit äußerster Vorsicht, da sie elektrische Komponenten oder Leiterplatten leicht beschädigen können, wenn sie mit ihnen in Kontakt kommen.
- Verwenden Sie zum Schutz vor Stromschlägen keine Matten, die zur Verringerung elektrostatischer Entladungen entwickelt wurden. Verwenden Sie stattdessen Gummimatten, die speziell als elektrische Isolatoren konzipiert wurden.
- Das Netzkabel des Netzteils muss einen Erdungsstecker umfassen und an eine geerdete elektrische Steckdose angeschlossen werden.
- Serverboard-Batterie: ACHTUNG Wenn die interne Batterie falsch herum installiert wird, besteht Explosionsgefahr, da die Pole umgekehrt werden. Diese Batterie darf nur durch eine Batterie des gleichen oder eines ähnlichen Typs, der vom Hersteller empfohlen wird, ersetzt werden. Entsorgen Sie verbrauchte Akkus gemäß den Anweisungen des Herstellers.

 DVD-ROM-Laser: ACHTUNG – Dieser Server ist möglicherweise mit einem DVD-ROM-Laufwerk ausgestattet. Um zu verhindern, dass Sie sich dem Laserstrahl und gefährlicher Strahlung aussetzen, dürfen Sie das Gehäuse nicht öffnen oder auf unkonventionelle Weise verwenden.
FCC-Konformität

Diese Appliance entspricht Teil 15 der FCC-Vorschriften. Der Betrieb unterliegt den folgenden Bedingungen:

- Diese Appliance darf keine abträglichen Interferenzen verursachen, und
- Diese Appliance muss alle empfangenen Interferenzen tolerieren, einschließlich Inferenzen, die zu unerwünschten Vorgängen führen.

Hinweis: Dieses Gerät wurde getestet und entspricht den Grenzwerten für ein digitales Gerät der Klasse A, gemäß Teil 15 der FCC-Vorschriften. Diese Grenzwerte sind so ausgelegt, dass sie bei einem Betrieb der Geräte im gewerblichen Umfeld einen ausreichenden Schutz vor abträglichen Interferenzen bieten. Das Gerät erzeugt und benutzt Hochfrequenzenergie und kann solche abstrahlen und kann, wenn es nicht gemäß den Anweisungen installiert und benutzt wird, die Funkkommunikation stören. Der Betrieb dieses Geräts in einem Wohngebiet verursacht wahrscheinlich abträgliche Interferenzen. Diese muss der Benutzer auf eigene Kosten beheben.

Vorsichtsmaßnahmen gegen elektrostatische Entladungen (ESD)

Elektrostatische Entladungen (ESD) werden von zwei Objekten mit unterschiedlichen elektrischen Ladungen erzeugt, die miteinander in Kontakt kommen. Mithilfe einer elektrischen Entladung wird diese Ladungsdifferenz neutralisiert, was zu Schäden an elektronischen Komponenten und Leiterplatten führen kann. Geräte, die gegenüber ESD empfindlich sind, wie z. B. Serverboards, Motherboards, PCIe-Karten, Laufwerke, Prozessoren und Speicherkarten, erfordern eine besondere Handhabung. Verwenden Sie die folgenden Vorsichtsmaßnahmen, die dazu beitragen, die Differenz der elektrischen Ladungen, die miteinander in Kontakt kommen, zu neutralisieren, bevor der Kontakt hergestellt ist, um so Ihr Gerät vor ESD zu schützen:

- Verwenden Sie eine Gummimatte, die speziell als elektrische Isolatoren konzipiert wurde. Verwenden Sie zum Schutz vor Stromschlägen keine Matte, die zur Verringerung elektrostatischer Entladungen entwickelt wurde.
- Tragen Sie eine geerdete Handschlaufe, um eine statische Entladung zu verhindern
- Tragen Sie antistatische oder gegen elektrostatische Entladungen (ESD) schützende Kleidung oder Handschuhe.
- Bewahren Sie alle Komponenten und Leiterplatten (PCBs) in ihrem antistatischen Verpackungen auf, bis sie verwendet werden.
- Berühren Sie einen geerdeten metallischen Gegenstand, bevor Sie die Karte aus der antistatischen Verpackung nehmen.
- Lassen Sie Komponenten oder Leiterplatten nicht mit Ihrer Kleidung in Kontakt kommen, da diese eine Ladung aufweisen kann, auch wenn Sie eine Handschlaufe tragen.
- Fassen Sie eine Karte nur an den Rändern an. Berühren Sie keine Komponenten, peripheren Chips, Speichermodule oder Kontakte.
- Vermeiden Sie es, beim Umgang mit Chips oder Modulen deren Pins zu berühren.
- Legen Sie das Serverboard und die Peripheriegeräte wieder in ihre antistatischen Verpackungen, solange sie nicht verwendet werden.
- Stellen Sie zum Zwecke der Erdung sicher, dass Ihre Appliance eine sehr gute Leitfähigkeit zwischen dem Netzteil, dem Gehäuse, den Montagehalterungen und dem Serverboard bietet.

Kapitel 12: Aktivieren von Sophos auf der Arcserve Appliance

Dieser Abschnitt enthält Informationen zum Aktivieren von Sophos auf der Arcserve Appliance.

Wichtig! Wenn Sie ein neuer Kunde von Arcserve Appliances mit Sophos Intercept X sind, das im Rahmen des Zustellungsprozesses vorinstalliert ist, wird eine E-Mail mit einfachen Aktivierungsanweisungen gesendet. Befolgen Sie die angegebenen Methoden, um den Aktivierungsprozess abzuschließen. Wenn Sie bereits Kunde sind, sind die Appliances der Arcserve nicht vorinstalliert. Es wird empfohlen, Sophos Intercept X manuell herunterzuladen und zu installieren. Informationen zum gesamten Installationsprozess finden Sie unter <u>Manuelle Installation von Sophos</u> Intercept X Advanced for Server auf Arcserve Appliances.

1. Nachdem Sie eine Willkommens-E-Mail von Sophos erhalten haben, klicken Sie auf den Link **Passwort einrichten**, um Ihr Passwort festzulegen.

Hinweis: Wenn Sie mehr als ein Kundenkonto beantragen, erhalten Sie die entsprechende Anzahl von Willkommens-E-Mails für jedes Konto separat von Sophos, um das Passwort entsprechend einzurichten.

Wenn Sie bereits über ein vorhandenes Kundenkonto verfügen und weiterhin dasselbe Kundenkonto verwenden möchten, um einen weiteren Arcserve Appliance Sophos zu aktivieren, erhalten Sie solche Willkommens-E-Mails nicht an die E-Mail-Adresse, die mit diesem Kundenkonto verknüpft ist. Sie erhalten eine E-Mail von Arcserve, die eine Zip-Datei und Anweisungen zum Aktivieren von Sophos enthält.

Welcome to Sophos Central			ø	Ø
do-not-reply@central.sophos.com	11:44 AM (0 minutes ago)	☆	*	:
SOPHOS				
Welcome				
A Sophos Central Admin account has been created for you by your company account to access your account, you must set up a password	i first.			
Set up my password				
Once you have your password set up, you can log into your account with the info below:				
Website: Sochos Central Admin				
Login: and a state of the state				
NOTE: Please contact your administrator if you think you received this email by mistake.				
powered by SOPHOS © 2013 - 2019 Sophos Limited. All rights reserved.				_

2. Es stehen zwei Methoden zum Aktivieren von Sophos auf der Arcserve Appliance zur Verfügung. **Hinweis:** Um weitere Arcserve Appliance Sophos zu aktivieren, wiederholen Sie die Schritte von Methode 1 bzw. Methode 2 nach Bedarf.

- Methode 1: Aktivieren von Sophos auf der Arcserve Appliance über die E-Mail von Arcserve.
- Methode 2: Aktivieren von Sophos auf der Arcserve Appliance mit dem Skript Customer_Boot.ps1

Methode 1: Aktivieren von Sophos auf der Arcserve Appliance über die E-Mail

Arcserve sendet Ihnen eine Zip-Datei per E-Mail zur Aktivierung von Sophos. Entpacken Sie die Datei. Der Ordner "Arcserve_Appliance_Sophos_Activation_YYYY-MM-DD-HH-MM-SS" enthält die folgenden Dateien:

- Config.xml: Die Konfigurationsdatei.
- Registration.txt: Die Registrierungsdatei.
- Arcserve_Appliance_Sophos_Activation.ps1: Powershell-Skript zum Aktivieren von Sophos.

Führen Sie die folgenden Schritte aus, um Sophos zu aktivieren:

- 1. Melden Sie sich bei Arcserve Appliance als Systemadministrator an.
- 2. Kopieren Sie die ZIP-Datei in Arcserve Appliance, und entpacken und extrahieren Sie die Datei nach Bedarf.
- 3. Öffnen Sie die Eingabeaufforderung, und geben Sie den Speicherort ein, der die extrahierten Dateien enthält.
- 4. Führen Sie Arcserve_Appliance_Sophos_Activation.ps1 aus.

#powershell .\ Arcserve_Appliance_Sophos_Activation.ps1

 Um die geschützte Arcserve Appliance anzuzeigen, melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Kennwort bei der Sophos Central-Seite an, und navigieren Sie dann zu "Geräte > Server".

Hinweis: Die E-Mail-Adresse, unter der Sie die ZIP-Datei erhalten haben, ist dieselbe E-Mail-Adresse, die Sie für die Anmeldung verwenden müssen.

