# Benutzerhandbuch zur Arcserve® Unified Data Protection Appliance

**Version 6.5** 

arcserve<sup>®</sup>

### **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.

© 2018 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 -Team stellt umfangreiche Ressourcen zur Lösung von technischen Problemen zur Verfügung und bietet einfachen Zugriff auf wichtige Produktinformationen.

### Support kontaktieren

Der Arcserve-Supportermöglicht 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 UDP 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 <a href="Arcserve.com/support">Arcserve.com/support</a>. 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: Appliance-Dokumentation	9
Sprachenunterstützung	10
Produktdokumentation	11
Kapitel 2: Einführung in die Arcserve UDP Appliance	12
Einführung	13
Arcserve Unified Data Protection	14
Arcserve UDP Agent (Linux)	15
Arcserve Replication and High Availability (Arcserve RHA)	16
Arcserve Backup	17
Sicherheitsmaßnahmen	18
In der Box enthaltene Gegenstände	19
Nicht in der Box enthalten	20
Verfügbare Modelle	21
Modelle 7100 - 7300v	22
Modelle 7400 - 7600v	24
Modelle 8100 - 8400	26
Steuerelemente und Anzeigen	28
Vorderseite 7100 - 7300v	29
Vorderseite 7400 - 7600v	32
Vorderseite 8100 - 8200	34
Vorderseite 8300 - 8400	36
Rückseite 7100 - 7300v	38
Rückseite 7400 - 7600v	40
Rückseite 8100 - 8200	42
Rückseite 8300 - 8400	44
Von der Appliance verwendete Ports	46
Arcserve UDP	47
Unter Microsoft Windows installierte Komponenten	48
Unter Linux installierte Komponenten	51
Per Remote-Zugriff durch UDP Linux geschützte Knoten	53
Arcserve Backup	54
Appliance für Linux-Unterstützung	55
Kapitel 3: Installieren der Arcserve UDP Appliance	57

So installieren Sie Arcserve Backup r17.5	58
So installieren Sie die 8100 - 8200 Series Appliance	59
So installieren Sie die 8300 - 8400 Series Appliance	60
Kapitel 4: Funktionsweise der Netzwerkkonfiguration	61
Konfiguration des NIC-Teaming-Prozesses	62
Deaktivieren des DHCP-Servers	64
Funktionsweise der Netzwerkkonfiguration auf der UDP-Appliance	65
Konfigurieren der IP-Adresse für den vorinstallierten Linux-Sicherungsserver	69
Aktivieren von Round-Robin auf dem DNS-Server zur Bereitstellung von Lastenausgleich	71
Kapitel 5: Aktualisieren von Arcserve UDP auf der Appliance	73
Anwenden einer Lizenz nach einem Upgrade der Arcserve-Software	74
Upgradesequenz auf der Arcserve UDP Appliance	75
Aktualisieren der Arcserve UDP Appliance, die als Arcserve UDP-Konsole und RPS ausgeführt wird	
Aktualisieren der Arcserve UDP Appliance, die nur als Arcserve UDP RPS ausgeführt w	ird <b>77</b>
Upgradeschritte bei Verwendung von mindestens zwei Arcserve UDP Appliances in de Umgebung	
Aktualisieren des Arcserve UDP Linux-Agenten auf der Arcserve UDP Appliance	79
Aktualisieren von Arcserve Backup auf der Arcserve UDP Appliance	80
Upgradesequenz für UDP-Konsole, RPS und Agent	81
Kapitel 6: Konfigurieren der Arcserve UDP Appliance	82
Konfiguration der Netzwerkeinstellungen für eine UDP Appliance	83
Übersicht über das Erstellen eines Plans mit dem UDP Appliance-Assistenten	85
Einrichten der Arcserve UDP Appliance und Erstellen von Plänen	86
Weitere Informationen zum Hinzufügen von Knoten zu einem Plan	93
Knoten nach Hostname/IP-Adresse hinzufügen	94
Knoten nach Active Directory hinzufügen	95
vCenter/ESX-Knoten hinzufügen	97
Hyper-V-Knoten hinzufügen	98
Konfigurieren der UDP Appliance als Gateway	99
Löschen der Konfiguration und Zurücksetzung der Appliance auf Werkseinstellungen	100
Zurücksetzen von Arcserve UDP auf Werkseinstellungen unter Verwendung der Startoption	. 101
Aktivieren des Arcserve-Produkts auf der Appliance	104
Kapitel 7: Erstellen von Sicherungsablaufplänen	105

Sicherungsablaufplan für Linux-Knoten erstellen	106
Sicherungsablaufplan für ein Bandgerät erstellen	107
Virtuellen On-Appliance-Standby-Plan erstellen	109
Kapitel 8: Reparieren der Arcserve UDP Appliance	110
Festplatte entfernen und ersetzen	111
Kapitel 9: Sicherheitsmaßnahmen	113
Allgemeine Sicherheitsmaßnahmen	114
Sicherheitsmaßnahmen zur Elektrik	116
FCC-Konformität	118
Vorsichtsmaßnahmen gegen elektrostatische Entladungen (ESD)	119
Kapitel 10: Arbeiten mit IPMI	120
So ändern Sie das IPMI-Kennwort	121
So aktualisieren Sie die IPMI-Firmware	122
Kapitel 11: Herstellen einer Verbindung zwischen dem Appliance-Server und dem Appliance-Erweiterungs-Shelf	123
Appliance-Infield-Erweiterung für alle verfügbaren Modelle	124
In der Box enthaltene Gegenstände	134
So stellen Sie eine Verbindung zwischen dem Appliance-Server und dem Applian Erweiterungs-Shelf her	nce- 137
So ändern Sie den Arcserve UDP-Datenspeicher	145
Hinzufügen eines Datenpfads auf dem Erweiterungs-Shelf zum Arcserve UDP-Daten speicher	- 146
Migrieren eines Hash-Ziels zur neuen SSD	147
Überprüfen der Gesamtkapazität des Datenspeichers <data name="" store=""> von der Ar serve UDP-Konsole</data>	c- 148
Fortsetzen aller Pläne von der Arcserve UDP-Konsole	149
Kapitel 12: Fehlerbehebung	151
Linux-Sicherungsserver kann über die Konsole keine Verbindung herstellen	152
Sichern einer UDP Appliance von einer anderen Appliance meldet duplizierte Kr ten	10- 154
Linux-Sicherungsserver kann das Netzwerk-DNS-Suffix nicht abrufen	156
Standardzeitzone auf der Appliance	157
Lizenzfehler, auch wenn Lizenzen verfügbar sind	158
Kapitel 13: Empfehlungen	159
Best Practices für die Netzwerkkonfiguration	160
Best Practices für die Migration der Arcserve UDP-Konsole	163
Rest Practices für eine Bare-Metal-Recovery (RMR) ohne Erhalten von Daten	165

	Best Practices für eine Bare-Metal-Recovery (BMR) und das Erhalten von Daten	176
	Best Practices für das Linux-Migrations-Tool	184
	Best Practices für das Dienstprogramm "Appliance-Image festlegen"	186
	Best Practices für vorinstallierte Linux-Sicherungsserver in der Arcserve UDP Appliance	189
	Best Practices für die Arcserve UDP-Appliance zum Sichern des Linux-Sicherungsservers selbst	191
	Best Practices zur Migration zwischen Arcserve UDP-Appliances	195
	Lösung 1	196
	Lösung 2	201
	Best Practices für Linux-Instant VM-Job auf Arcserve UDP-zu Hyper-V auf lokaler Appliance	204
	Best Practices zum Hinzufügen von "Replizieren" zu einem remote verwalteten RPS-Task einer anderen Appliance	205
	Best Practices zum Durchführen eines Virtual Standby (VSB)-Task, bei dem der Monitor eine andere Appliance ist	207
K	Kapitel 14: Lizenzhinweise	209
	putty	210

## **Kapitel 1: Appliance-Dokumentation**

Im Benutzerhandbuch zur Arcserve UDP-Appliance finden Sie hilfreiche Informationen zur Verwendung der Arcserve UDP-Appliance. Grundlegende Informationen zum Kennenlernen der UDP-Appliance finden Sie in der Einführung. Die übrigen Abschnitte enthalten Anweisungen zum Installieren und Verwenden der Arcserve UDP-Appliance.

Dieser Abschnitt enthält folgende Themen:

Sprachenunterstützung	 10
Produktdokumentation	 11

Kapitel 1: Appliance-Dokumentation 9

### 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
- Portugiesisch (Brasilien)
- Spanisch

### **Produktdokumentation**

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

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 für Windows – Benutzerhandbuch

Enthält ausführliche Informationen über die Verwendung des Arcserve UDP-Agent 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 für Linux – Benutzerhandbuch

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

## **Kapitel 2: Einführung in die Arcserve UDP Appliance**

Dieser Abschnitt enthält folgende Themen:

<u>Einführung</u>	.13
Sicherheitsmaßnahmen	.18
In der Box enthaltene Gegenstände	. 19
Nicht in der Box enthalten	. 20
Verfügbare Modelle	21
Steuerelemente und Anzeigen	. 28
Von der Appliance verwendete Ports	.46

### Einführung

Die Arcserve UDP Appliance ist die erste vollständige und besonders kostengünstige Datenschutz-Appliance mit Assured Recovery™. Jede Arcserve UDP 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 UDP Appliance bietet unübertroffene Agilität und Effektivität sowie drastische Vereinfachungen von Disaster Recovery-Aktivitäten.

Die Arcserve UDP Appliance ist vollständig in die führende Arcserve Unified Data Protection-Software integriert, die bereits in der neuesten 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.

Die folgende Software ist in der Arcserve UDP Appliance vorinstalliert:

- Windows-Betriebssystem Version 2012 R2 Standard Server oder Standard Server 2016
- Arcserve UDP
- Arcserve UDP Agent (Linux)
- Arcserve Backup
- Arcserve Replication and High Availability (RHA)

Jede Arcserve UDP Appliance wird mit einer dreijährigen Gewährleistung für die Hardware ausgeliefert. Ausführliche Informationen zu dieser Gewährleistung erhalten Sie auf arcserve.com/Udp-Appliance-Warranty.

### **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) für 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.

### **Arcserve UDP Agent (Linux)**

Arcserve UDP Agent (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 UDP Agent (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 UDP Agent (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 UDP Agent (Linux) ist auf einem virtuellen Rechner in der Appliance vorinstalliert. Dieser virtuelle Rechner wird zum Linux-Sicherungsserver. Arcserve UDP Agent (Linux) ist in der UDP Appliance unter dem Standardinstallationspfad 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 UDP 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 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 Kompatibilitätsmatrix.

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.

Weitere Informationen zum Installieren und Konfigurieren von Arcserve Replication and High Availability finden Sie in der Onlinedokumentation.

### **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 Agents und Optionen.

Arcserve Backup bietet umfassenden Datenschutz für verteilte Umgebungen und bietet virenfreie Sicherungs- und Wiederherstellungsvorgänge. Mit einer umfangreichen Palette an Optionen und Agents 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.

Die UDP Appliance 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 Komponenten, die in der UDP Appliance installiert sind, können Sie das Ziel von Arcserve UDP auf ein Band sichern. Weitere Informationen zu den unterstützten Betriebssystemen finden Sie in der Kompatibilitätsmatrix.

Sie können das vollständige Installationspaket von Arcserve Backup von der Arcserve-Website herunterladen, um weitere Komponenten zu installieren. Weitere Informationen finden Sie in der Online-Dokumentation zu Arcserve Backup r17.5.

Arcserve Backup Server verwendet die folgenden Standard-Anmeldeinformationen:

Benutzername: caroot

Kennwort: Arcserve

### Sicherheitsmaßnahmen

Lesen Sie aus Sicherheitsgründen alle Anweisungen und befolgen Sie sie, bevor Sie eine Arcserve UDP Appliance entpacken, anschließen, installieren, einschalten oder betreiben. 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 - Sicherheitsmaßnahmen</u>.

### In der Box enthaltene Gegenstände

Die folgenden Gegenstände sind in der Box enthalten:

- Arcserve UDP Appliance (Aufkleber mit 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)
- Schiene/Rack-Montageset 2 äußere Schienen mit Schnellmontierung, 2 innere Schienenerweiterungen, 3 Schienenadapter (nur Standardschienenmontage) und Befestigungsteile (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 das gesamte Verpackungsmaterial auf und wenden Sie sich sofort an den Arcserve-Support unter https://www.arcserve.com/support.

### Nicht in der Box enthalten

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

- Überwachen
- Tastatur
- Externes Speichergerät (bei Bedarf)

## Verfügbare Modelle

Die Appliances der Arcserve UDP 7000 Series und 8000 Series sind in einer Vielzahl verschiedener Modelle erhältlich, die an Ihren spezifischen Anforderungen ausgerichtet sind:

- Modelle 7100 7300v
- Modelle 7400 7600v
- Modelle 8100 8400

## Modelle 7100 - 7300v

Arcserve UDP Appliance-Modelle 7100 - 7300v

Arcserve UDP 7000 Series Appliances							
Appliance-Modell	7100	7200	7200V	7300	7300V		
Sicherungsspeicherkapazität							
Reine Speicherkapazität *	3 TB	6 TB	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							
rungen auf Blockebene, erweiterte Virtualisierun Standby, Unterstützung	Einheitliche Verwaltungskonsole, globale Deduplizierung, unbegrenzte inkrementelle Sicherungen auf Blockebene, Komprimierung, Verschlüsselung, WAN-optimierte Replikation, erweiterte Virtualisierungsunterstützung, Sicherung ohne Agenten, Virtuelles Remote-Standby, Unterstützung für Bandlaufwerke, anwendungskonforme Sicherungen, granulare Wiederherstellung, einheitliche Berichte und Dashboard.						
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-			1 x 600 W		
undant)					
Stromverbrauch					
(Wattzahl beim Leer-	93/116/143	122/164/143	125/167/145	125/167/145	129/188/152
lauf/Laden/Starten)					
Wechselspannungs-			100 - 240 V		
und Frequenzbereich			100 - 240 V		
Amperewert			7,5 A max.		
l					

<sup>1</sup> TB = 1.000.000.000.000 Byte

<sup>\*\*</sup> Für V-Modelle wird der für die Sicherung verfügbare Speicherplatz um die Größe der Virtual Standby-VMs reduziert.

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

## Modelle 7400 - 7600v

Arcserve UDP Appliance-Modelle 7400 - 7600v

Arcserve UDP 7000 Series Appliances						
Appliance-Modell	7400	7400V	7500	7500V	7600	7600V
Sicherungsspeicherkapazität						
Reine Speicherkapazität *	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						
rungen auf Blockebene, erweiterte Virtualisierun Standby, Unterstützung	Einheitliche Verwaltungskonsole, globale Deduplizierung, unbegrenzte inkrementelle Sicherungen auf Blockebene, Komprimierung, Verschlüsselung, WAN-optimierte Replikation, erweiterte Virtualisierungsunterstützung, Sicherung ohne Agenten, Virtuelles Remote-Standby, Unterstützung für Bandlaufwerke, anwendungskonforme Sicherungen, granulare Wiederherstellung, einheitliche Berichte und Dashboard.					
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		& 2 x 1 GbE (RJ4	45) und 4 :	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)	SAS	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)						
Maximalgewicht (lb)		,	52	lb		
Netzteile (einzeln oder red- undant)	2 x 920 W					
Stromverbrauch (Wattzahl beim Leer- lauf/Laden/Starten)	208/257/ 358	208/257/ 358	208/257/ 358	208/257/ 358	240/296/ 369	240/296/ 369
Wechselspannungs- und Frequenzbereich	100 - 240 V					
Amperewert		11 A max.				

<sup>1</sup> TB = 1.000.000.000.000 Byte

<sup>\*\*</sup> Für V-Modelle wird der für die Sicherung verfügbare Speicherplatz um die Größe der Virtual Standby-VMs reduziert.

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

## Modelle 8100 - 8400

Arcserve UDP Appliance-Modelle 8100 - 8400

Arcserve UDP 8000 Series Appliances									
Appliance-Modell	UDP 8100	UDP 8200	UDP 8300	UDP 8400					
Quellensicherung*	12 TB bis 18 TB	24 TB bis 36 TB	48 TB	96 TB bis 240 TB					
System-RAM	32 GB	32 GB	64 GB	128 GB					
Max. RAM **	64 GB/96 G	96 GB/128 GB/192 GB							
SSD-Laufwerk	120 GB SSD	200 GB SSD	480 GB SSD	1,2 TB SSD					
Prozessor	E5 2609 V4, 8-CORE 1,7 GHZ	E5-2620 V4, 8-CORE 2,1 GHZ	E5 2640 V4, 10- CORE 2,4 GHZ	E5 2650 V4, 12- CORE, 2,2 GHZ					
RAID-Karte	9361	L-4i	936	51-8i					
RAID-Kon- figuration	RAID-5 n	nit BBU		-6 mit 3U					
Laufwerkschächte	4		12						
			6 x 4 TB SAS 12G 7 x 4	6 x 8 TB SAS 12G 7 x 8					
Laufwerke	3 x 2 TB SAS 12G verke 4 x 2 TB SAS 12G	3 x 4 TB SAS 12G 4 x 4 TB SAS 12G	TB SAS 12G 8 x 4	TB SAS 12G 8 x 8					
			TB SAS 12G	12G					
			9 x 4 TB SAS	9 x 8 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	
DIMMs/Max.		GB	GB		
DIMMs	4 x 8 GB DDR4-2400/ 8			DDR4-	
DIIVIIVIS				2400/	
		8	8		
Karten	L	.SI SAS9200-8E			
			2 x, 920 W,		
		Hot-Swap-			
Netzteile	2 x, Hot-Swap-fähig, red	undant 500 W Wech-	fähig, red-		
	selstrom, F		undant, hoch-		
	Seistroin, F	Tatillulli	effizient	t,	
			Wechse	Istrom,	
			Platinur	n	

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

<sup>\*\*</sup>Arcserve Appliances verfügen über zusätzlichen RAM für Virtual Standby-/Instant VM-Wiederherstellung auf den Appliances. 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.

