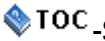
Arcserve® Appliance Benutzerhandbuch

Version 7.0

arcserve

Arcserve® Appliance Onlinehilfe

Version 7.0

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

-Symbol.**

arcserve

Rechtliche Hinweise

Kontakt zum Arcserve-Support

Das Arcserve-Support

Support kontaktieren

Der Arcserve-Support ermöglicht Ihnen Folgendes:

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

Rückgaberichtlinie für die Arcserve Appliance

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

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

Für die RMA-Anforderung erforderliche Informationen:

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

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

Inhalt

Kapitel 1: Informationen zu Arcserve Appliance Dokumentation

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

Dieser Abschnitt enthält folgende Themen:

Sprachenunterstützung

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

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

Diese Version ist in den folgenden Sprachen verfügbar:

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

Produktdokumentation

Wenn Sie die Arcserve UDP-Dokumentation erhalten möchten, klicken Sie auf diesen Link zur 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-Agenten in einem Windows-Betriebssystem. Dieses Handbuch enthält Informationen z. B. zur Installation und Konfiguration des Agent und zum Schutz und zur Wiederherstellung der Windows-Knoten.

- **Arcserve UDP-Agent für Linux – Benutzerhandbuch**

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

Kapitel 2: Einführung in die Arcserve Appliance

Dieser Abschnitt enthält folgende Themen:

Einführung

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

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

Folgende Software ist auf der Arcserve Appliance vorinstalliert:

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

Arcserve Appliance wird mit Hardware-Garantie definiert. Genauere Informationen zu dieser Garantie finden Sie unter arcserve.com/arcserve-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.

Weitere Informationen finden Sie im Arcserve UDP Lösungshandbuch.

Arcserve Unified Data Protection Agent for Linux

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

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

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

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

Der Linux-Sicherungsserver verwendet die folgenden Standard-Anmeldeinformationen:

- Benutzername: root
- Kennwort: Arcserve

Hinweis: Es wird empfohlen, das Standardkennwort zu ändern.

Arcserve Backup

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

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

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

Arcserve Backup Server verwendet die folgenden Standard-Anmeldeinformationen:

- Benutzername: caroot
- Kennwort: Arcserve

Arcserve Replication and High Availability (Arcserve RHA)

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

Hinweis: Arcserve RHA ist nicht in der Anwendung vorinstalliert. Weitere Informationen zum Installieren und Konfigurieren von Arcserve RHA finden Sie im Installationshandbuch

Sicherheitsmaßnahmen

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

Weitere Informationen zu den Sicherheitsmaßnahmen finden Sie im Anhang - Sicherheitsmaßnahmen.

In der Box enthaltene Gegenstände

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

- 8000-Serie
- 9000-Serie

In der Box der Appliance 8000 Series enthaltene Gegenstände

Folgende Gegenstände sind in der Box enthalten:

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

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

In der Box der Appliance 9000 Series enthaltene Gegenstände

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

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

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

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

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

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

Nicht in der Box enthaltene Gegenstände

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

- Überwachung
- Tastatur
- Externes Speichergerät (bei Bedarf)

Verfügbare Modelle

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

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

Modelle 7100 - 7300v

Arcserve Appliance Modelle 7100 - 7300v

Arcserve Appliance Spezifikationen für die 7000-Serie					
Appliance-Modell	**7100**	**7200**	**7200V**	**7300**	**7300V**
Sicherungsspeicherkapazität					
Reine Speicherkapazität*	3 TB	6 TB	6 TB	9 TB	9 TB
Nutzbare Sicherungskapazität**	2,8 TB	5,8 TB	5,8 TB	8,8 TB	8,8 TB
Geschützte Kapazität (Quelldaten)***	Bis zu 8 TB	Bis zu 17 TB	Bis zu 17 TB	Bis zu 26 TB	Bis zu 26 TB
Standardfunktionen					
Einheitliche 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 virtuelle Maschinen	N/V	Bis zu 3 virtuelle Maschinen
Gewährleistung und technische 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 rackmontierten 19 Zoll-Schienen)				
Remoteverwaltungs- und Netzwerkschnittstellen-Ports	1 x IPMI und 2 x 1 GbE (RJ45)				
Festplattentyp und RAID-Konfiguration	4 x 1 TB SAS (RAID 5)	4 x 2 TB SAS (RAID 5)	4 x 2 TB SAS (RAID 5)	4 x 3 TB SAS (RAID 5)	4 x 3 TB SAS (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 redundant)	1 x 600 W				
Stromverbrauch (Wattzahl beim Leerlauf/Laden/Starten)	93/116/143	122/164/143	125/167/145	125/167/145	129/188/152
Wechselspannungs- und Frequenzbereich	100 - 240 V				
Amperewert	7,5 A max.				

1 TB = 1.000.000.000.000 Byte

** Für V-Modelle wird der für die Sicherung verfügbare Speicherplatz um die Größe der Virtual Standby-VMs reduziert.

***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 Appliance Modelle 7400 - 7600v

Arcserve Appliance Spezifikationen für die 7000-Serie						
Appliance-Modell	**7400**	**7400V**	**7500**	**7500V**	**7600**	**7600V**
Sicherungsspeicherkapazität						
Reine Speicherkapazität*	16 TB	16 TB	20 TB	20 TB	30 TB	30 TB
Nutzbare Sicherungskapazität**	15,8 TB	15,8 TB	19,8 TB	19,8 TB	29,8 TB	29,8 TB
Geschützte Kapazität (Quelldaten)***	Bis zu 46 TB	Bis zu 46 TB	Bis zu 58 TB	Bis zu 58 TB	Bis zu 90 TB	Bis zu 90 TB
Standardfunktionen						
Einheitliche 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 virtuelle Maschinen	N/V	Bis zu 9 virtuelle Maschinen	N/V	Bis zu 12 virtuelle Maschinen
Gewährleistung und technische Daten						
Gewährleistung für das gesamte Systemdepot	3 Jahre					
Abmessungen (H x B x T in Zoll)	3,5" x 17,2" x 25,6" (2HE - mit rackmontierten 19 Zoll-Schienen)					
Remoteverwaltungs- und Netzwerkschnittstellen-Ports	1 x IPMI & 2 x 1 GbE (RJ45) und 4 x 1 GbE (RJ45). Optional 2 x 10 Gb					
Festplattentyp und RAID-Konfiguration	10 x 2 TB SAS (RAID 6)	10 x 2 TB SAS (RAID 6)	12 x 2 TB SAS (RAID 6)	12 x 2 TB SAS (RAID 6)	12 x 3 TB SAS (RAID 6)	12 x 3 TB SAS (RAID 6)
Konnektivität für externe Bandsicherung (SAS, SATA-Controller, FC)	1 x PASS					
System-RAM insgesamt	64 GB	96 GB	64 GB	96 GB	128 GB	192 GB
SSD-Laufwerk	240 GB SSD	240 GB SSD	480 GB SSD	480 GB SSD	480 GB SSD	480 GB SSD

(Für Deduplizierungs-Hashtabellen)						
Maximalgewicht (lb)	52 lb					
Netzteile (einzeln oder redundant)	2 x 920 W					
Stromverbrauch (Wattzahl beim Leerlauf/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.					

1 TB = 1.000.000.000.000 Byte

** Für V-Modelle wird der für die Sicherung verfügbare Speicherplatz um die Größe der Virtual Standby-VMs reduziert.

***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 Appliance Modelle 8100 - 8400

Arcserve Appliance Spezifikationen für die 8000-Serie				
Appliance-Modell	**UDP 8100**	**UDP 8200**	**UDP 8300**	**UDP 8400**
Quellensicherung*	12 TB bis 18 TB	24 TB bis 36 TB	48 TB bis 128 TB	96 TB bis 240 TB
System-RAM	32 GB	32 GB	64 GB	128 GB
Max. RAM **	64 GB/96 GB/160 GB		96 GB/128 GB/192 GB	160 GB/192 GB/256 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	9361-4i		9361-8i	
RAID-Konfiguration	RAID-5 mit BBU		RAID-6 mit BBU	
Laufwerkschächte	4		12	
Laufwerke	3 x 2 TB SAS 12G 4 x 2 TB SAS 12G	3 x 4 TB SAS 12G 4 x 4 TB SAS 12G	6 x 4 TB SAS 12G 7 x 4 TB SAS 12G 8 x 4 TB SAS 12G 9 x 4 TB SAS	6 x 8 TB SAS 12G 7 x 8 TB SAS 12G 8 x 8 TB SAS 12G 9 x 8 TB SAS

			12G 10 x 4 TB SAS 12G 11 x 4 TB SAS 12G 12 x 4 TB SAS 12G	12G 10 x 8 TB SAS 12G 11 x 8 TB SAS 12G 12 x 8 TB SAS 12G
DIMMs/Max. DIMMs	4 x 8 GB DDR4-2400/ 8		4 x 16 GB DDR4-2400/ 8	4 x 32 GB DDR4-2400/ 8
Karten	LSI SAS9200-8E			
Netzteile	2 x, Hot-Swap-fähig, redundant 500 W, Wechselstrom, Platinum		2 x, 920 W, Hot-Swap-fähig, redundant, hocheffizient, Wechselstrom, Platinum	

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

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

Modelle 9012 - 9504DR

Arcserve Appliance Modelle 9012 - 9504DR

Arcserve Appliance Spezifikationen für die 9000-Serie										
Appliance-Modell	**9012**	**9024**	**9048**	**9072-DR**	**9096-DR**	**9144-DR**	**9192-DR**	**9240-DR**	**9288-DR**	**9360-DR**	**9504DR**

Nutzbare Kapazität	4 TB	8 TB	16 TB	24 TB	32 TB	48 TB	64 TB	80 TB	96 TB	120 TB	168 TB
Quellensicherung	12 TB	24 TB	48 TB	72 TB	96 TB	144 TB	192 TB	240 TB	288 TB	360 TB	504 TB
System-RAM	6 x 8 GB (48 GB)			12 x 16 GB (192 GB)							12 x 32 GB (384 GB)
Max. RAM / DIMMS	176 GB / 10 DIMMS			576 GB / 24 DIMMS							768 GB / 24 DIMMS
SSD-Laufwerk	480 GB SSD			2 x 1,9 TB SSD (RAID1)							
Prozessor	Intel Xeon Silber 4108, 8-CORE 1,8 GHz			Intel Xeon Silber 4114, 10-CORE, 2,2 GHz							
Anzahl der Prozessoren	1			2							
RAID-Karte	PERC H730P Low-Profile Adapter 2 GB NV Cache			PERC H730P, MiniCard, 2 GB NV Cache							
RAID-Konfiguration	RAID-5			RAID-6							
Laufwerkschächte	4			16							
Erweiterungs-Kit	NA			11	10	8	6	4	6	4	NA
RAID 2	NA			6							
Laufwerke	3 x 2 TB	3 x 4 TB	3 x 8 TB	5 x 8 TB	6 x 8 TB	8 x 8 TB	10 x 8 TB	12 x 8 TB	10 x 12 TB	12 x 12 TB	16 x 12 TB
Base PCIe-Karten	Integrierte Broadcom 5720 Dual-Port 1Gb LOM			Broadcom 5720 QP 1Gb Network Tochterkarte SAS 12Gbps externe HBA-Controller							Broadcom 5720 QP 1Gb SAS 12Gbps HBA extern Dual-

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

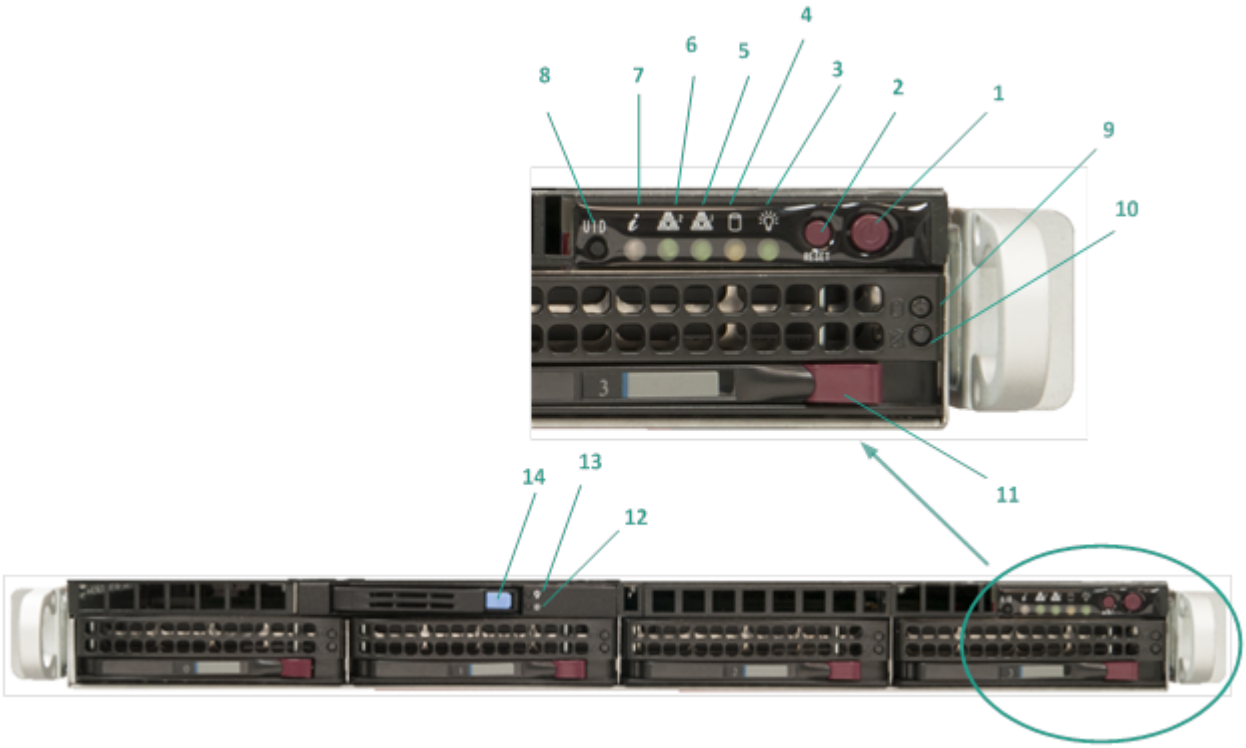
Steuerelemente und Anzeigen

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

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

Vorderseite 7100 - 7300v

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



Nummer	Steu-erelement/Anzeige	Beschreibung
1	Netzschalter	Zum Ein- und Ausschalten der Stromversorgung für die Appliance-Komponenten. Beim Ausschalten wird die Haupt-Stromversorgung ausgeschaltet, die Appliance wird jedoch weiterhin mit Standby-Strom versorgt. Um sicherzustellen, dass die 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	**Gelb blinkend:** Zeigt Aktivität auf mindestens

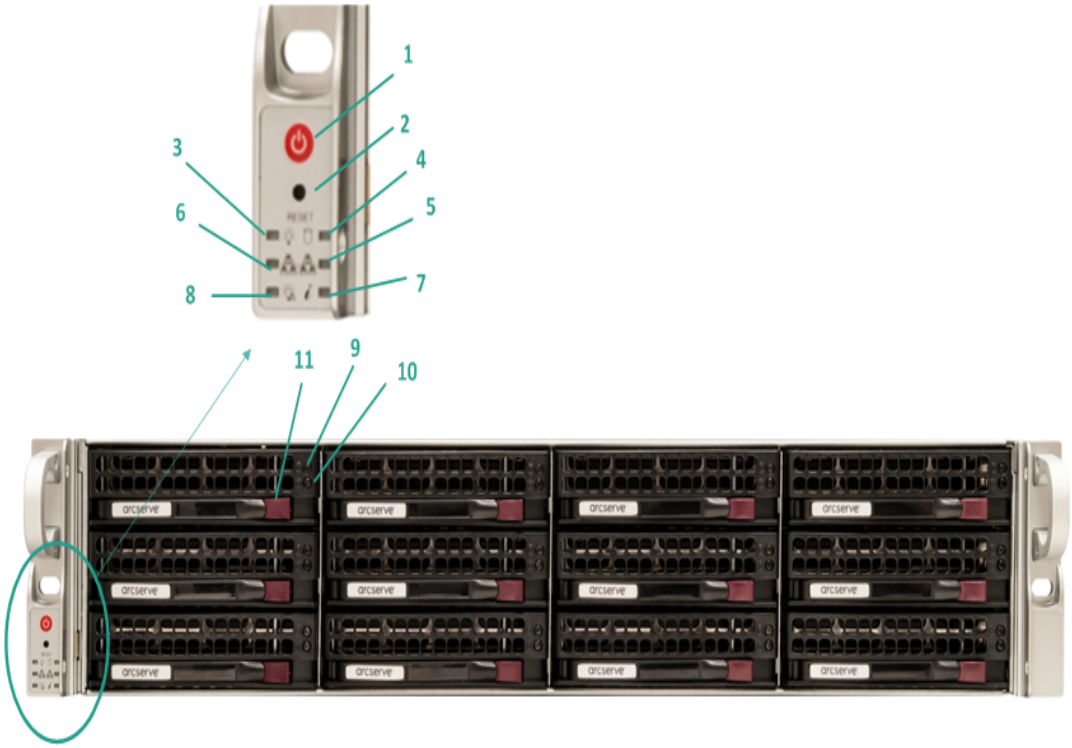
		einer der Festplatten an.
5	Netzwerkkarten-LED (NIC1)	**Gelb blinkend:** Zeigt Netzwerkaktivität im Netzwerk 1 (Port ETH0) an.
6	Netzwerkkarten-LED (NIC2)	**Gelb blinkend:** Zeigt Netzwerkaktivität im Netzwerk 2 (Port ETH1) an.
7	Informations-LED	**Stetig rot:** Eine Überhitzungs-Bedingung ist aufgetreten. (Dies kann durch eine Überlastung eines Kabels verursacht werden.) ***Rot blinkend – schnell (1 Sekunde):** Lüfterfehler. Überprüfen Sie, ob der Lüfter nicht mehr betriebsbereit ist. ***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. **Blau blinkend:** Remote-UID wurde aktiviert. Verwenden Sie diese Funktion, um den Server von einem externen Standort aus zu suchen.
8	Schaltfläche "Geräte-ID (UID)"	Zum Ein- oder Ausschalten der Universal Information-LED (blau) auf der Vorder- und Rückseite der Appliance. Wenn die blaue LED aktiviert ist, kann die Appliance problemlos in einem Rack lokalisiert werden (von vorne oder hinten).
9	Festplatten-LED	**Grün blinkend**: Zeigt Aktivität auf der entsprechenden Festplatte an.
10	Festplatten-LED	***Stetig rot**: Zeigt einen Ausfall der entsprechenden Festplatte an. Mit der Arcserve Appliance werden bei Ausfall einer Festplatte die restlichen Datenträger sofort aktiviert. Damit wird sichergestellt, dass keine Daten verloren gehen und die Appliance normal weiterarbeitet. Daher ist es zum Schutz vor Problemen im Zusammenhang mit Ausfällen mehrerer Festplatten wichtig, eine Festplatte schnellstmöglich auszutauschen, um den potenziellen Datenverlust zu minimieren.
11	Verriegelung Festplatte	Zum Entriegeln und Entfernen der Festplatte.
12	SSD (Solid State Drive)-LED	***Stetig rot**: Zeigt einen Laufwerksausfall an.
13	SSD (Solid State Drive)-LED	**Stetig grün**: Zeigt Laufwerkaktivität an.