	SOPHOS CENTRAL Admin	Servers	our servers				
	Overview	Computers	Mobile Devices	Servers Servers			
•	Dashboard	Search	Q Show	all servers	✓ All Health	Status	*
▲	Alerts						
٨	Threat Analysis Center 🕨	Name		IP		0S	
	Logs & Reports						
<u>,1</u>	People						
50	Devices						

Sophos wird auf der Appliance aktiviert.

Methode 2: Aktivieren von Sophos auf der Arcserve Appliance mithilfe eines Skripts

Dieser Abschnitt enthält Informationen zum Aktivieren von Sophos auf der Arcserve Appliance mithilfe des Skripts Customer_Boot.ps1.

Befolgen Sie diese Schritte:

 Um sich bei der Sophos Central-Seite anzumelden, öffnen Sie <u>htt-</u> <u>ps://cloud.sophos.com</u>, und verwenden Sie Ihre E-Mail-Adresse und Ihr Kennwort.

Hinweis: Wenn Sie mehrere E-Mail-Adressen mit verschiedenen Arcserve Appliance Sophos-Kundenkonten verknüpft haben, wählen Sie eine gewünschte E-Mail-Adresse aus, um das entsprechende Konto zum Aktivieren von Sophos zu verwenden.

2. Navigieren Sie zur Seite "Schutzgeräte" unter "Serverschutz", und klicken Sie auf den Link "Befehlszeile anzeigen".



- 3. Kopieren Sie die Mcstoken- und Verwaltungsserverinformationen.
- 4. Melden Sie sich als Administrator beim Arcserve Appliance-System an.
- 5. Öffnen Sie die Eingabeaufforderung, und geben Sie den Ordnerspeicherort "C:\Program Files\Arcserve\Appliance\Sophos\Customer_Boot" ein.

#cd "C:\Program Files\Arcserve\Appliance\Sophos\Customer_Boot"

6. Führen Sie Customer_Boot.ps1 aus.

#powershell .\Customer_Boot.ps1

- 7. Geben Sie die Werte des MCS-Tokens und des Verwaltungsservers basierend auf der Eingabeaufforderung für die Befehlszeile ein, und warten Sie dann, bis die Befehlsausführung abgeschlossen ist.
- 8. Um die geschützte Arcserve Appliance anzuzeigen, melden Sie sich bei der Sophos Central-Seite an, und navigieren Sie dann zu "Geräte > Server".

	SOPHOS CENTRAL Admin	S	Servers	our servers		-		
	Overview	9	Computers	Mobile Devices	Servers			
•	Dashboard	1	Search	Q Show	all servers	✓ All Healt	n Status	•
▲	Alerts							
٨	Threat Analysis Center 🕨		Name		IP		0S	
	Logs & Reports							
<u>,1</u>	People							
50	Devices							

Sophos wird auf der Appliance aktiviert.

Manuelle Installation von Sophos Intercept X Advanced for Server auf Arcserve Appliances

Die Integration von Arcserve Appliances mit Sophos Intercept X Advanced for Server ermöglicht 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

Hinweis: Wenn die Arcserve Appliances am oder nach dem 15. Oktober 2019 an Sie ausgeliefert wurden, ist Sophos Intercept X vorinstalliert. Im Rahmen des Zustellungsprozesses wird Ihnen eine E-Mail mit den Aktivierungsanweisungen zugesandt. Folgen Sie ansonsten den Anweisungen unten, um Sophos Intercept X manuell zu installieren.

- 1. Erstellen Sie auf der Arcserve Support-Website ein Konto.
- 2. Um eine kostenlose Kopie von Sophos Intercept X Advanced anzufordern, senden Sie eine E-Mail an den Arcserve Support unter <u>SophosAc</u>-

tRequest@Arcserve.com, und fügen Sie alle relevanten Details hinzu. 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 Arcserve Appliances als Administrator oder als Benutzer mit lokalen Administratorrechten an.

Hinweis: Melden Sie sich bei den Appliances aus Sicherheitsgründen nicht über die Active Directory-Domäne an.

- 5. Melden Sie sich von Ihrer Appliance aus bei Sophos Central an, und folgen Sie dann Schritt 3 und 4.
- 6. Öffnen Sie das Dialogfeld Produkteinrichtung, und wählen Sie dann **Ser**verschutz aus.

	Product Setup	×
	Choose a product below to get started.	
🕲 Endpoint Protection	٥	Mobile
Server Protection	⊜	Wireless
😣 Email Security	٥	Device Encryption
🤣 Web Gateway	(3)	Phish Threat
😂 Firewall Managemer	nt	

 Klicken Sie im Abschnitt "Serverschutz" auf Windows Server Installer herunterladen, und speichern Sie dann das Installationsprogramm SophosSetup.exe in einem Ordner auf der Appliance.

SOPHOS	Protect Devices	Page - an anarotad
Dermen Conduct Area Area Conductor Cond	Non-declaration for independent and assume PM Compared Part Institution Compared Part Institution C	Which Caterways Which Caterways Amage and the Amage and
Anne Anne Anne Anne Anne Anne Anne Anne	(2) Unified Endpoint Management and Mobile Security Data surgepted at Hittis Twee Datase. (2) Use fix evolves start is using order protect a factor	Server Protection Server and the anti-balance More space and the anti-balance More space and and protection More space and and protection More space and and protection More space and anti-balance To any set Loss are encoded more space The space and anti-balance more space The space and anti-balance more space

8. Um das Installationsprogramm zu starten, öffnen Sie den Ordner, und doppelklicken Sie dann auf **SophosSetup.exe**.

Hinweis: Wenn Antivirenprodukte auf Ihrer Appliance vorhanden sind, wird empfohlen, diese vor dem Starten des Installationsprogramms zu deinstallieren.

9. Klicken Sie auf Installieren.



10. Um die Appliance sofort neu zu starten, klicken Sie auf **Fertig stellen**. Um die Appliance später neu zu starten, deaktivieren Sie die Option **Jetzt Computer neu starten**.



11. Um den Schutzstatus anzuzeigen, öffnen Sie die Schnittstelle **Sophos Inter**cept X.

SOPHOS Status Ev	vents	Admin login – 🗙
Your com	puter is protected	Scan
Malware and PUAs O detections	Web Threats O requests blocked	Malicious Behavior O detections
(ii) Controlled Items O user notifications	Malicious Traffic O connections detected	© Exploits O detections
		Help About

Der Status gibt an, dass die Arcserve Appliance vor Ransomware-Angriffen, Malware, Webbedrohungen und Zero-Day-Exploits geschützt ist.

12. 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:

- Es ist erforderlich, dass Sie über Internetzugang in der Appliance verfügen, um "Sophos Intercept X Advanced" und alle dazugehörigen Updates zu installieren. Sophos Intercept X ist Cloud-basiert, und es sind keine Offline-Installationsprogramme verfügbar.
- Wenn Sie bereits eine andere Appliance erworben haben und über ein Sophos-Konto über Arcserve verfügen, verwenden Sie dasselbe Konto für alle Arcserve Appliances.
- 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 f
 ür Sophos Intercept X Advanced for Server wie Malwaredefinitionsupdates und Versionsaktualisierungen zu erhalten, benötigen Sie eine g
 ültige und aktive Wartung f
 ür Ihre Appliance.

Für weitere Unterstützung wenden Sie sich bitte telefonisch an den technischen Support von Arcserve (+1.844.765.7043), oder <u>online</u>, oder an Ihr lokales Arcserve-Supportbüro.

Kapitel 12: Aktualisieren der Firmware für Arcserve Appliance 9000 Series

Dieser Abschnitt enthält folgende Themen:

Upgrade der BIOS-Firmware für Arcserve Appliance 9000 Series	
Aktualisieren der iDRAC-Firmware für Arcserve Appliance 9000 Series	

Upgrade der BIOS-Firmware für Arcserve Appliance 9000 Series

In diesem Abschnitt wird beschrieben, wie Sie Folgendes tun können:

Anzeigen der BIOS-Firmwareversion

Verwenden Sie eine der folgenden Methoden, um die BIOS-Firmwareversion anzuzeigen:

- Methode 1: BIOS-Firmware-Version von iDRAC Web Interface anzeigen
- Methode 2: BIOS-Firmware-Version von BIOS Arcserve Appliance 9000 Series anzeigen

Methode 1: BIOS-Firmware-Version von iDRAC Web Interface anzeigen

- 1. Navigieren Sie zur iDRAC-Weboberfläche.
- 2. Um sich anzumelden, geben Sie Folgendes ein:
 - Benutzername: root
 - Kennwort: ARCADMIN

Integrated Remote Acce	ss Controller 9 Enterpris	e		
* Dashboard System	n∨ 🛢 Storage∨	Configuration >>	\blacksquare Maintenance \checkmark	0, iDRAC Settin
Graceful Shutdown Health Information	Identify System	More Actions •	rmation	
SYSTEM I	IS HEALTHY	Power State Model	ON	
System Health Healthy Details	Storage Health Healthy Details>	Host Name Operating System Operating System Version Service Tag BIOS Version	APPLIANCE9144 Windows Server 20 10.0 5Q6PHQ2 1.4.9	216
		iDRAC Firmware Version	3.21.21.21 s 4c:d9.8f04.c6.a4	

Auf der Seite iDRAC-Dashboard werden die Systeminformationen angezeigt, die die BIOS-Firmwareversion enthalten.

Methode 2: BIOS-Firmware-Version von BIOS Arcserve Appliance 9000 Series anzeigen

- 1. Wenn das System gestartet wird, drücken Sie F11, um Setup zu öffnen.
- Um die BIOS-Version anzuzeigen, navigieren Sie zu System-Setup > iDRAC-Einstellungen oder System-BIOS.