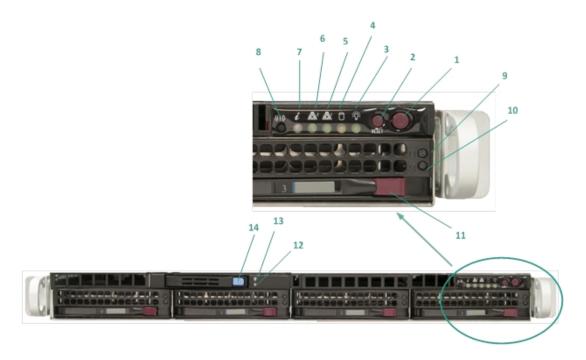
### **Steuerelemente und Anzeigen**

Die Arcserve UDP Appliance enthält auf der Vorder- und Rückseite sowie auf den einzelnen Laufwerksträgern verschiedenen Steuerelemente und Anzeigen (LEDs). 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
- Rückseite 7100 7300v
- Rückseite 7400 7600v
- Rückseite 8100 8200
- Rückseite 8300 8400

## **Vorderseite 7100 - 7300v**

Die Vorderseite der Arcserve UDP Appliance enthält Bedienfeldtasten, Bedienfeld-LEDs und Laufwerksträger-LEDs. In der folgenden Tabelle werden diese Elemente beschrieben.



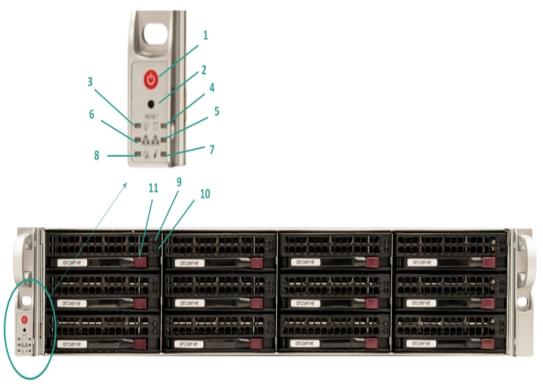
Nummer	Steuerelement/Anzeige	Beschreibung
		Zum Ein- und Ausschalten der Stromversorgung
		für die Appliance-Komponenten. Beim Aus-
		schalten wird die Haupt-Stromversorgung aus-
1	Netzschalter	geschaltet, die Appliance wird jedoch weiterhin
1	Netzschalter	mit Standby-Strom versorgt. Um sicherzustellen,
		dass die Appliance vollständig von der Strom-
		versorgung getrennt ist, ziehen Sie vor War-
		tungsarbeiten das Netzkabel ab.
2	Schaltfläche "Zurück-	7um Noustart der Appliance
2	setzen"	Zum Neustart der Appliance.
	Netz-LED	Stetig grün: Zeigt an, dass das Netzteil der App-
2		liance mit Strom versorgt wird.
3		Diese LED sollte normalerweise leuchten, wenn die
		Appliance in Betrieb ist.
4	Geräteaktivitäts-LED	Gelb blinkend: Zeigt Aktivität auf mindestens
4		einer der Festplatten an.
5	Netzwerkkarten-LED (NIC1)	Gelb blinkend: Zeigt Netzwerkaktivität im Netz-
5	INGLEWEIKKAITEII-LED (NICT)	werk 1 (Port ETH0) an.
6	Netzwerkkarten-LED (NIC2)	Gelb blinkend: Zeigt Netzwerkaktivität im Netz-

		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): Lüf-
7		terfehler. Überprüfen Sie, ob der Lüfter nicht mehr betriebsbereit ist.
	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. Verwenden Sie diese Funktion, um den Server von
		einem externen Standort aus zu suchen.
8	Schaltfläche "Geräte-ID	Zum Ein- oder Ausschalten der Universal Information-LED (blau) auf der Vorder- und Rückseite der Appliance.
	(UID)"	Wenn die blaue LED aktiviert ist, kann die Appliance problemlos in einem Rack lokalisiert werden (von vorne oder hinten).
		Grün blinkend: Zeigt Aktivität auf der ent-
9	Festplatten-LED	sprechenden Festplatte an.
		*Stetig rot: Zeigt einen Ausfall der ent- sprechenden Festplatte an.
10	Festplatten-LED	Wenn bei der Arcserve UDP Appliance eine Fest- platte ausfällt, laufen sofort die restlichen Lauf- werke an, um sicherzustellen, dass keine Daten verloren gehen und die Appliance weiterhin nor- mal funktioniert. Daher ist es zum Schutz vor Pro-
		blemen im Zusammenhang mit Ausfällen mehrerer Festplatten wichtig, eine Festplatte schnellstmöglich auszutauschen, um den poten- ziellen 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		Stetig grün: Zeigt Laufwerkaktivität an.
	SSD (Solid State Drive)-LED	<b>Grün blinkend</b> : Zeigt an, dass auf das Laufwerk zugegriffen wird.
14	Verriegelung SSD (Solid State Drive)	Zum Entriegeln und Entfernen des SSD-Laufwerks.
		1

\* Eine stetig rote oder rot blinkende LED weist auf irgendeine Art von Fehler hin. Um dieses Problem schnell zu lösen, wenden Sie sich an unseren Support-Website auf arcserve.com/support.

### Vorderseite 7400 - 7600v

Die Vorderseite der Arcserve UDP Appliance enthält Bedienfeldtasten, Bedienfeld-LEDs und Laufwerksträger-LEDs. In der folgenden Tabelle werden diese Elemente beschrieben.



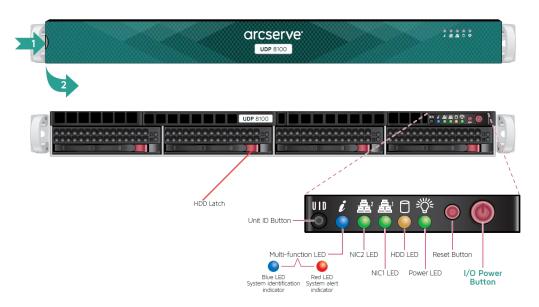
Num- mer	Steu- erelement/Anzeige	Beschreibung
1	Netzschalter	Zum Ein- und Ausschalten der Stromversorgung für die Appliance-Komponenten. Beim Ausschalten wird die Haupt-Stromversorgung ausgeschaltet, die Appliance wird jedoch weiterhin mit Standby-Strom versorgt. Um sicherzustellen, dass die Appliance 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 Appliance mit Strom versorgt wird.  Diese LED sollte normalerweise leuchten, wenn die Appliance in Betrieb ist.
4	Geräteaktivitäts-LED	<b>Gelb blinkend:</b> Zeigt Aktivität auf mindestens einer der Festplatten an.
5	Netzwerkkarten-LED (NIC1)	<b>Gelb blinkend:</b> Zeigt Netzwerkaktivität im Netzwerk 1 (Port ETHO) an.

6	Netzwerkkarten-LED (NIC	Gelb blinkend: Zeigt Netzwerkaktivität im Netzwerk 2 (Port ETH1) an.
7		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 betriebs- bereit ist.
	Informations-LED	*Rot blinkend – langsam (4 Sekunden): Stromausfall. 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.
		<b>Blau blinkend:</b> Remote-UID wurde aktiviert. Verwenden 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	<b>Grün blinkend</b> : Zeigt Aktivität auf der ent- sprechenden Festplatte an.
10		*Stetig rot: Zeigt einen Ausfall der entsprechenden Festplatte an.
	Festplatten-LED	Wenn bei der Arcserve UDP Appliance eine Festplatte ausfällt, laufen sofort die restlichen Laufwerke an, um sicherzustellen, dass keine Daten verloren gehen und die Appliance weiterhin normal funktioniert. Daher ist es zum Schutz vor Problemen im Zusammenhang mit Ausfällen mehrerer Festplatten wichtig, eine Festplatte schnellstmöglich auszutauschen, um den potenziellen Datenverlust zu minimieren.
11	Verriegelung Festplatte	Zum Entriegeln und Entfernen der Festplatte.
	1 202 2 0 223 10 1000	J

<sup>\*</sup> Eine stetig rote oder rot blinkende LED weist auf irgendeine Art von Fehler hin. Um dieses Problem schnell zu lösen, wenden Sie sich an unseren Support-Website auf <u>arcserve.com/support</u>.

### Vorderseite 8100 - 8200

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



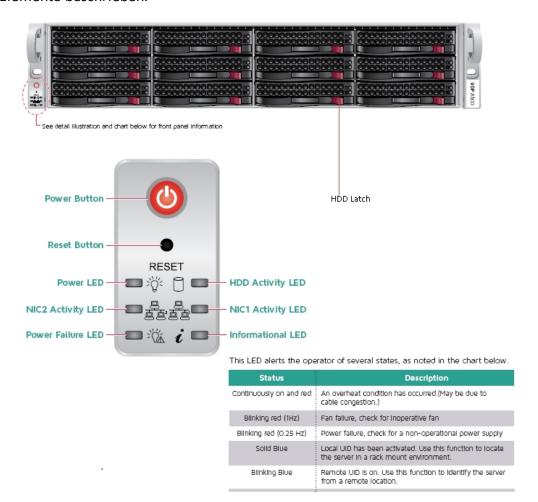
Steuerelement/Anzeige	Reschreihung	
Stedereleinent/Anzeige		
	Zum Ein- und Ausschalten der Stromversorgung für die App-	
	liance-Komponenten. Beim Ausschalten wird die Haupt-Strom-	
Netzschalter	versorgung ausgeschaltet, die Appliance wird jedoch weiterhin	
IVC123CHarter	mit Standby-Strom versorgt. Um sicherzustellen, dass die App-	
	liance vollständig von der Stromversorgung getrennt ist, zie-	
	hen Sie vor Wartungsarbeiten das Netzkabel ab.	
Schaltfläche "Zurück-	Zum Neustart der Appliance.	
setzen"		
	Stetig grün: Zeigt an, dass das Netzteil der Appliance mit Strom	
Note IED	versorgt wird.	
Netz-LED	Diese LED sollte normalerweise leuchten, wenn die Appliance in	
	Betrieb ist.	
HDD-LED	Gelb blinkend: Zeigt Aktivität auf mindestens einer der Fest-	
חטט-נבט	platten an.	
Notarrandilo atom LED (NIC1)	Gelb blinkend: Zeigt Netzwerkaktivität im Netzwerk 1 (Port	
Netzwerkkarten-LED (NIC1)	ETH0) an.	
Notauralikartan LED (NICA)	Gelb blinkend: Zeigt Netzwerkaktivität im Netzwerk 2 (Port	
Netzwerkkarten-LED (NIC2)	ETH1) an.	
Informations LED	Stetig rot: Eine Überhitzungs-Bedingung ist aufgetreten.	
Informations-LED	<b>Hinweis:</b> Dies kann durch eine Überlastung eines Kabels ver-	

	ursacht werden.
	*Rot blinkend – schnell (1 Sekunde): Lüfterfehler. Überprüfen Sie, ob der Lüfter nicht mehr betriebsbereit ist.
	*Rot blinkend – langsam (4 Sekunden): Stromausfall. Über- prüfen Sie, ob die Stromversorgung außer Betrieb ist.
	<b>Stetig blau:</b> Lokale UID ist aktiviert. Verwenden Sie diese Funktion, um den Server in einer Rack-Umgebung zu suchen.
	<b>Blau blinkend:</b> 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 (blau) auf der Vorder- und Rückseite der Appliance.
Schaltfläche "Geräte-ID (UID)"	Wenn die blaue LED aktiviert ist, kann die Appliance problemlos in einem Rack lokalisiert werden (von vorne oder hinten).
Festplatten-LED	<b>Grün blinkend</b> : Zeigt Aktivität auf der entsprechenden Fest- platte an.
	*Stetig rot: Zeigt einen Ausfall der entsprechenden Festplatte
	an.
Festplatten-LED	Wenn bei der Arcserve UDP Appliance eine Festplatte ausfällt, laufen sofort die restlichen Laufwerke an, um sicherzustellen, dass keine Daten verloren gehen und die Appliance weiterhin normal funktioniert. Daher ist es zum Schutz vor Problemen im Zusammenhang mit Ausfällen mehrerer Festplatten wichtig,
	eine Festplatte schnellstmöglich auszutauschen, um den potenziellen Datenverlust zu minimieren.
Verriegelung Festplatte	Zum Entriegeln und Entfernen der Festplatte.
SSD (Solid State Drive)-LED	*Stetig rot: Zeigt einen Laufwerksausfall an.
	Stetig grün: Zeigt Laufwerkaktivität an.
SSD (Solid State Drive)-LED	<b>Grün blinkend</b> : Zeigt an, dass auf das Laufwerk zugegriffen wird.
Verriegelung SSD (Solid State Drive)	Zum Entriegeln und Entfernen des SSD-Laufwerks.

<sup>\*</sup> Eine stetig rote oder rot blinkende LED weist auf irgendeine Art von Fehler hin. Um dieses Problem schnell zu lösen, wenden Sie sich an unseren Support-Website auf <u>arcserve.com/support</u>.

### Vorderseite 8300 - 8400

Die Vorderseite der Arcserve UDP 8300 - 8400 Appliance enthält Bedienfeldtasten, Bedienfeld-LEDs und Laufwerksträger-LEDs. In der folgenden Tabelle werden diese Elemente beschrieben.

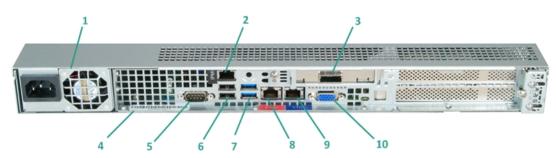


Steuerelement/Anzeige	Beschreibung
Netzschalter	Zum Ein- und Ausschalten der Stromversorgung für die Appliance-Komponenten. Beim Ausschalten wird die Haupt-Stromversorgung ausgeschaltet, die Appliance wird jedoch weiterhin mit Standby-Strom versorgt. Um sicherzustellen, dass die Appliance vollständig von der Stromversorgung getrennt ist, ziehen Sie vor Wartungsarbeiten das Netzkabel ab.
Schaltfläche "Zurück- setzen"	Zum Neustart der Appliance.
Netz-LED	<b>Stetig grün:</b> 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)	<b>Gelb blinkend:</b> Zeigt Netzwerkaktivität im Netzwerk 1 (Port ETHO) an.
Netzwerkkarten-LED (NIC2)	<b>Gelb blinkend:</b> Zeigt Netzwerkaktivität im Netzwerk 2 (Port ETH1) an.
	<b>Stetig rot:</b> 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.
	<b>Stetig blau:</b> Lokale UID wurde aktiviert. Verwenden Sie diese Funktion, um den Server in einer Rack-Umgebung zu suchen.
	<b>Blau blinkend:</b> 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	<b>Grün blinkend</b> : Zeigt Aktivität auf der entsprechenden Fest- platte an.
	*Stetig rot: Zeigt einen Ausfall der entsprechenden Festplatte an.
	Wenn bei der Arcserve UDP Appliance eine Festplatte ausfällt, laufen sofort die restlichen Laufwerke an, um sicherzustellen,
Festplatten-LED	dass keine Daten verloren gehen und die Appliance weiterhin normal funktioniert. Daher ist es zum Schutz vor Problemen im
	Zusammenhang mit Ausfällen mehrerer Festplatten wichtig, eine Festplatte schnellstmöglich auszutauschen, um den potenziellen Datenverlust zu minimieren.
Verriegelung Festplatte	Zum Entriegeln und Entfernen der Festplatte.
<del></del>	

<sup>\*</sup> Eine stetig rote oder rot blinkende LED weist auf irgendeine Art von Fehler hin. Um dieses Problem schnell zu lösen, wenden Sie sich an unseren Support-Website auf arcserve.com/support.

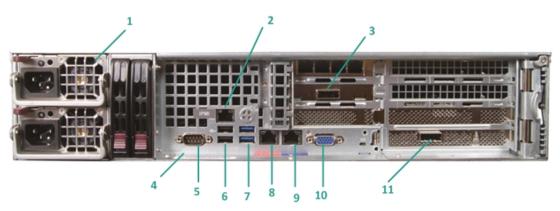
### **Rückseite 7100 - 7300v**



Nummer	Name des Steu- erelements bzw. der Anzeige	Beschreibung
		Ermöglicht eine hocheffiziente Stromversorgung der Appliance.
1	Netzteil	Hinweis: Mithilfe des Hauptnetzschalters wird die Appliance mit der Stromversorgung verbunden oder von ihr getrennt. Beim Ausschalten über diesen Schalter wird die Haupt-Stromversorgung ausgeschaltet, die Appliance wird jedoch weiterhin mit Standby-Strom versorgt. 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 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 Informationen zum Ändern des IPMI-Kennworts finden Sie unter So ändern Sie das IPMI-Kennwort.
3	Port für externes Spei- chergerät (SAS-Port für Band- laufwerk)	Zum Anschluss eines externen Speichergeräts (Festplatte, Bandlaufwerk usw.) an die Appliance. Mit diesen 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 seriellen 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.
8	E/A-Port 1 für Netz- werkdaten	Zur Übertragung von Netzwerkdaten zwischen dem Netzwerk und der Appliance. ((ETH0 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).