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

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

Vorderseite 7400 - 7600v

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



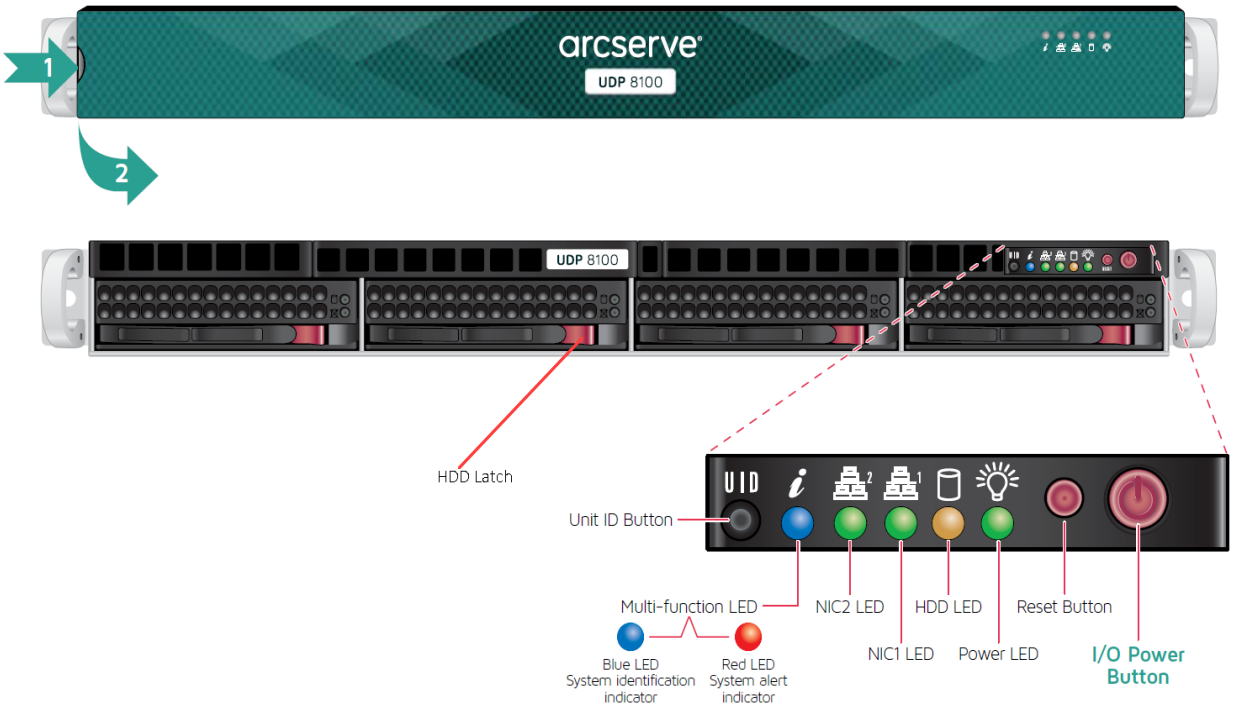
Nummer	Steuerelement/Anzeige	Beschreibung
1	Netzschalter	Zum Ein- und Ausschalten der Stromversorgung für die Appliance-Komponenten. Beim Ausschalten wird die Haupt-Stromversorgung ausgeschaltet, die Appliance wird jedoch weiterhin mit Standby-Strom versorgt. Um sicherzustellen, dass die Appliance vollständig von der Stromversorgung getrennt ist, ziehen Sie vor Wartungsarbeiten das Netzkabel ab.
2	Schaltfläche "Zurücksetzen"	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	**Gelb blinkend:** Zeigt Aktivität auf mindestens einer der Festplatten an.
5	Netzwerkkarten-LED (NIC1)	**Gelb blinkend:** Zeigt Netzwerkaktivität im Netzwerk

		1 (Port ETH0) an.
6	Netzwerkkarten-LED (NIC2)	**Gelb blinkend:** Zeigt Netzwerkaktivität im Netzwerk 2 (Port ETH1) an.
7	Informations-LED	**Stetig rot:** Eine Überhitzungs-Bedingung ist aufgetreten. (Dies kann durch eine Überlastung eines Kabels verursacht werden.) ***Rot blinkend – schnell (1 Sekunde):** Lüfterfehler. Überprüfen Sie, ob der Lüfter nicht mehr betriebsbereit ist. ***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. **Blau blinkend:** 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	**Grün blinkend**: Zeigt Aktivität auf der entsprechenden Festplatte an.
10	Festplatten-LED	***Stetig rot**: Zeigt einen Ausfall der entsprechenden Festplatte an. Mit der Arcserve Appliance werden bei Ausfall einer Festplatte die restlichen Datenträger sofort aktiviert. Damit wird sichergestellt, dass keine Daten verloren gehen und die Appliance normal weiterarbeitet. Daher ist es zum Schutz vor Problemen im Zusammenhang mit Ausfällen mehrerer Festplatten wichtig, eine Festplatte schnellstmöglich auszutauschen, um den potenziellen Datenverlust zu minimieren.
11	Verriegelung Festplatte	Zum Entriegeln und Entfernen der Festplatte.

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

Vorderseite 8100 - 8200

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



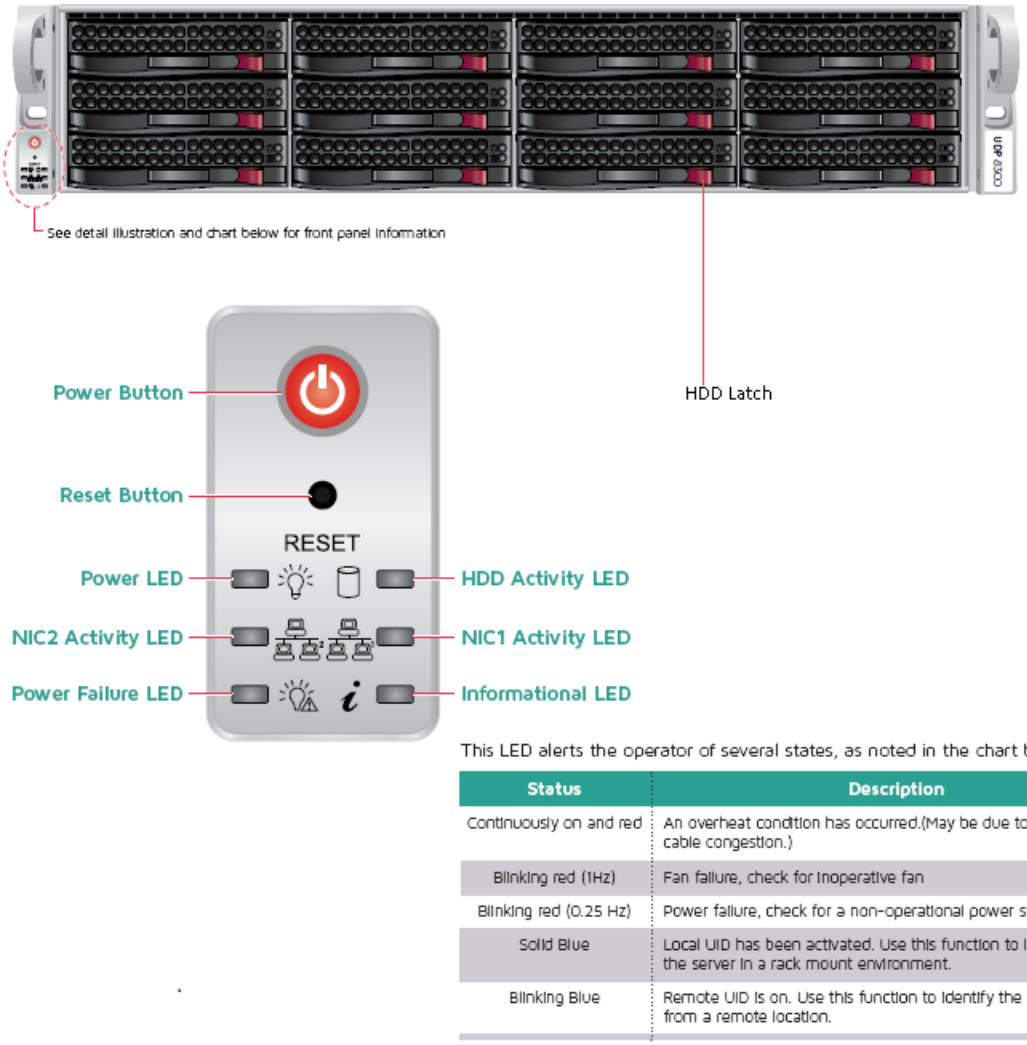
Steuerelement/Anzeige	Beschreibung
Netzschalter	Zum Ein- und Ausschalten der Stromversorgung für die Appliance-Komponenten. Beim Ausschalten wird die Haupt-Stromversorgung ausgeschaltet, die Appliance wird jedoch weiterhin mit Standby-Strom versorgt. Um sicherzustellen, dass die Appliance vollständig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

Netzwerkkarten-LED (NIC2)	**Gelb blinkend:** Zeigt Netzwerkaktivität im Netzwerk 2 (Port ETH1) an.
Informations-LED	**Stetig rot:** Eine Überhitzungs-Bedingung ist aufgetreten. **Hinweis:** Dies kann durch eine Überlastung eines Kabels verursacht werden. ***Rot blinkend – schnell (1 Sekunde):** Lüfterfehler. Überprüfen Sie, ob der Lüfter nicht mehr betriebsbereit ist. ***Rot blinkend – langsam (4 Sekunden):** Stromausfall. Überprüfen Sie, ob die Stromversorgung außer Betrieb ist. **Stetig blau:** Lokale UID ist aktiviert. Verwenden Sie diese Funktion, um den Server in einer Rack-Umgebung zu suchen. **Blau blinkend:** Remote-UID ist aktiviert. Verwenden Sie diese Funktion, um den Server von einem externen Standort aus zu suchen.
Schaltfläche "Geräte-ID (UID)"	Zum Ein- oder Ausschalten der Universal Information-LED (blau) auf der Vorder- und Rückseite der Appliance. Wenn die blaue LED aktiviert ist, kann die Appliance problemlos in einem Rack lokalisiert werden (von vorne oder hinten).
Festplatten-LED	**Grün blinkend**: Zeigt Aktivität auf der entsprechenden Festplatte an.
Festplatten-LED	***Stetig rot**: Zeigt einen Ausfall der entsprechenden Festplatte an. Mit der Arcserve Appliance werden bei Ausfall einer Festplatte die restlichen Datenträger sofort aktiviert. Damit wird sichergestellt, dass keine Daten verloren gehen und die Appliance normal weiterarbeitet. Daher ist es zum Schutz vor Problemen im Zusammenhang mit Ausfällen mehrerer Festplatten wichtig, eine Festplatte schnellstmöglich auszutauschen, um den potenziellen Datenverlust zu minimieren.
Verriegelung Festplatte	Zum Entriegeln und Entfernen der Festplatte.
SSD (Solid State Drive)-LED	***Stetig rot**: Zeigt einen Laufwerksausfall an.
SSD (Solid State Drive)-LED	**Stetig grün**: Zeigt Laufwerkaktivität an. **Grün blinkend**: Zeigt an, dass auf das Laufwerk zugegriffen wird.
Verriegelung SSD (Solid State Drive)	Zum Entriegeln und Entfernen des SSD-Laufwerks.

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

Vorderseite 8300 - 8400

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



This LED alerts the operator of several states, as noted in the chart below.

Status	Description
Continuously on and red	An overheat condition has occurred.(May be due to cable congestion.)
Blinking red (1Hz)	Fan failure, check for inoperative fan
Blinking red (0.25 Hz)	Power failure, check for a non-operational power supply
Solid Blue	Local UID has been activated. Use this function to locate the server in a rack mount environment.
Blinking Blue	Remote UID is on. Use this function to identify the server from a remote location.

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 "Zurücksetzen"	Zum Neustart der Appliance.
Netz-LED	**Stetig grün:** Zeigt an, dass das Netzteil der Appliance mit Strom

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

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

Vorderseite 9012 - 9048

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

Nummer	Steuerelement/Anzeige	Symbol	Beschreibung
1	Linkes Bedienfeld	NA	Enthält den Systemstatus und die System-ID, die Status-LED und die Anzeige für iDRAC Quick Sync 2 (drahtlos). **Hinweis:** Die Anzeige für iDRAC Quick Sync 2 steht nur bei bestimmten Konfigurationen zur Verfügung. • **LED-Status:** Ermöglicht es Ihnen, die alle fehlgeschlagenen Hardware-Komponenten zu identifizieren. Es gibt bis zu fünf Status-LEDs und eine allgemeine Systemzustands-LED-Leiste (Gehäusezustand und System-ID). Weitere Informationen finden Sie unter link. • **Quick Sync 2 (drahtlos):** Zeigt an, dass das System für eine schnelle Synchronisierung aktiviert ist. Die Funktion "Quick Sync" (Schnelle Synchronisierung) ist optional. Diese Funktion ermöglicht die Verwaltung des Systems mit mobilen Geräten. Diese Funktion liefert eine aggregierte Bestandsaufnahme der Hardware und Firmware sowie verschiedene auf Diagnosen und Informationen auf Systemebene, die bei der Fehlerbehebung verwendet werden können. Weitere Informationen finden Sie unter link.
2	Laufwerksteckplätze	NA	Hier können Sie Laufwerke installieren,

			die auf Ihrem System unterstützt werden. Weitere Informationen über Laufwerke finden Sie unter Link.
3	Optisches Laufwerk (optional)	NA	Ein optionales schlankes SATA DVD-ROM-Laufwerk oder ein DVD+/-RW-Laufwerk.
4	VGA-Anschluss		Hier können Sie ein Anzeigegerät an das System anschließen. Weitere Informationen finden Sie unter link.
5	USB-Port (optional)		Der USB-Anschluss ist USB 2.0-kompatibel.
6	Rechtes Bedienfeld	NA	Enthält den Netzschalter, USB-Port, iDRAC Direct micro-Port und die iDRAC-Direktstatus-LED.
7	Informationsetikett	NA	Das Informationsetikett ist ein ausblendbarer Bereich mit Systeminformationen, wie Serviceetikett, NIC, MAC-Adresse und so weiter. Wenn Sie sicheren standardmäßigen Zugriff auf iDRAC haben, enthält das Etikett auch das sichere iDRAC-Standardkennwort.

Vorderseite 9072DR - 9504DR

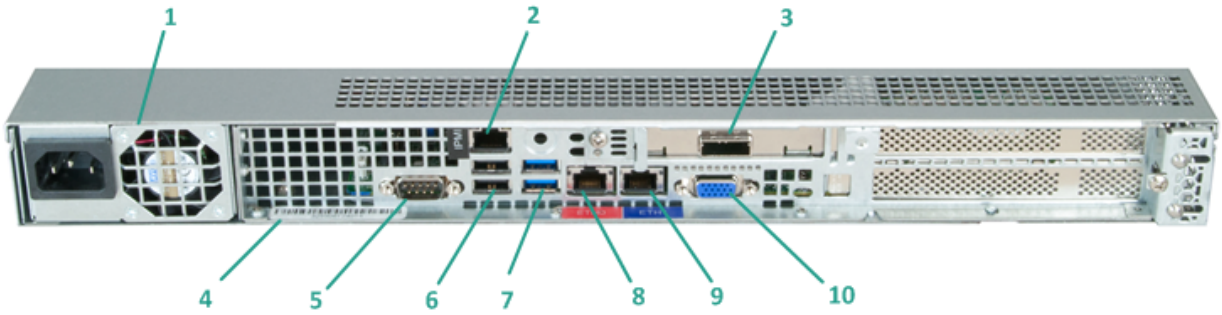
Die Vorderseite des Arcserve Appliance enthält Schaltflächen des Bedienfeldes, LEDs des Bedienfeldes und LEDs des Datenträgers. In der folgenden Tabelle werden diese Elemente beschrieben.

Nummer	Steuerelement/Anzeige	Symbol	Beschreibung
1	Linkes Bedienfeld	NA	Enthält den Systemstatus und System-ID, Status-LED und die Anzeige

			für iDRAC Quick Sync 2 (drahtlos).
2	Laufwerksteckplätze	NA	Hier können Sie Laufwerke installieren, die auf Ihrem System unterstützt werden. Weitere Informationen finden Sie unter link.
3	Rechtes Bedienfeld	NA	Enthält den Netzschalter, VGA-Port, iDRAC Direct Micro USB-Anschluss und zwei USB 2.0-Ports.
4	Informationsetikett	NA	Das Informationsetikett ist ein ausblendbarer Bereich mit Systeminformationen, wie Serviceetikett, NIC, MAC-Adresse und so weiter. Wenn Sie sicheren standardmäßigen Zugriff auf iDRAC haben, enthält das Etikett auch das sichere iDRAC-Standardkennwort.

Rückseite 7100 - 7300v

Die Rückseite enthält die Netzteile, die Kabelanschlüsse und die Ports für die Appliance.

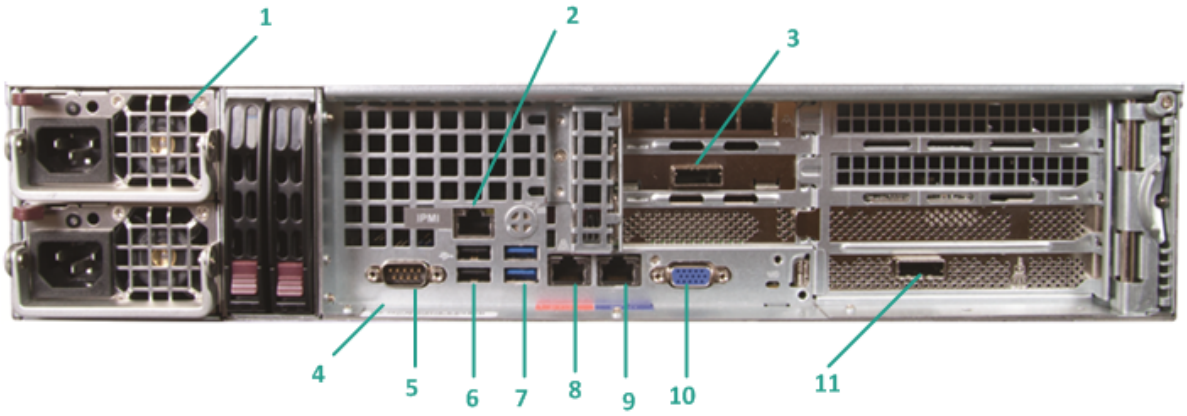


Nummer	Name des Steuerelements bzw. der Anzeige	Beschreibung
1	Netzteil	Ermöglicht eine hocheffiziente Stromversorgung der Appliance. **Hinweis:** Mithilfe des Hauptnetzschalters wird die Appliance mit der Stromversorgung verbunden oder von ihr getrennt. Beim Ausschalten über diesen Schalter wird die 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 (Remoteverwaltung)	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 Speichergerät (SAS-Port für Bandlaufwerk)	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 zuge-

		wiesen 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

Die Rückseite enthält die Netzteile, die Kabelanschlüsse und die Ports für die Appliance.

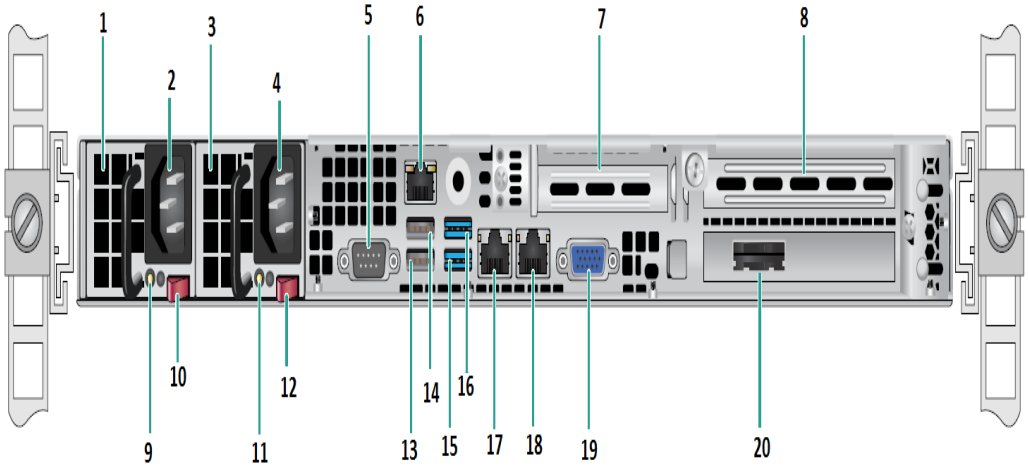


Nummer	Name des Steuerelements bzw. der Anzeige	Beschreibung
1	Doppelnetzteil	Ermöglicht eine hocheffiziente Stromversorgung der Appliance. **Hinweis:** Mithilfe des Hauptnetzschalters wird die Appliance mit der Stromversorgung verbunden oder von ihr getrennt. Der Vorteil eines Doppelnetzteils besteht 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.
2	IPMI-Port (Remoteverwaltung)	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 Speichergerät (SAS-Port für Bandlaufwerk)	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 Netzwerkdaten	Zur Übertragung von Netzwerkdaten zwischen dem Netzwerk und der Appliance. ((ETH0 für Netzwerk 1)
9	E/A-Port 2 für Netzwerkdaten	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 Speichergerät (Automatischer Bandwechsler/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

Die Rückseite enthält die Netzteile, die Kabelanschlüsse und die Ports für die Appliance.