System Setup		Help About Exit
iDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.6.11	
iDRAC Firmware Version	3.21.23.22 (Build 7)	
iDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
IDRAC MAC Address	D0:94:66:7A:D7:B2	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	Yes	

Auf der Seite wird die Firmware-Version angezeigt.

System Setup		Help About Exit
iDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.4.9	
iDRAC Firmware Version	3.21.21.21 (Build 30)	
iDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
iDRAC MAC Address		
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	No	

Herunterladen des aktualisierten Pakets für BIOS

Sie können das neueste BIOS-Firmwarepaket eines bestimmten Modells der Arcserve Appliance 9000 Series von der <u>Dell</u>-Website herunterladen oder den Arcserve-Support kontaktieren.

BIOS aktualisieren

- 1. Kopieren Sie das Upgradepaket auf den lokalen Datenträger der Arcserve Appliance 9000 Series.
- 2. Starten Sie das Upgradepaket, und folgen Sie dann den Anweisungen, um das Upgrade abzuschließen.
- 3. Starten Sie das System neu, um das Update abzuschließen.



Hinweis: Stellen Sie sicher, dass alle Anwendungen geschlossen sind, bevor Sie den Aktualisierungsvorgang starten.



Überprüfen des aktualisierten BIOS

Verwenden Sie eine der folgenden Methoden:

- Überprüfen des aktualisierten BIOS mithilfe von Systemprotokollen
- Überprüfen des aktualisierten BIOS über iDRAC Web Interface oder BIOS

Überprüfen des aktualisierten BIOS mithilfe von Systemprotokollen

- Melden Sie sich bei iDRAC an, und navigieren Sie dann zu Wartung > SupportAssist > Starten einer Sammlung.
- 2. Überprüfen Sie das Protokoll, und stellen Sie sicher, dass während des Aktualisierungsvorgangs keine Fehler aufgetreten sind.

5CTNHQ2 > Hardwa	re → Logs → Lifecyd	le Log		
	2019-08-29 15:40:34	U5R0032	The session for root from 10.57.12.37 using GUI is logged off.	
	2019-08-29 15:10:35	SRV088	The SupportAssist Save to Local operation is successfully completed.	
	2019-08-29 15:10:34	SRV002	The SupportAssist Save to Local operation is started.	
	2019-08-29 15:10:20	SRV108	The SupportAssist job JID_670625874264 is completed.	
	2019-08-29 15:10:20	SRV088	The SupportAssist Collection operation is successfully completed.	
	2019-08-29 15:10:20	SRV096	The SupportAssist Collection TSR20190829021014_5CTNHQ2.zip is successfully created.	
	2019-08-29 15:10:13	SRV007	The SupportAssist System information collection operation is successfully completed.	
	2019-08-29 15:10:13	LOG009	The current Lifecycle Log is successfully created for the view or export operation.	
	2019-08-29 15:10:07	LOG008	The complete Lifecycle Log was successfully created for an export operation.	
	2019-08-29 15:09:47	SRV006	The SupportAssist System information collection operation is started.	
	2019-08-29 15:09:47	SRV001	The SupportAssist Collection operation is started by iDRAC_GUL	
	2019-08-29 15:09:47	SRV106	The Debug Logs are excluded from the SupportAssist collection because the Collection data is being filtered information.	for personally identifiable
	2019-08-29 15:09:47	SRV107	The Storage Logs are excluded from the SupportAssist collection because the Collection data is being filtere information.	d for personally identifiable
	2019 00 29 15:09:17	SRV007	The Support/axist Collection Job HD_070625074264 to successfully created	
	2019-08-29 15:09:25	RAC1195	User root via IP 10.57.12.37 requested state / configuration change to SupportAssist using GUI.	
	2019-08-29 15:08:53	SEL9901	OEM software event.	
	2019-08-29 15:08:53	OSE1002	C: boot completed.	
	2019-08-29 15:08:46	PR36	Version change detected for BIOS firmware. Previous version: 1.6.11, Current version: 2.2.11	

Überprüfen des aktualisierten BIOS über iDRAC Web Interface oder BIOS

Melden Sie sich bei der iDRAC-Weboberfläche an, oder geben Sie das System-BIOS ein, um die aktualisierte BIOS-Firmwareversion anzuzeigen.

Aktualisieren der iDRAC-Firmware für Arcserve Appliance 9000 Series

In diesem Abschnitt wird beschrieben, wie Sie Folgendes tun können:

Anzeigen der iDRAC-Firmwareversion

Verwenden Sie eine der folgenden Methoden, um die iDRAC-Firmwareversion anzuzeigen:

- Methode 1: iDRAC-Firmwareversion von iDRAC Web Interface anzeigen
- Methode 2: iDRAC-Firmwareversion von BIOS Arcserve Appliance 9000 Series anzeigen

iDRAC-Firmwareversion von iDRAC Web Interface anzeigen

Befolgen Sie diese Schritte:

- 1. Navigieren Sie zur iDRAC-Weboberfläche.
- 2. Um sich anzumelden, geben Sie Folgendes ein:
 - Benutzername: root
 - Kennwort: ARCADMIN

Integrated Hemote Aco	ess Controller 9 Enterpr	se		
🕈 Dashboard 🛛 🗏 Syste	m∨ ≣ Storage∨	Configuration V	Maintenance V	0. iDRAC Settings
Dashboard				
O Graceful Shutdown	Identify System	More Actions 👻		
Health Information		System Inform	mation	ç
	IO USALTUN	Power State	ON	
STSTEM	IS HEALTHY	Model		
System Health	Storage Health	Host Name	APPLIANCE9144	
Healthy Details	Healthy Details	Operating System	Windows Server 2016	5
		Operating System Version	10.0	
		Service Tag	5Q6PHQ2	
		BIOS Version	1.4.9	
		iDRAC Firmware Version	3.21.21.21	
		200101410144	1-10-01-01-01-01	

Das iDRAC-Dashboard zeigt die Systeminformationen an, die die iDRAC-Firmwareversion enthalten.

integrated Remote Access Controller 9 Enterprise							
 Maintenance ∨ 0_* iDRAC Settings ∨ Dashboard System ∨ System Oraceful Shutdown Identify System More Actions 							
Health Information							
SYSTEM	IS HEALTHY	Power State Model	ON				
System Health	Storage Health	Host Name Operating System	appliance9012 Microsoft Windows 2016 Server, Stan dard x64 Edition				
		Operating System Version	Version 10.0 (Build 14393) (x64)				
		Service Tag	SCTNHQ2				
		BIOS Version	1.6.11				
		iDRAC Firmware Version	3 21 23 22				
		IDRAC MAC Address	d0.94.66.7a.d7.b2				

Methode 2: iDRAC-Firmwareversion von BIOS Arcserve Appliance 9000 Series anzeigen

Befolgen Sie diese Schritte:

- 1. Wenn das System gestartet wird, drücken Sie F11, um Setup zu öffnen.
- 2. Um die iDRAC-Version anzuzeigen, navigieren Sie zu System-Setup > iDRAC-Einstellungen oder System-BIOS.

System Setup		Help About Exit
iDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.6.11	
IDRAC Firmware Version	3.21.23.22 (Build 7)	
IDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
iDRAC MAC Address	D0:94:66:7A:D7:B2	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	Yes	

Auf der Seite wird die Firmware-Version angezeigt.

System Setup		Help About Exit
iDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.4.9	
iDRAC Firmware Version	3.21.21.21 (Build 30)	
IDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
iDRAC MAC Address	54:48:10:FB:C5:20	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	No	

Herunterladen des aktualisierten Pakets für iDRAC

Sie können das neueste iDRAC-Firmwarepaket eines bestimmten Modells der Arcserve Appliance 9000 Series von der <u>Dell</u>-Website herunterladen oder den Arcserve-Support kontaktieren.

iDRAC aktualisieren

Befolgen Sie diese Schritte:

- 1. Kopieren Sie das Upgradepaket auf den lokalen Datenträger der Arcserve Appliance 9000 Series.
- 2. Starten Sie das Upgradepaket, und folgen Sie dann den Anweisungen, um das Upgrade abzuschließen.

Hinweis: Stellen Sie sicher, dass alle Anwendungen geschlossen sind, bevor Sie den Aktualisierungsvorgang starten.

iDRAC with	Lifecycle Controller 3.34.34.34, A00
.1	
Success	×
•	Device: iDRAC, Application: iDRAC Update Successful.
1	The update completed successfully.
Bunning val	OK I
	Elapsed time: 6m13s

3. Während des Aktualisierungsvorgangs wird die Verbindung zwischen iDRAC und der virtuellen Konsole einige Minuten lang getrennt. Melden Sie sich bei iDRAC an, und starten Sie die virtuelle Konsole neu. Das Upgrade wird

jetzt abgeschlossen.

Integrated Remote Access Controller 9 Enterprise									
👬 Dashboard 🗉 System V 😺 Storage V 💷 Configuration V 🖂 Maintenance V 💁 IDRAC Settings V									
Dashboard									
Craceful Shuddown + I identify System More Actions +									
III Health Informat	II Health Information II System Information								
		IO LICALTUN		Power State	ON				
SYSTEM IS HEALTHY				Model					
System Health Storage Health				Host Name	WIN-SUQL6R8CBIC				
S Healthy	Detailsa	S Healthy	Details+	Operating System	Microsoft Windows 2016 Server, Standard x64 Edition				
		,		Operating System Version	Version 10.0 (Build 17763) (x64)				
			Service Tag	606//HQ2					
				BIOS Version	2.2.11				
				IDRAC Firmware Version	3.34.34.34				
				IDRAC MAC Address	54.48.10 fb:c5.20				

Überprüfen des aktualisierten BIOS

Verwenden Sie eine der folgenden Methoden:

- Überprüfen des aktualisierten iDRAC mithilfe von Systemprotokollen
- Überprüfen des aktualisierten iDRAC von iDRAC Web Interface oder BIOS

Überprüfen des aktualisierten iDRAC mithilfe von Systemprotokollen

- Melden Sie sich bei iDRAC an, und navigieren Sie dann zu Wartung > SupportAssist > Starten einer Sammlung.
- 2. Überprüfen Sie das Protokoll, und stellen Sie sicher, dass während des

2019-08-29 09:31:51 VME0007 Virtual Console session created. 2019-08-29 09:31:51 VM60001 Virtual Console session started. 2019-00-29 09:31:51 USR0030 Successfully logged in using root, from 50:57:12:37 and W
 2019-06-29
 09/31-45
 USR0000
 Successfully logged in using mot. from 50:57:12:37 and GUR.