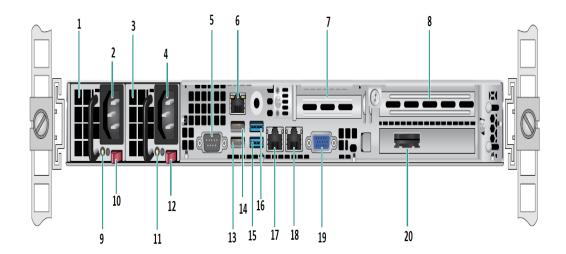
#### Rückseite 7400 - 7600v



Nummer	Name des Steu- erelements bzw. der Anzeige	Beschreibung	
		Ermöglicht eine hocheffiziente Stromversorgung der Appliance.	
1	Doppelnetzteil	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 Appliance wird jedoch weiterhin mit Standby-Strom versorgt. Um sicherzustellen, dass die Appliance vollständig von der Stromversorgung getrennt ist, ziehen Sie vor Wartungsarbeiten das Netzkabel ab.	
	IDMI Port (Porce	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 überwachen.	
2	IPMI-Port (Remo- teverwaltung)	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 Informationen zum Ändern des IPMI-Kennworts finden Sie unter So ändern Sie das	

		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 seriellen 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.
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.

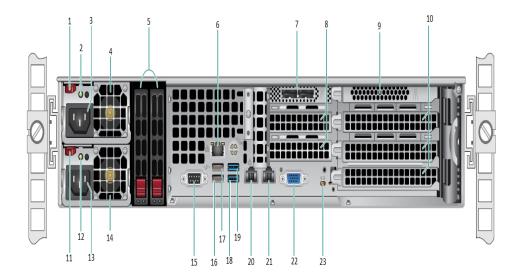
#### **Rückseite 8100 - 8200**



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	
	Port für externes Speichergerät	
20	(SAS-Port für Bandlaufwerkoption)	

#### Rückseite 8300 - 8400



Num-	Name des Steuerelements bzw. der	
mer	Anzeige	
1	Netzteilmodul Nr. 1 – Verriegelung	
2	Netzteilmodul Nr. 1 – Power-Good-LED	
3	Netzteilmodul 1 Steckdose	
4	Netzteilmodul 1 Lüfter	
5	Hintere SSDs (optional)	
6	IPMI-Port (Remoteverwaltung)	
7	Externe SAS HBA-Ports	
8	PCI-Erweiterungssteckplätze halber Länge	
9	Interner RAID-Controller	
10	PCI-Erweiterungssteckplätze voller Länge	
11	Netzteilmodul Nr. 2 – Verriegelung	
12	Netzteilmodul Nr. 2 – Power-Good-LED	
13	Netzteilmodul Nr. 2 – Wechselstrombuchse	
14	Netzteilmodul Nr. 2 – Lüfter	
15	COM-Port	
16	USB-Port 1 (2. Generation)	
17	USB-Port 2 (2. Generation)	
18	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

### Von der Appliance verwendete Ports

Die folgende Tabellenliste bietet Informationen zu Ports, die von Arcserve UDP, Arcserve Backup und der Appliance für Linux-Unterstützung verwendet werden:

- Arcserve UDP
- Arcserve Backup
- Appliance für Linux-Unterstützung

#### **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:

Po-	Po-	Ini-			
rt	rt-	tiiert	Abhörprozess	Beschreibung	
#	typ	von			
143- 3	тср	Remo	calcrur eve	Gibt den Standard-Kommunikations-Port zwischen der Arcserve UDP-Konsole und den Microsoft SQL Server-Datenbanken an, wenn diese sich auf unterschiedlichen Computern befinden.	
		Java		Hinweis: Sie können den standardmäßigen Kommunikationsport während der Instal- lation von SQL Server ändern.	
409- 0	ТСР	Arc- serve UDP Agent	HATransServer.exe	Überträgt Daten für Virtual Standby-Aufgaben im Proxy-Modus.	
500- 0- 506- 0	TCP	Arc- serve UDP- Ser- ver	GDDServer.exe	Reserviert für den Arcserve-UDP den RPS Global Deduplizierungs-Datenspeicher-Dienst (GDD). Ein Arcserve UDP-GDD-Datenspeicher verwendet 3 freie Ports, die mit 5000 beginnen. Sie werden benötigt, wenn der Datenspeicher mit GDD aktiviert oder die Wiederherstellungsaufgabe verwendet wird.	
605- 2	ТСР	Arc- serve Back- up- GDB	CA.ARC- ser- ve.CommunicationFoundation WindowsService.exe	CA.ARC- ser- ve.CommunicationFoundation.WindowsServic Kommunikation, über die die Arcserve UDP- Konsole und der Primärserver des globalen Arcserve Backup-Dashboards Daten syn- chronisieren können.	ce.exe
605- 4	TCP	Arc- serve Back- up		CA.ARC- ser- ve.CommunicationFoundation.WindowsServic Kommunikation, über die die Arcserve UDP- Konsole und der Arcserve Backup-Pri- märserver Daten synchronisieren können.	ce.exe
800- 6				Zum Herunterfahren von Tomcat, das von der Arcserve UDP-Konsole verwendet wird.	

801- 4	ТСР	Arc- serve UDP Con- sole	Tomcat7.exe	Gibt den Standard-Port für HTTP/HTTPS-Kommunikation zwischen Remote-Verwaltungskonsolen und dem Arcserve UDP-Server an. Gibt den Port der Standard-HTTP/HTTPS-Kommunikation zwischen Remote-Verwaltungskonsolen und dem Arcserve UDP-Agent an. Hinweis: Sie können den standardmäßigen Kommunikationsport während der Installation der Arcserve UDP-Komponenten ändern.
801-		Arc- serve UDP- Ser- ver	httpd.exe	Gibt den Standard-Port für HTTP/HTTPS-Kommunikation zwischen dem Arcserve UDP-Server und den Arcserve UDP-Konsolen an.  * Gibt den freigegebenen Standard-Port und den einzigen Port an, den Sie öffnen müssen, wenn Sie den Arcserve UDP-Server als Replikationsziel verwenden. Öffnen Sie nicht die Ports 5000 - 5060, da diese von Datenspeichern mit aktivierter globaler Deduplizierung verwendet werden.  Hinweis: Sie können den standardmäßigen Kommunikationsport während der Installation der Arcserve UDP-Komponenten ändern.
801-	ТСР	Arc- serve UDP Con- sole	Tomcat7.exe	Gibt den Standard-Port für HTTP/HTTPS-Kommunikation zwischen Remote-Verwaltungskonsolen und dem Arcserve UDP-Server an.  Gibt den Port der Standard-HTTP/HTTPS-Kommunikation zwischen Remote-Verwaltungskonsolen und dem Arcserve UDP-Agent an.  Hinweis: Sie können den standardmäßigen Kommunikationsport während der Installation der Arcserve UDP-Komponenten ändern.
801- 6	ТСР	Arc- serve UDP- Ser- ver	Tomcat7.exe	Reserviert für die Kommunikation von Arcserve UDP Server-Webdiensten mit dem RPS-Port-Freigabedienst für Arcserve UDP auf dem gleichen Server.

			<b>Hinweis:</b> Der Port kann nicht angepasst werden und kann für die Firewall-Einstellung ignoriert werden.
180- 05		CA.ARC- ser- ve.CommunicationFoundation WindowsService.exe	Zum Herunterfahren von Tomcat, das von Arcserve UDP Server oder Agent verwendet N. 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 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.
67	UDP	Arcserve UDP- Linux	bootpd	Wird für den PXE-Boot-Server verwendet. Nur erforderlich, wenn der Benutzer die PXE-Startfunktion verwenden möchte. Dieser Port ist für die eingehende Kommunikation erforderlich.  Hinweis: Die Portnummer kann nicht angepasst werden.
69	UDP	Arcserve UDP- Linux	tffpd	Wird für den PXE-Boot-Server verwendet. Nur erforderlich, wenn der Benutzer die PXE-Startfunktion verwenden möchte. Dieser Port ist für die eingehende Kommunikation erforderlich.  Hinweis: Die Portnummer kann nicht angepasst werden.
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.
18005	ТСР	Arcserve UDP- Linux	Java	Verwendet von Tomcat. Kann für die Firewall-Ein- stellungen ignoriert wer- den.

## Per Remote-Zugriff durch UDP Linux geschützte Knoten

Der folgende Port ist für Sicherungs- und andere Aufträge in 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.

<sup>\*</sup> 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	Initiiert 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 Appliance 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 Appliance auf den Port 8014 des Linux-Backup- Server-Agent um.
8019	ТСР			NAT-Port-Umleitung leitet 8019 auf der Appliance auf den SSH-Port 22 des Linux-Sicherungsservers um.
8021	ТСР			NAT -Port-Umleitung leitet 8021 auf der Appliance 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 Appliance auf den Port 8036 des Linux-Sicherungsservers 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 werden 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 anderer Linux-Knoten mit dem Port 50003 in die Cloud gesichert wer- den kann.
50004	ТСР	NAT -Port-Umleitung leitet 50004 auf der Appliance auf den Linux-Sicherungsserver um, damit ein anderer Linux-Knoten mit dem Port 50004 in die Cloud gesichert werden kann.

## **Kapitel 3: Installieren der Arcserve UDP Appliance**

#### Dieser Abschnitt enthält folgende Themen:

So installieren Sie Arcserve Backup r17.5	58
So installieren Sie die 8100 - 8200 Series Appliance	59
So installieren Sie die 8300 - 8400 Series Appliance	60

#### So installieren Sie Arcserve Backup r17.5

Arcserve Backup r17.5 ist nicht auf der Appliance vorinstalliert. Sie können Arcserve Backup r17.5 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 r17.5 aus. Fahren Sie andernfalls mit Schritt 2 fort.

2. Geben Sie das Administratorkennwort ein, und das Skript wird generiert. Dieses hilft Ihnen dabei, Arcserve Backup r17.5 zu installieren.

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. Die erstmalige Einrichtung und Wartung müssen von entsprechend geschultem Personal vorgenommen werden.

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. Die erstmalige Einrichtung und Wartung müssen von entsprechend geschultem Personal vorgenommen werden.

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

## **Kapitel 4: Funktionsweise der Netzwerkkonfiguration**

Dieser Abschnitt enthält folgende Themen:

onfiguration des NIC-Teaming-Prozesses	62
Deaktivieren des DHCP-Servers	64
unktionsweise der Netzwerkkonfiguration auf der UDP-Appliance	65
onfigurieren der IP-Adresse für den vorinstallierten Linux-Sicherungsserve	<u>r</u> 69
ktivieren von Round-Robin auf dem DNS-Server zur Bereitstellung von Las enausgleich	
aktivieren von Round-Robin auf dem DNS-Server zur Bereitstellung von Las enausgleich	

Kapitel 4: Funktionsweise der Netzwerkkonfiguration 61

#### **Konfiguration des NIC-Teaming-Prozesses**

Die Arcserve UDP 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 den Arcserve UDP Appliance-Assistenten über den Windows-Desktop.

**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.

- 2. Wählen Sie im Server-Manager Extras > Routing und Remote-Zugriff. Das Dialogfeld "Routing und RAS" wird geöffnet.
- 3. Klicken Sie mit der rechten Maustaste auf den Knoten des Appliance-Servers, und wählen Sie Routing und RAS deaktivieren aus.

**Hinweis**: Wenn andere Routing- und Remote-Zugriffsfunktionen für andere Zwecke konfiguriert sind, sollten sie diese nach dem Durchführen dieser Schritten neu konfigurieren.

- 4. Klicken Sie im Bestätigungsdialogfeld auf Ja, um den Router zu deaktivieren und die Konfiguration zu entfernen.
- 5. Klicken Sie mit der rechten Maustaste auf den Knoten des Appliance-Servers, und wählen Sie Routing und RAS konfigurieren und aktivieren aus.
  - Der Assistent zum Einrichten des Routing- und Remote-Zugriffsservers wird geöffnet.
- 6. Klicken Sie auf Abbrechen und öffnen Sie eine Windows-Eingabeaufforderung.

#### 7. Führen Sie folgenden Befehl aus:

C:\\Program Files\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 *Appliance.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

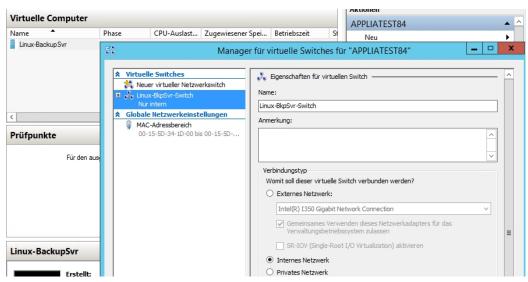
## Funktionsweise der Netzwerkkonfiguration auf der UDP-Appliance

Mit der Netzwerkkonfiguration auf der Appliance soll sichergestellt werden, dass der integrierte Linux-Sicherungsserver (virtueller Name in Hyper-V-Manager: Linux-BackupSvr) hinter der NAT arbeiten kann. Dies bewirkt Folgendes:

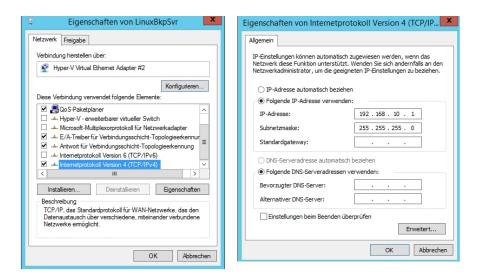
- Der Benutzer muss den Hostnamen des integrierten Linux-Sicherungsservers nicht ändern.
- Der Benutzer speichert eine IP-Adresse für den Linux-Sicherungsserver im Netzwerk.
- Der Linux-Sicherungsserver kann eine Verbindung zu jedem beliebigen Rechner im öffentlichen Netzwerk herstellen.
- Jeder Rechner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

#### Details der Netzwerkkonfiguration:

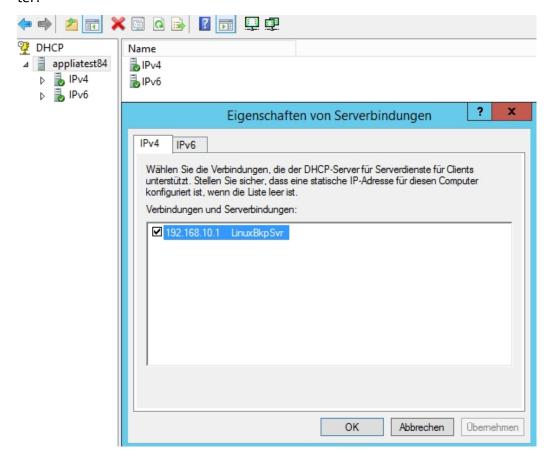
Auf dem Hyper-V-Manager gibt es einen rein internen virtuellen Switch (*Linux-BkpSvr-Switch*), der nur von Linux-BackupSvr verwendet wird.



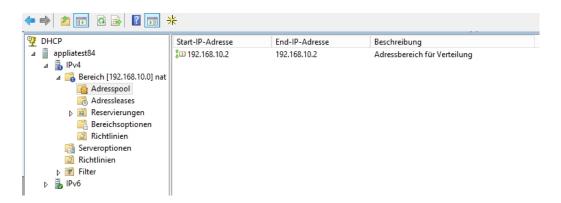
Unter Systemsteuerung\Netzwerk und Internet\Netzwerkverbindungen wird ein "Hyper-V-Adapter für virtuelles Ethernet" namens "LinuxBkpSvr" angezeigt. Die IPv4-Adresse für diesen Switch wurde standardmäßig auf "192.168.10.1" festgelegt, wie unten gezeigt.



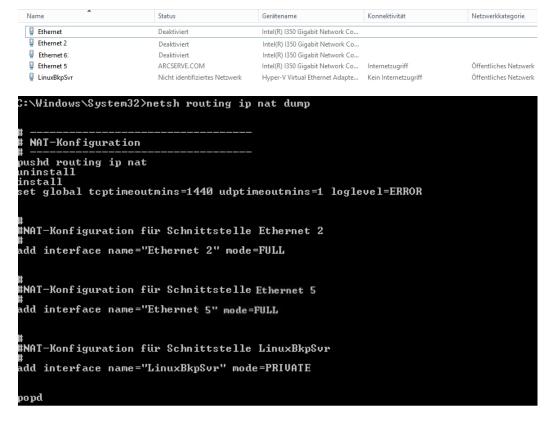
 Der DHCP-Server auf dem Appliance-Rechner wurde standardmäßig konfiguriert; der DHCP-Server funktioniert nur auf dem virtuellen Hyper-V-Adapter.



Standardmäßig ist 192.168.10.2 nur einmal im Adresspool enthalten, um sicherzustellen, dass der integrierte Linux-Sicherungsserver die IP-Adresse 192.168.10.2 abrufen kann.



NAT wurde auf dem Appliance-Rechner konfiguriert.