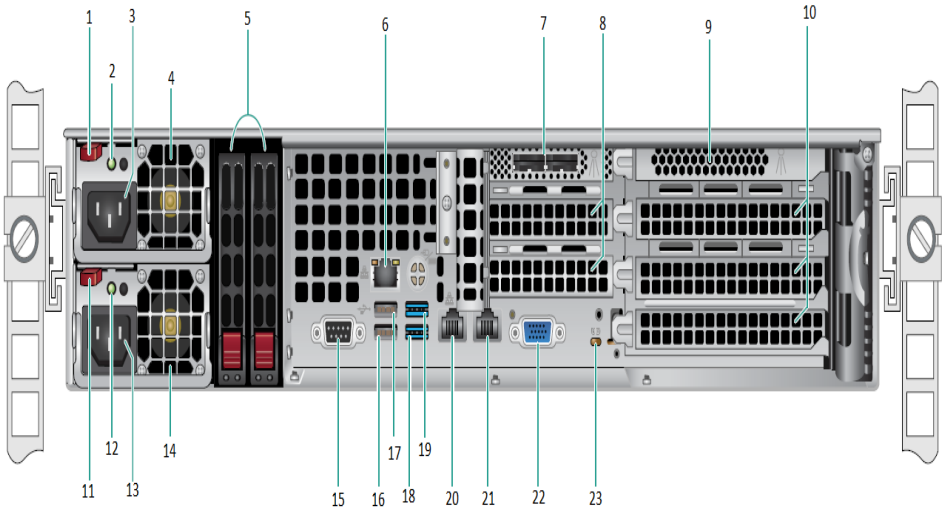


Nummer	Name des Steuerelements bzw. der Anzeige
1	Netzteilmodul Nr. 1
2	AC-Anschlussbuchse Nr. 1
3	Netzteil Nr. 2
4	AC-Anschlussbuchse Nr. 2
5	COM-Port
6	IPMI-Port (Remoteverwaltung)
7	Low-Profile PCI-Erweiterungssteckplatz
8	PCI-Erweiterungssteckplatz
9	Power Good-LED 1
10	Netzteilschalter 1
11	Power-Good-LED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

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

Rückseite 8300 - 8400

Die Rückseite enthält die Netzteile, die Kabelanschlüsse und die Ports für die Appliance.

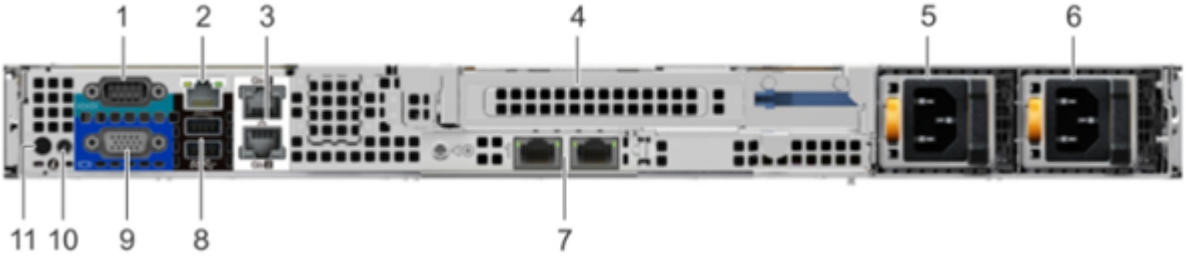


Nummer	Name des Steuerelements bzw. der Anzeige
1	Netzteilmodul Nr. 1 – Verriegelung
2	Netzteilmodul Nr. 1 – Power-Good-LED
3	Netzteilmodul 1 Steckdose
4	Netzteilmodul 1 Lüfter
5	Hintere SSDs (optional)
6	IPMI-Port (Remoteverwaltung)
7	Externe SAS HBA-Ports
8	PCI-Erweiterungssteckplätze halber Länge
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

Rückseite 9012 - 9048

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

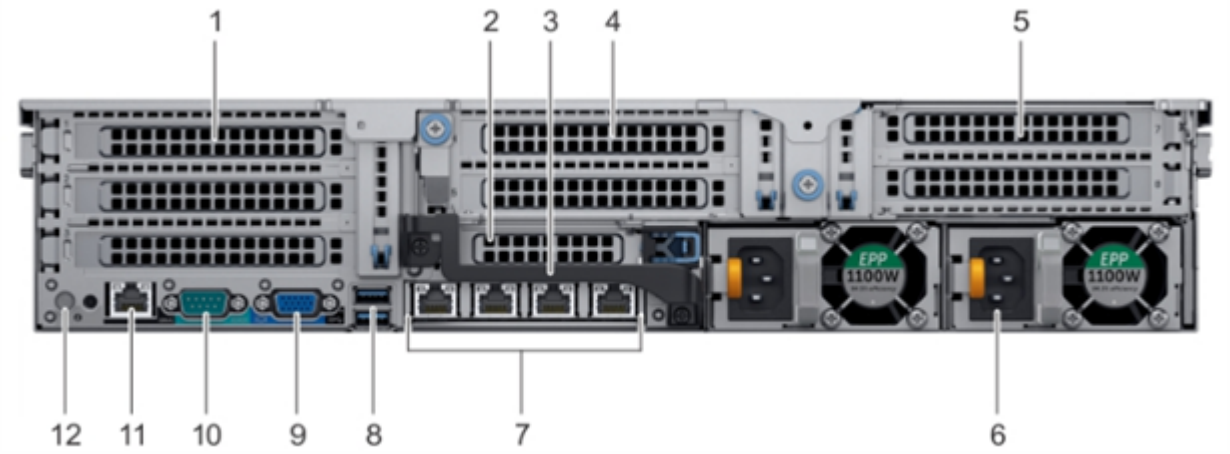


Nummer	Steuerelement/Anzeige	Symbol	Beschreibung
1	Serieller Port		Über diesen Port können Sie ein Peripheriegerät an das System anschließen. Weitere Informationen finden Sie unter link.
2	Dedizierter iDRAC9-Netzwerkport		Verwenden Sie den iDRAC9 dedizierte Netzwerkport, um sicher auf den eingebetteten iDRAC auf einem separaten Management-Netzwerk zuzugreifen. Weitere Informationen finden Sie unter link.
3	Ethernet-Ports (2)		Verwenden Sie die Ethernet-Ports, um das Local Area Networks (LAN) mit dem System zu verbinden. Weitere Informationen finden Sie unter link.
4	Riser-Steckplatz (volle Höhe)		Verwenden Sie Kartensteckplätze, um PCIe-Erweiterungskarten voller Höhe mit dem Riser voller Höhe zu verbinden.
5	Netzteil		Weitere Informationen zu den Netzteilkonfigurationen finden Sie unter Link.
6	Netzteil		Weitere Informationen zu den Netzteilkonfigurationen finden Sie unter Link.

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

Rückseite der 9072DR - 9504 DR

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



Nummer	Steuerelement/Anzeige	Symbol	Beschreibung
1	PCIe-Erweiterungssteckplatz (3) (volle Höhe)	NA	Der PCIe-Erweiterungssteckplatz (Riser 1) verbindet bis zu drei PCIe-Erweiterungskarten voller Höhe mit dem System. Weitere Informationen finden Sie unter link.
2	PCIe-Erweiterungssteckplatz (halbe Höhe)	NA	Der PCIe-Erweiterungssteckplatz (Riser 2) verbindet eine PCIe-Erweiterungskarte halber Höhe mit dem System. Weitere Informationen finden Sie unter link.
3	Rückwärtiges Handle	NA	Das rückwärtige Handle kann entfernt werden, um alle externe Kabel zu PCIe-Karten, die in der PCIe Erweiterungssteckplatz 6 installiert sind, zu entfernen.
4	PCIe-Erweiterungssteckplatz (2) (volle Höhe)	NA	Der PCIe-Erweiterungssteckplatz (Riser 2) verbindet bis zu zwei PCIe-Erweiterungskarten voller Höhe mit dem System. Weitere Informationen finden Sie unter link.
5	PCIe-Erweiterungssteckplatz (2) (volle	NA	Der PCIe-Erweiterungssteckplatz (Riser

	Höhe)		3) verbindet bis zu zwei PCIe-Erweiterungskarten voller Höhe mit dem System. Weitere Informationen finden Sie unter link.
6	Netzteil (2)	NA	Weitere Informationen finden Sie unter link.
7	NIC-Ports		Die NIC-Ports, die auf der Netzwerk-Tochterkarte (NDC) integriert sind, stellen die Verbindung zum Netzwerk her. Weitere Informationen zu den unterstützten Konfigurationen finden Sie unter diesem Link.
8	USB-Port (2)		Die USB-Ports sind 9-polig und 3.0-kompatibel. Mit diesen Ports verbinden Sie USB-Geräte mit dem System.
9	VGA-Anschluss		Hier können Sie ein Anzeigegerät an das System anschließen. Weitere Informationen finden Sie unter link.
10	Serieller Port		Über diesen Port können Sie ein Peripheriegerät an das System anschließen. Weitere Informationen finden Sie unter link.
11	Dedizierter iDRAC9-Port		Dieser Port ermöglicht den Remote-Zugriff auf iDRAC. Weitere Informationen finden Sie unter link.
12	Schaltfläche "System-ID"		Die Schaltfläche "System-ID (ID)" steht auf der Vorder- und Rückseite der Systeme zur Verfügung Klicken Sie auf die Schaltfläche, um ein System in einem Rack zu identifizieren, indem Sie die Schaltfläche "System-ID" aktivieren. Mit der Schaltfläche "System-ID" können Sie auch iDRAC zurücksetzen und mithilfe des schrittweisen Modus auf das BIOS zugreifen.

Von der Appliance verwendete Ports

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

- Arcserve UDP
- Arcserve Backup
- Appliance 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:

Port #	Porttyp	Initiiert von	Abhörprozess	Beschreibung
1433	TCP	Remote-Java	sqlsrvr.exe	Gibt den Standard-Kommunikations-Port zwischen der Arcserve UDP-Konsole und den Microsoft SQL Server-Datenbanken an, wenn diese sich auf unterschiedlichen Computern befinden. **Hinweis:** Sie können den standardmäßigen Kommunikationsport während der Installation von SQL Server ändern.
4090	TCP	Arcserve UDP Agent	HATransServer.exe	Überträgt Daten für Virtual Standby-Aufgaben im Proxy-Modus.
5000-5060	TCP	Arcserve UDP-Server	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 Wiederherstellung

				herstellungsaufgabe verwendet wird.
6052	TCP	Arc-serve Backu-p-GDB	CA.ARCserve.CommunicationFoundation. WindowsService.exe	Kommunikation, über die die Arcserve UDP-Konsole und der Primärserver des globalen Arcserve Backup-Dashboards Daten synchronisieren können.
6054	TCP	Arc-serve Backu-p	CA.ARC-ser-ve.CommunicationFoundation.WindowsService.exe	Kommunikation, über die die Arcserve UDP-Konsole und der Arcserve Backup-Primärserver Daten synchronisieren können.
8006				Zum Herunterfahren von Tomcat, das von der Arcserve UDP-Konsole verwendet wird.
8014	TCP	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.
8014	TCP	Arc-	httpd.exe	Gibt den Standard-

		serve UDP-Server		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.
8015	TCP	Arcserve UDP Console	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.
8016	TCP	Arcserve UDP-Server	Tomcat7.exe	Reserviert für die Kommunikation von Arcserve UDP Server-Webdiensten mit dem RPS-Port-Freigabedienst für Arcserve UDP auf dem gleichen Server. **Hinweis:** Der Port kann nicht angepasst werden und kann für die Firewall-Einstellung ignoriert werden.
180-05			CA.ARCserve.CommunicationFoundation.WindowsService.exe	Zum Herunterfahren von Tomcat, das von Arcserve UDP Server oder vom Agenten verwendet wird.

Unter Linux installierte Komponenten

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

Port #	Porttyp	Initiiert von	Abhörprozess	Beschreibung
22	TCP	SSH-Dienst		Arcserve UDP Linux – Abhängigkeit von Drittanbietern. 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	TCP	Arcserve UDP-Linux	Java	Gibt die Standard-Ports für HTTP/HTTPS-Kommunikation zwischen den Remote-Konsolen und dem Arcserve UDP Agent

				für Linux an. Dieser Port ist für eingehende und ausgehende Kommunikation erforderlich.
18005	TCP	Arcserve UDP-Linux	Java	Verwendet von Tomcat, kann für die Firewall-Einstellung ignoriert werden.

Durch UDP Linux remote geschützter 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.

* 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 #	Porttyp	Initiiert von	Abhörprozess	Beschreibung
135	TCP			Microsoft-Portzuordnung
445	TCP		MSRPC über Named Pipes	
6050	TCP/UDP	CASUniversalAgent	Univagent.exe	Arcserve Universal Agent
6502	TCP	Arcserve Communication Foundation	CA.ARCserve.CommunicationFoundation.WindowsService.exe	Arcserve Communication Foundation
6502	TCP	CASTapeEngine	Tapeng.exe	Arcserve-Bandprozess
6503	TCP	CASJobEngine	Jobengine.exe	Arcserve-Jobprozess
6504	TCP	CASDBEngine	DBEng.exe	Arcserve-Datenbankprozess
7854	TCP	CASportmapper	Catirpc.exe	Arcserve-Portmapper
4152-3	TCP	CASDiscovery	CASDSCSVC.EXE	Arcserve-Discovery-Dienst
4152-4	UDP	CASDiscovery	CASDSCSVC.EXE	Arcserve-Discovery-Dienst
9000-9500	TCP		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	TCP			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	TCP			NAT-Port-Umleitung leitet 8018 auf der Appliance auf den Port 8014 des Linux-Backup-Server-Agenten um.
8019	TCP			NAT-Port-Umleitung leitet 8019 auf der Appliance auf den SSH-Port 22 des Linux-Sicherungsservers um.
8021	TCP			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	TCP			NAT-Port-Umleitung leitet 8036 auf der Appliance auf den Port 8036 des Linux-Sicherungsservers um.
50000	TCP			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	TCP			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 werden kann.
50002	TCP			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 werden kann.
50003	TCP			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 werden kann.
50004	TCP			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.

Hinzufügen von Ports zur CentOS 6.6 X64-Firewall

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

Befolgen Sie diese Schritte:

1. Navigieren Sie zum folgenden Pfad:

   vi /etc/sysconfig/iptables

2. Fügen Sie folgende fett markierte Zeilen manuell in der Datei *Iptables* hinzu, falls sie nicht bereits vorhanden sind:

   # Firewall-Konfiguration wie von system-config-firewall geschrieben

   # Die manuelle Anpassung dieser Datei wird nicht empfohlen.

   **filter*

   :INPUT ACCEPT [0:0]

   :FORWARD ACCEPT [0:0]

   :OUTPUT ACCEPT [0:0]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

-A INPUT -p icmp -j ACCEPT

-A INPUT -i lo -j ACCEPT

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

-A INPUT -j REJECT --reject-with icmp-host-prohibited

-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT

3. Speichern Sie die Datei *iptables*.
4. Starten Sie den Service *iptables* mit folgendem Befehl erneut:

   /etc/init.d/iptables restart

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

Kapitel 3: Installieren der Arcserve Appliance

Dieser Abschnitt enthält folgende Themen:

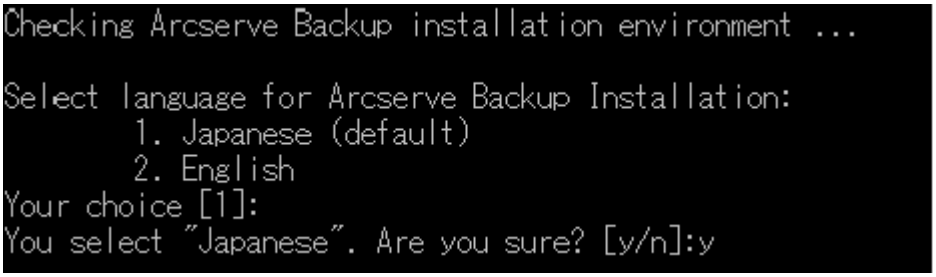
So installieren Sie Arcserve Backup 18.0

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

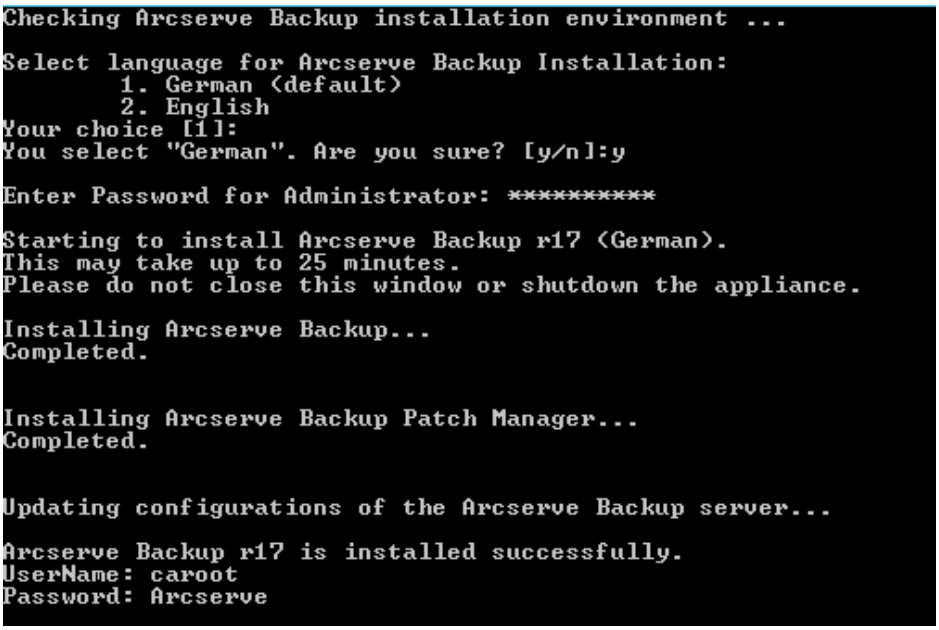
Befolgen Sie diese Schritte:

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

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



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



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

- Benutzername = caroot
- Kennwort = Arcserve

So installieren Sie die 8100 - 8200 Series Appliance

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

Vollständige Informationen zur Installation finden Sie unter 8100 - 8200 Appliance-Installation.

So installieren Sie die 8300 - 8400 Series Appliance

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

Vollständige Informationen zur Installation finden Sie unter 8300 - 8400 Appliance-Installation.

So installieren Sie die 9012 - 9048 Series Appliance

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

Vollständige Informationen zur Installation finden Sie unter 9012 - 9048 Appliance-Installation.

So installieren Sie die 9072-9504DR Series Appliance

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

Vollständige Informationen zur Installation finden Sie unter 9072-9504DR Appliance-Installation.

Kapitel 4: Aktualisieren von Arcserve UDP auf der Appliance

Dieser Abschnitt enthält folgende Themen:

Anwenden einer Lizenz nach einem Upgrade der Arcserve-Software

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

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

Upgradesequenz aufArcserve Appliance

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

- Aktualisieren von Arcserve UDP
  - Aktualisieren der Arcserve-Appliance als Arcserve-Konsole und RPS
  - Aktualisieren der Arcserve-Appliance als Arcserve UDP-RPS
  - Upgradeschritte bei Verwendung von mindestens zwei Arcserve Appliances in der Umgebung
- Aktualisieren des Arcserve Linux-Agenten auf der Arcserve UDP Appliance
- Aktualisieren von Arcserve Backup auf der Arcserve Appliance
- Upgradesequenz für UDP-Konsole, RPS und Agent

Aktualisieren der Arcserve Appliance als Arcserve UDP-Konsole und RPS

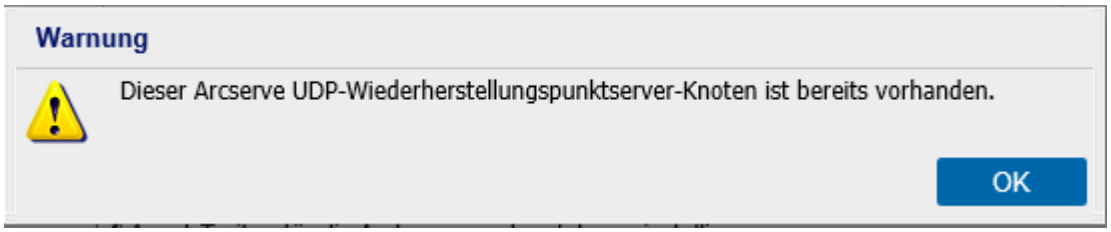
Aktualisieren Sie diese Arcserve Appliance und beachten Sie anschließend die beschriebene Aktualisierungssequenz, um die Umgebung zu aktualisieren.