 2019-06-29
 09/28:22
 RA/C0721
 Remote share mounted successfully/192:57:25:8/tool/come
 2019-08-29 09:28:56 DIS002 Auto Discovery feature disabled. 2019-06-29 09:20:25 IPA0500 The IDBAC IP Address changed from 0.0.0.0 to 10.57:25:23. 2019-08-29 09-28:54 PR36 Version-change detected for Lifecycle Controller firmware. Previous version:321.23.22, Current version:3.34.34.34 2019-06-29 09:20:12 RAC0182 The IDRAC firmware was reborded with the following reason user initiated. 2019-06-29 09:27:22 P50000 Power Septh 2: 50:55 = 0:4; IOUT = 0:4; VOUT = 0:4; IOUT = 0:4; 2019-06-29 09:25:58 SUP1906 Firmware update successful. 2019-06-29 09:24:23 SUP1905 Firmware update programming flash. 2019-06-29 OR:24:22 SUP1903 Firmware update verify image headers. 2019-06-29 09-24-16 SUP1904 Firmware update checkoumming image. 2019-00-29 09:24:55 SUP1911 Firmware update initialization complete
 2019-06-29
 09:24:55
 50:P1511
 Firmware update initialization complete.

 2019-06-29
 09:24:56
 50:P1501
 Firmware update initializing.

 2019-06-29
 09:02:59
 L00:205
 Lifecycle Log and head update initializing.
 2019-08-29 09:02:56 SEL9901 OEM software event. 2019-08-29-08-02:55 OSE1002 C-boot-completed. 2019-08-29-08-02:22 SYS1003 System CPU Resetting. 2019-08-29 08-42-17 5Y51000 System is turning on. 2019-00-29 08-42-07 SYS1001 System's turning off. 2019-08-29-08-42-07 SY51003 System/CPU Resetting 2019-08-29 08-40:28 LOG009 The surrent Lifecycle Logie au

Aktualisierungsvorgangs keine Fehler aufgetreten sind.

Überprüfen des aktualisierten iDRAC von iDRAC Web Interface oder BIOS

Melden Sie sich bei der iDRAC-Weboberfläche an, oder geben Sie das System-BIOS ein, um die aktualisierte BIOS-Firmwareversion anzuzeigen.

Kapitel 13: Fehlerbehebung

Dieser Abschnitt enthält folgende Themen:

Linux-Sicherungsserver kann über die Konsole keine Verbindung herstellen	266
Sichern einer Arcserve Applianceaus duplizierten Knoten anderer Appliance-Berichte	268
Linux-Sicherungsserver kann nicht mit einem Knoten im Netzwerk kommunizieren	269
Linux-Sicherungsserver kann das Netzwerk-DNS-Suffix nicht abrufen	.271
Standardzeitzone auf der Appliance	.272
Lizenzfehler, auch wenn Lizenzen verfügbar sind	.273
ARCserve UDP-Konsole zeigt beim Hinzufügen einer replizierten Remote-Konsole zu einer remote verwalteten RPS-Task einen Fehler an	274
Die VSB-Task kann nicht mit einer anderen Appliance als Überwachungsserver durch- geführt werden	276

Linux-Sicherungsserver kann über die Konsole keine Verbindung herstellen

Problem

Wenn ich versuche, über die Arcserve UDP-Konsole eine Verbindung mit meinem Linux-Sicherungsserver herzustellen, schlägt der Verbindungsversuch fehl und ich sehe ein rotes Zeichen.

Lösung

Wenn Verbindungsversuche über die Konsole zu einem Linux-Sicherungsserver fehlschlagen, können Sie die Verbindung auf Fehler untersuchen, um das Problem zu ermitteln.

Fehlersuche bei einem Verbindungsproblem

- 1. Starten Sie den Hyper-V-Manager, stellen Sie eine Verbindung mit dem virtuellen Rechner des Linux-Sicherungsservers her und melden Sie sich an.
- 2. Führen Sie folgenden Befehl aus:

service network restart

3. Überprüfen Sie, ob die dem Linux-Sicherungsserver zugewiesene IP-Adresse 192.168.10.2 ist. Um dies zu überprüfen, führen Sie den folgenden Befehl aus:

ifconfig

- 4. Wenn die IP-Adresse 192.168.10.2 lautet, navigieren Sie zu der Arcserve UDP-Konsole und aktualisieren Sie den Linux-Sicherungsserver-Knoten, mit dem Sie gerade versuchen, eine Verbindung herzustellen.
- Lautet die IP-Adresse nicht 192.168.10.2, befolgen Sie die Anweisungen im Abschnitt "Fehlerbehebung über die DHCP Microsoft Management Console (MMC)".

Fehlerbehebung über die DHCP Microsoft Management Console (MMC)

Wichtig! Stellen Sie sicher, dass der DHCP-Server-Dienst auf der Appliance ordnungsgemäß ausgeführt wird.

- 1. Starten Sie die DHCP-MMC über Server-Manager, Extras, DHCP.
- 2. Erweitern Sie den Linux-Server-Knoten, IPV4 und Bereich, und stellen Sie sicher, dass der Bereich mit dem Namen 192.168.10.0 in diesem Knoten enthalten ist.

- 3. Erweitern Sie die Adressen-Leases, und löschen Sie alle anderen Lease-Einträge.
- 4. Melden Sie sich beim Linux-Sicherungsserver an, und führen Sie den folgenden Befehl aus:

service network restart

5. Navigieren Sie zu der Arcserve UDP-Konsole und aktualisieren Sie den Linux-Sicherungsserver-Knoten, mit dem Sie gerade versuchen, eine Verbindung herzustellen.

Jetzt kann über die Konsole eine Verbindung zum Linux-Sicherungsserver hergestellt werden.

Sichern einer Arcserve Applianceaus duplizierten Knoten anderer Appliance-Berichte

Problem

Beim Sichern der Appliance B von der Appliance A aus erhalte ich die folgende Fehlermeldung im Aktivitätsprotokoll:

"Die folgenden Knoten sind dupliziert: Appliance_B, Appliance_A. Daher haben sie dieselbe Agenten-ID, was zu unerwarteten Ergebnissen führen kann. Das Problem duplizierter Knoten kann entstehen, wenn der Knoten mit einem anderen Knotennamen (z. B. dem DNS-Namen oder der IP-Adresse) hinzugefügt wurde oder wenn einige Rechner durch Klonen voneinander eingerichtet wurden."

Fall 1: Appliance B wird als RPS zur UDP-Konsole von Appliance A hinzugefügt.

Beispiel: Auf Appliance B können Sie die Appliance mit dem UDP-Assistenten konfigurieren und Folgendes wählen: "Diese Appliance funktioniert als Instanz des Arcserve UDP Recovery Point Server, der von einer anderen Arcserve UDP-Konsole verwaltet wird."

Lösung

- 1. Halten Sie den Datenspeicher auf dem Appliance-B-Knoten vom RPS-Bereich der UDP-Konsole aus an.
- Melden Sie sich bei Appliance B an, und löschen Sie den Registrierungsschlüssel der Knoten-ID, die sich unter [HKEY_LOCAL_ MACHINE\SOFTWARE\CA\ARCserve Unified Data Protection\Engine] befindet.
- Starten Sie den Arcserve UDP Agent Web Service vom Appliance-B-Knoten aus neu.
- 4. Starten Sie den Arcserve UDP RPS-Datenspeicherdienst vom Appliance-B-Knoten aus neu.
- 5. Gehen Sie in der UDP-Konsole zum Bereich "Knoten", "Alle Knoten", und aktualisieren Sie den Appliance-B-Knoten.
- 6. Gehen Sie zum Bereich "Recovery Point Server", und aktualisieren Sie den Appliance-B-Knoten.
- 7. Importieren Sie den vorhandenen Datenspeicher mit dem ursprünglichen Sicherungsziel auf den Appliance-B-RPS.

Fall 2: Appliance B wird nur als Agent-Knoten zur UDP-Konsole von Appliance A hinzugefügt.

Beispiel: Ein Plan schützt Appliance B über eine agentenbasierte Sicherungsaufgabe auf der UDP-Konsole von Appliance A.

- Melden Sie sich bei Appliance B an, und löschen Sie den Registrierungsschlüssel der Knoten-ID, die sich unter [HKEY_LOCAL_ MACHINE\SOFTWARE\Arcserve Unified Data Protection\Engine] befindet.
- 2. Starten Sie den Arcserve UDP Agent-Dienst von Appliance B aus neu.
- 3. Gehen Sie in der UDP-Konsole zum Bereich "Knoten", "Alle Knoten", und aktualisieren Sie den Knoten von Appliance B aus.

Linux-Sicherungsserver kann nicht mit einem Knoten im Netzwerk kommunizieren

Problem

Linux-Sicherungsserver kann nicht mit einem Knoten im Netzwerk kommunizieren

Lösung

Wenn der Appliance-Windows-Server nicht mit einem Knoten im Netzwerk kommunizieren kann, kann der Linux-Sicherungsserver auch nicht mit einem Knoten kommunizieren.