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

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.

```
Iroot@Linux-BackupSvr network-scripts1# cat ifcfg-eth0
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=dhcp
DEFROUTE=yes
NAME="etho"
[root@Linux-BackupSvr network-scripts]# ifconfig
          Link encap:Ethernet HWaddr 00:15:5D:0A:04:00
eth0
           inet6 addr: fe80::215:5dff:fe0a:400/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:481943 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100859 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36784482 (35.0 MiB) TX bytes:21795976 (20.7 MiB)
lo
          Link encap:Local Loopback
           inet addr:127.0.0.1 Mask:255.0.0.0
           inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

# 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. Informationen zur Kommunikation des vorinstallierten Linux-Sicherungsservers mit dem Appliance-Server finden Sie in der Einführung zur Netzwerkkonfiguration für den vorinstallierten Linux-Sicherungsserver.

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.
- 2. Ändern Sie die IP-Adresse für *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 für "Appliance\_IPAddress" ist auf die Netzwerkschnittstelle LinuxBkpSvr (Hyper-V-Adapter für virtuelles Ethernet) festgelegt, die zur Kommunikation mit diesem vorinstallierten Linux-Sicherungsserver verwendet wird.
- Die IP-Adresse für "Linux\_IPAddress" ist auf den vorinstallierten Linux-Sicherungsserver festgelegt.
- Stellen Sie sicher, dass "Appliance\_IPAddress" und "Linux\_IPAddress" die IP-Adresse desselben Subnetzwerks verwenden.

So sieht die Datei nach dem Ändern 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.

Führen Sie die Eingabeaufforderung aus, und geben Sie den folgenden Befehl ein:

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 RFC 1794.

## 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>

Auf diese Weise erhält ein Resolver immer IPAddress1, wenn er eine Abfrage für Altname1 sendet, und IPAddress2, wenn er eine Abfrage für Altname2 sendet.

# **Kapitel 5: Aktualisieren von Arcserve UDP auf der Appliance**

Dieser Abschnitt enthält folgende Themen:

Anwenden einer Lizenz nach einem Upgrade der Arcserve-Software	74
Upgradesequenz auf der Arcserve UDP Appliance	75
Upgradesequenz für UDP-Konsole, RPS und Agent	81

Kapitel 5: Aktualisieren von Arcserve UDP auf der Appliance 73

## Anwenden einer Lizenz nach einem Upgrade der Arcserve-Software

Nach einem Upgrade von Arcserve UDP auf v6.5 oder von Arcserve Backup auf r17.5 funktioniert der ursprüngliche Lizenzschlüssel auf der Arcserve UDP Appliance nicht mehr. Um die neuen Lizenzschlüssel für Arcserve Unified Data Protection v6.5 und Arcserve Backup r17.5 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 **Arcserve-Produktaktivierung** im *Arcserve Unified Data Protection-Lösungshandbuch*.

Weitere Informationen zum Hinzufügen eines Lizenzschlüssels für Arcserve UDP finden Sie unter *Zuweisen von Arcserve Backup-Komponentenlizenzen* im *Arcserve Backup-Administrationshandbuch*.

### Upgradesequenz auf der Arcserve UDP Appliance

Das Upgrade von Arcserve UDP Appliance v5.0 auf Arcserve UDP v6.5 kann eine der folgenden Sequenzen umfassen:

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

## Aktualisieren der Arcserve UDP Appliance, die als Arcserve UDP-Konsole und RPS ausgeführt wird

Aktualisieren Sie diese Arcserve UDP Appliance. Führen Sie anschließend die <u>Upgradesequenz</u> aus, um die Umgebung zu aktualisieren.

## Aktualisieren der Arcserve UDP Appliance, die nur als Arcserve UDP RPS ausgeführt wird

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

## Upgradeschritte bei Verwendung von mindestens zwei Arcserve UDP Appliances in der Umgebung

- Aktualisieren Sie die vollständige Produktionsumgebung. Details finden Sie unter <u>Upgradesequenz</u>.
- Falls eine Warnmeldung wie die folgende angezeigt wird, wenn Sie nach dem Upgrade über die Arcserve UDP-Konsole eine Appliance als RPS hinzufügen, finden Sie weitere Informationen im Thema <u>Sichern einer UDP Appliance von einer anderen Appliance meldet duplizierte Knoten</u> im Abschnitt Fehlerbehebung.

## Aktualisieren des Arcserve UDP Linux-Agenten auf der Arcserve UDP Appliance

- Aktualisieren Sie zuerst die Arcserve UDP-Konsole, die die Umgebung des Linux-Sicherungsserver verwaltet.
- Aktualisieren Sie anschließend den Linux-Sicherungsserver auf der Arcserve UDP Appliance. Details finden Sie in der Arcserve Unified Data Protection Agent for Linux – Online-Hilfe.

## Aktualisieren von Arcserve Backup auf der Arcserve UDP Appliance

Informationen zum Upgrade auf Arcserve UDP-Appliance finden Sie im **Arcserve Backup-Implementierungshandbuch**.

### 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 Richtlinie zur Abwärtsunterstützung der Replikation sollten Sie den Ziel-RPS immer vor dem Quell-RPS aktualisieren.

## Kapitel 6: Konfigurieren der Arcserve UDP Appliance

Dieser Abschnitt enthält folgende Themen:

Konfiguration der Netzwerkeinstellungen für eine UDP Appliance	83
Übersicht über das Erstellen eines Plans mit dem UDP Appliance-Assistenten	85
Einrichten der Arcserve UDP Appliance und Erstellen von Plänen	86
Weitere Informationen zum Hinzufügen von Knoten zu einem Plan	93
Konfigurieren der UDP Appliance als Gateway	99
Löschen der Konfiguration und Zurücksetzung der Appliance auf Werkseinstellun	<u>igen</u> 100
Zurücksetzen von Arcserve UDP auf Werkseinstellungen unter Verwendung der S	
option	101
Aktivieren des Arcserve-Produkts auf der Appliance	104

Kapitel 6: Konfigurieren der Arcserve UDP Appliance 82

## Konfiguration der Netzwerkeinstellungen für eine UDP Appliance

Um die Arcserve UDP Appliance verwalten zu können, muss die Appliance zunächst in Ihr Netzwerk aufgenommen werden. 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" für die Microsoft-Lizenzbedingungen geöffnet. Lesen und akzeptieren Sie die Bedingungen.
- 2. Das UDP-Dialogfeld **Endbenutzer-Lizenzvereinbarung** wird geöffnet. Lesen und akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 3. Geben Sie einen Hostnamen für die Appliance ein. Das Zuweisen eines Namens erleichtert die Identifizierung der Appliance im Netzwerk.

Um Ihre Appliance als Mitglied einer Domäne in Ihrem Netzwerk hinzuzufügen, klicken Sie auf die Option **Diese Arcserve UDP-Appliance zu einer Domäne hinzufügen**, und geben Sie die Domäne, den Benutzernamen und das Kennwort an.

**Hinweis**: Die Felder für Domäne, Benutzername und Kennwort werden angezeigt, wenn die Option ausgewählt ist.

**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 Neustarten der Appliance können Sie auf die Appliance über die folgende URL von jedem beliebigen anderen Rechner zugreifen:

https://<Hostname>:8015

- 4. Klicken Sie auf Speichern.
- 5. 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.

- 6. Um eine Netzwerkverbindung zu bearbeiten, klicken Sie im Feld **Netzwerkverbindungen** auf **Bearbeiten**.
- 7. Das Dialogfeld **Netzwerkverbindung** wird geöffnet.
- 8. 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.
- 9. 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.
- 10. Das Fenster für die Anmeldung wird erneut geöffnet. Geben Sie den Benutzernamen und das Kennwort ein, und drücken Sie die **Eingabetaste**.
- 11. Wenn das Fenster "Konfiguration" für die Appliance erneut geöffnet wird, klicken Sie auf **Assistenten starten**.

## Übersicht über das Erstellen eines Plans mit dem UDP Appliance-Assistenten

Ein Plan ist eine Sammlung von Schritten, mit denen definiert wird, welche Knoten wann gesichert werden sollen. Mit der Arcserve UDP-Appliance können Sie einfache Pläne erstellen. Das Erstellen eines Plans mit dem Assistenten der UDP-Appliance erfolgt in drei Schritten:

- 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 Lösungs-handbuch*.

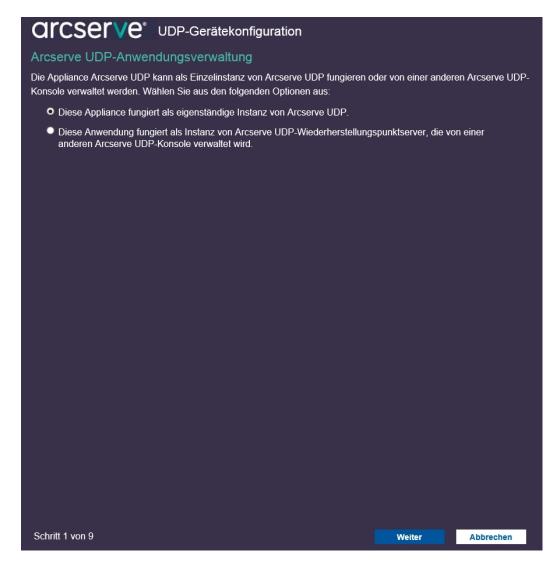
## Einrichten der Arcserve UDP Appliance und Erstellen von Plänen

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 im Konfigurations-Assistenten für die Arcserve UDP Appliance sind optional. Sie können diese überspringen, die UDP-Konsole direkt öffnen und Pläne erstellen.

#### **Befolgen Sie diese Schritte:**

- 1. Melden Sie sich bei der Arcserve UDP-Konsole an.
- Der Unified Data Protection-Assistent öffnet zuerst das Dialogfeld Arcserve UDP Appliance-Verwaltung. 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.



3. 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.

4. Klicken Sie auf Weiter.

**Hinweis:** Um den Assistenten zu schließen und die Arcserve UDP-Konsole zu öffnen, klicken Sie auf **Abbrechen.** 

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.

- 5. Geben Sie das Verschlüsselungskennwort für diesen Datenspeicher ein und bestätigen Sie es.
- 6. Klicken Sie auf Weiter.
- 7. Das Dialogfeld **E-Mail und Warnmeldungen** wird geöffnet.

Dieses Dialogfeld ermöglicht Ihnen die Definition des E-Mail-Servers zum Senden von Warnmeldungen und der Empfänger, die die Warnmeldungen erhalten. Sie können Optionen auswählen, mit denen festgelegt wird, ob die Empfänger die Warnmeldungen auf Basis von erfolgreichen Aufträgen, fehlgeschlagenen Aufträgen oder beidem erhalten.

8. 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.

- 9. Klicken Sie auf Weiter.
- 10. Das Dialogfeld **Replikation zum Remote-RPS** wird geöffnet.
- 11. 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-Lösungs-handbuch*.

#### **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.

12. 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.

- 13. Klicken Sie auf Weiter.
- 14. Das Dialogfeld Plan erstellen wird geöffnet.

Mit diesem Dialogfeld können Sie einen einfachen Plan erstellen, in dem Sie die Knoten, die Sie schützen möchten, und den Sicherungsablaufplan angeben.

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

- a. Klicken Sie auf Planerstellung abbrechen.
- b. Das Dialogfeld **Nächste Schritte** wird geöffnet.
- c. Klicken Sie auf **Fertig stellen**, um die UDP-Konsole zu öffnen und Pläne zu erstellen.
- 15. 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.

◆ Von einem Hyper-V-Server importieren

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.

16. Nachdem die Knoten zu Ihrem Plan hinzugefügt wurden, klicken Sie auf **Weiter**.

Das Dialogfeld Sicherungsablaufplan wird geöffnet.



- 17. 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**.

18. Klicken Sie auf Weiter.

Das Dialogfeld Bestätigung des Plans wird geöffnet.

19. 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:

20. 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.

21. Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden, und öffnen Sie die Arcserve UDP-Konsole.

## Weitere Informationen zum Hinzufügen von Knoten 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 mithilfe des UDP Appliance-Assistenten hinzufügen. Im Assistenten können Sie Knoten mithilfe der folgenden Methoden hinzufügen:

- Manuelle Eingabe der IP-Adresse oder des Hostnamens für den Knoten (Knoten nach Hostname/IP-Adresse hinzufügen)
- 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
   (Hyper-V-Knoten hinzufügen)

### 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 UDP Agent (Windows) installiert.

#### **Befolgen Sie diese Schritte:**

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

#### 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.

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.

- (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.

### 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.

2. Klicken Sie auf Durchsuchen.

Die erkannten Knoten werden angezeigt.

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 ent-
	fernen, wählen Sie die Knoten aus, und klicken Sie auf <b>Entfernen</b> .

6	Klick	an Sia	auf 1	Neiter
D.	NIIICKI	-11 310	auı <b>v</b>	vener

### 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:**

 Geben Sie im Dialogfeld Knoten nach vCenter/ESX hinzufügen die folgenden Details zum vCenter/ESX-Server an, und klicken Sie auf Verbinden.

#### 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.

- 2. Die erkannten Hostnamen werden angezeigt. Erweitern Sie einen Hostnamen, um die Knoten anzuzeigen.
- 3. Wählen Sie die Knoten aus, die Sie hinzufügen möchten, und klicken Sie auf **Zur Liste hinzufügen**.

Die ausgewählten Knoten werden im rechten Fensterbereich hinzugefügt.

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

### 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.

#### 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.

Klicken Sie auf Verbinden.

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

- 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.

### Konfigurieren der UDP Appliance als Gateway

Sie können die Arcserve UDP Appliance als Gateway konfigurieren.

#### Befolgen Sie diese Schritte:

- 1. Deinstallieren Sie die Arcserve UDP-Konsole von der Arcserve UDP Appliance.
- 2. Klicken Sie in der Arcserve UDP-Konsole auf die Registerkarte Ressourcen.
- 3. Navigieren Sie im linken Fensterbereich der Arcserve UDP-Konsole zu **Infrastrukturen**, und klicken Sie auf **Standorte**.
- 4. Klicken Sie auf Standort hinzufügen.
- 5. Befolgen Sie die Anweisungen des Assistenten **Standort hinzufügen**, um das Arcserve UDP Remote Management Gateway auf der Arcserve UDP Appliance zu installieren.

**Hinweis:** Klicken Sie nach der Installation des Arcserve UDP Remote Management Gateway in der Arcserve UDP-Appliance auf **Assistenten starten**. Die Arcserve UDP-Konsole wird nicht durch den Assistenten gestartet. Um auf die Arcserve UDP-Konsole zuzugreifen, geben Sie die URL der Arcserve UDP-Konsole direkt an.

## Löschen der Konfiguration und Zurücksetzung der Appliance auf Werkseinstellungen

Mithilfe der Funktion zum Zurücksetzen auf Werkseinstellungen können Sie Ihre Arcserve UDP Appliance auf einen fehlerfreien und nicht konfigurierten Status 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:

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.

### Zurücksetzen von Arcserve UDP auf Werkseinstellungen unter Verwendung der Startoption

Sie können UDP auch über das Startmenü der UDP Appliance auf die Werkseinstellungen zurücksetzen. Mithilfe der Funktion zum Zurücksetzen auf Werkseinstellungen von UDP können Sie Ihre Arcserve UDP Appliance auf einen fehlerfreien und nicht konfigurierten Status zurücksetzen.

Hinweis: Sie können während des Zurücksetzens von UDP auf die Werkseinstellungen auch die Option zum Erhalten von Sicherungsdaten wählen.

#### **Befolgen Sie diese Schritte:**

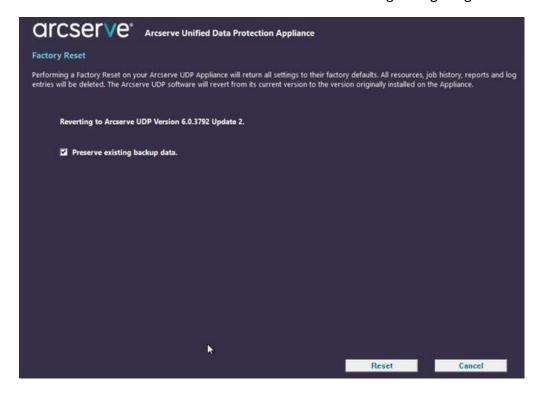
1. Drücken Sie F11, um das Startmenü aufzurufen.



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 auf Volume X:\ und Volume Y:\ bleiben unverändert.

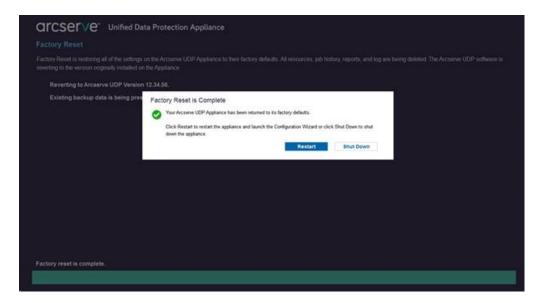
- Wenn Sie die Option zum Erhalten vorhandener Sicherungsdaten deaktivieren, werden alle Daten auf den entsprechenden Volumes C:\, X:\ und Y:\ im ursprünglichen Betriebssystem neu erstellt.
- 3. Klicken Sie auf "Zurücksetzen".

Ein Bestätigungsdialogfeld wird angezeigt.



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

- 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.



### Aktivieren des Arcserve-Produkts auf der Appliance

Weitere Informationen zum Aktivieren des Arcserve-Produkts auf der Appliance finden Sie unter dem Thema <u>Aktivieren der Arcserve-Produktlizenz online</u> im Lösungshandbuch.

### Kapitel 7: Erstellen von Sicherungsablaufplänen

Mit UDP Appliance können Sie Sicherungsablaufpläne 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:

Sicherungsablaufplan für Linux-Knoten erstellen	106
Sicherungsablaufplan für ein Bandgerät erstellen	107
Virtuellen On-Appliance-Standby-Plan erstellen	109

Kapitel 7: Erstellen von Sicherungsablaufplänen 105

### Sicherungsablaufplan für Linux-Knoten erstellen

Linux-Knoten können über die Appliance-Konsole gesichert werden. Der Linux-Sicherungsserver wurde bereits zur Konsole hinzugefügt.

#### **Befolgen Sie diese Schritte:**

- 1. Öffnen Sie die 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

UDP 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.

Der folgenden Prozess liefert eine Übersicht darüber, wie das Schreiben auf ein Bandgerät mit der UDP Appliance funktioniert:

#### 1. Bandgerät an der UDP Appliance anschließen

Auf der Rückseite der UDP Appliance befindet sich ein Port zum Anschluss eines Bandgeräts. Nachdem Sie das Bandgerät angeschlossen haben, identifiziert UDP Appliance automatisch das Bandgerät.

#### 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 zum Konfigurieren und Verwalten des Geräts finden Sie unter "Verwalten von Geräten und Medien im Arcserve Backup für Windows Administrationshandbuch".

## 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 über das Erstellen eines Sicherungsablaufplans für verschiedene Knoten finden Sie unter "Erstellen von Plänen zum Schutz von Daten" im Lösungshandbuch.

#### 4. Bandsicherungsauftrag über Backup Manager starten

Öffnen Sie Backup Manager und erstellen Sie einen Plan zur Sicherung von Daten auf das Bandgerät. Hier sind die Quelldaten das Ziel der UDP-Sicherungsablaufplans, und das Ziel ist das Bandgerät.

**Hinweis:** Weitere Informationen zum Erstellen eines Bandsicherungsablaufplans finden Sie unter "Sichern und Wiederherstellen von D2D/UDP-Daten im Arcserve Backup for Windows Administrationshandbuch.

### Virtuellen On-Appliance-Standby-Plan erstellen

Die Appliance kann als virtueller Standby-Rechner fungieren. Diese Funktion ist in die folgenden Appliance-Serien integriert:

- Arcserve UDP Appliance 7200V
- Arcserve UDP Appliance 7300V
- Arcserve UDP Appliance 7400V
- Arcserve UDP Appliance 7500V
- Arcserve UDP Appliance 7600V
- Arcserve UDP Appliance 8100
- Arcserve UDP Appliance 8200
- Arcserve UDP Appliance 8300
- Arcserve UDP Appliance 8400

Voraussetzung: Sie müssen über einen erfolgreichen Sicherungsplan verfügen.

#### Befolgen Sie diese Schritte:

- 1. Öffnen Sie die Appliance-Konsole.