Aktualisieren der Arcserve Appliance als Arcserve UDP-RPS

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

Aktualisierungsschritte für mindestens zwei in der Umgebung verwendete Arcserve Appliance

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



Aktualisieren von Arcserve UDP Linux Agent auf der Arcserve Appliance

Befolgen Sie diese Schritte:

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

Weitere Informationen finden Sie unter *Online-Hilfe zu Arcserve Unified Data Protection Agent für Linux*.

Aktualisieren von Arcserve Backup auf der Arcserve Appliance

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

Upgradesequenz für UDP-Konsole, RPS und Agent

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

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

   Hinweis: Wiederholen Sie Schritt 5 und 6 für jeden Standort.
7. Aktualisieren Sie den Arcserve UDP Virtual Standby Monitor.

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

Kapitel 5: Konfigurieren der Arcserve Appliance

Dieser Abschnitt enthält folgende Themen:

Konfigurieren der Netzwerkeinstellungen für Arcserve Appliance

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

Befolgen Sie diese Schritte:

1. Nach dem Einschalten der Appliance wird das Fenster "Einstellungen" für die Microsoft-Lizenzbedingungen geöffnet. Lesen und akzeptieren Sie die Bedingungen.

   Das UDP-Dialogfeld **Endbenutzer-Lizenzvereinbarung** wird geöffnet.

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

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

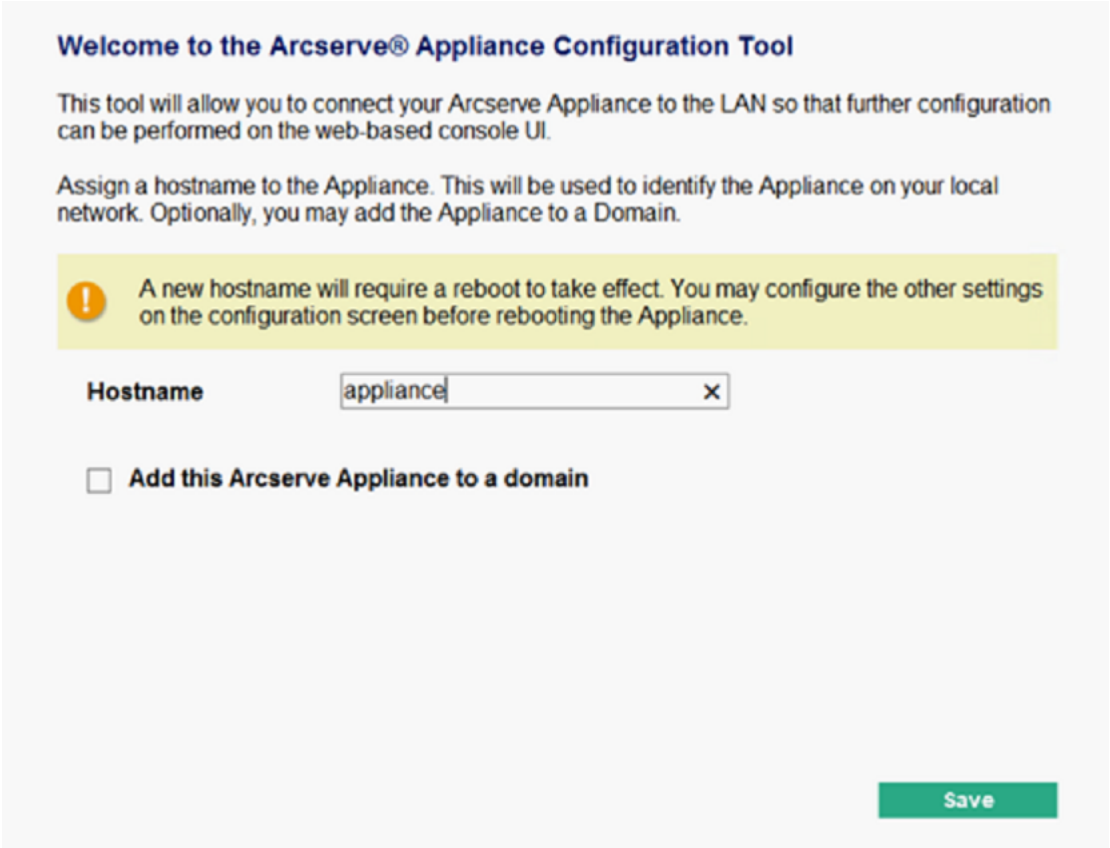
3. Geben Sie die folgenden Details ein:

   Hostname

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

   Fügen Sie diese Arcserve Appliance zu einer Domäne hinzu

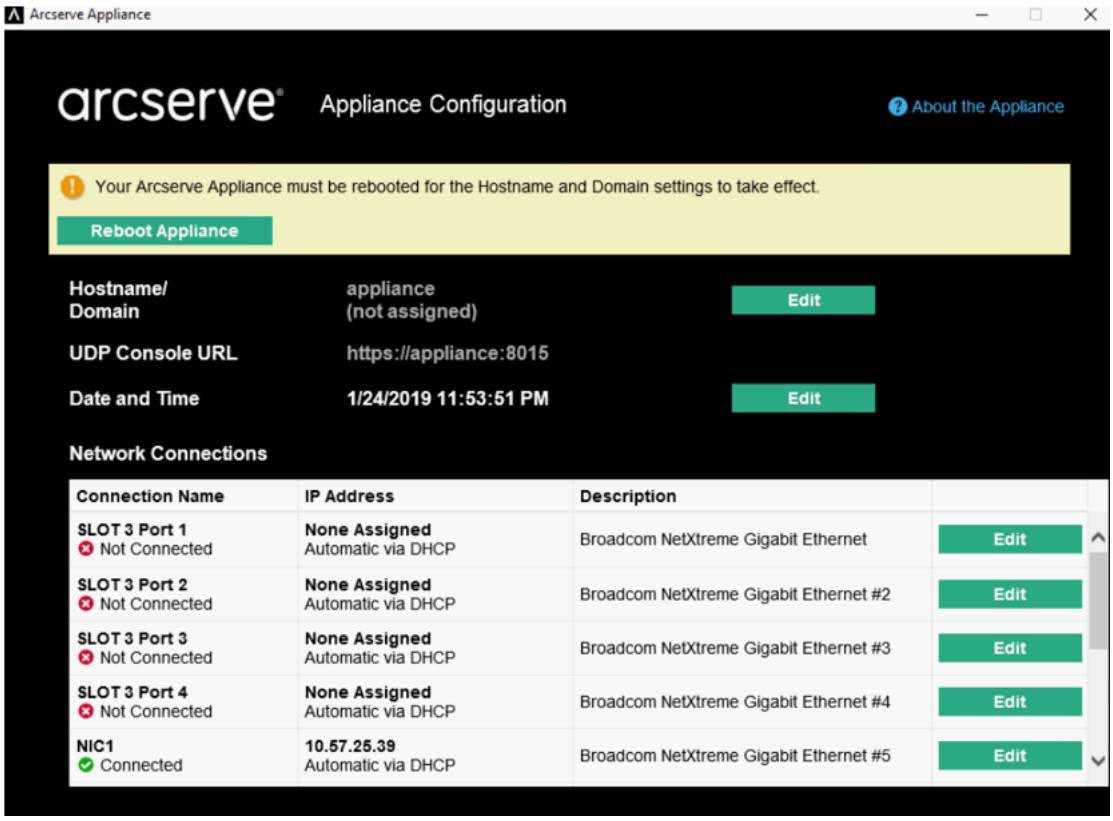
   Aktivieren Sie das Kontrollkästchen, um die Appliance als Mitglied einer Domäne in Ihrem Netzwerk aufzunehmen. Geben Sie die Werte in die Felder "Domäne", "Benutzername" und "Kennwort" an, die angezeigt werden, wenn die Option aktiviert ist.



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

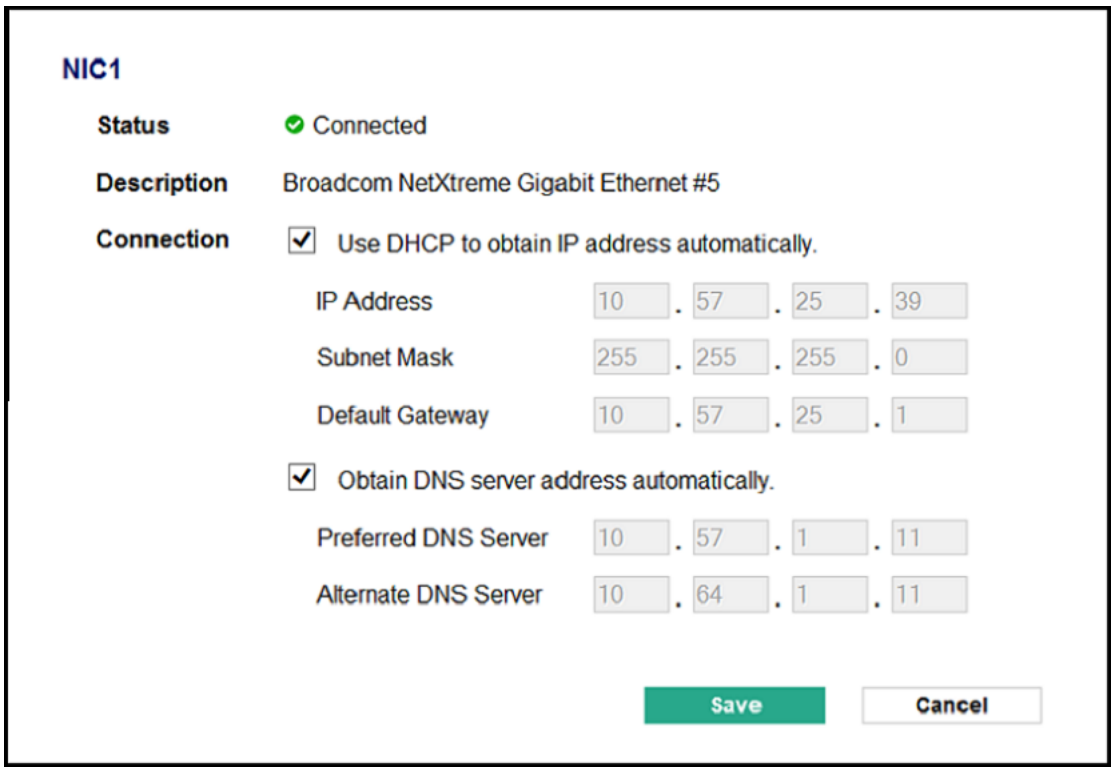
4. Klicken Sie auf **Speichern**.

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



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

Das Dialogfeld **Netzwerkverbindung** wird geöffnet.



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

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

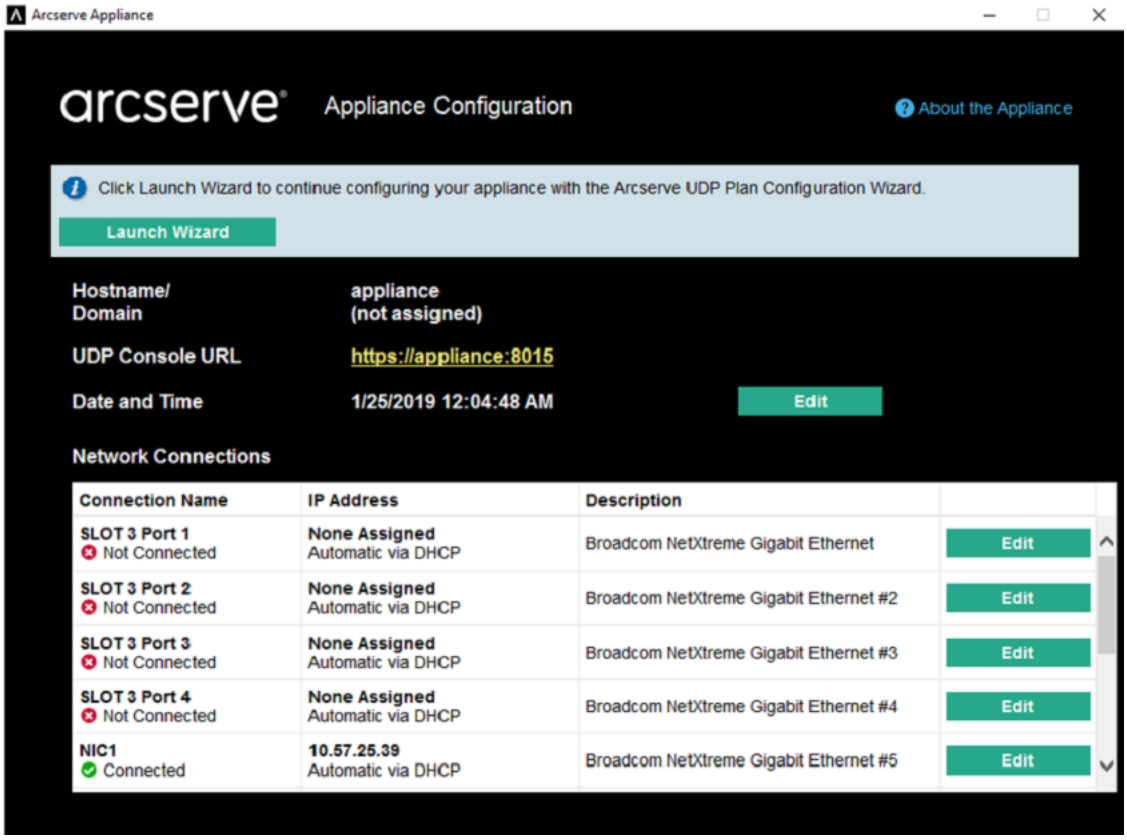
7. Um die Änderungen zu übernehmen, klicken Sie auf **Appliance neu starten**, um die Appliance neu zu starten.

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

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

Der Bildschirm "Arcserve Appliance-Konfiguration" wird angezeigt.

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



Einrichten derArcserve Appliance

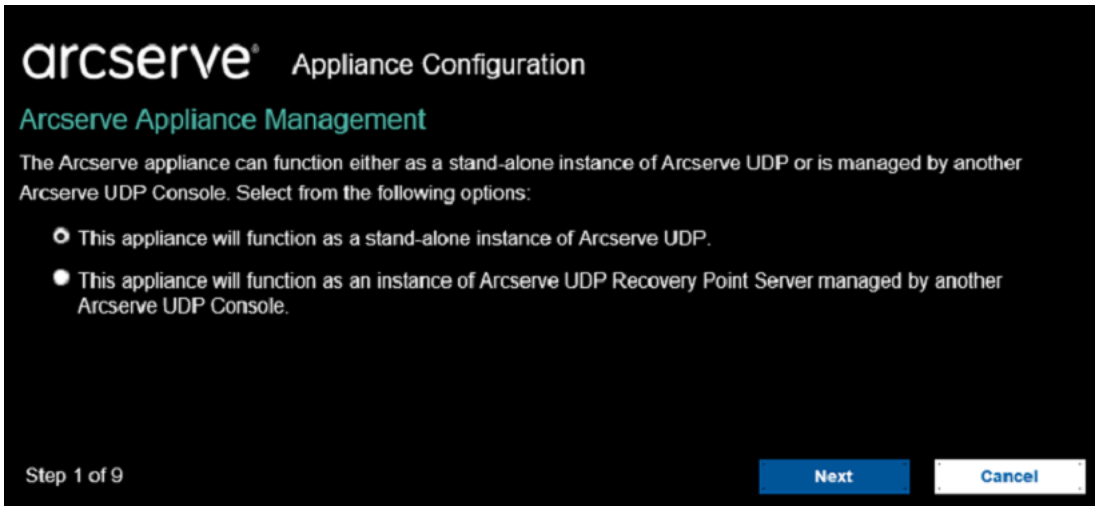
Nach dem Neustart der Appliance mit dem neuen Hostnamen wird der Unified Data Protection-Assistent geöffnet. Der Assistent ermöglicht das Erstellen eines einfachen Sicherungsablaufplans. In dem Plan können Sie die Knoten festlegen, die Sie schützen möchten, und den Zeitplan für das Ausführen von Sicherungen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

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

Befolgen Sie diese Schritte:

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

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

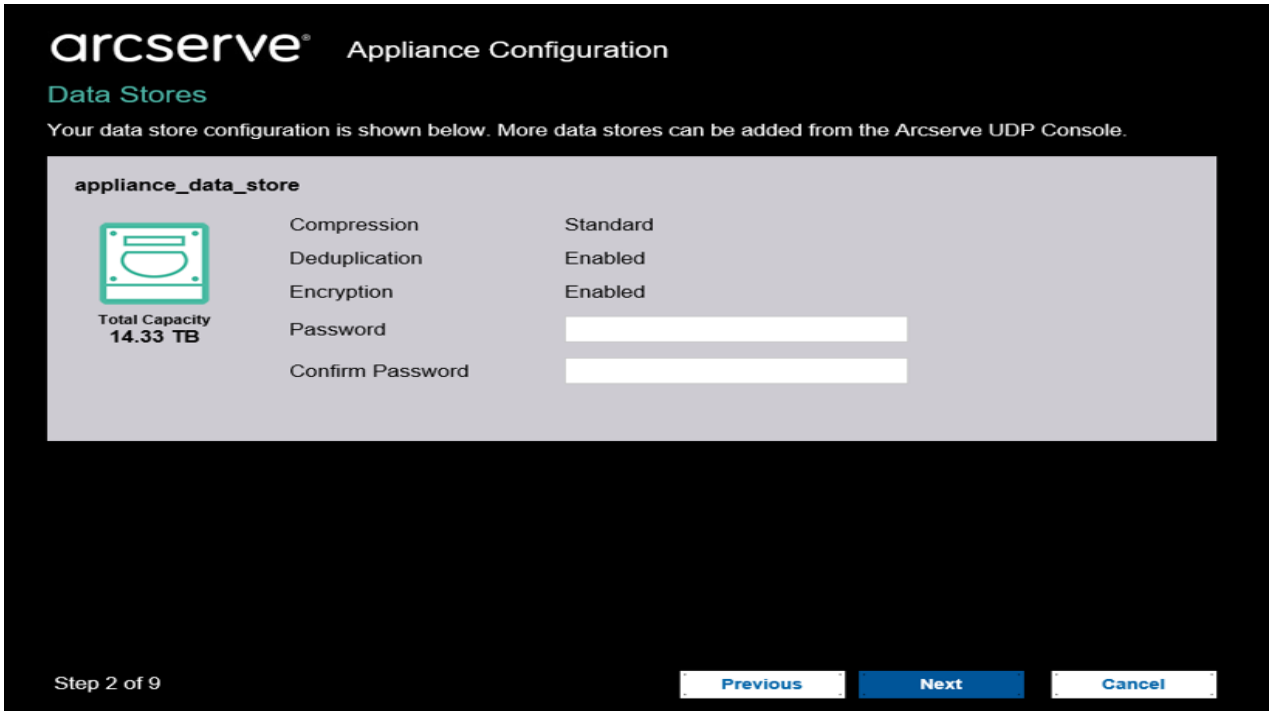


2. Wählen Sie aus, ob die Appliance lokal (Standard) oder über eine andere UDP-Konsole verwaltet werden soll. Wenn die Appliance von einer anderen UDP-Konsole verwaltet wird, geben Sie die URL der UDP-Konsole, den Benutzernamen und das Kennwort an.
3. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Datenspeicher** wird geöffnet. Ein Datenspeicher ist ein physischer Speicherbereich auf der Appliance und wird als Ziel für Ihre Sicherungen verwendet.

Standardmäßig erstellt Arcserve UDP einen Datenspeicher mit dem Namen <hostname>_data_store. Für diesen Datenspeicher sind Deduplizierung und Verschlüsselung aktiviert. Weitere Informationen zu Deduplizierung und Verschlüsselung finden Sie unter *Datendeduplizierung* im Arcserve UDP-Lösungshandbuch.

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



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

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

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

   Dienst

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

   E-Mail-Server

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

Port

Gibt die Portnummer des E-Mail-Servers an.

Authentifizierung erforderlich

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

Betreff

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

In

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

Empfänger

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

Optionen

Gibt die Verschlüsselungsmethode für den Kommunikationskanal an.