Befolgen Sie diese Schritte:

- 1. Überprüfen Sie, ob der Knoten vom Appliance-Windows-Server aus verfügbar ist.
- 2. Navigieren Sie zu folgendem Speicherort, um zu überprüfen, ob der Netzwerkadapter LinuxBkpSvr vorhanden ist, wie im Folgenden dargestellt:

```
Bedienfeld > Netzwerk und Internet > Netz-
werkverbindungen
```

3. Wenn LinuxBkpSvr nicht verfügbar ist, navigieren Sie zum folgenden Speicherort, und überprüfen Sie, ob die Flag-Datei adapterNameChanged.flag vorhanden ist:

```
C:\Programme\Arcserve\Unified Data Pro-
tection\Engine\BIN\Appliance
```

Falls vorhanden, entfernen Sie die Datei adapterNameChanged.flag.

4. Navigieren Sie zum folgenden Speicherort, und starten Sie Routing und RAS-Management:

Server-Manager > Tools > Routing und Remote-Zugriff

5. Überprüfen Sie, ob alle verfügbaren Netzwerkschnittstellen und LinuxBkpSvr zum NAT hinzugefügt werden, wie im Folgenden dargestellt.

Wenn alle Netzwerkschnittstellen und LinuxBkpSvr bereits aufgelistet sind, überprüfen Sie, ob die verschiedenen physischen Netzwerkschnittstellen mit anderen Sub-Netzwerk verbunden sind. Diese Aktion löst das Kommunikationsproblem des Linux-Sicherungsservers.

Wenn alle Netzwerkschnittstellen und *LinuxBkpSvr* aufgeführt sind, fahren Sie mit dem nächsten Schritt fort.

6. Löschen Sie die Datei dhcpdone.flag von folgendem Speicherort:

```
C:\Programme\Arcserve\Unified Data Pro-
tection\Engine\BIN\Appliance
```

 Geben Sie mithilfe der Befehlszeile den Ordner c:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance ein, und führen Sie resetdhcp.ps1 (siehe unten) aus.

C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance>powershell.\resetdhcp.ps1

Wenn das Skript erfolgreich ausgeführt wird, wird das Kommunikationsproblem für den Linux-Sicherungsserver gelöst.

Linux-Sicherungsserver kann das Netzwerk-DNS-Suffix nicht abrufen

Wenn Sie die statische IP-Adresse auf den Appliance-Server festlegen, kann nach dem Neustart des Netzwerkdiensts das Netzwerk-DNS-Suffix nicht ordnungsgemäß vom Linux-Sicherungsserver abgerufen werden. Dies führt zu Kommunikationsproblemen zwischen dem Linux-Sicherungsserver und der UDP-Konsole. Sie können dann aufgrund der Kommunikationsprobleme diesen Linux-Sicherungsserver nicht mehr verwenden, um den Linux-Knoten zu schützen.

Problem

Der Status des Linux-Sicherungsservers wird auf der UDP-Konsole als getrennt angezeigt. Der **Aktualisierungsknoten** kann den Linux-Sicherungsserver nicht erfolgreich aktualisieren, und das gelbe Warnsymbol ändert sich nicht in Grün. Dies tritt auf, wenn die statische IP-Adresse auf den Appliance-Server festgelegt ist, aufgrund dessen der Linux-Sicherungsserver dann das DNS-Netzwerksuffix nicht ordnungsgemäß abrufen kann.

Lösung

Um dieses Problem zu lösen, können Sie die Datei "file/etc/resolv.conf" direkt auf dem Linux-Rechner mit dem richtigen DNS-Suffix aktualisieren.

Standardzeitzone auf der Appliance

Problem

Die Standardzeitzone ist (UTC-08:00) Pacific Time (USA und Kanada), unabhängig davon, welche Region Sie auswählen, wenn Sie die Appliance erstmalig in Betrieb nehmen.

Lösung

Navigieren Sie zum Arcserve Backup Appliance-Assistenten, klicken Sie auf Bearbeiten, und legen Sie Datum und Uhrzeit fest, um die Zeitzone zu ändern.

Lizenzfehler, auch wenn Lizenzen verfügbar sind

Weitere Informationen zu lizenzbezogenen Fehlern in der Appliance bei verfügbaren Lizenzen finden Sie über den Link.

ARCserve UDP-Konsole zeigt beim Hinzufügen einer replizierten Remote-Konsole zu einer remote verwalteten RPS-Task einen Fehler an

Wenn Sie bei Arcserve UDP-Appliance v6.5 Update1 einen Task Zu einem remote verwalteten RPS replizieren hinzufügen und den Hostnamen/die IP eines anderen Appliance-Rechners als Recovery Point Server (RPS) in das Feld Remote-Konsole eingeben, wird folgende Fehlermeldung in der Arcserve UDP-Konsole angezeigt.

Hinweis: Dieser Fehler wird in einerArcserve Appliance mit der Standardversion Arcserve UDP v6.5 Update 3 oder höher behoben.

Fehlermeldung: Wählen Sie eine Remote-Konsole aus.

resources			
Modify a Plan	Agent-Based Windows Backup Plan	Pause this plan	Save Cancel Help
Task1: Backup: Agent-Based 📀 Windows	Task Type Replicate to a remote	ely-managed RPS 👻	⊗ Delete Task
Task2: Replicate to a remotely- managed RPS	Source Destination	n Schedule	
	Remote Console	10.10.255.255 (administrator) 👻 0	Add
Add a Task	Username	administrator	Please select a remote console.
Product Installation	Password		
	Port	8015	
	Protocol Enable Proxy:	○ HTTP ● HTTPS	
		Connect	

Dieses Problem entsteht durch die Verwendung derselben GUID auf der lokalen und der Remote-Konsole.

Gehen Sie folgendermaßen vor, um den remote verwalteten RPS-Task auf einer anderen Appliance zu unterstützen:

1. Löschen Sie die GUID auf der lokalen Appliance aus dem folgenden Registrierungspfad:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Management\Console\GUID

2. Löschen Sie die GUID aus der Datenbank mithilfe der folgenden Befehle in PowerShell:

\$database = 'arcserveUDP'
\$server = 'localhost\arcserve_app'
\$sqlconn = New-Object System.Data.SqlClient.SqlConnection
\$sqlconn.ConnectionString = "Data Source=\$server;Initial Catalog=\$database;Integrated Security=SSPI;"
\$sqlconn.Open()
\$sqlcmd = New-Object System.Data.SqlClient.SqlCommand
\$sqlcmd.Connection = \$sqlconn
\$sqlcmd.CommandText = "delete from as_edge_configuration where ParamKey='ConsoleUuid'''
\$sqlcmd.ExecuteNonQuery()
\$sqlconn.Close()

- 3. Starten Sie den UDP Management Service auf dem lokalen Appliance-Rechner.
- 4. Führen Sie die folgenden Schritte in der UDP-Konsole des lokalen Rechners aus:
 - a. Wählen Sie Alle Knoten in der Knotenansicht.
 - b. Klicken Sie mit der rechten Maustaste, und klicken Sie auf Aktualisieren.
 - c. Klicken Sie auf **OK**, um alle Knoten zu aktualisieren.
- 5. Wählen Sie alle RPS-Knoten in der Ansicht "Recovery Point Servers" aus, klicken Sie mit der rechten Maustaste, und klicken Sie auf **Aktualisieren**, um alle RPS-Knoten zu aktualisieren.

Der Task Zu einem remote verwalteten RPS replizieren wird zwischen zwei Appliance-Rechnern erfolgreich unterstützt.

Die VSB-Task kann nicht mit einer anderen Appliance als Überwachungsserver durchgeführt werden

Wenn Sie auf Arcserve Appliance v6.5 Update1 einen VSB-Task durchführen und eine andere Appliance als Monitor verwenden, schlägt der VSB-Task fehl, und im Aktivitätsprotokoll wird die folgende Fehlermeldung angezeigt.

Hinweis: Dieses Problem wurde für die Arcserve Appliance mit der Standardversion Arcserve UDP v6.5 Update 3 oder höher behoben.

CITCSETVE [®] unified data protection							ages (1) ,	administrator	• Help •
da	ashboard resour	rces jobs	reports log	settings	high availabili	ty			
Severity	All	Node Name	10.10.255.255	× Job ID 3	× J	ob Type Virtual S	tandby -	Pafrash Pasat	Export Dalata
Time	All	Generated From	vsb2	× Message	×			Reflesii Reset	Export Delete
Severity	Time	SiteName	Node Name	Generated From	n Job ID	Job Type	Message		
0	7/18/2017 3:04:20 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	The Virtual Standb	y job failed.	
0	7/18/2017 3:04:20 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	Synchronize source	e machine adapter i	nformation to Virtual Standby
0	7/18/2017 3:04:20 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	The Virtual Standb	y job copied data to	aling 0 Bytes, the elapsed tim
0	7/18/2017 3:04:20 AM	Local Site		vsb2	3	Virtual Sta	Failed to convert s	ession S000000000	to the host for VM [UDPVM]
0	7/18/2017 3:04:20 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	An unexpected err new backup to sta	or has occurred whe rt the Virtual Standby	n attempting to convert session (job. If the problem persists, (
0	7/18/2017 3:04:20 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	Failed to connect t	o remote server [10.	57.21.10], port = 4090.
0	7/18/2017 3:02:40 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	Failed to connect t	o remote server [10.	57.21.10], port = 4090.
0	7/18/2017 3:01:28 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	Try VDDK advano	ed transport mode (S	AN or HotAdd).
0	7/18/2017 3:01:12 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	Upload meta data	to VM [UDPVM_WIN	I-92KBNU8J439].
0	7/18/2017 3:01:12 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	Begin to convert s	ession S000000000	4.
0	7/18/2017 3:01:12 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	Virtual Standby job	will convert session	S000000001.
0	7/18/2017 3:01:04 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	VM was created. \	/M name is [UDPVM	_WIN-92KBNU8J439].
0	7/18/2017 3:00:49 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	The source machin 971de742d347]] o	ne is [10.57.27.33], t n Recovery Point Se	he backup destination is [X:Va rver [vsb2], and the data store
0	7/18/2017 3:00:48 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	The monitor serve	r is [10.57.21.10] and	is used as a proxy for data tr
0	7/18/2017 3:00:48 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	Start a Virtual Star	ndby job with destina	tion type VMware ESX Server
0	7/18/2017 3:00:48 AM	Local Site	10.10.255.255	vsb2	3	Virtual Sta	Virtual Standby job	started.	