- 2. Navigieren Sie zu den Plänen, und ändern Sie den Sicherungsplan.
- 3. Fügen Sie eine Virtual Standby-Aufgabe hinzu.
- 4. Aktualisieren Sie die Quelle, das Ziel und virtuelle Rechnerkonfigurationen.

**Hinweis:** Weitere Informationen zu den Konfigurationen finden Sie im Thema zur *Erstellung eines Virtual Standby-Plans* im Lösungshandbuch.

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

# **Kapitel 8: Reparieren der Arcserve UDP Appliance**

Dieser	Abschnitt	enthält folgende	Themen:
--------	-----------	------------------	---------

Easthlatte entformen und ersetzen	111
i estidiatte entremen una ersetzen	 444

Kapitel 8: Reparieren der Arcserve UDP Appliance 110

#### Festplatte entfernen und ersetzen

Wenn bei der Arcserve UDP Appliance eine Festplatte ausfällt, laufen sofort die restlichen Laufwerke an, um sicherzustellen, dass keine Daten verloren gehen und die Appliance weiterhin normal funktioniert. 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 UDP 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.
- 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.

# Kapitel 9: Sicherheitsmaßnahmen

Dieser Abschnitt enthält folgende Themen:

Allgemeine Sicherheitsmaßnahmen	114
Sicherheitsmaßnahmen zur Elektrik	116
FCC-Konformität	118
Vorsichtsmaßnahmen gegen elektrostatische Entladungen (ESD)	119

Kapitel 9: Sicherheitsmaßnahmen 113

#### Allgemeine Sicherheitsmaßnahmen

Im Folgenden finden Sie allgemeine Sicherheitsmaßnahmen, die Sie beachten sollten, um sich selbst vor Verletzungen 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)으로전 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 으로합니다

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

- Überprüfen Sie die Box, in der die Appliance geliefert wurde, und stellen Sie sicher, dass keine sichtbaren Anzeichen von Beschädigungen vorliegen. 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 Nähe von mindestens einer geerdeten Steckdose platziert werden. Je nach Modell enthält die Appliance entweder ein einzelnes Netzteil oder ein redundantes Netzteil und benötigt 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 entfernt wurden, abseits von der Appliance oder auf einem Tisch, damit Sie nicht versehentlich darauf 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

Im Folgenden finden Sie Sicherheitsmaßnahmen zur Elektrik, die Sie beachten sollten, um sich selbst vor Verletzungen 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 Nähe frei liegender elektrischer Stromkreise sollte eine andere Person, die mit den Ausschalt-Bedienelementen vertraut ist, in der Nähe 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-Akku: VORSICHT: Es besteht Explosionsgefahr, wenn der Onboard-Akku verkehrt herum eingebaut wird, da so die Polarität vertauscht wird. Dieser Akku darf nur gegen einen Akku des gleichen oder eines gleichwertigen Typs ausgetauscht werden, der vom Hersteller empfohlen wurde. Entsorgen Sie verbrauchte Akkus gemäß den Anweisungen des Herstellers.

DVD-ROM-Laser: VORSICHT: 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 10: Arbeiten mit IPMI**

Dieser Abschnitt enthält folgende Themen:

So ändern Sie das IPMI-Kennwort	
So aktualisieren Sie die IPMI-Firmware	

Kapitel 10: Arbeiten mit IPMI 120

#### 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:

 Starten Sie Ihr System. Daraufhin wird ein Startbildschirm angezeigt. Drücken Sie in diesem Bildschirm die Entf-Taste. 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.

2. Wählen Sie die Registerkarte "IPMI" im oberen Bereich des BIOS-Hauptbildschirms.

**Hinweis**: Standardmäßig ist die Konfigurationsadressquelle auf DHCP festgelegt.

- 3. 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.
- 4. Notieren Sie die IP-Adresse für die Station.
- 5. 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.

- 6. Geben Sie im Feld Benutzername Ihren Benutzernamen ein. (Standardmäßig ADMIN)
- 7. Geben Sie im Feld Kennwort Ihr Kennwort ein. (Standardmäßig ARCADMIN)
- 8. Die Startseite angezeigt wird (IPMI-Hauptbildschirm).
- 9. Klicken Sie in der oberen Leiste auf die Option Konfiguration. Der Bildschirm "Konfiguration" wird angezeigt.
- 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. Daraufhin wird das Fenster "Benutzer ändern" angezeigt.
- 13. Geben Sie Ihren Benutzernamen ein. (ADMIN)
- 14. Aktivieren Sie das Kontrollkästchen Kennwort ändern, um das Kennwort zu ändern. Das Kennwortfeld ist 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 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:

1. 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.

# Kapitel 11: Herstellen einer Verbindung zwischen dem Appliance-Server und dem Appliance-Erweiterungs-Shelf

Dieser Abschnitt enthält folgende Themen:

Appliance-Infield-Erweiterung für alle verfügbaren Modelle	124
In der Box enthaltene Gegenstände	134
So stellen Sie eine Verbindung zwischen dem Appliance-Server und dem Appliance- Erweiterungs-Shelf her	137
So ändern Sie den Arcserve UDP-Datenspeicher	145

Kapitel 11: Herstellen einer Verbindung zwischen dem Appliance-Server und dem Appliance-

# 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	BESCHREIBUNG
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)	2. 8100 – 8-TB- Erweiterungs- Shelf enthält eingebaute und vor- konfigurierte SSD 240 GB.  3. 8100 verfügt über 2 und 3 als optionale Steckplätze. Ein freier Steckplatz ist obligatorisch für die App- liance-Infield- Erwei- terung/Me-

				mit Add-on-
				Karten gefüllt
				sind, müssen
				Sie min-
				destens einen
				Steckplatz frei
				machen, um
				die Infield-
				Erweiterung
				verwenden zu
				können, vor-
				zugsweise
				Steckplatz 3.
			5.	Der SAS-
				Anschluss
				wird zwischen
				der Appliance
				und dem
				Erweiterungs-
				Shelf ver-
				wendet.
			6.	8100 – Erwei-
				terungs-Shelf
				enthält RAID
				6.
			7	Erweiterungs-
			/.	Shelf enthält
				zwei Netz-
				teile.
			0	
			8.	Folgen Sie
				den <b>Anwei</b> -
				sungen zum
				Hinzufügen eines Daten-
				pfads im
				Erwei-
				terungs-
				handbuch,
				nachdem Sie
<u> </u>				

								das Erweiterungs-Shelf angeschlossen haben. Wenn eine neue SSD erforderlich ist, folgen Sie den Anweisungen unter HASH-Ziel zu neuer SSD migrieren im Erweiterungshandbuch.
8200	8, 12	8 (6 x 2-TB-Fest-platten) ODER 16 (6 x 4-TB-Fest-platten)	220	8 TB NA 16 TB 280	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)	2.	Modell 8200 unterstützt 8- TB- oder 16- TB-Infield- Erweiterung. Clients kön- nen jeweils nur ein Erwei- terungs-Shelf anschließen.  8200 – 16-TB- Erweiterungs- Shelf enthält eingebaute und vor- konfigurierte SSD 480 GB.  8200 verfügt über 2 und 3 als optionale Steckplätze. Ein freier Steckplatz ist

				obligatorisch
				für die App- liance-Infield-
				Erwei-
				terung/Me-
				gaRAID SAS
				9380-8e.
			4.	Wenn beide
				optionalen
				Steckplätze
				mit Add-on-
				Karten gefüllt
				sind, müssen
				Sie min-
				destens einen
				Steckplatz frei
				machen, um
				die Infield-
				Erweiterung
				verwenden zu
				können, vor-
				zugsweise
				Steckplatz 3.
			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.	Folgen Sie den Anweisungen zum Hinzufügen eines Datenpfads im Erweiterungshandbuch, nachdem Sie das Erweiterungs-Shelf angeschlossen haben.
						9.	Wenn eine neue SSD erforderlich ist, folgen Sie den Anwei- sungen unter HASH-Ziel zu neuer SSD migrieren im Erwei- terungs- handbuch.
8300	16, 20, 24, 28, 32, 36, 40	8 (6 x 2-TB-Fest-platten) ODER 16 (6 x 4-TB-Fest-platten) ODER 40 (12 x 4-TB-Fest-	8 TB - NA 16 TB - 560 40 TB - 790	2, 5, 6	LSI SAS 9200 – 8E HBA Qlogic Dual-Port HBA Quad- Port 1G Netz- werk- karte  Dual-Port 10G SPF +		Modell 8300 unterstützt 8- TB-, 16-TB- oder 40-TB- Infield-Erwei- terung. Cli- ents können jeweils nur ein Erwei- terungs-Shelf anschließen. 8300 – 16-TB- /40-TB-Erwei-

				und dem Erweiterungs- Shelf ver- wendet.
			6.	Erweiterungs- Shelf enthält RAID-6 (6 x 4- TB-Fest- platten).
			7.	Erweiterungs- Shelf enthält zwei Netz- teile.
			8.	Folgen Sie den Anweisungen zum Hinzufügen eines Datenpfads im Erweiterungshandbuch, nachdem Sie das Erweiterungs-Shelf angeschlossen haben.
			9.	Wenn eine neue SSD erforderlich ist, folgen Sie den Anwei- sungen unter HASH-Ziel zu neuer SSD migrieren im Erwei- terungs-

								handbuch.
								(Nur für App-
								liance 8300:
								Beim Ver-
								binden mit
								einem 40-TB-
								Appliance-
								Erweiterungs-
								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).
						LSI SAS	1.	Modell 8400
		8				9200 – 8E		unterstützt 8-
		J		8		HBA		TB-, 16-TB-
		(6 x 2-TB-		ТВ		Qlogic		oder 40-TB-
	32,40,48,56,6- 4,72,80	Fest-		- NA 16 TB - NA	2, 5, 6	Dual-Port		Infield-Erwei-
		platten)				НВА		terung. Cli-
		ODER				Quad- Port 1G		ents können
		16 (6 x 4-	1200					jeweils nur
8400						Netz-		ein Erwei-
		TB-Fest-				werk-		terungs-Shelf
		platten)				karte		anschließen.
		ODER		40			2.	8400 – erfor-
		40 (12 x		ТВ		Dual-Port		dert keine
		40 (12 x 4-TB-Fest-		– NA		10G SPF +		zusätzliche
		platten)		INA		Dual-Port		SSD.
		,				10G Kup-	3.	8400 verfügt
						fer		<u> </u>

		T			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 Add-on-
					Karten gefüllt
			Infield-		sind, müssen
			Erwei- terung		Sie min-
			(MegaRAI	_	destens einen
			D SAS		Steckplatz frei
			9380-8e)		machen, 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.	Erweiterungs-
					Shelf enthält
					RAID 6.

			7.	Erweiterungs- Shelf enthält zwei Netz-
				teile.
			8.	Folgen Sie
				den <b>Anwei</b> -
				sungen zum
				Hinzufügen
				eines Daten-
				pfads im
				Erwei-
				terungs-
				handbuch,
				nachdem Sie
				das Erwei-
				terungs-Shelf
				angeschlossen
				haben.

### In der Box enthaltene Gegenstände

Die folgenden Gegenstände sind in der Box enthalten:

Hinweis: Wenn Gegenstände in der Box beschädigt sind, kontaktieren Sie Arcserve.

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 Arcserve UDP-Pläne an. Überprüfen Sie die Arcserve UDP-Konsole, um sicherzustellen, dass auf dem Appliance-Server keine Jobs ausgeführt werden, und halten Sie alle Pläne an.
- 4. Schalten Sie den Appliance-Server aus, und trennen Sie das Netzkabel vom Netzteil.

**Hinweis:** Trennen Sie den Computer von der Stromversorgung, um Schäden am System oder das Risiko eines Stromschlags zu vermeiden.

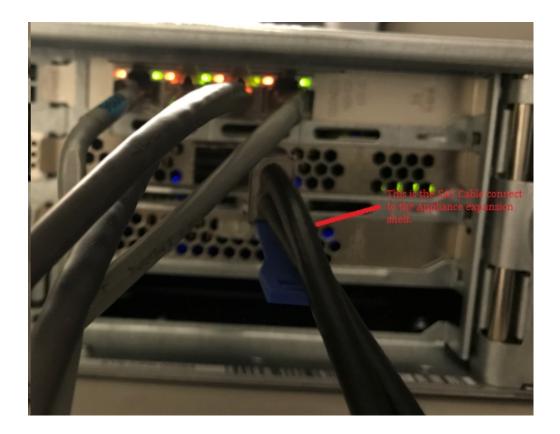
- 5. Entfernen Sie die Abdeckung des Appliance-Server-Gehäuses.
- 6. Schließen Sie den *MegaRAID Controller 9380-8e* an einem freien PCI-e-Steckplatz des Appliance-Servers an.

#### **Befolgen Sie diese Schritte:**

- 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. Bewahren Sie die Halterungsschraube gegebenenfalls auf.
- d. Richten Sie den MegaRAID Controller 9380-8e an einem PCIe-Steckplatz aus.
- e. Drücken Sie den RAID Controller behutsam, aber mit Kraft nach unten, um ihn korrekt im Steckplatz zu platzieren.



- 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 das SAS-Kabel zwischen dem *MegaRAID Controller 9380-8e* des Appliance-Servers und dem MegaRAID Controller im Appliance-Erweiterungs-Shelf.

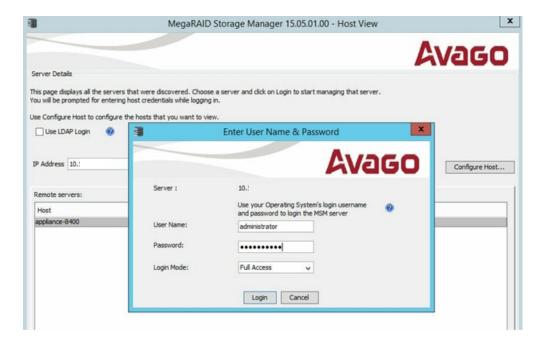


10. Setzen Sie die SSD ein (nur für Appliance 8300 + Erweiterungs-Shelf mit 40 TB).

**Hinweis:** Wenn ein Appliance-Erweiterungs-Shelf mit 40 TB mit einer Appliance 8300 verbunden ist, setzen Sie die SSD mit 2 TB (im Lieferumfang des Appliance-Erweiterungs-Shelf) in den leeren SATA-Steckplatz an der Rückseite der Appliance 8300 ein.



- 11. Schalten Sie das Appliance-Erweiterungs-Shelf ein. Schließen Sie die Netzkabel des Appliance-Erweiterungs-Shelf an, und schalten Sie das Appliance-Erweiterungs-Shelf ein.
- 12. Schalten Sie den Appliance-Server ein. Schließen Sie die Netzkabel des Appliance-Servers erneut an, und schalten Sie den Appliance-Server ein.
- 13. Melden Sie sich beim MegaRAID Storage Manager an. Melden Sie sich beim Appliance-Server an, öffnen Sie den MegaRAID Storage Manager, und melden Sie sich mit den Administrator-Anmeldeinformationen an.

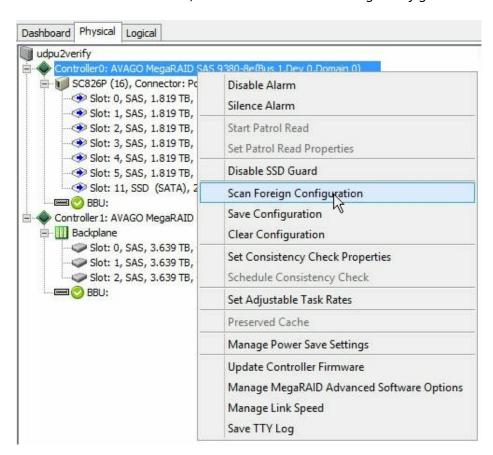


14. Überprüfen Sie den RAID-Controller über den MegaRAID Storage Manager.

#### **Befolgen Sie diese Schritte:**

- a. Auf der Registerkarte "Physisch" oder "Logisch" sind zwei Controller aufgelistet.
- Wählen Sie den Controller 9380-8e, und stellen Sie sicher, dass alle mit dem Controller 9380-8e verbundenen 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*.



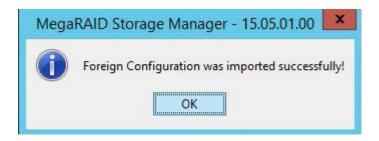
Wählen Sie "Fremde Datenträger importieren", und klicken Sie auf "OK".



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



Klicken Sie auf OK.



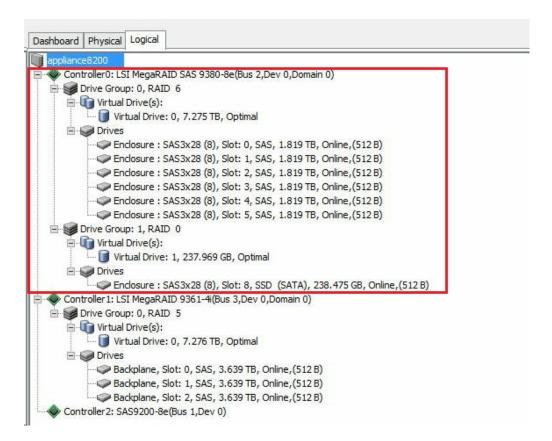
Alle Laufwerke im Erweiterungs-Shelf sind nun online.

Auf der Registerkarte "Logisch" werden die Datenträger angezeigt, die mit RAID-6 konfiguriert wurden. Für andere Module des Erweiterungs-Shelf wird eine SSD als RAID-0 festgelegt und unter *LSI MegaRAID SAS 9380-8e* aufgelistet.

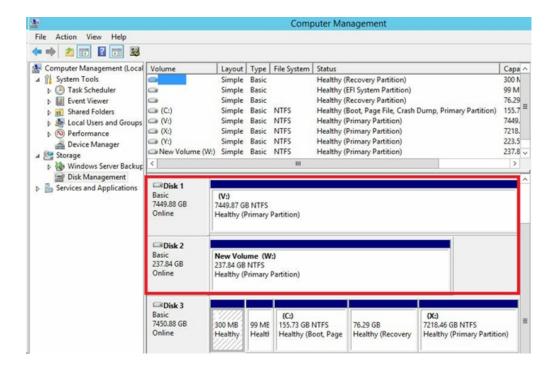
Appliance-Server 8100 + Erweiterungs-Shelf mit 8 TB;

Appliance-Server 8200 + Erweiterungs-Shelf mit 16 TB;

Appliance-Server 8300 + Erweiterungs-Shelf mit 16 TB;



15. Überprüfen Sie die Datenträger in der Datenträgerverwaltung. Öffnen Sie die Datenträgerverwaltung. Wenn der Datenträger im Appliance-Erweiterungs-Shelf nicht formatiert ist, formatieren Sie ihn als NTFS, und vergeben Sie einen Laufwerkbuchstaben wie "V:". Wenn die SSD nicht formatiert ist, formatieren Sie sie auch als NTFS, und vergeben Sie einen Laufwerkbuchstaben wie "W:".



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
- Überprüfen der Gesamtkapazität des Datenspeichers <data store name> über die Arcserve UDP-Konsole
- Fortsetzen aller Pläne von der Arcserve UDP-Konsole

## Hinzufügen eines Datenpfads auf dem Erweiterungs-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 <data store name> -NewDataPath <new data
folder>

as\_gddmgr.exe -DataPath Display <data store name>

### Migrieren eines Hash-Ziels zur neuen SSD

**Hinweis:** Dieser Schritt ist nur erforderlich, wenn Sie eine neue SSD für das 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 *<data store name>* gestoppt wird. Stoppen Sie andernfalls den Datenspeicher *<data store name>* über die Arcserve UDP-Konsole.
- 3. Ändern Sie den Datenspeicher < data store name > über die Arcserve UDP-Konsole, und legen Sie das Hash-Ziel auf W:\Arcserve\data\_store\hash fest.
- 4. Speichern Sie die Änderung des Datenspeichers.
- 5. Starten Sie den Datenspeicher *<data store name>* über die Arcserve UDP-Konsole.

# Überprüfen der Gesamtkapazität des Datenspeichers <a href="https://data.com

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 12: Fehlerbehebung**

Dieser Abschnitt enthält folgende Themen:

Linux-Sicherungsserver kann über die Konsole keine Verbindung herstellen	152
Sichern einer UDP Appliance von einer anderen Appliance meldet duplizierte Knoten	154
Linux-Sicherungsserver kann das Netzwerk-DNS-Suffix nicht abrufen	156
Standardzeitzone auf der Appliance	157
Lizenzfehler, auch wenn Lizenzen verfügbar sind	158

Kapitel 12: Fehlerbehebung 151

# 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.
- 5. 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 UDP Appliance von einer anderen Appliance meldet duplizierte Knoten

#### **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 Agent-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
- 3. 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 Agentenknoten 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 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 Sie die statische IP-Adresse auf den Appliance-Server festlegen, wodurch dann vom Linux-Sicherungsserver das Netzwerk-DNS-Suffix nicht ordnungsgemäß abgerufen werden 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

Um dieses Problem zu lösen, wechseln Sie zum Arcserve Backup Appliance-Assistenten und klicken auf Bearbeiten, Datum und Uhrzeit, 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.

## **Kapitel 13: Empfehlungen**

Dieser Abschnitt enthält folgende Themen:

Best Practices für die Netzwerkkonfiguration	. 160
Best Practices für die Migration der Arcserve UDP-Konsole	. 163
Best Practices für eine Bare-Metal-Recovery (BMR) ohne Erhalten von Daten	.165
Best Practices für eine Bare-Metal-Recovery (BMR) und das Erhalten von Daten	. 176
Best Practices für das Linux-Migrations-Tool	.184
Best Practices für das Dienstprogramm "Appliance-Image festlegen"	. 186
Best Practices für vorinstallierte Linux-Sicherungsserver in der Arcserve UDP Appliance	.189
Best Practices für die Arcserve UDP-Appliance zum Sichern des Linux-Sicherungsservers selbst	.191
Best Practices zur Migration zwischen Arcserve UDP-Appliances	. 195
Lösung 1	. 196
Lösung 2	. 201
Best Practices für Linux-Instant VM-Job auf Arcserve UDP-zu Hyper-V auf lokaler App- liance	- . <b>20</b> 4
Best Practices zum Hinzufügen von "Replizieren" zu einem remote verwalteten RPS- Task einer anderen Appliance	. 205
Best Practices zum Durchführen eines Virtual Standby (VSB)-Task, bei dem der Monitor eine andere Appliance ist	. 207

Kapitel 13: Empfehlungen 159

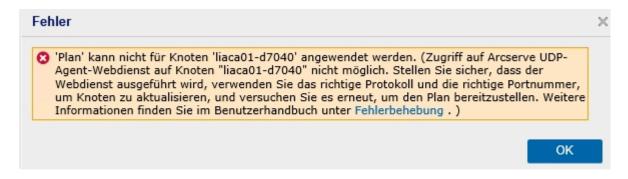
### Best Practices für die Netzwerkkonfiguration

- 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 <u>Deaktivieren des DHCP-Servers</u> im Appliance-Benutzerhandbuch.
- Bei einem Verbindungsproblem zwischen der Appliance und einem Agent-Knoten, wenn die Appliance und der Agent-Knoten im Netzwerk online sind. Das Problem tritt auf, wenn mehrere Netzwerkschnittstellen mit demselben Subnetzwerk in der Appliance verbunden sind.

#### **Problem**

Wenn die Appliance und der Agent-Knoten in einem Subnetzwerk online sind. Die folgenden Symptome können auftreten:

• In der Arcserve UDP-Konsole wird bei der Bereitstellung des Plans für den Agent-Knoten folgende Fehlermeldung angezeigt:



 Der Sicherungsjob des Agent-Knotens schlägt wie unten angegeben fehl:



 Pingen Sie den Agent-Knoten von der Appliance, und überprüfen Sie, ob der Agent-Knoten verbunden ist:

```
C:\Users\Administrator>ping 10.57.52.13

Ping wird ausgeführt für 10.57.52.13 mit 32 Bytes Daten:
Antwort von 10.57.52.13: Bytes=32 Zeit<1ms TTL=128
```

Pingen Sie den Appliance-Hostnamen vom Agent-Knoten, wenn die Appliance NICHT verbunden ist:

```
C:\Users\Administrator>ping appliatest76

Ping wird ausgeführt für appliatest76 [10.57.52.47] mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.

Ping-Statistik für 10.57.52.47:
Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
(100% Verlust),
```

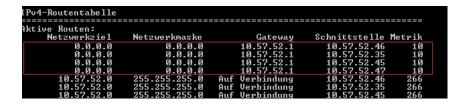
#### Lösung

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-Servers</u> im Appliance-Benutzerhandbuch.
- Gehen Sie auf der Appliance und auf dem Agent-Knoten folgendermaßen vor:

#### Schritte auf der Appliance:

- 1. 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 Appliance auf:



#### 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>ping 10.57.52.46
Ping wird ausgeführt für 10.57.52.46 mit 32 Bytes Daten:
Antwort von 10.57.52.46: Bytes=32 Zeit=1ms TTL=128
Antwort von 10.57.52.46: Bytes=32 Zeit(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 die Migration der Arcserve UDP-Konsole

In der Arcserve UDP-Appliance können Sie die Arcserve UDP-Konsole mit der *ConsoleMigration.exe* in 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>ConsoleMigration.exe
-BackupDB

Backed up DB and version files completed.

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

Der Ordner DB Migration wird erstellt.

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

<UDP Home> \Management\BIN\Appliance\

3. Wenn die neue Arcserve UDP-Konsole eine Arcserve UDP-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 es sich bei der Arcserve UDP-Konsole nicht um eine Arcserve UDP-Appliance handelt, 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\DB\_Migration\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

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 Protection\Management\BIN\Appliance\DB_Migration\logs".

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

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

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

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

**Hinweis:**In Arcserve UDP v6.5 Update 4 wird die Option *-force* im Befehl *ConsoleMigration.exe* eingeführt, um die Migration der Recovery-Sicherungsdatenbankdateien auf der Zielkonsole unter folgenden Umständen zu erzwingen:

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

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

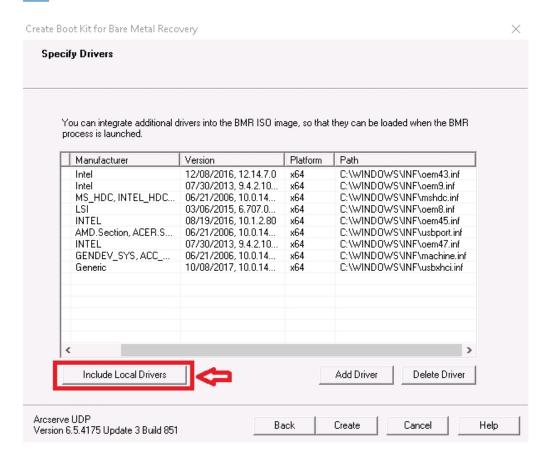
# Best Practices für eine Bare-Metal-Recovery (BMR) ohne Erhalten von Daten

Sie können auf der Arcserve UDP Appliance eine Bare-Metal-Recovery mithilfe des Arcserve UDP-Bootkits ausführen.

#### **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.



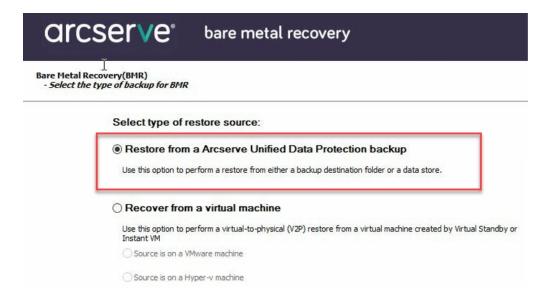
2. Starten Sie die Arcserve UDP Appliance mit dem BMR-ISO-Image oder dem USB-Stick.

Das Arcserve Bare-Metal-Recovery Setup wird angezeigt.

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

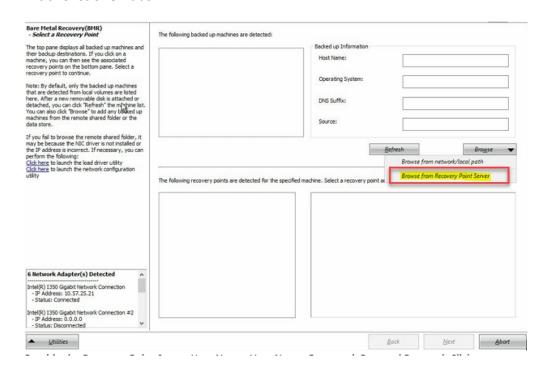


4. Wählen Sie die Option Wiederherstellung von einer Arcserve Unified Data Protection-Sicherung aus, und klicken Sie auf Weiter.



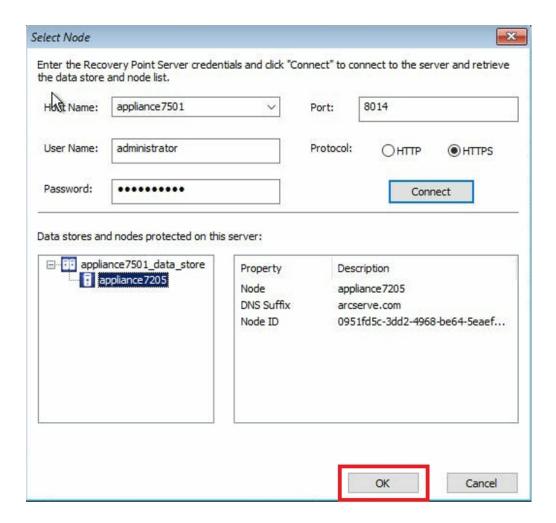
Das Fenster **Assistent zum Auswählen eines Wiederherstellungspunkts** wird angezeigt.

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



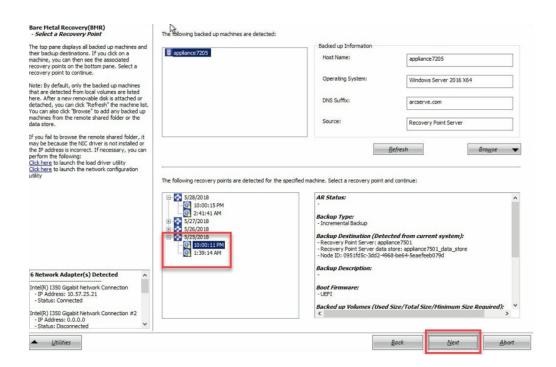
Das Fenster Knoten auswählen wird angezeigt.

- 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.



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

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



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



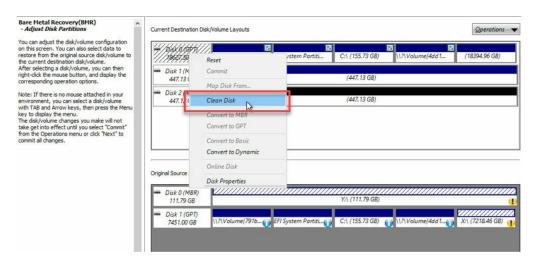
Das Dialogfeld Bare-Metal-Recovery (BMR) – Wiederherstellungsmodus auswählen wird angezeigt.

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

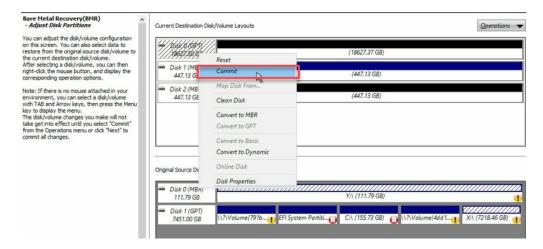


Das Dialogfeld Bare-Metal-Recovery (BMR) – Datenträgerpartitionen anpassen wird angezeigt.

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

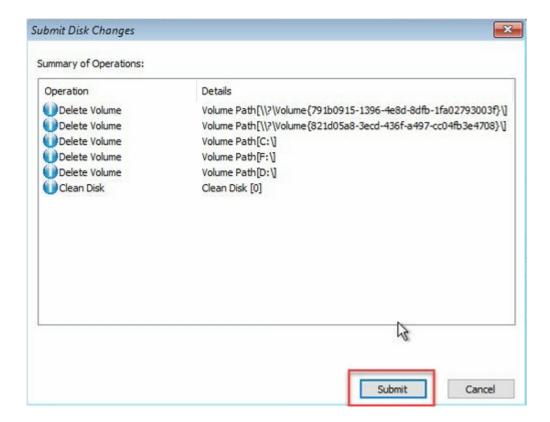


13. Klicken Sie nach der Reinigung der Festplatte mit der rechten Maustaste auf denselben Datenträger, und klicken Sie auf **Commit**.

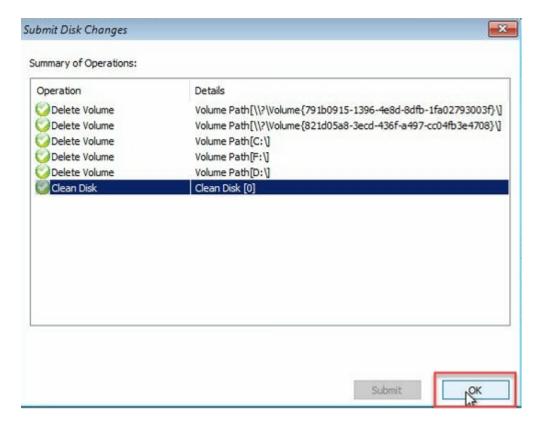


Das Fenster **Datenträgeränderungen übergeben** wird angezeigt.

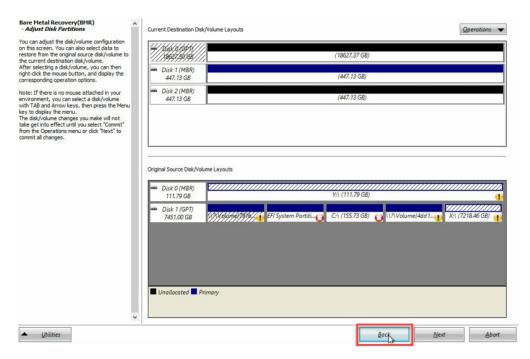
14. Klicken Sie auf Übergeben.



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



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



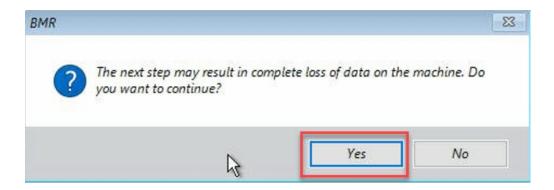
Das Dialogfeld Bare-Metal-Recovery (BMR) – Wiederherstellungsmodus auswählen wird angezeigt.

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



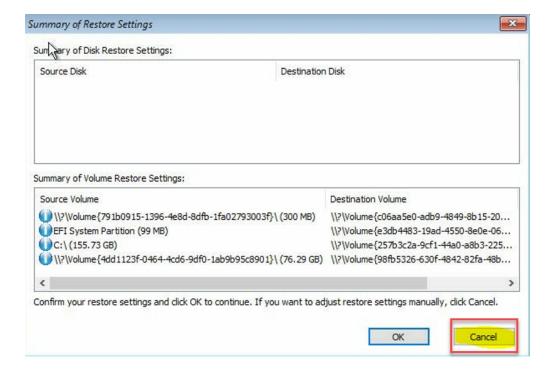
Das Dialogfeld BMR wird angezeigt.

18. Klicken Sie auf Ja.



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

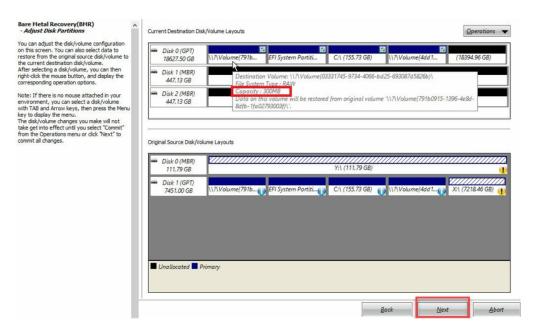
19. Klicken Sie auf Abbrechen.



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

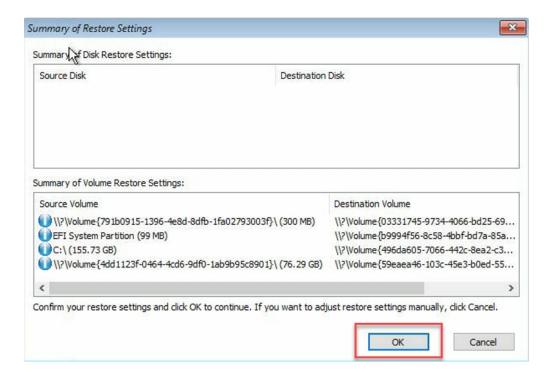
20. Vergleichen und überprüfen Sie, ob die Kapazität der ersten vier Partitionen auf der Registerkarte Aktuelle Zieldatenträger/Volume-Layouts dem größten verfügbaren GPT-Datenträger auf der Registerkarte Ursprüngliche Quelldatenträger/Volume-Layouts entspricht, und klicken Sie aufWeiter.

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



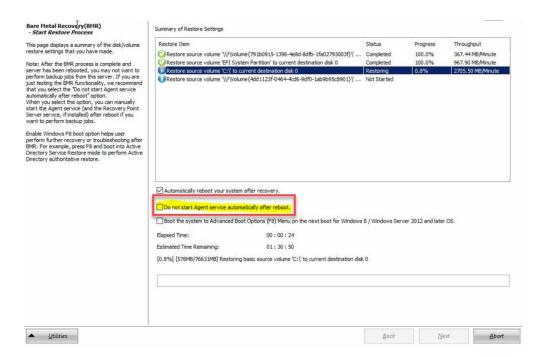
Das Dialogfeld **Übersicht über die Wiederherstellungseinstellungen** wird angezeigt.

#### 21. Klicken Sie auf OK.



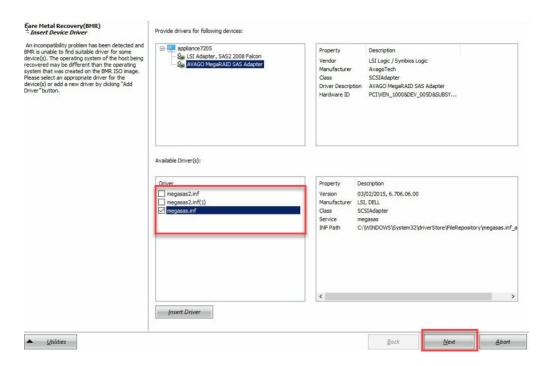
Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungsprozess starten** wird angezeigt.

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



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**.



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



Der BMR-Prozess wird erfolgreich abgeschlossen.

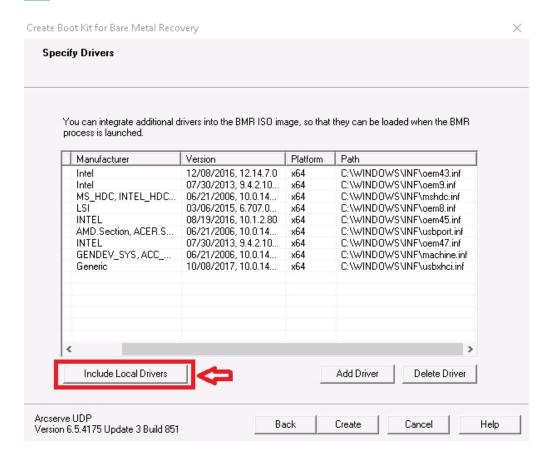
# Best Practices für eine Bare-Metal-Recovery (BMR) und das Erhalten von Daten

Sie können auf der Arcserve UDP Appliance eine Bare-Metal-Recovery mithilfe des Arcserve UDP-Bootkits ausführen.

#### 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.



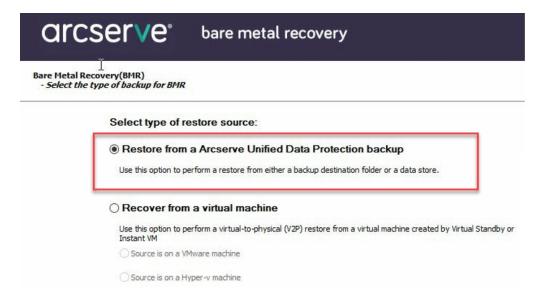