Verbindung per Proxy-Server aufbauen

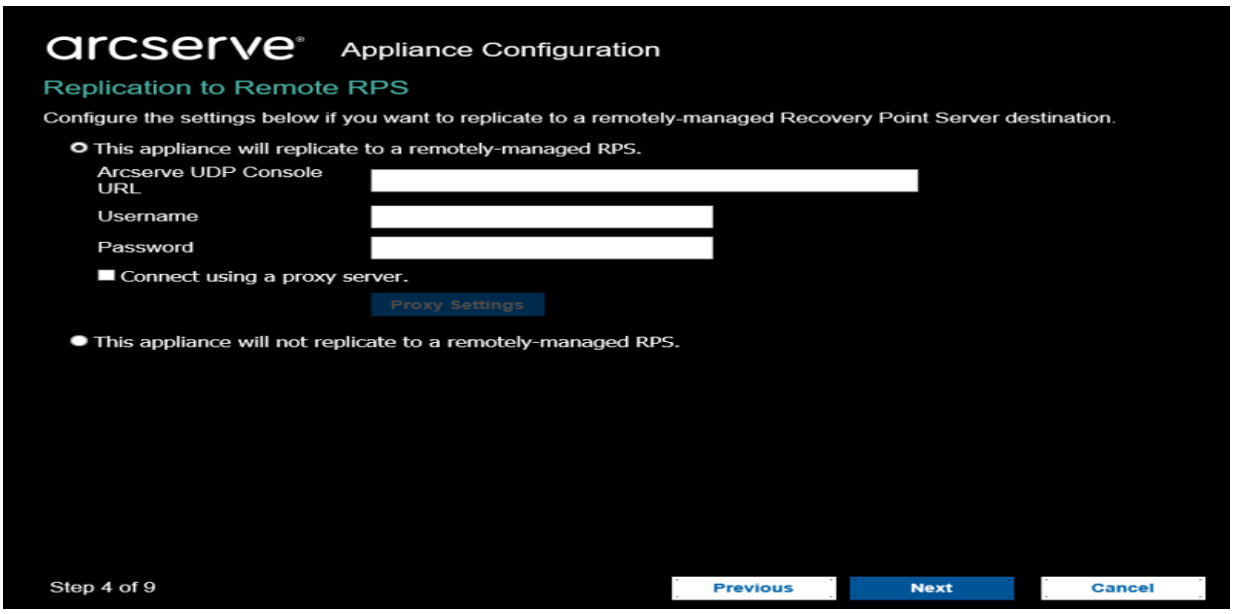
Gibt den Benutzernamen und die Portnummer des-Proxy-Servers an, wenn Sie die Verbindung mit dem E-Mail-Server über einen Proxy-Server herstellen. Geben Sie außerdem einen Benutzernamen und ein Kennwort an, falls der Proxy-Server eine Authentifizierung verlangt.

Test-E-Mail senden

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

7. Klicken Sie auf **Weiter**.

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



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

   URL der Arcserve UDP-Konsole

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

   Benutzername und Kennwort

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

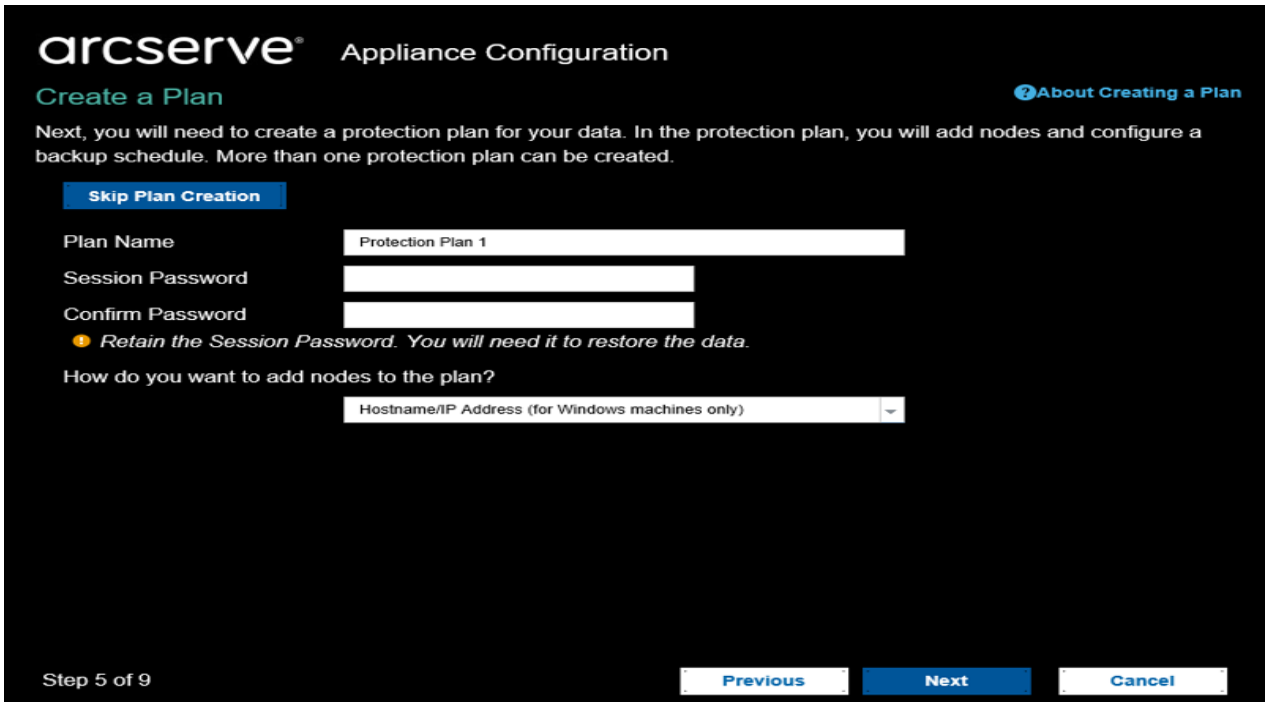
   Verbindung per Proxy-Server aufbauen

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

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

11. Klicken Sie auf **Weiter**.

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



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

a. Klicken Sie auf **Planerstellung abbrechen**.

   Das Dialogfeld **Nächste Schritte** wird geöffnet.

b. Klicken Sie auf **Fertig stellen**, um die UDP-Konsole zu öffnen und Pläne zu erstellen.

12. Um einen Plan zu erstellen, geben Sie die folgenden Details an:

Name des Plans

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

Sitzungskennwort

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

Wie möchten Sie Knoten zum Plan hinzufügen?

Gibt die Methode an, mit der Knoten zum Plan hinzugefügt werden. Wählen Sie eine der folgenden Methoden:

- Hostname/IP-Adresse

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

- Knoten werden von Active Directory erkannt

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

- Von einem vCenter/ESX-Server importieren

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

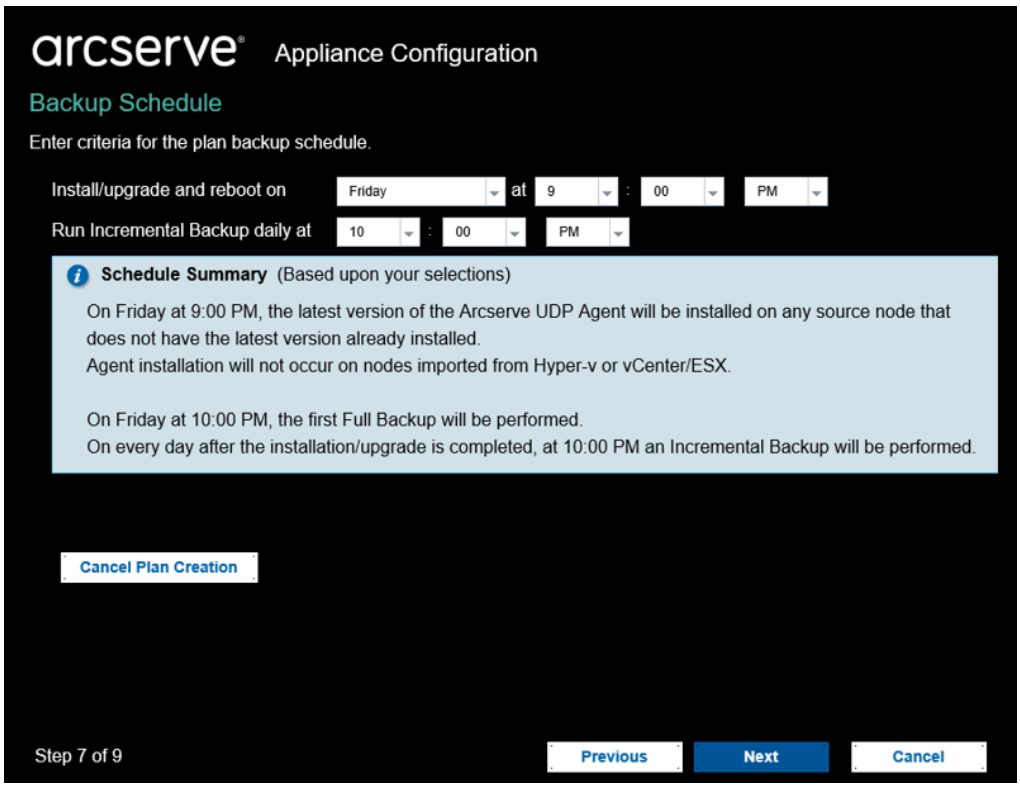
- Von einem Hyper-V-Server importieren

  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.

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

Das Dialogfeld **Sicherungsablaufplan** wird geöffnet.



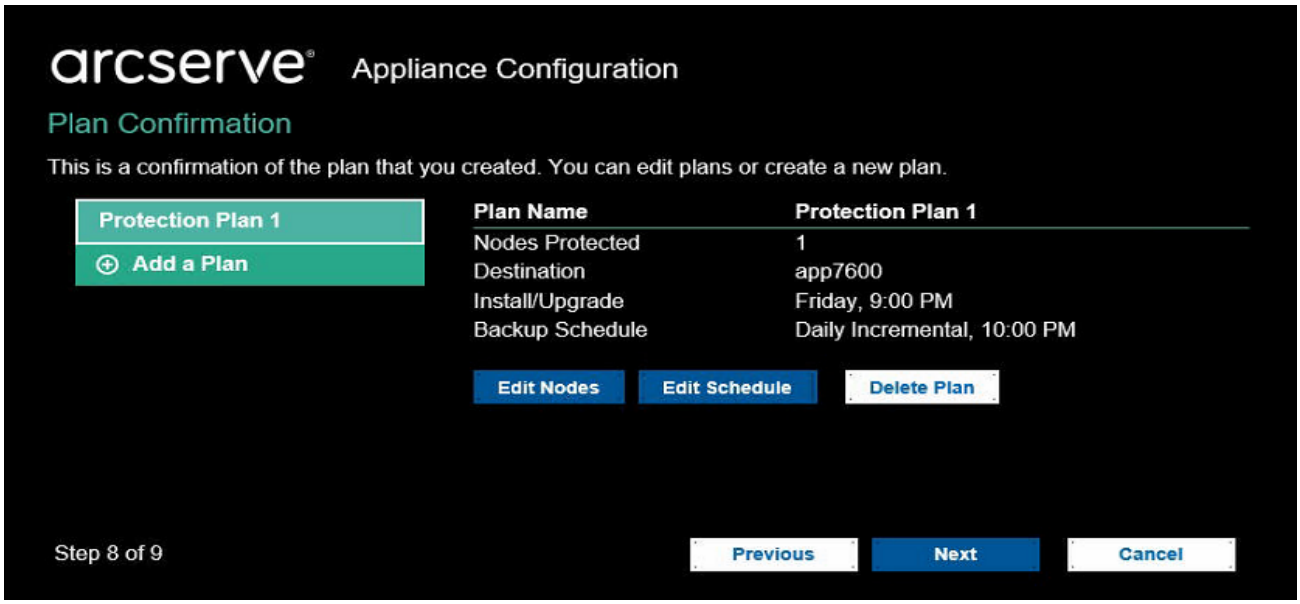
14. Geben Sie den folgenden Plan ein:

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

      Hinweis: Wenn die Sicherung vor dem Zeitpunkt der Installation bzw. Aktualisierung geplant ist, wird die Sicherung automatisch für den nächsten Tag geplant. Wenn Sie beispielsweise die Agenteninstallation für Freitag 21:00 Uhr und die Sicherung für 20:00 Uhr planen, wird die Sicherung am Samstag um 20:00 Uhr durchgeführt.
    - **Planerstellung abbrechen:** Um den Plan abzubrechen, den Sie gerade erstellt haben, klicken Sie auf **Planerstellung abbrechen**.

15. Klicken Sie auf **Weiter**.

    Das Dialogfeld **Bestätigung des Plans** wird geöffnet.



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

    Knoten bearbeiten

    Fügen Sie die Quellknoten hinzu, die Sie schützen möchten.

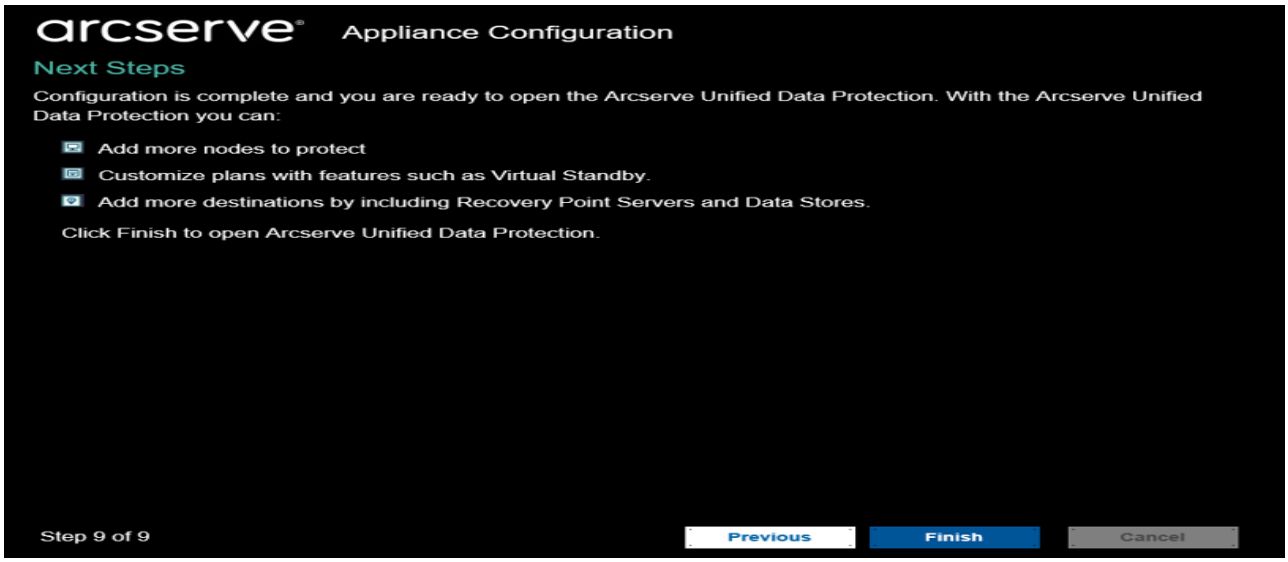
    Bearbeiten eines Ablaufplans

    Ändert den Sicherungsablaufplan:

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

    Das Dialogfeld **Nächste Schritte** wird geöffnet.

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



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

Konfigurieren derArcserve Appliance als Gateway

Sie können Arcserve Appliance als Gateway konfigurieren.

Befolgen Sie diese Schritte:

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

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

Kapitel 6: Arbeiten mit Arcserve Appliance

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

Dieser Abschnitt enthält folgende Themen:

Aktivieren eines Arcserve-Produkts auf der Appliance

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

Erstellen eines Plans mithilfe des Arcserve Appliance-Assistenten

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

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

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

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

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

Hinzufügen eines Knotens zu einem Plan

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

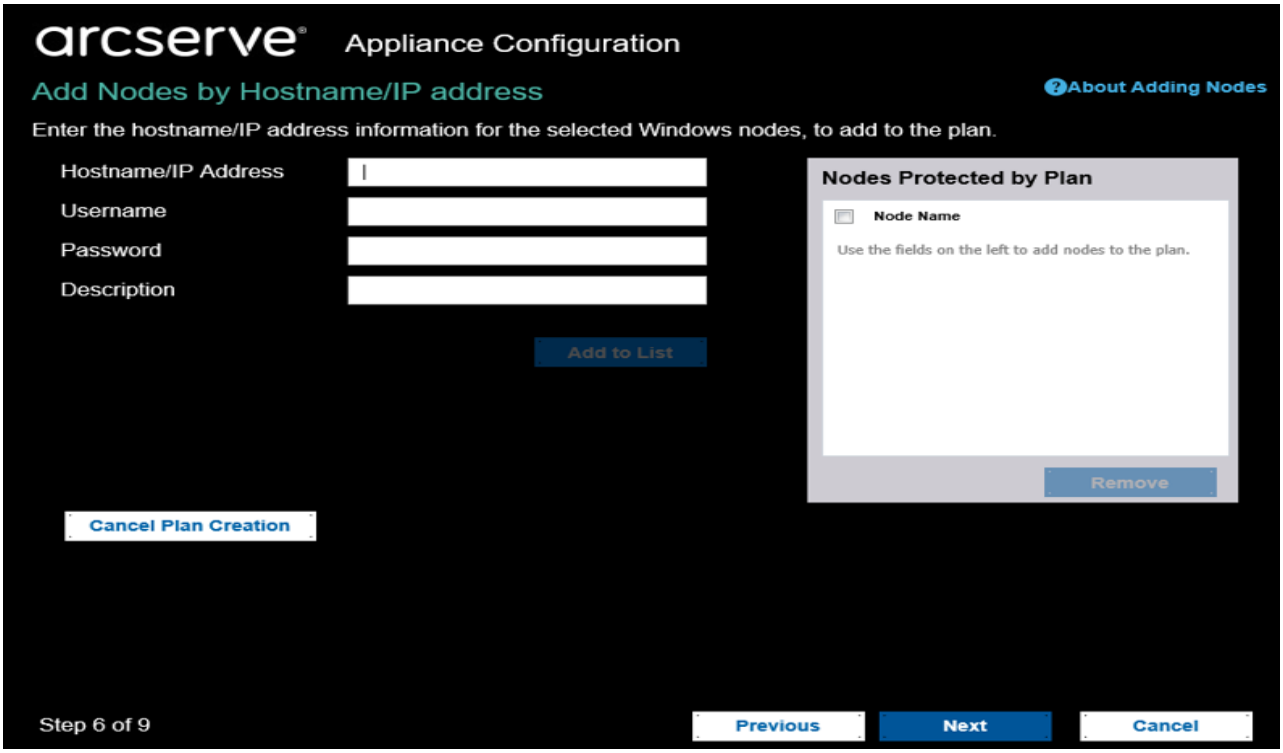
- Manuelle Eingabe der IP-Adresse oder des Hostnamens für den Knoten (Knoten nach Hostname/IP-Adresse hinzufügen)
- Erkennen von Knoten aus einem Active Directory (Knoten nach Active Directory hinzufügen)
- Importieren von VM-Knoten von ESX/vCenter-Servern (vCenter/ESX-Knoten hinzufügen)
- Importieren 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 Unified Data Protection Agent für Windows installiert.

Befolgen Sie diese Schritte:

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



Hostname/IP-Adresse

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

Benutzername

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

Kennwort

Gibt das Benutzerkennwort an.

Beschreibung

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

Planerstellung abbrechen

Bricht den gerade erstellten Plan ab.

2. Klicken Sie auf **Zur Liste hinzufügen**.

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

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

   Die Knoten werden zum Plan hinzugefügt.

Knoten nach Active Directory hinzufügen

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

Befolgen Sie diese Schritte:

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

   Benutzername

   Gibt Domäne und Benutzernamen im Format Domäne\Benutzername an.