Fehlermeldung: Verbindung zum Remote-Server fehlgeschlagen [IP], port = 4090.

Dieses Problem entsteht dadurch, dass dieselbe GUID sowohl auf der Monitor-Appliance als auch auf dem Arcserve UDP-RPS-Appliance-Rechner vorhanden ist.

Gehen Sie folgendermaßen vor, um den VSB Task zu unterstützen:

1. Beenden Sie alle UDP-Dienste auf Arcserve UDP-RPS-Appliance mit dem folgenden Befehl in der Befehlszeile:

C:\Programme\Arcserve\Unified Data Protection\Management\BIN> cmdutil.exe /stopall

2. Löschen Sie die GUID auf der lokalen Appliance mit dem folgenden Registrierungspfad: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\GUID

3. Starten Sie alle UDP-Dienste auf Arcserve UDP-RPS-Appliance mit dem folgenden Befehl in der Befehlszeile:

C:*Program Files**Arcserve**Unified Data Protection**Management**BIN> cmdutil.exe /startall*

- 4. Gehen Sie von der UDP-Konsole des lokalen Rechners aus folgendermaßen vor:
 - a. Wählen Sie in der Pläneansicht die Option Alle Pläne aus.
 - b. Klicken Sie mit der rechten Maustaste, und klicken Sie auf Jetzt bereitstellen.
 - c. Klicken Sie auf **OK**, um alle Pläne bereitzustellen.

Die Aufgabe "Virtual Standby" wird jetzt unterstützt.

Kapitel 14: Best Practices

In diesem Abschnitt werden die folgenden Themen behandelt:

Best Practices für die Netzwerkkonfiguration	. 279
Best Practices für Windows-Defender mit PowerShell-cmdlets	. 282
Konfigurieren des vorinstallierten Linux-Sicherungsservers für externes Netzwerk	. 282
Bewährte Methoden zum Ersetzen des Werkseinstellungs-Image wenn mit Sophos gesichert	.283
Bewährte Verfahren zum Erstellen von Deduplizierungsdatenspeichern über Volu- mes hinweg	293
Best Practices für die Netzwerkkonfiguration

- Wenn mehrere Netzwerkschnittstellen in der Produktionsumgebung verbunden sind, stellen Sie sicher, dass die einzelnen Netzwerkadapter mit unterschiedlichen Subnetzwerken verbunden sind.
- Wenn in der zu schützenden Produktionsumgebung kein Linux-Knoten vorhanden ist, empfehlen wir, VM Linux-BackupSvr, den DHCP-Server-Dienst und den RRAS auf der Appliance anzuhalten.

Weitere Informationen finden Sie unter Deaktivieren des DHCP-Servers.

Wenn sowohl der Appliance als auch die Agent-Knoten auf dem gleichen Subnetzwerk online sind, tritt ein Verbindungsproblem zwischen der Appliance und einen Agent-Knoten auf, wenn mehrere Netzwerkschnittstellen mit dem gleichen Subnetzwerk in der Appliance verbunden sind.

Problem

Wenn die Appliance und die Agent-Knoten auf dem gleichen Subnetzwerk online sind, können die folgenden Symptome auftreten:

 In der Arcserve UDP-Konsole wird bei der Bereitstellung des Plans f
ür den Agent-Knoten folgende Fehlermeldung angezeigt:

Error	×
Onable to apply 'backup settings' to node '10.57.52.13'. (Failed to connect to Arcserve UDP Recovery Point Server appliatest76. Verify that server name, port number, and protocol (http/https) inputs are all correct and the web service is started on the specified host. For other reasons, see Troubleshooting in the User Guide.)	
OK	

 Der Sicherungsjob des Agent-Knotens schlägt wie unten angegeben fehl:

0	12/25/ Local Site	10.57.52.13	10.57.52.13	26	Backup	Pailed to run backup job. Pailed to connect to Arcserve UDP Recovery Point Server appliatest76. Verify that server name, port number, and protocol (http/https) inputs are all correct and the web service is started on the specified host. For other reasons, see Troubleshooting
-						in the User Guide.

 Pingen Sie den Agent-Knoten von der Appliance, und überprüfen Sie, ob der Agent-Knoten verbunden ist:

C:∖Windows\system32>pin;	g 10.57.52	.13	
Pinging 10.57.52.13 wit	h 32 bytes	of data:	
Reply from 10.57.52.13:	bytes=32	time<1ms	TTL=127
Reply from 10.57.52.13:	bytes=32	time=1ms	TTL=127
Reply from 10.57.52.13:	bytes=32	time<1ms	TTL=127
Reply from 10.57.52.13:	bytes=32	time<1ms	TTL=127

 Pingen Sie den Appliance-Hostnamen vom Agent-Knoten, wenn die Appliance NICHT verbunden ist:

C:\Users	s∖Administrate	or≻ping appliat	test76		
Pinging Request Request Request Request	appliatest76 timed out. timed out. timed out. timed out.	[10.57.52.47]	with 32	2 bytes	of data:
Ping sta Pacł	atistics for : kets: Sent = 4	10.57.52.47: 4, Received = 6), Lost	= 4 (10	10% loss),

Lösung

Um das Verbindungsproblem zwischen der Appliance und dem Agent-Knoten zu beheben, führen Sie einen der folgenden Schritte aus:

 Wenn kein Linux-Knoten in der Produktionsumgebung verfügbar ist, halten Sie den DHCP-Server-Dienst und RRAS-Dienst auf der Appliance an, und überprüfen Sie, ob das Problem behoben wurde.

Weitere Informationen finden Sie unter <u>Deaktivieren des DHCP-</u> <u>Servers</u>.

 Gehen Sie auf der Appliance und auf dem Agent-Knoten folgendermaßen vor:

Schritte auf der Appliance:

- Führen Sie *ipconfig /all* in der DOS-Befehlseingabeaufforderung aus, um die verfügbaren IPv4-Adressen auf der Appliance zu erhalten:
- 2. Führen Sie *Route Print* in der DOS-Befehlseingabeaufforderung aus, um die IPv4-Routentabelle abzurufen, und zeichnen Sie die Reihenfolge für alle verfügbaren IPv4-Adressen auf der App-

liance auf:

IPv4 Route Table				
Active Routes:				=====
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0	0.0.0	10.57.52.1	10.57.52.46	10
0.0.0.0	0.0.0.0	10.57.52.1	10.57.52.35	10
0.0.0	0.0.0.0	10.57.52.1	10.57.52.45	10
0.0.0	0.0.0.0	10.57.52.1	10.57.52.47	10
10.57.52.0	255.255.255.0	On-link	10.57.52.46	266
10.57.52.0	255.255.255.0	On-link	10.57.52.35	266
10.57.52.0	255.255.255.0	On-link	10.57.52.45	266

Schritte auf dem Agent-Knoten:

 Versuchen Sie über die DOS-Befehlseingabeaufforderung, jede verfügbare IPv4-Adresse der Appliance einzeln gemäß der obigen Reihenfolge zu pingen, um die erste IPv4 der Appliance abzurufen, die auf dem Agent-Knoten verbunden ist:

C:\Users\Administrator>j	ping 10.57.52.46
Pinging 10.57.52.46 wit)	h 32 bytes of data:
Reply from 10.57.52.46:	bytes=32 time<1ms TTL=128
Reply from 10.57.52.46:	bytes=32 time<1ms TTL=128
Reply from 10.57.52.46:	bytes=32 time<1ms TTL=128
Reply from 10.57.52.46:	bytes=32 time<1ms TTL=128

2. Ändern Sie die Datei C:\Windows\System32\drivers\etc\hosts, um einen Datensatz für das Paar oben abgerufene IPv4/Appliance-Hostname hinzuzufügen und die Datei zu speichern.

Best Practices für Windows-Defender mit PowerShellcmdlets

Sie können die Defender-cmdlets mithilfe der folgenden Befehle abrufen:

- PS C:\> (Get-MpPreference).ExclusionPath
 Ruft den Ausschlusspfad von Defender ab.
- PS C:\> (Get-MpPreference).ExclusionProcess
 Ruft Ausschlussprozesse von Defender ab.
- PS C:\> Add-MpPreference -ExclusionPath "full_path_of_the_folder_or_file"
 Ordner oder Dateien der Ausschlussliste werden ausgeschlossen.
- PS C:\> Add-MpPreference -ExclusionProcess "full_path_of_executable_programs"

Dateien, die durch die Prozesse geöffnet wurden, werden ausgeschlossen.

PS C:\> Remove-MpPreference –ExclusionPath "full_path_of_the_folder"
 Entfernt einen Ordner aus der Ausschlussliste.