2. Starten Sie die Arcserve UDP Appliance mit dem BMR-ISO-Image oder dem USB-Stick.

Das Arcserve Bare-Metal-Recovery Setup wird angezeigt.

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

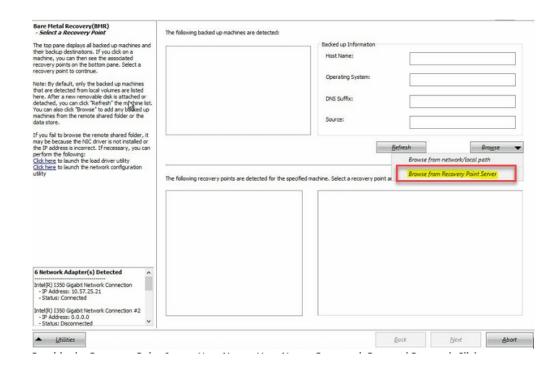


4. Wählen Sie die Option Wiederherstellung von einer Arcserve Unified Data Protection-Sicherung aus, und klicken Sie auf Weiter.



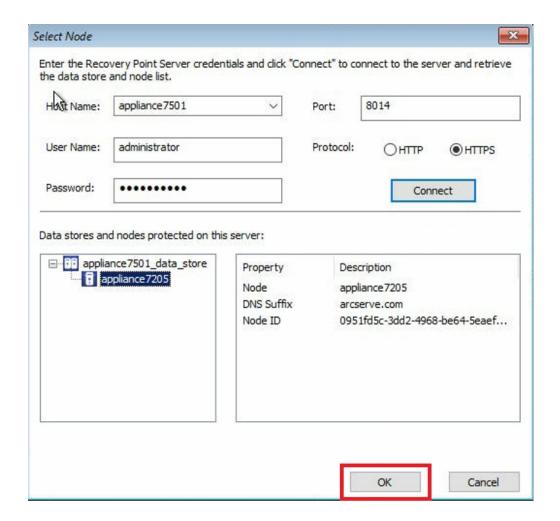
Das Fenster **Assistent zum Auswählen eines Wiederherstellungspunkts** wird angezeigt.

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



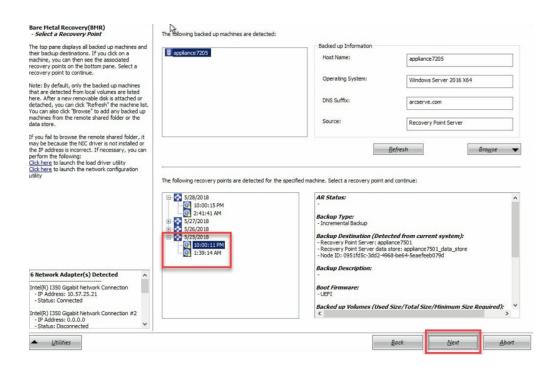
Das Fenster Knoten auswählen wird angezeigt.

- 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**.



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

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



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

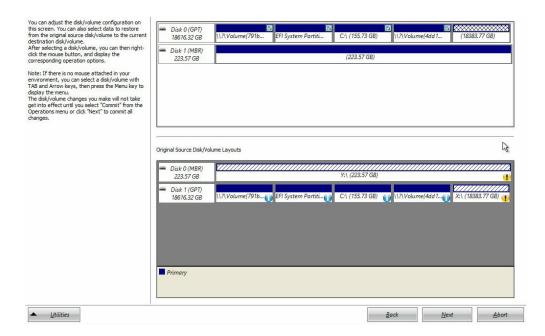


Das Dialogfeld Bare-Metal-Recovery (BMR) – Wiederherstellungsmodus auswählen wird angezeigt.

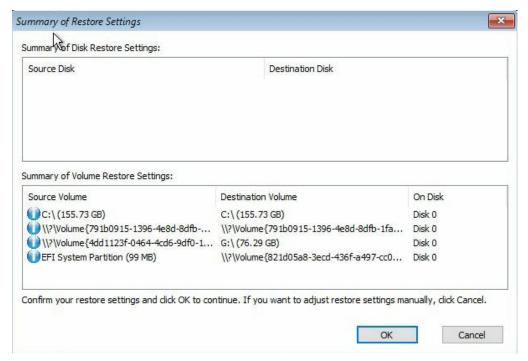
11. Wählen Sie Erweiterter Modus aus, und klicken Sie auf Weiter.



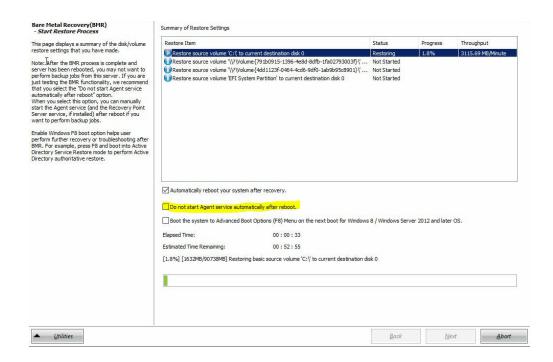
12. Klicken Sie im Dialogfeld Bare-Metal-Recovery (BMR) – Datenträgerpartitionen anpassen auf Weiter.



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



14. 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.



Der BMR-Prozess wurde erfolgreich abgeschlossen.

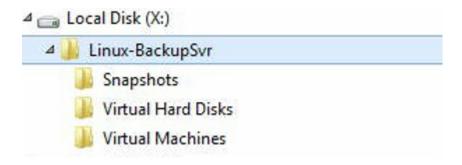
## **Best Practices für das Linux-Migrations-Tool**

**Wichtig!** Das Linux-Migrations-Tool steht nur in Arcserve UDP 6.5 Update 4 zur Verfügung.

Das Linux-Migrations-Tool (Linux\_migration.ps1) ist ein neues, in Arcserve UDP 6.5 Update 4 eingeführtes Feature, mit dem Sie den vorinstallierten Linux-Sicherungsserver der Arcserve UDP Appliance von der vorherigen Version von CentOS wie z. B. CentOS 6.6 zu CentOS 7.4 migrieren können.

#### **Befolgen Sie diese Schritte:**

- 1. Melden Sie sich bei der Arcserve UDP Appliance mit den Anmeldeinformationen des Administrators an.
- 2. Aktualisieren Sie die vorherigen Versionen der Arcserve UDP-Konsole in der Appliance auf Arcserve UDP 6.5 Update 4.
- 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 zu CentOS 7.4 werden alle Einstellungen des Linux-Sicherungsservers wie Linux-Sicherungspläne, Linux-Knoten und Linux-Jobs migriert und in der Arcserve UDP Appliance-Konsole konfiguriert.

# Best Practices für das Dienstprogramm "Appliance-Image festlegen"

Das Dienstprogramm "Appliance-Image festlegen" unterstützt Sie dabei, das ursprüngliche Appliance-Image im aktuellen System durch das gewünschte Appliance-Image der verfügbaren Versionen der Arcserve UDP-Appliance zu ersetzen.

Herunterladen des Appliance-Images von Arcserve UDP 6.5 Update 2:

#### Für Windows 2012 R2

Sie können das Appliance-Image von dieser <u>URL</u> herunterladen.

**Hinweis:** Der md5 für den Download des Appliance-Images lautet *1E9FB62D395EF1812B1DBE9EDB8F2C6E*.

Führen Sie nach dem Ausführen des Dienstprogramms eine Rücksetzung auf die Werkseinstellungen durch, um die Appliance unter Verwendung der in der Arcserve UDP-Konsole verfügbaren Werkseinstellungen auf die gewünschte Version der Arcserve UDP-Appliance zurückzusetzen. Das Dienstprogramm "Appliance-Image festlegen" ist für Arcserve UDP-Appliance 6.5 Update 1 und höher verfügbar.

**Hinweis:** Die Version des als Ersatz verwendeten Appliance-Images muss höher als die *ursprüngliche Arcserve UDP-Version* sein, die auf der Arcserve UDP-Appliance installiert ist.

Zur Überprüfung der ursprünglichen Arcserve UDP-Version melden Sie sich bei der Arcserve UDP-Konsole an, navigieren zu **Einstellungen** und wählen **Zurücksetzen auf Werkseinstellungen**, um Details zur Version aufzurufen.



Beispielszenario für das Ersetzen des Images zum Zurücksetzen auf Werkseinstellungen für UDP 6 Update 1 durch das Image zum Zurücksetzen auf Werkseinstellungen für UDP 6.5 Update 1

Das folgende Beispiel beschreibt, wie Sie das Image zum Zurücksetzen auf Werkseinstellungen ersetzen. Sie können den gleichen Vorgang auch für andere Versionen verwenden.

Verwenden des Dienstprogramms "Appliance-Image festlegen", um von Arcserve UDP Appliance 6 Update 1 zu Arcserve UDP Appliance 6.5 Update 1 zurückzukehren

Wenn die installierte Arcserve UDP-Version auf der Appliance Arcserve UDP 6 Update 1 ist, können Sie die Appliance auf Arcserve UDP 6.5 Update 1 aktualisieren.

Führen Sie zum Aktualisieren die folgenden Schritte aus:

- 1. Laden Sie das Appliance-Image von Arcserve UDP-Appliance 6.5 Update 1 herunter, und führen Sie das Dienstprogramm "Appliance-Image festlegen" aus. Führen Sie die folgenden Schritte aus, um das Dienstprogramm "Appliance-Image festlegen" zu verwenden:
  - a. Laden Sie das Appliance-Image von Arcserve UDP 6.5 Update 1 über die <u>URL</u> herunter, oder <u>wenden Sie sich an den Support</u>, um den Download zu erhalten.

**Hinweis:** Der md5 für den Download des Appliance-Images lautet *9F568A4BDC6B42972C5177284591B835*.

b. Öffnen Sie die Windows-Befehlszeile, und führen Sie den folgenden Befehl aus:

C:\Programme\Arcserve\Unified Data Protection\Management\bin\Appliance\SetImage.exe —applianceimage <vollständiger Pfad des gerade heruntergeladenen Appliance-Images>

Nachdem der Schritt der *Überprüfung der Appliance-Images abge-schlossen* ist, wird die folgende Frage angezeigt:

Sind Sie sicher, dass Sie die Datei appliance.wim ersetzen möchten?

- c. Geben Sie y bzw. yes ein, um das Image zu ersetzen, oder geben Sie n bzw. no ein, um die Ausführung zu beenden.
- d. Nach Abschluss der Image-Replikation wird in der Befehlszeile folgende Meldung angezeigt:

Ersetzen des Appliance-Images abgeschlossen.

```
aPS C:\Program Files\Arcserve\Unified Data Protection\Management\bin\Appliance> .\SetImage.exe -applianceimage C:\temp\a pliance.wim

Start to check appliance image, this may need about 30 minutes, please wait...

Mounting the old appliance image, please wait...

Unmounting the old appliance image, please wait...

Mounting the new appliance image, please wait...

Unmounting the new appliance image, please wait...

Check appliance images finished.

Are you sure you want to replace the appliance.wim file? <y|n>:y

Start to replace appliance image, please wait...