   Kennwort

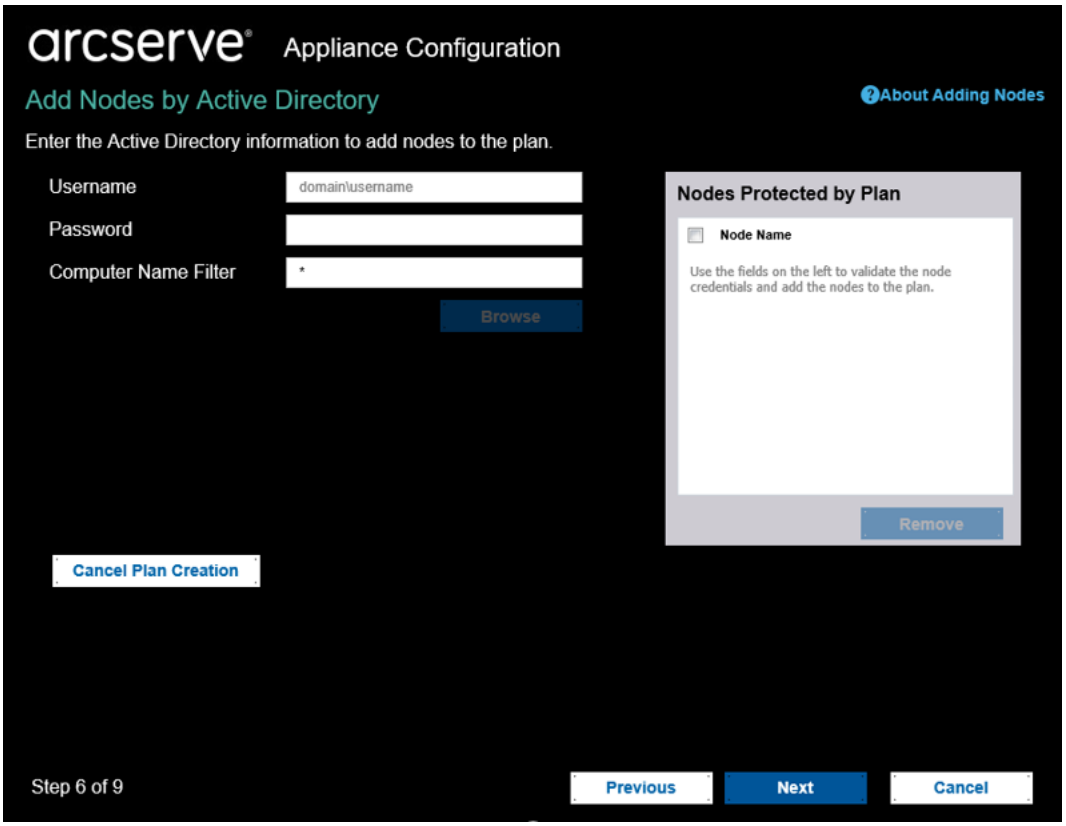
   Gibt das Benutzerkennwort an.

   Computernamenfilter

   Gibt den Filter zum Erkennen der Knotennamen an.

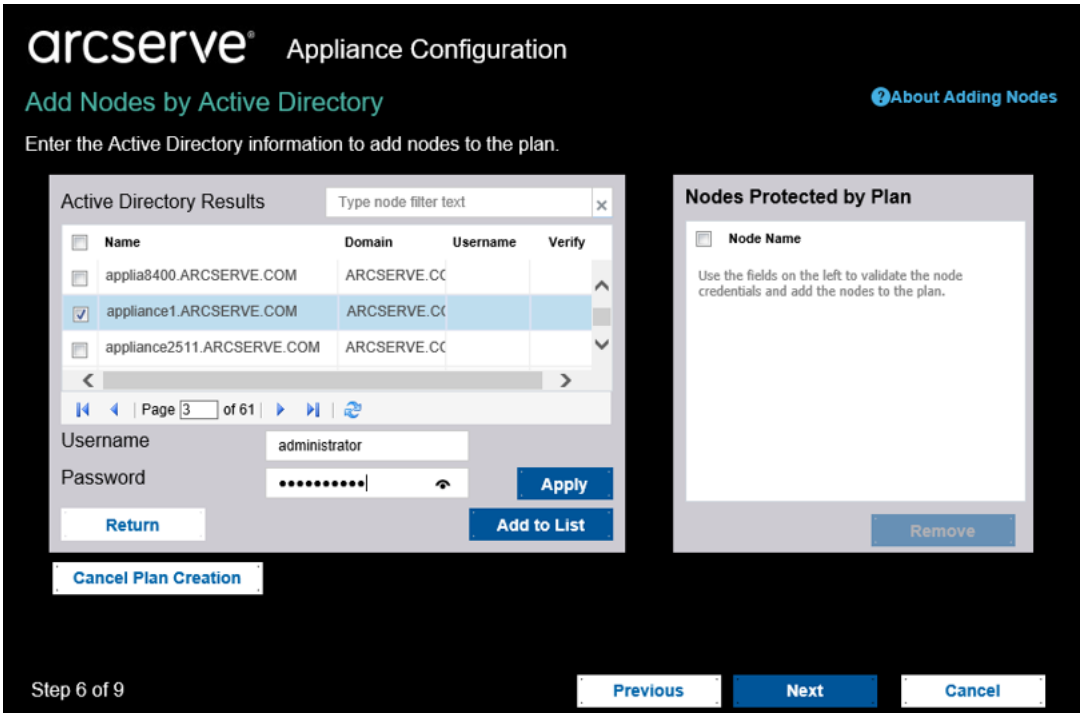
   Planerstellung abbrechen

   Bricht den gerade erstellten Plan ab.



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 entfernen, wählen Sie die Knoten aus, und klicken Sie auf **Entfernen**.

6. Klicken Sie auf **Weiter**.

   Die Knoten werden zum Plan hinzugefügt.

vCenter/ESX-Knoten hinzufügen

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

Befolgen Sie diese Schritte:

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

Hostname/IP-Adresse

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

Port

Gibt die Portnummer an, die verwendet werden soll.

Protokoll

Gibt das Protokoll an, das verwendet werden soll.

Benutzername

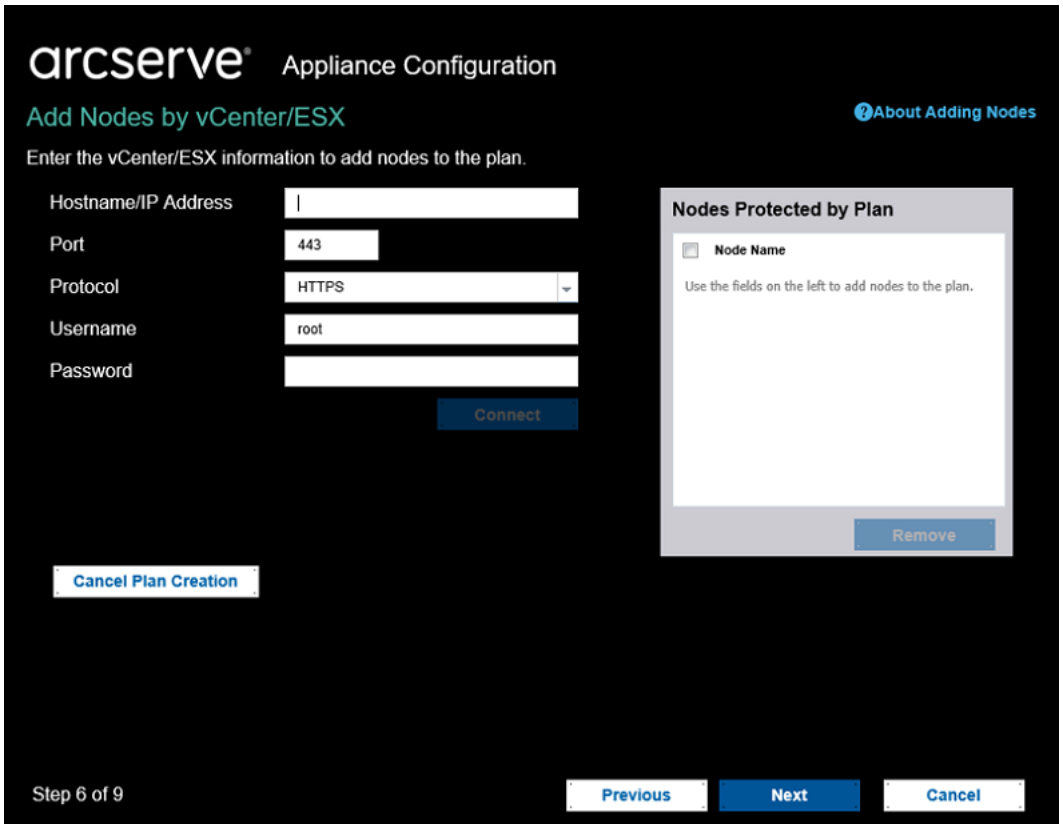
Gibt einen Benutzernamen auf dem Server an.

Kennwort

Gibt das Benutzerkennwort an.

Planerstellung abbrechen

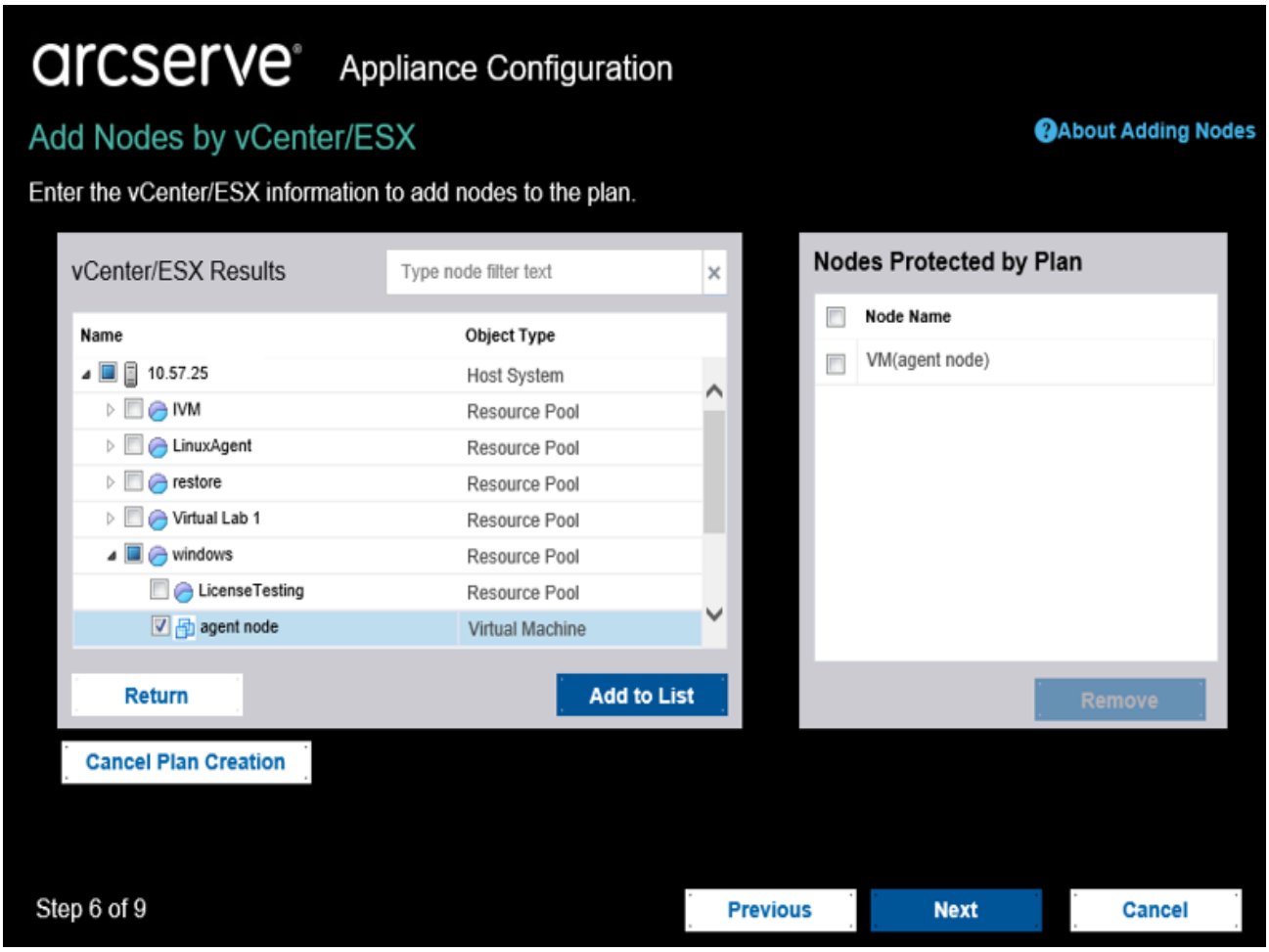
Bricht den gerade erstellten Plan ab.



2. Klicken Sie auf **Verbinden**.

   Die erkannten Hostnamen werden angezeigt.

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



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

   Die ausgewählten Knoten werden im rechten Fensterbereich hinzugefügt.

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

6. Klicken Sie auf **Weiter**.

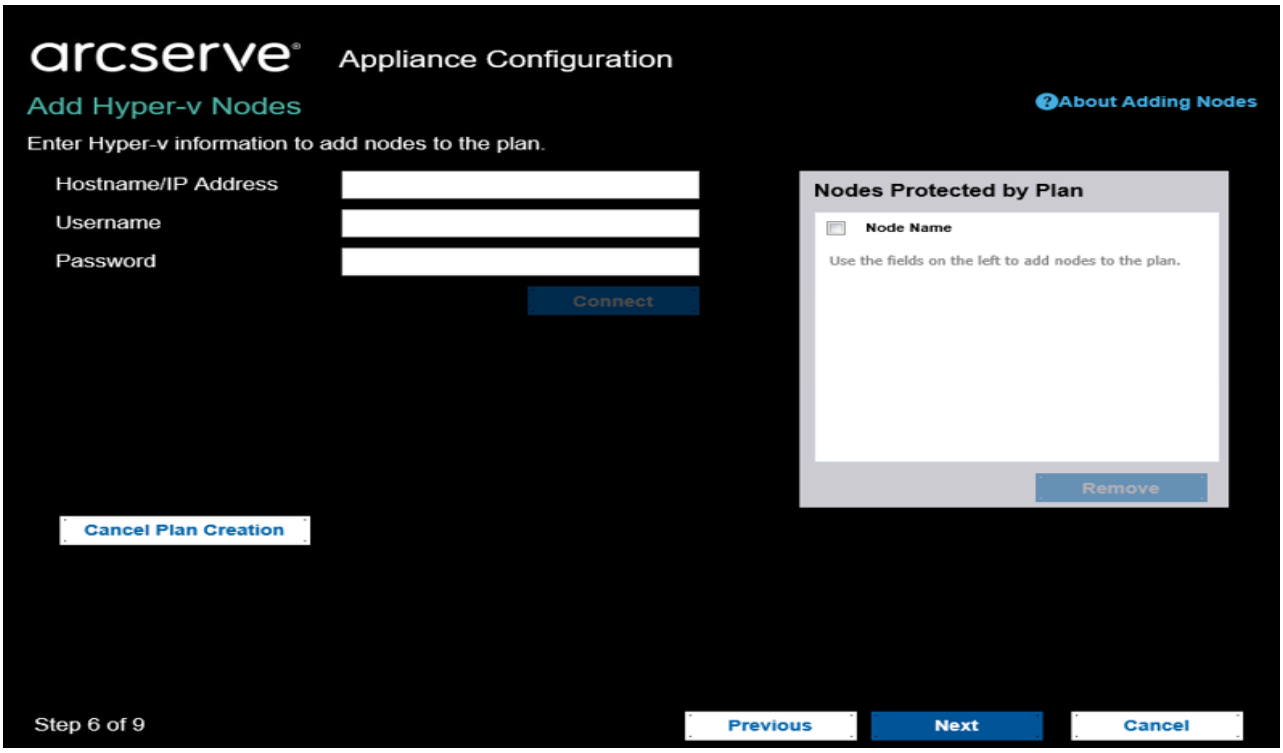
   Die Knoten werden zum Plan hinzugefügt.

Hyper-V-Knoten hinzufügen

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

Befolgen Sie diese Schritte:

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



Hostname/IP-Adresse

Gibt den Namen oder die IP-Adresse des Hyper-V-Servers an. Um virtuelle Rechner zu importieren, die in Hyper-V-Clustern sind, geben Sie entweder den Cluster-Knotennamen oder den Hyper-V-Hostnamen an.

Benutzername

Gibt den Namen eines Hyper-V-Benutzers mit Administratorrechten an.

Hinweis: Verwenden Sie für Hyper-V-Cluster ein Domänenkonto mit Administratorrechten des Clusters. Für eigenständige Hyper-V-Hosts empfehlen wir, ein Domänenkonto zu verwenden.

Kennwort

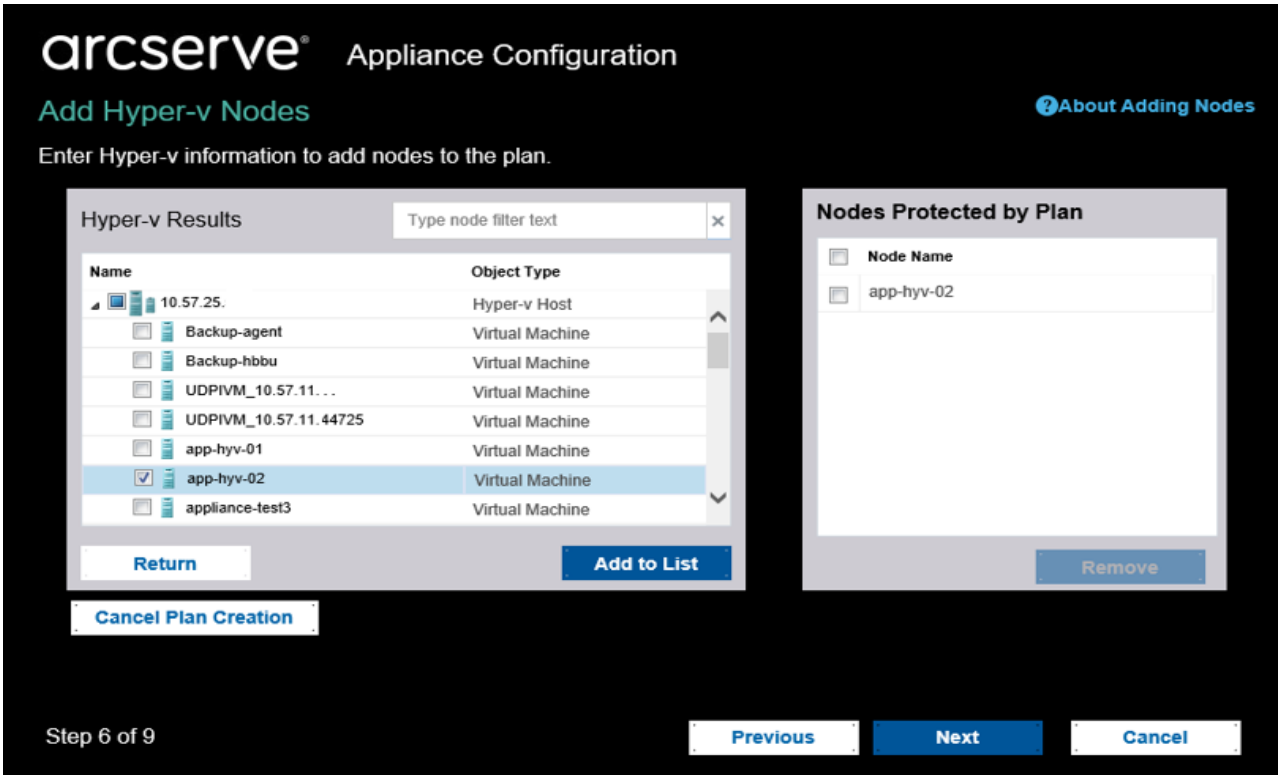
Gibt das Kennwort für den Benutzernamen an.

Planerstellung abbrechen

Bricht den gerade erstellten Plan ab.

2. Klicken Sie auf **Verbinden**.

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



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

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

   Die Knoten werden zum Plan hinzugefügt.

Sicherungsablaufplan für Linux-Knoten erstellen

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

Befolgen Sie diese Schritte:

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

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

Sicherungsablaufplan für ein Bandgerät erstellen

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

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

1. **Schließen Sie das Bandgerät an dieArcserve Appliance an**

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

2. **Bandgerät mit Backup Manager konfigurieren**

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

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

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

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

   Hinweis: Weitere Informationen zum Erstellen eines Sicherungsplan für unterschiedliche Knoten finden Sie unter 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. Die Quelldaten sind das Ziel des UDP-Sicherungsplans und das Ziel des Bandgeräts.

Hinweis: Weitere Informationen zum Erstellen eines Sicherungsplan finden Sie unter Sichern und Wiederherstellen von D2D/UDP-Daten im *Arcserve Backup-Administrationsleitfaden*.

Virtuellen On-Appliance-Standby-Plan erstellen

Die Arcserve Appliancekann als virtueller Standby-Rechner fungieren.

Befolgen Sie diese Schritte:

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

   Hinweis: Weitere Informationen zu den Konfigurationen finden Sie im Thema zur Erstellung eines Virtual Standby-PlansArcserve UDP im Lösungshandbuch.
6. Speichern Sie den Plan, und führen Sie ihn aus.