Konfigurieren des vorinstallierten Linux-Sicherungsservers für externes Netzwerk

Befolgen Sie diese Schritte:

- 1. Deaktivieren Sie den DHCP-Server. Weitere Informationen finden Sie unter Deaktivieren des DHCP-Servers.
- 2. Öffnen Sie zum Deaktivieren von RRAS "Routing und RAS", und klicken Sie auf **Routing und RAS deaktivieren**.

🚊 Routing and	Remote Access	– 🗆 X			
File Action \	/iew Help				
(+ + 🔃 🕻					
Routing and F	emote Access Routing and Remote Access				
APPLI	Configure and Enable Routing and Remote Access	mote Access			
🔄 Re	Disable Routing and Remote Access	secure remote access to			
~ <u>∎</u> ₽	Enable DirectAccess	nfigure the following: rivate networks. eway.			
페이지	All Tasks				
별 이 별 <	Delete Refresh	chuy.			
	Properties				
	Help	server, on the Action menu,			
	click Add Server.				

- 3. Gehen Sie wie folgt vor, um Linux-Sicherungsservernetzwerk auf ein externes Netzwerk festzulegen:
 - a. Öffnen Sie den Hyper-V-Manager.
 - b. Erstellen Sie einen neuen externen virtuellen Netzwerk-Switch.
 - c. Ändern Sie die Einstellung des VM-Netzwerkadapters f
 ür den Linux-Sicherungsserver, um den neu erstellten externen virtuellen Netzwerk-Switch zu verwenden.
 - d. Überprüfen Sie die Netzwerkeinstellung des Linux-Sicherungsservers, und stellen Sie sicher, dass die IP-Adresse und das DNS über den externen virtuellen Netzwerk-Switch abgerufen werden.
 - e. Entfernen Sie den ursprünglichen Linux-Sicherungsserver aus der UDP-Konsole.
 - f. Fügen Sie den Linux-Sicherungsserver mit Angabe der folgenden Informationen erneut zur UDP-Konsole hinzu:
 - Hostname: Linux-BackupSvr
 - Port: 8014

Bewährte Methoden zum Ersetzen des Werkseinstellungs-Image wenn mit Sophos gesichert

Nachdem Sophos aktiviert wurde und auf Arcserve Appliance ausgeführt wurde, können Sie das Werkseinstellungs-Image standardmäßig nicht mit dem Set

Appliance Image Utility ersetzen. Andernfalls schlägt die Ausführung von Setlmage.exe fehl, wie in der Abbildung unten gezeigt.



Bevor Sie den Befehl SetImage.exe ausführen, um das Werkseinstellungs-Image zu ersetzen, wenn Sophos auf Arcserve Appliance ausgeführt wird, überprüfen Sie, ob das Image bereits bereitgestellt wurde.

Wie in der Abbildung angegeben, wird die folgende Eingabeaufforderung angezeigt: Ein Unterverzeichnis oder eine Datei C:\Programmdateien\Arcserve\Unified Data Protection\Management\BIN\Appliance\mount ist bereits vorhanden.



Führen Sie die folgenden Schritte aus, um die Bereitstellung des Bildes aufzuheben:

 Um den Ordner zu suchen, öffnen Sie Windows-Explorer, und wechseln Sie zu C:\Programmdateien\Arcserve\Unified Data Protection\Management\BIN\Appliance\mount. Klicken Sie mit der rechten Maustaste auf den Ordner, und klicken Sie dann auf "Eigenschaften > Registerkarte Sicherheit > Erweitert".

mount Properties			×
Previous Versions	Customize	N	IFS Sharing
General	Sharing		Security
Object name: C:\Pro	gram Files\Arcsen	ve\Unified D	ata Protection
Group or user names:			
SCREATOR OWN	ER		
SYSTEM			
🚨 Administrators 🛲	Administrato	ors)	
Sers (initialitie), U	lsers)		
To change permissions	, click Edit.		Edit
Permissions for CREAT OWNER	OR	Allow	Deny
Full control			^
Modify			
Read & execute			
List folder contents			
Read			
Write			~
For special permissions click Advanced.	or advanced setti	ngs,	Advanced
	ОК	Cancel	Apply

2. Um den Besitzer des Bereitstellungsordners in einen lokalen Administrator zu ändern, klicken Sie auf den Link **Ändern**.

Aktivieren Sie auf der Seite "Erweiterte Sicherheitseinstellungen" die folgenden Optionen, um die Kontrolle über die Unterordner innerhalb des Ordners zu übernehmen und die Unterordnerberechtigungen durch die Einstellungen aus dem übergeordneten Ordner zu ersetzen:

- Ersetzen des Besitzes für Untercontainer und Objekt
- Ersetzen Sie alle untergeordneten Objektberechtigungseinträge durch vererbbare Berechtigungseinträge von diesem Objekt

ame:	C:\Program File	s\Arcserve\Unified Data Protection	n\Management\BIN\	Appliance\mount	
wner:	TrustedInstaller	Change			
ermissions	Auditing	Effective Access			
r additional	information daub Select User	or Group	dife a namiosian an	×	-and click Edit (if available).
Type	Princi Select this o	object type:			lies to
Allow	SYSTE User, Group	p, or Built-in security principal		Object Types	folder, subfolders and file
Allow	Admi From this los	cation:			folder, subfolders and file
Allow	Users dilition			Locations	folder, subfolders and file
	Users Enter the ob	eject name to select (<u>examples</u>):			folders only
Allow	CREA	dministrator		Check Names	folders and files only
Add	F Advance	ed	OK	Cancel	1
Enable inh	eritance				_

Wenden Sie alle Änderungen an. Stellen Sie für Bereitstellungsordner, Unterordner und Dateien sicher, dass der Besitzer in einen lokalen Administrator geändert wird.

3. Um die Bereitstellung des Bildes aufzuheben, führen Sie den folgenden Befehl mithilfe der Eingabeaufforderung aus:

C:\>DISM /unmount-image /mountdir:"C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\mount" /discard

Führen Sie die folgenden Schritte aus, um den Befehl SetImage.exe auszuführen, um das Werkseinstellungs-Image zu ersetzen, wenn Sophos auf Arcserve Appliance ausgeführt wird:

1. Melden Sie sich als Administrator beim Arcserve Appliance-System an. Verwenden Sie Ihre E-Mail-Adresse und Ihr Kennwort, um auf die Sophos Central Admin-Seite <u>https://cloud.sophos.com/manage/</u> zuzugreifen.



2. Navigieren Sie zu Geräte > Server, und klicken Sie dann auf den Servernamen Ihrer Arcserve Appliance.

		Servers View and manage your	servers						
	Overview	Computers	Mobile Devices	Servers					
EB Da	shboard	Search	Q Show a	di servers	✓ All Health	Status 👻			
A 14	erts								
Φm	reat Analysis Center 🕨	□ ① NHE		p		05	LAST ACTIVE	Ŧ	GROUP
E Log	gs & Reports			10.57.25.29 🔵		Windows Server 2016 Standard	Sep 23, 2019 1:30 AM		
12 Pe	ople								
₩C De	vices								

3. Klicken Sie auf der Registerkarte ZUSAMMENFASSUNG für das Feld "Manipulationsschutz" auf **Details anzeigen**.

	1 SUMMARY	EVENTS	STATUS	Ø EXCLUSIONS	## APPLICATIONS	POLICIES
	Recent Events					View More
	🗉 🗇 Oct 8, 2019 6-27 (M Real time protecti	on re-enabled			
app814 Windows Server 2018 Standard	🗉 🗇 Oct 8, 2019 6-261	M Update succeeded				
Delete	🗉 🗇 Oct 8, 2019 6 26 1	M New server protect	ted: app014			
Scan Now	Oct 8, 2019 6 26 1	M Real time protecti	on disabled			
Lock Down	A Oct 8, 2019 6:251	M Application sychol	it was blocked by an endpo	oint finewall		
Degrese						
	Agent Summary					
	Last Sophos Central Activity	15 minutes ago				
	Last Agent Update	an hour ago	Update Successful 🖌	Update Now		
	Agent Version	10.8.4 VE3.74.1	Ratease Notes 💋			
		installed compon	ent versions Y			
	IPv4 Addresses	10.57.25.29				
		192.168.10.1				
	IPv6 Address	fe80.:9095.bd7	e79e2:a021			
	Operating System	Windows Serve	r 2019 Standard			
	Lockdown Status	Not installed	1			
	Group	No-group Char	ge group			
	Tamper Protection	On - Disable 1	amper Protection		1	
		Vew details ¥			Activate Windows Go to System in Control Pan	el to activate Windows.

4. Aktivieren Sie unter "Kennwort anzeigen" das Kontrollkästchen. Notieren Sie sich das Kennwort, das im Textfeld angezeigt wird.

Tamper Protection	On - Disable Tamper Protection
	Hide details 🛧
Tamper Protection Password Deta	ails
CURRENT PASSWORD	
Show Pessword	
Generate New Password	

5. Klicken Sie auf Manipulationsschutz deaktivieren.

Tamper Protection	On - Disable Tamper Protection
	Hide details 🔨
Tamper Protection Password Details	5
CURRENT PASSWORD	
23233333333	
Show Password	
Generate New Password	
Der Manipulationsschutz wird deaktiviert.	

Tamper Protection	Off - Enable Tamper Protection
	Sophos recommends that you enable tamper protection.
	Tamper protection ensures that users with local administrator rights can't uninstall Sophos Central Endpoint software or change settings.