Replace appliance image completed.
```

2. Gehen Sie folgendermaßen vor, um die Version Update 1 der Appliance wiederherzustellen:

**Hinweis:** Nach dem Ersetzen des Appliance-Images in der Arcserve UDP-Konsole wird die ursprüngliche Arcserve UDP-Version in die gewünschte Appliance-Version geändert.

a. Navigieren Sie in der Arcserve UDP-Konsole zu **Einstellungen**, und wählen Sie **Zurücksetzen auf Werkseinstellungen**.



Die *ursprüngliche Arcserve UDP-Version* wird in Arcserve UDP Appliance 6.5 Update 1 geändert.

**Hinweis**: Laden Sie die Seite neu, wenn die gewünschte Appliance-Version nach dem Ersetzen des Appliance-Images nicht in der *ursprünglichen Arcserve UDP-Version* angezeigt wird.

b. Klicken Sie auf **Zurücksetzen auf Werkseinstellungen**, um die aktuelle Version der Appliance auf die neue Arcserve UDP-Appliance-Version 6.5 Update 1 zurückzusetzen.

Weitere Informationen zum Zurücksetzen auf die Werkseinstellungen finden Sie über den Link.

# Best Practices für vorinstallierte Linux-Sicherungsserver in der Arcserve UDP Appliance

Wenn Sie den in der Arcserve UDP Appliance vorinstallierten Linux-Sicherungsserver auf v6.5 Update 2 aktualisieren, müssen Sie manuell einige Ports in Linux hinzufügen, das nach dem Upgrage die CentOS 6.6 x64-Firewall verwendet.

#### Befolgen Sie diese Schritte:

- 1. Navigieren Sie zum folgenden Pfad:
- vi /etc/sysconfig/iptables
- 2. Die iptables-Datei muss die folgenden Zeilen, die unten in Fettdruck aufgeführt sind, enthalten. Wenn dies nicht der Fall ist, müssen Sie diese manuell hinzufügen:
  - # 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

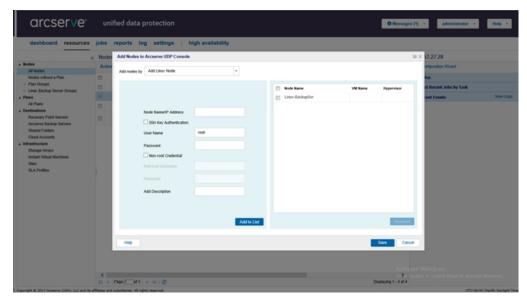
- -A INPUT -m state --state ESTABLISHED, RELATED -j ACCEPT
- -A INPUT -p icmp -j ACCEPT
- -A INPUT -i lo -j ACCEPT
- -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
- -A INPUT -j REJECT --reject-with icmp-host-prohibited
- -A FORWARD -j REJECT --reject-with icmp-host-prohibited COMMIT
- 3. Speichern Sie die iptables-Datei.
- 4. Starten Sie den iptables-Dienst mit folgendem Befehl neu: /etc/init.d/iptables restart

Sie haben die Ports der CentOS 6.6 x64-Firewall erfolgreich hinzugefügt.

# Best Practices für die Arcserve UDP-Appliance zum Sichern des Linux-Sicherungsservers selbst

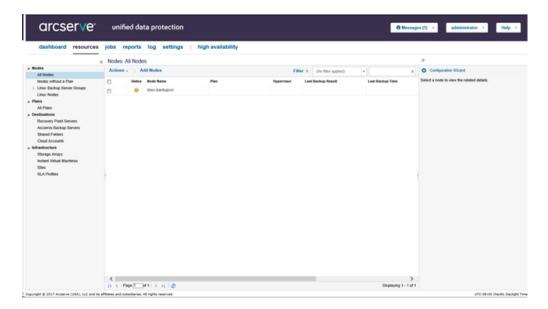
Wenn Sie den Linux-Sicherungsserver selbst in der Arcserve UDP-Appliance sichern möchten, gehen Sie folgendermaßen vor:

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



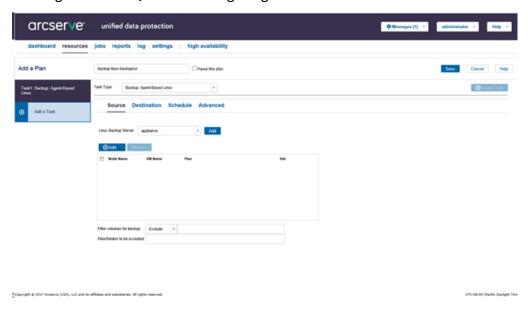
6. Klicken Sie auf Speichern.

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

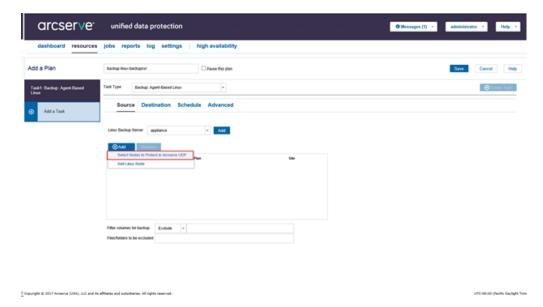


7. Navigieren Sie zu **Alle Pläne**, und erstellen Sie einen agentenbasierten Linux-Plan.

Die Registerkarte Quelle wird angezeigt.

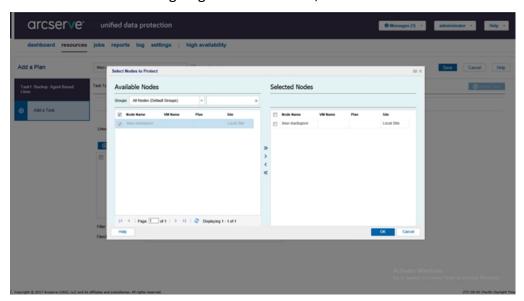


8. Wählen Sie in der Dropdown-Liste "Hinzufügen" die Option *Auswählen von zu schützenden Knoten in Arcserve UDP*.



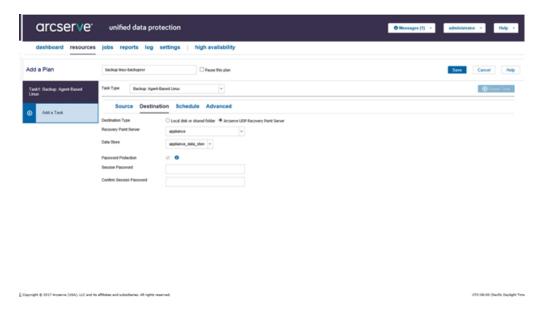
Das Dialogfeld "Zu schützende Knoten auswählen" wird geöffnet.

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

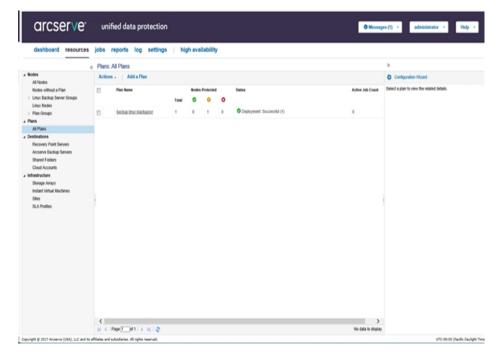


Die Registerkarte Ziel wird angezeigt.

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.



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



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

# Best Practices zur Migration zwischen Arcserve UDP-Appliances

In diesem Thema werden zwei Lösungen vorgestellt, wie Benutzer die Migration von einer vorhandenen Arcserve UDP-Appliance in eine andere neue Arcserve UDP-Appliance durchführen können.

Lassen Sie uns beispielsweise die Arcserve UDP-Appliance 8200 zur Arcserve UDP-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 UDP-Appliance 8200 kein Job ausgeführt wird.

Weitere Informationen zur Konsolenmigration finden Sie im Thema <u>Best Practices</u> für die Migration der Arcserve UDP-Konsole.

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

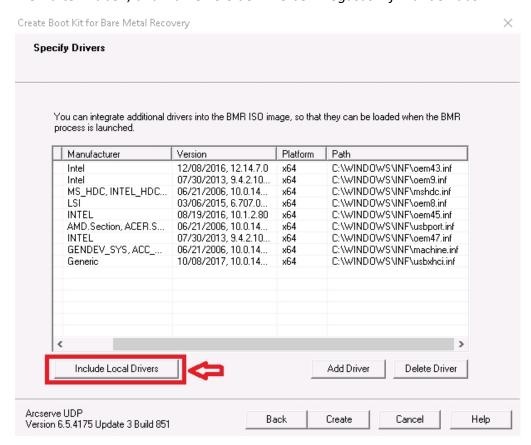
Um eine BMR von einer vorhandenen UDP-Appliance auf einer anderen neuen UDP-Appliance durchzuführen, gehen Sie folgendermaßen vor:

 Erstellen Sie einen Datenspeicher auf der neuen Arcserve UDP-Appliance 8400, und sichern Sie die Arcserve UDP-Appliance 8200 in diesem Datenspeicher.

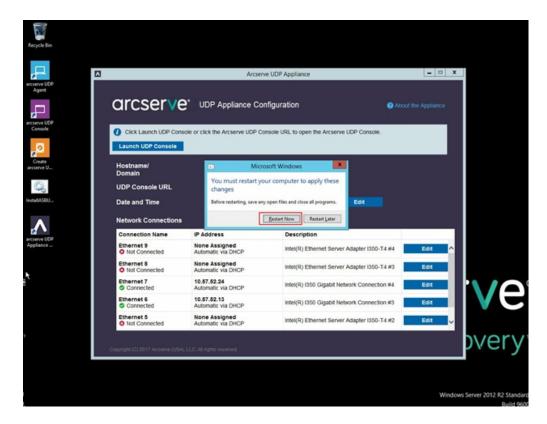
Hinweis: Die folgende Warnung können Sie einfach ignorieren:

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.



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



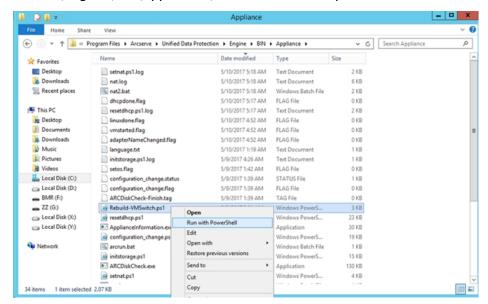
4. Erstellen Sie jetzt den Netzwerk-Switch auf Appliance 8400 neu.

Befolgen Sie diese Schritte:

a. Öffnen Sie "Routing und RAS", und klicken Sie auf **Routing und RAS** deaktivieren.



- b. Führen Sie den folgenden Befehl mit PowerShell aus:
  - C:\Programme\Arcserve\Unified Data Pro-

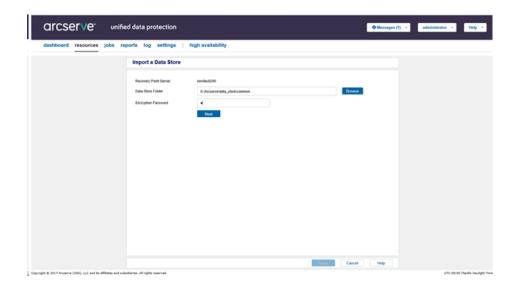


### tection\Engine\BIN\Appliance\Rebuild-VMSwitch.ps1

- 5. 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. Beenden Sie alle UDP-Dienste auf UDP-Appliance 8200 mit dem folgenden Befehl in der Befehlszeile:
    - C:\Programme\Arcserve\Unified Data Protection\Management\BIN> cmdutil.exe /stopall
  - b. Kopieren Sie alle Daten auf den Datenträgern X und Y von UDP-Appliance 8200 manuell nach Appliance 8400.

```
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>cmdutil.exe /stopall
opall
Start to kill process explorer.exe
Killing process explorer.exe
Process killed.
Start to kill process D2DUDgc.exe
Stopping service 'Arcserve UDP Agent Service'...
Service Stopped.
Stopping service 'Arcserve UDP RPS Data Store Service'...
Service 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.
 topping service 'Arcserve UDP Management Port Sharing Service'...
Service Stopped.
Stopping service 'Arcserve UDP Agent Explorer Extension Service'...
Service 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.
Start Windows Explorer.
```

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



# Lösung 2

#### Arcserve UDP Appliance-Migrationslösung

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 UDP-Appliance 8200 kein Job ausgeführt wird.
- Sie haben die Arcserve UDP-Konsole von UDP Appliance 8200 zu 8400 migriert.

**Hinweis:** Weitere Informationen über das Migrieren der Arcserve UDP-Konsole von Appliance 8200 zu 8400 finden Sie unter <u>Best Practices für die Migration der Arcserve UDP-Konsole.</u>

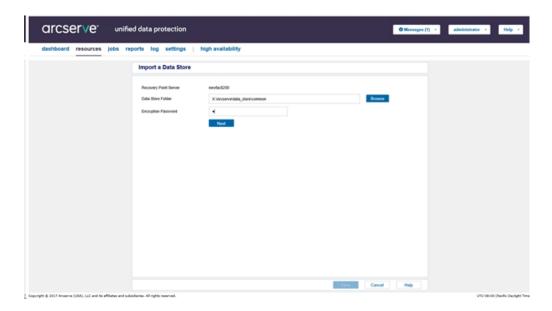
### **Befolgen Sie diese Schritte:**

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

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

```
_ 0 X
                             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>cmdutil.exe /st
opall
Start to kill process explorer.exe
Killing process explorer.exe
Process killed.
Start to kill process D2DUDgc.exe
Stopping service 'Arcserve UDP Agent Service'...
Service Stopped.
Stopping service 'Arcserve UDP RPS Data Store Service'...
Service 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.
Stopping service 'Arcserve UDP Agent Explorer Extension Service'...
Service 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.
Start Windows Explorer.
```

- 2. Kopieren Sie alle Daten auf den Datenträgern X und Y von Arcserve UDP-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.



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

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

# Best Practices für Linux-Instant VM-Job auf Arcserve UDP-zu Hyper-V auf lokaler Appliance

Mit der Arcserve UDP-Appliance können Sie das Netzwerk so konfigurieren, dass ein Linux-Instant VM-Job zu Hyper-V auf einer lokalen Appliance ausgeführt wird.

#### Befolgen Sie diese Schritte:

- 1. Öffnen Sie den Hyper-V-Manager.
- 2. Erstellen Sie einen neuen externen virtuellen Netzwerk-Switch.
- 3. Öffnen Sie "Routing und RAS", und klicken Sie auf **Routing und RAS deak- tivieren**.



- 4. 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.

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

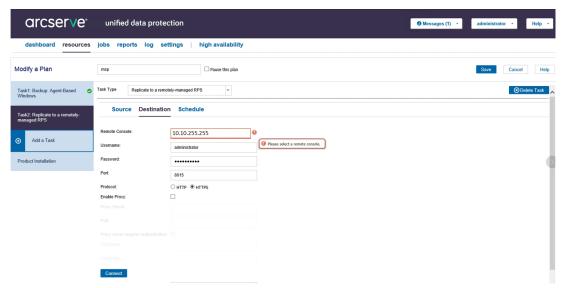
Jetzt können Sie den Linux-Instant VM-Job zu Hyper-V auf einer lokalen Appliance erfolgreich ausführen.

# Best Practices zum Hinzufügen von "Replizieren" zu einem remote verwalteten RPS-Task einer anderen Appliance

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:** Dieses Problem wurde für die UDP Appliance mit der Standardversion Arcserve UDP v6.5 Update 3 oder höher behoben.

Fehlermeldung: Wählen Sie eine Remote-Konsole aus.



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 Cata-

log=\$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. Gehen Sie von der UDP-Konsole des lokalen Rechners aus folgendermaßen vor:
  - a. Wählen Sie Alle Knoten in der Knotenansicht.
  - b. Klicken Sie mit der rechten Maustaste, und wählen Sie *Aktualisieren* aus.
  - c. Klicken Sie auf **OK**, um alle Knoten zu aktualisieren.
- 5. Wählen Sie alle RPS-Knoten in der Recovery Point Server-Ansicht aus, klicken Sie mit der rechten Maustaste, und wählen Sie *Aktualisieren*, um alle RPS-Knoten zu aktualisieren.

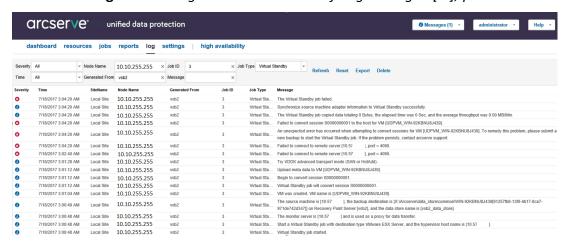
Der Task Zu einem remote verwalteten RPS replizieren wird zwischen zwei Appliance-Rechnern erfolgreich unterstützt.

# Best Practices zum Durchführen eines Virtual Standby (VSB)-Task, bei dem der Monitor eine andere Appliance ist

Wenn Sie auf Arcserve UDP 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 UDP Appliance mit der Standardversion Arcserve UDP v6.5 Update 3 oder höher behoben.

**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 Alle Pläne in der Planansicht.
  - b. Klicken Sie mit der rechten Maustaste, und wählen Sie *Jetzt bereitstellen*.
  - c. Klicken Sie auf **OK**, um alle Pläne bereitzustellen.

Der VSB Task wird erfolgreich unterstützt.

# **Kapitel 14: Lizenzhinweise**

Teile dieses Produkts enthalten Software von anderen Herstellern. Der nach-
folgende Abschnitt enthält Informationen zur Software von anderen Herstellern

Dieser Abschnitt enthält folgende Themen:

nutty	210

# putty

Dieses Produkt enthält die Komponente "putty", die folgende Details umfasst:

Komponentenname	putty	
Kom-	Hannaii andiah anturiahah una Cira an Takhana	
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	
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	
	htt- p://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html PuTTY is copyright 1997-2015 Simon Tatham.  Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, and CORE SDI S.A.	
Lizenztext	Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including 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 NO EVENT
	SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR
	OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
	OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH
	THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
	SOFTWARE.
	htt-
	p://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html
	PuTTY is copyright 1997-2015 Simon Tatham.
	Portions copyright Robert de Bath, Joris van Rantwijk, Delian Del-
	chev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas
	Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Kha-
	lifa, Markus Kuhn, Colin Watson, Christopher Staite, and 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,
Copyright-Text	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 NO EVENT
	SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR
	OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
	OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH
	THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
	Auf dem Appliance-Rechner verwenden wir putty.exe zur Kom-
   Verwendungszweck	munikation mit dem Linux-Sicherungsserver, um das Sys-
	temgebietsschema und das UDP-Linux-Gebietsschema zu ändern.
Änderungen erfor-	
derlich	Nein
	I