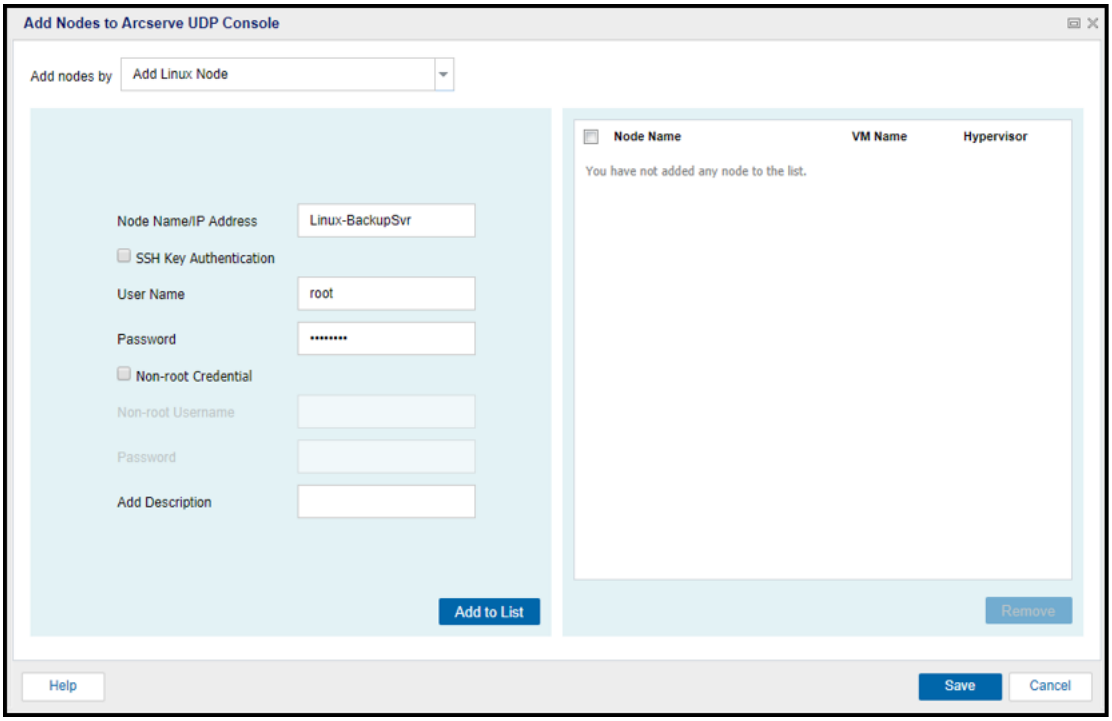
Erstellen eines Plans zur Sicherung von Linux-Sicherungsserver

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

Befolgen Sie diese Schritte:

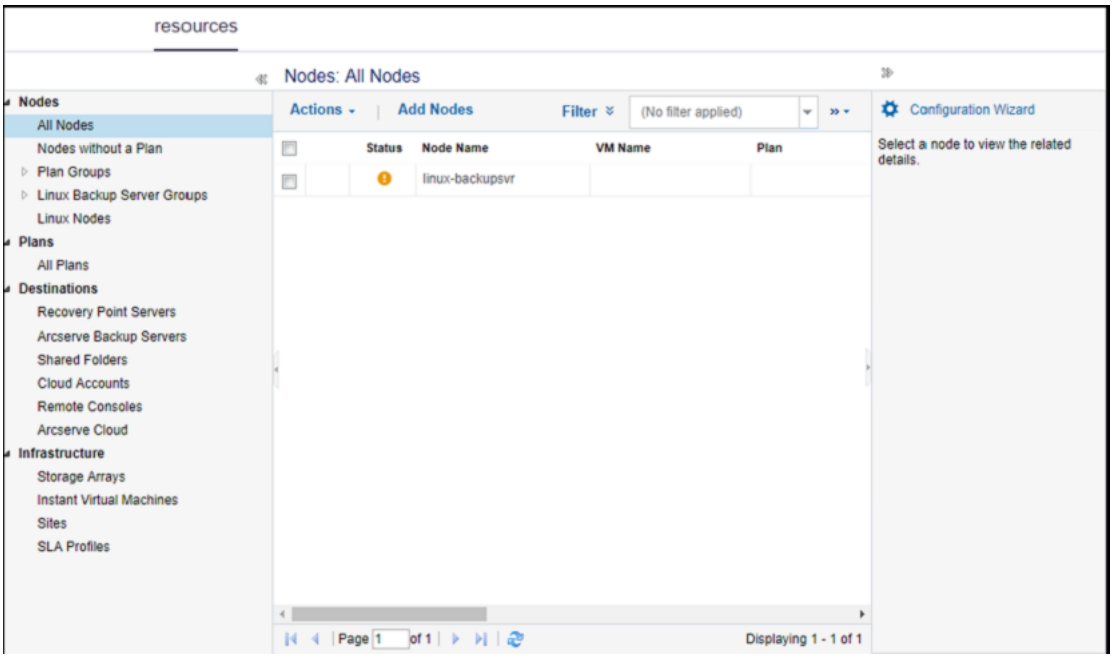
1. Klicken Sie in der Arcserve UDP-Konsole auf die Registerkarte **Ressourcen**.
2. Klicken Sie im rechten Fensterbereich auf **Alle Knoten**.
3. Klicken Sie im mittleren Fensterbereich auf **Knoten hinzufügen**.

   Das Dialogfeld **Knoten zu Arcserve UDP-Konsole hinzufügen** wird geöffnet.
4. Wählen Sie in der Dropdown-Liste **Hinzufügen von Knoten nach** die Option *Linux-Knoten hinzufügen*.
5. Geben Sie die Anmeldeinformationen für den Knoten ein, und klicken Sie auf **Zur Liste hinzufügen**.



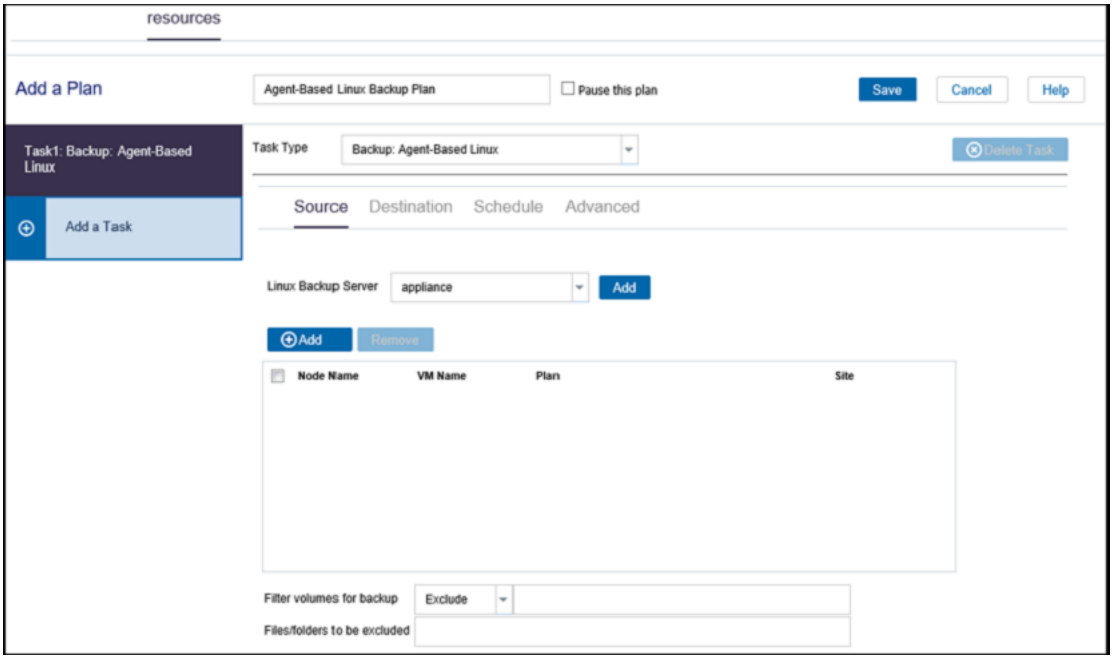
6. Klicken Sie auf **Speichern**.

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

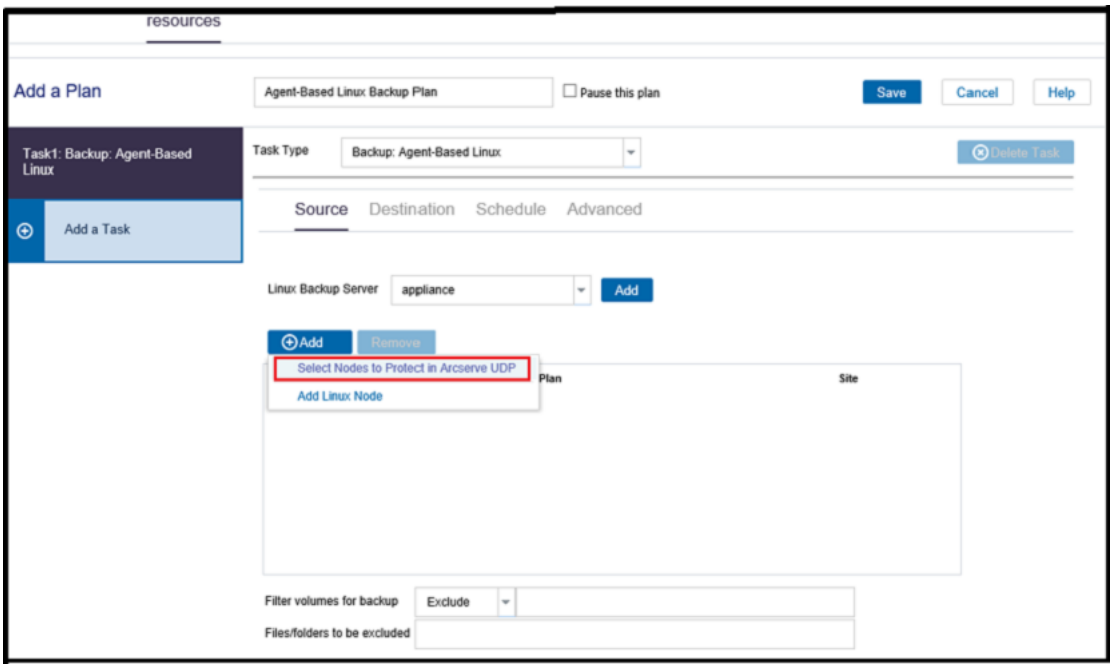


7. Navigieren Sie zu **Alle Pläne**, und erstellen Sie einen agentenbasierten Linux-Plan.

Die Registerkarte **Quelle** wird angezeigt.

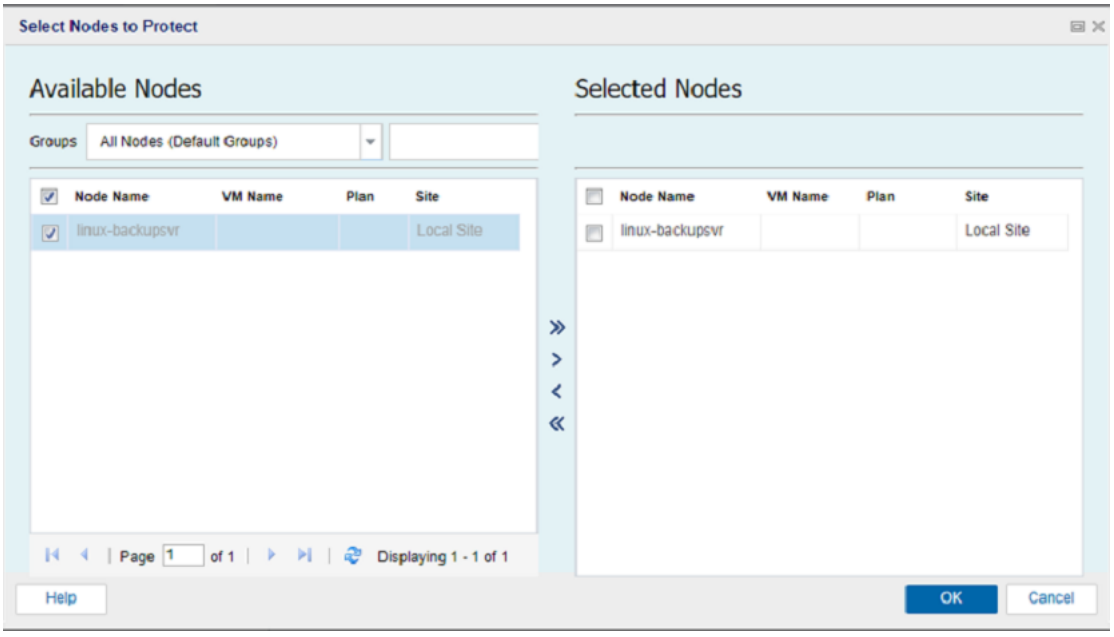


8. Wählen Sie den Drop-down-Liste **Hinzufügen** die Option *In Arcserve UDP zu schützende Knoten* aus.



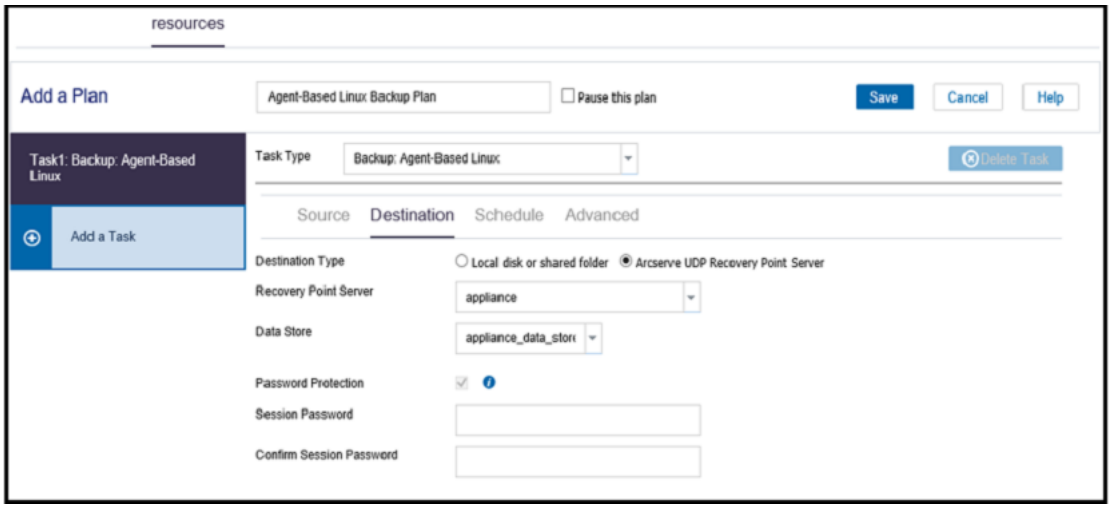
Das Dialogfeld "**Zu schützende Knoten auswählen**" wird geöffnet.

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

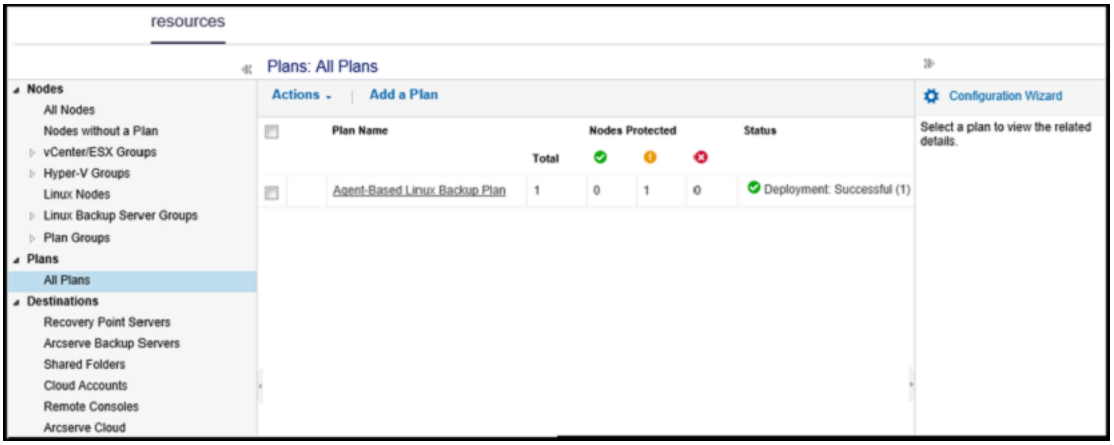


Die Registerkarte **Ziel** wird angezeigt.

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.

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

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

Befolgen Sie diese Schritte:

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

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

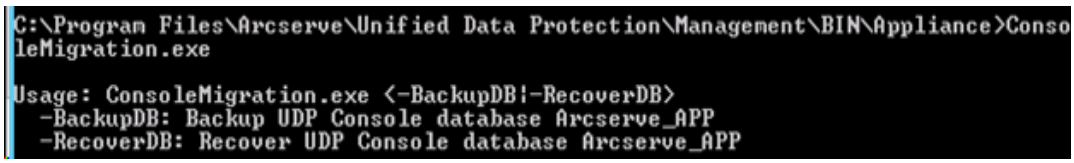
   Hinweis: Der Linux-Sicherungsserver *Linux-BackupSvr* wird während des Vorgangs neu gestartet.
4. Zum Ausführen eines Linux-Instant VM-Job zum lokalen Hyper-V wählen Sie den neu hinzugefügten virtuellen Netzwerk-Switch aus.

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

Migrieren der Arcserve UDP-Konsole mithilfe von ConsoleMigration.exe

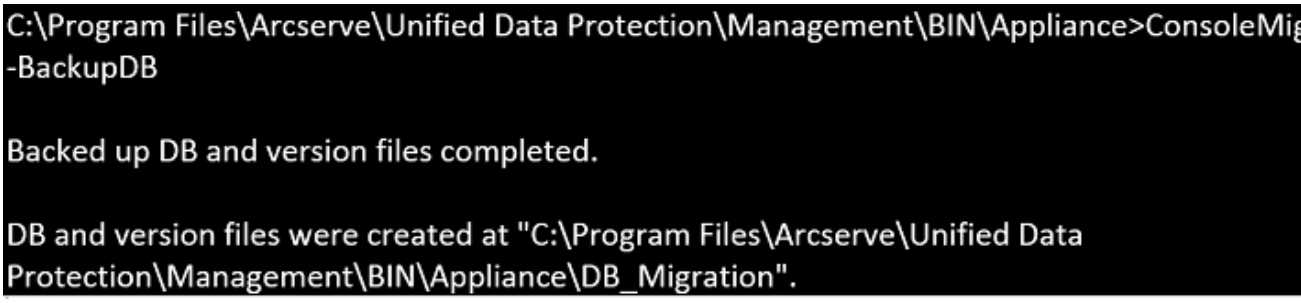
Auf der Arcserve Appliance können Sie die Arcserve UDP-Konsole mit *ConsoleMigration.exe* auf eine andere Appliance migrieren. Ab Arcserve UDP 6.5 Update 2 oder höher können Sie die Arcserve UDP-Konsole zwischen zwei beliebigen Arcserve UDP-Konsolen migrieren, auch wenn sie nicht zur Appliance gehören.

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



Gehen Sie zum Abschließen des Migrationsvorgangs folgendermaßen vor:

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



   Der Ordner *DB_Migration* wird erstellt.

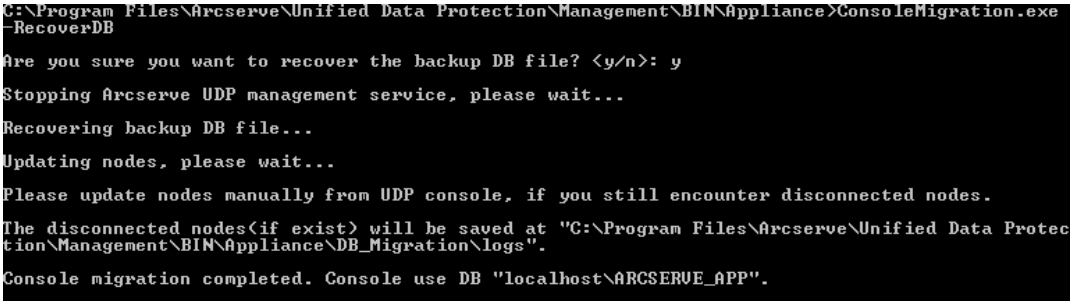
2. Kopieren Sie in der neuen Arcserve UDP-Konsole den Ordner *DB_Migration* in den folgenden Pfad:

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

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

   Hinweis: Wenn die Arcserve UDP-Konsole keineArcserve Appliance ist, überspringen Sie diesen Schritt.