6. Starten Sie Sophos Endpoint, und klicken Sie dann auf Admin Login.



7. Geben Sie das in Schritt 4 notierte Kennwort für den Manipulationsschutz ein.

SOPHOS	Status	Events		Admin login	-	×
	E	nter tamper protection password				
	•	•••••)		
		Log in	Cancel			
				He	PIA	bout

8. Aktivieren Sie auf der Registerkarte "Einstellungen" die Option Sophos-Zentralrichtlinie bis zu 4 Stunden lang zur Fehlersuche aufheben, und deaktivieren Sie die Optionen Ransomware-Erkennung und Erkennung von bösartigem Verhalten (HIPS).

SOPHOS	Status	Events	Settings	- ×
 Override Soph 	os Central Polic	cy for up to 4 h	nours to troubleshoot	
Deep learnin C Enable deep Real Time So Files Internet	g Iearning canning		Runtime Protection Ransomware Detection Safe Browsing Exploit Mitigation Network Threat Protection Malicious Behavior Detection (HIPS) 	1
Controls on U Peripheral C Application C Web Control Data Loss Pr Tamper Prote	Jsers ontrol control revention action		Computer Controls Windows Firewall 	_
				Help About

9. Um das Werkseinstellungs-Image zu ersetzen, führen Sie SetImage.exe aus. SetImage.exe wird erfolgreich ausgeführt.

Führen Sie die folgenden Schritte aus, um die Standardkonfiguration von Sophos nach der erfolgreichen Ausführung von SetImage.exe wiederherzustellen:

1. Um den Manipulationsschutz in Sophos Central Admin zu aktivieren, klicken Sie auf **Manipulationsschutz aktivieren**.

Tamper Protection	Off Enable Tamper Protection
	A Sophos recommends that you enable tamper protection.
	Tamper protection ensures that users with local administrator rights can't uninstall Sophos Central Endpoint software or change settings.

2. Deaktivieren das Kontrollkästchen Sophos-Zentralrichtlinie bis zu 4 Stunden lang zur Fehlersuche aufheben.

SOPHOS	Status	Events	Settings	-	Admin logout] -	×
Override Sopho	os Central Polic	y for up to 4 h	ours to troubleshoot				

 Um den Status der Sophos-Einstellungen zu überprüfen, warten Sie einige Minuten, und melden Sie sich dann mit dem Kennwort für den Manipulationsschutz bei Sophos Endpoint an.

SOPHOS	Status	Events		Admin login] –	×
	I	Enter tamper protection password				
		•••••)		
		Log in	Cancel			
				He	P A	bout

Jetzt wurden die Sophos-Einstellungen auf die Standardeinstellungen wiederhergestellt.



Bewährte Verfahren zum Erstellen von Deduplizierungsdatenspeichern über Volumes hinweg

Mit as_gddmgr.exe, einem Befehlszeilentool, können Sie weitere Datenpfade über Volumes hinweg hinzufügen, um die Speicherkapazität des vorhandenen Deduplizierungsdatenspeichers zu erweitern.

Führen Sie die folgenden Schritte aus, um Deduplizierungsdatenspeicher über Volumes hinweg zu erstellen:

- 1. Melden Sie sich bei der Benutzeroberfläche der Arcserve UDP-Konsole an, und erstellen Sie dann einen Deduplizierungsdatenspeicher ohne erweiterten Datenpfad. Weitere Informationen finden Sie unter <u>Hinzufügen von</u> Datenspeichern.
- 2. Stoppen Sie den Datenspeicher. Weitere Informationen finden Sie unter Stoppen von Datenspeichern.
- 3. Öffnen Sie die Eingabeaufforderung, und geben Sie dann den folgenden Befehl ein, um die aktuelle Pfadkonfiguration des Datenspeichers anzuzeigen:

as_gddmgr.exe -DataPath Display <Name des Datenspeichers>

Der folgende Beispieldatenspeicher verfügt über einen primären Datenpfad auf X:\volume:



4. Um die Speicherkapazität des Deduplizierungsdatenspeichers zu erweitern, geben Sie den folgenden Befehl ein:

as_gddmgr.exe -DataPath Add <Name des Datenspeichers> -NewDataPath <neue Datenordner>

Hinweis: Stellen Sie sicher, dass sich der primäre Pfad und alle erweiterten Pfade nicht auf demselben Volume befinden.

Der folgende Beispieldatenspeicher verfügt über einen erweiterten Datenpfad auf W:\volume:

C:\Users\Administrato Successfully load dat Successfully added no The data store has 1	or>"c:\Program Files\Ar ta store configuration w expanded data path f expanded data path(s)	rcserve\Unified Data Pr information. for the data store. now:	rotection\Ungine\bin\as_gddmgr.exe"	-OutsPath Add	appliancetest_data_store	-NewOataPath W:	\Arcserve\data_store\data1
	Volume capacity	Used space	Free space				
Frimary data path :	X:\Arcserve\data_stor 59605 GB	e\data\ 2 GB	59603 GB				
Expanded data pathi:	W:\Arcserve\data_stor 14678 GB	e\data1 90 GB	14588 68				
fotal	74283 68	92.68	74191 68				

- 5. Wiederholen Sie Schritt 4 nach Bedarf.
- 6. Kehren Sie zur Benutzeroberfläche der Arcserve UDP-Konsole zurück, und starten Sie den Datenspeicher. Weitere Informationen finden Sie unter <u>Starten von Datenspeichern</u>.

arcserve	UN	IFIED D	NATA PROTECTION	O Upd	ate server un	evailable. I	O Messag	os (1) 🔹	administrato	e e	Help +
dashboard resources	jobs	s reg	ports log settings	high	ı availabilit	У		* appliag	catact > applie	acatast s	fata ctoro
All Nodes	~ 1	Action	Add a Recovery Point Se	nt Server				Config	vation Wizard	iceus _C	ata_store
Nodes without a Plan			Name	Status	Plan Count	Stored Data	Deduplication	O Status			
 Linux Backup Server Groups Plans 	1	•	appliancetest					Stopped	I		
All Plans			appliancetest data store	0	0	0 Byte	0%	✓ Setting	5		
Recovery Point Servers Arcserve Backup Servers Shared Folders	ł		Modity Delete Start					Compr	ession Type 5on Algorithm	Standard AES-256 X \Arcsen	veidata storeice
Cloud Accounts Remote Consoles Accenve Cloud	I.		Browse Recovery RPS Jumpstart	Points				Concu	tent Active Nodes	mmon 20	
 Infrastructure 								Dedu	plication		
Storage Arrays	~	-						Data	File Path	X:Wrcsen	reidata_storeid

Kapitel 15: Lizenzhinweise

Teile dieses Produkts enthalten Software von anderen Herstellern. Der nachfolgende Abschnitt enthält Informationen zur Software von anderen Herstellern.

Dieser Abschnitt enthält folgendes Thema:

<u>PuTTY</u>

PuTTY

Dieses Produkt enthält die Komponente "PuTTY", die folgende Details umfasst:

Komponentenname	PuTTY
Kom- ponentenhersteller	Ursprünglich entwickelt von Simon Tatham
Komponentenversion	0.64
Rechtlicher Hinweis	htt- p://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html
Projektname	Appliance Rhodium
Komponententyp	Open Source
Quell-Code-URL	http://the.earth.li/~sgtatham/putty/0.64/
Erforderliche Plattform (en)	Windows 2012 R2, Windows 2016, Windows 2019
Komponenten-URL	http://the.earth.li/~sgtatham/putty/0.64/x86/
URL der Kom- ponentenversion	http://the.earth.li/~sgtatham/putty/0.64/x86/
Beschreibung	Auf dem Appliance-Rechner verwenden wir putty.exe zur Kom- munikation mit dem Linux-Sicherungsserver, um das Sys- temgebietsschema und das UDP-Linux-Gebietsschema zu ändern.
Funktionen	Appliance
Lizenztext	htt- p://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html PuTTY is copyright 1997-2019 Simon Tatham. Copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Jus- tin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svya- toslav Kuzmich, Nico Williams, Viktor Dukhovni und CORE SDI S.A. Permission is hereby granted, free of charge, to any person obtai- ning a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, inclu- ding without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF

	ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN KEINEM FALL SIND DIE COPYRIGHT-INHABER FÜR ANSPRÜCHE, KLAGEN ODER GEWÄHRLEISTUNGEN WEDER IM RAHMEN DES VERTRAGS, NOCH AUFGRUND VON UNRECHT ODER ANDEREN GRÜNDEN VERANTWORTLICH, DIE DURCH DIE SOFTWARE, DEREN NUTZUNG ODER ANDEREM UMGANG MIT DER SOFTWARE ODER IM ZUSAMMENHANG DAMIT ENTSTEHEN.
	htt- p://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html
	PuTTY is copyright 1997-2019 Simon Tatham.
Copyright-Text	Copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Jus- tin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svya- toslav Kuzmich, Nico Williams, Viktor Dukhovni und CORE SDI S.A.
	Permission is hereby granted, free of charge, to any person obtai- ning a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, inclu- ding without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
	The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
	THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN KEINEM FALL SIND DIE COPYRIGHT-INHABER FÜR ANSPRÜCHE, KLAGEN ODER GEWÄHRLEISTUNGEN WEDER IM RAHMEN DES VERTRAGS, NOCH AUFGRUND VON UNRECHT ODER ANDEREN GRÜNDEN VERANTWORTLICH, DIE DURCH DIE SOFTWARE, DEREN NUTZUNG
	ZUSAMMENHANG DAMIT ENTSTEHEN.
Verwendungszweck	Auf dem Appliance-Rechner verwenden wir putty.exe zur Kom- munikation mit dem Linux-Sicherungsserver, um das Sys- temgebietsschema und das UDP-Linux-Gebietsschema zu ändern.
Änderungen erfor- derlich	Nein