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



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

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

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

Hinweis: AbArcserve UDP v6.5 Update 4 wird die Option ***-force*** im Befehl ***ConsoleMigration.exe*** eingeführt, um die Migration der Sicherungsdatenbankdatei für die Wiederherstellung auf die Zielkonsole unter folgenden Bedingungen zu erzwingen:

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

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

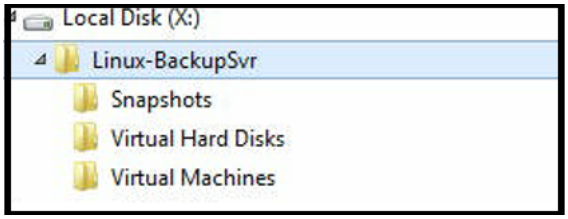
Migrieren des vorinstallierte Linux-Sicherungsservers in CentOS 7.4

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

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

Befolgen Sie diese Schritte:

1. Melden Sie sich bei der Arcserve Appliance mit den Anmeldeinformationen des Administrators an.
2. Aktualisieren Sie die früheren Versionen von Arcserve UDP in Arcserve Appliance und Linux-Sicherungsserver auf Arcserve UDP V6.5 Update 4 oder höher. Der Linux-Agent auf dem Linux-Sicherungsserver muss auch auf die gleiche Version der Arcserve UDP-Konsole aktualisiert werden
3. Laden Sie *Linux-BackupSvr.zip* über den Link herunter (MD5 für diesen Download ist *0A51C1020CB8EA569B9DCEAF7BF226E0*), und extrahieren Sie die Dateien auf die lokale Festplatte. Beispiel: Wenn Sie die Dateien auf Laufwerk X: extrahieren, wird der Pfad wie unten angezeigt.



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

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

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

   Linux_migration.ps1 –path X:\Linux-BackupSvr

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

   Die Befehlszeile zeigt den Status der Migration an.

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

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

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

Durchführen der Migration zwischen Arcserve Appliances

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

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

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

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

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

- Lösung 1
- Lösung 2

Lösung 1

Bare-Metal-Recovery (BMR)-Lösung

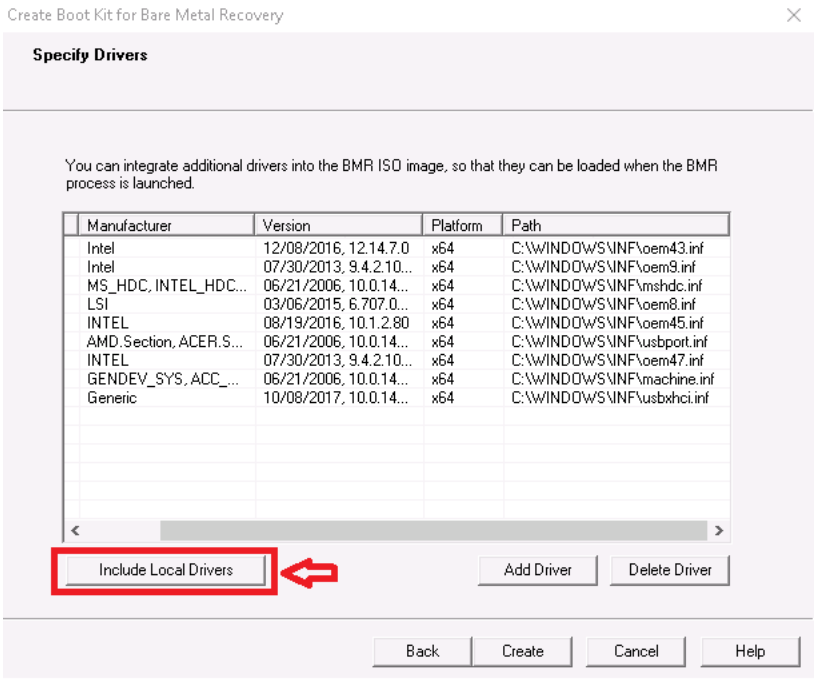
Gehen Sie wie folgt vor, um BMR aus der vorhandenen Arcserve Appliance auf einer anderen neuen Arcserve Appliance auszuführen:

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

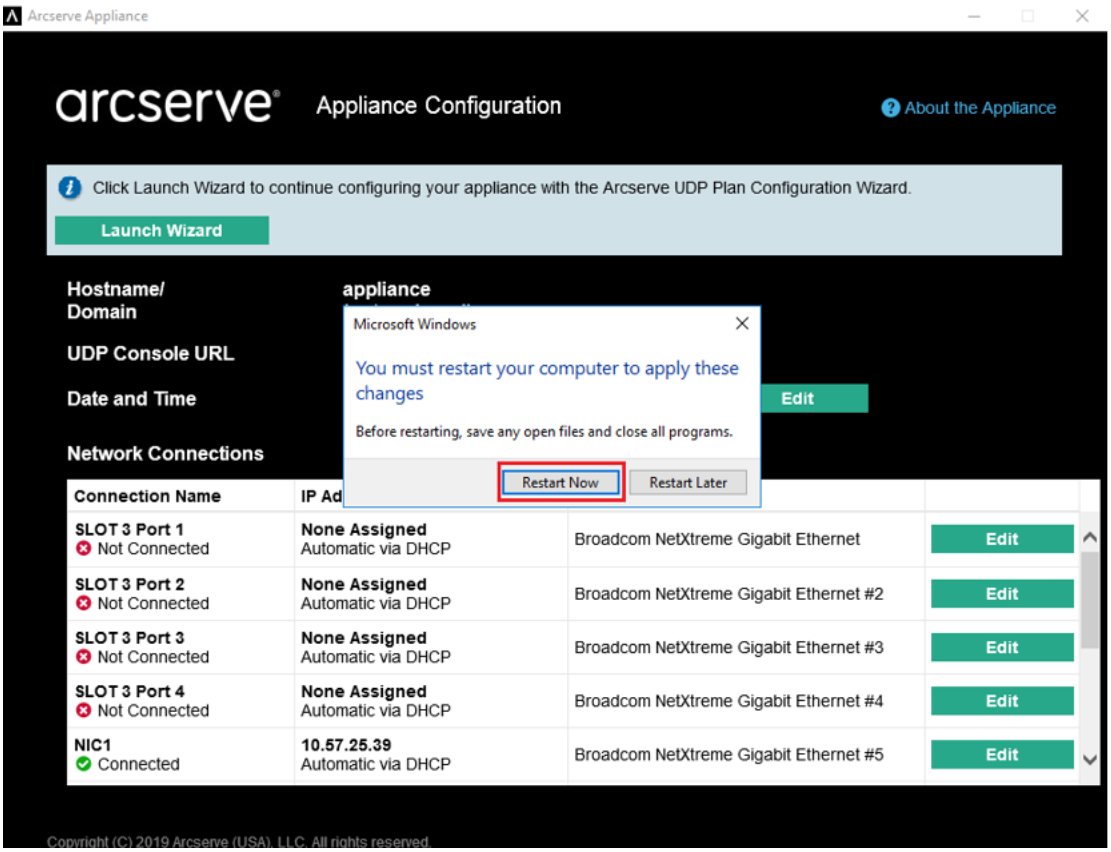
   Hinweis: Die folgende Warnung können Sie einfach ignorieren:

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

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



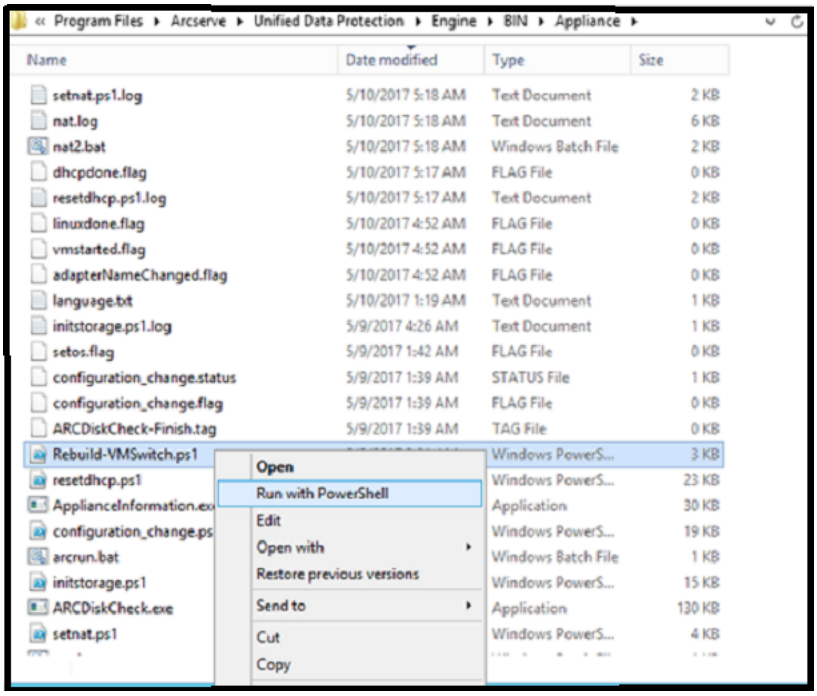
3. Starten Sie Appliance 8400 nach der BMR entsprechend der Systemeingabeaufforderung neu.



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

   Führen Sie den folgenden Befehl mit PowerShell aus:

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

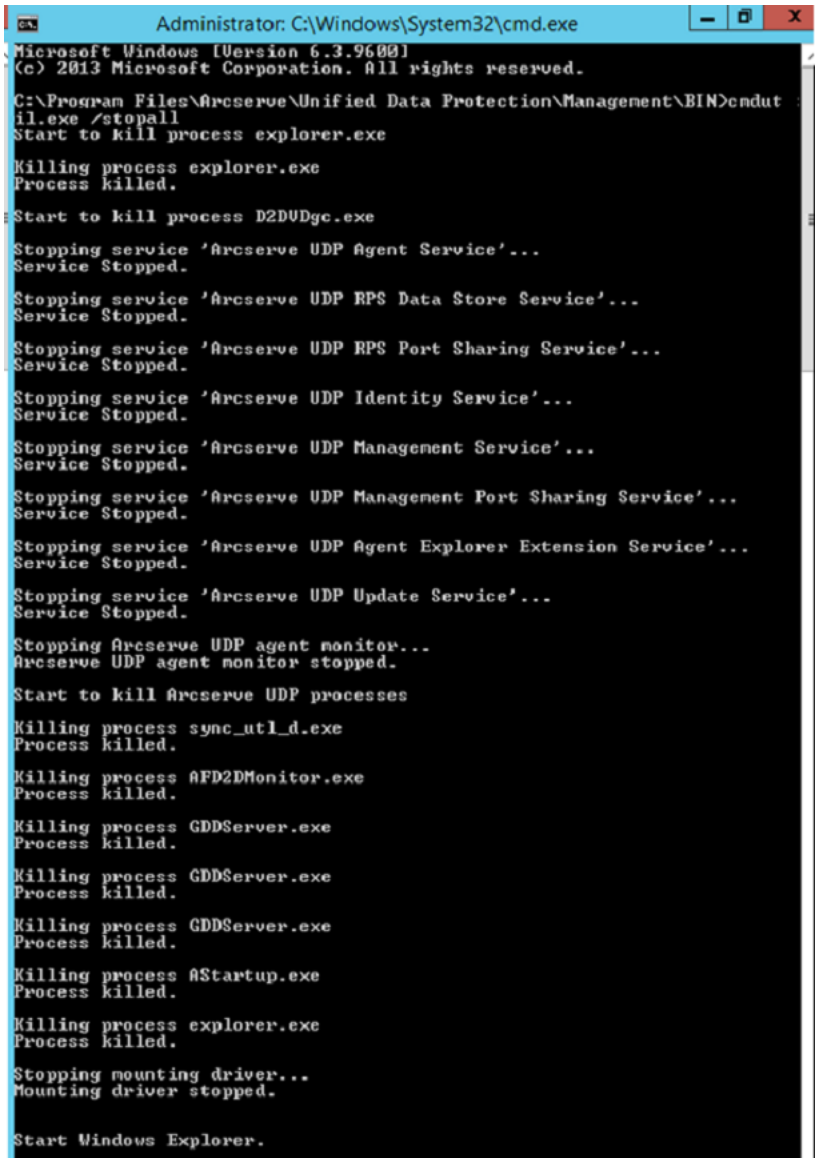


5. Führen Sie nun die folgenden Schritte aus, um die Daten auf Appliance 8200 nach Appliance 8400 zu kopieren und die Daten auf Appliance 8400 zu importieren:

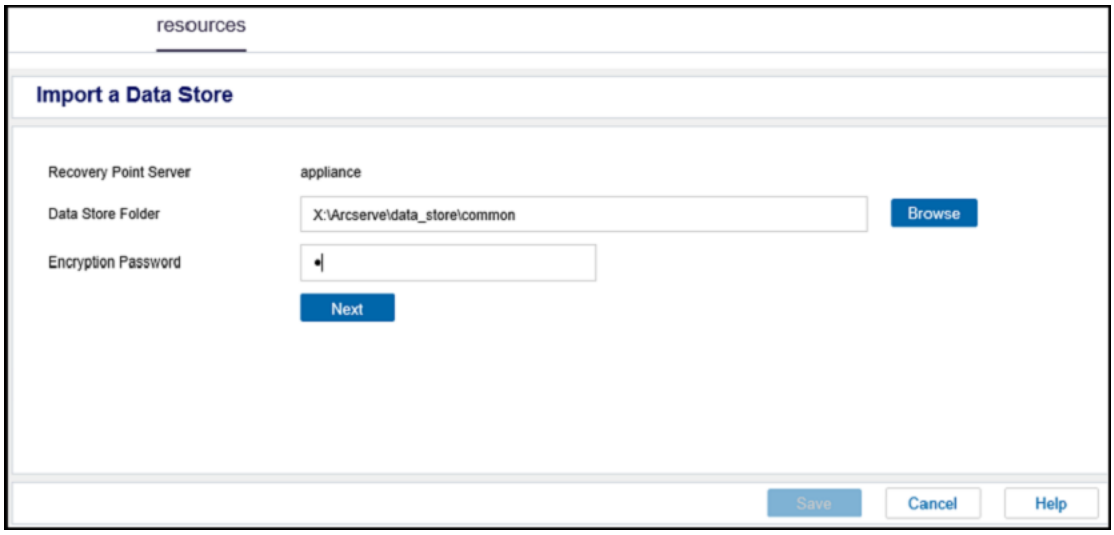
   a. Halten Sie alle UDP-Services auf der Arcserve Appliance 8200 mithilfe des folgenden Befehls aus der Befehlsauforderungszeile an:

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

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



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


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

Lösung 2

Migrieren der Arcserve Appliance-Lösung

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

Voraussetzungen:

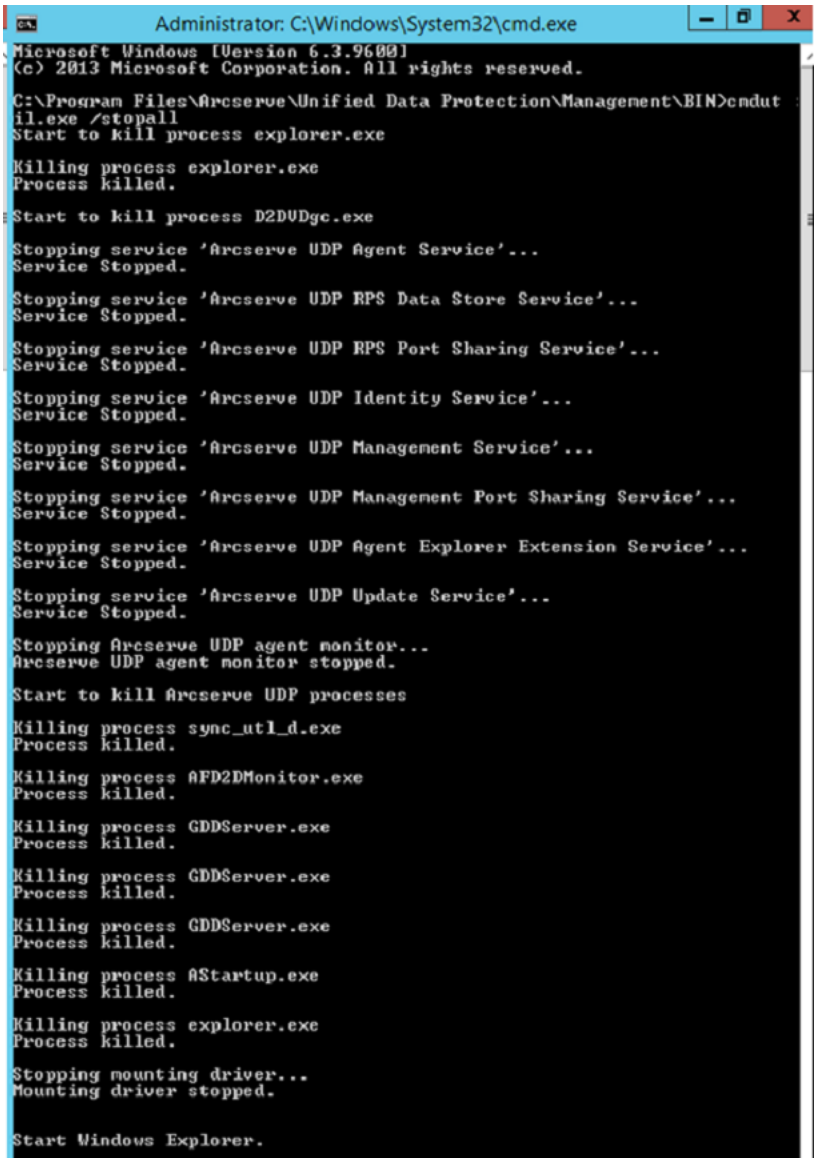
- Vergewissern Sie sich, dass auf Arcserve Appliance- 8200 kein Job ausgeführt wird.
- Sie haben die Arcserve UDP-Konsole von Arcserve Appliance 8200 auf 8400 migriert.

  Hinweis: Weitere Informationen zur Migration der Arcserve UDP-Konsole von Appliance 8200 auf 8400 finden Sie unter Migration der Arcserve UDP-Konsole mit ConsoleMigration.exe.

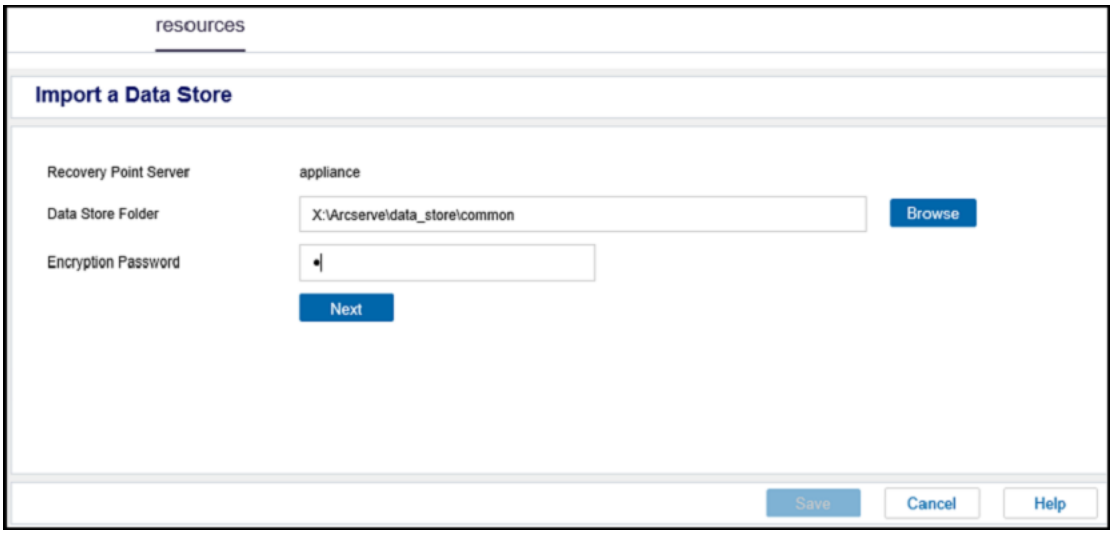
Befolgen Sie diese Schritte:

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

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



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



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

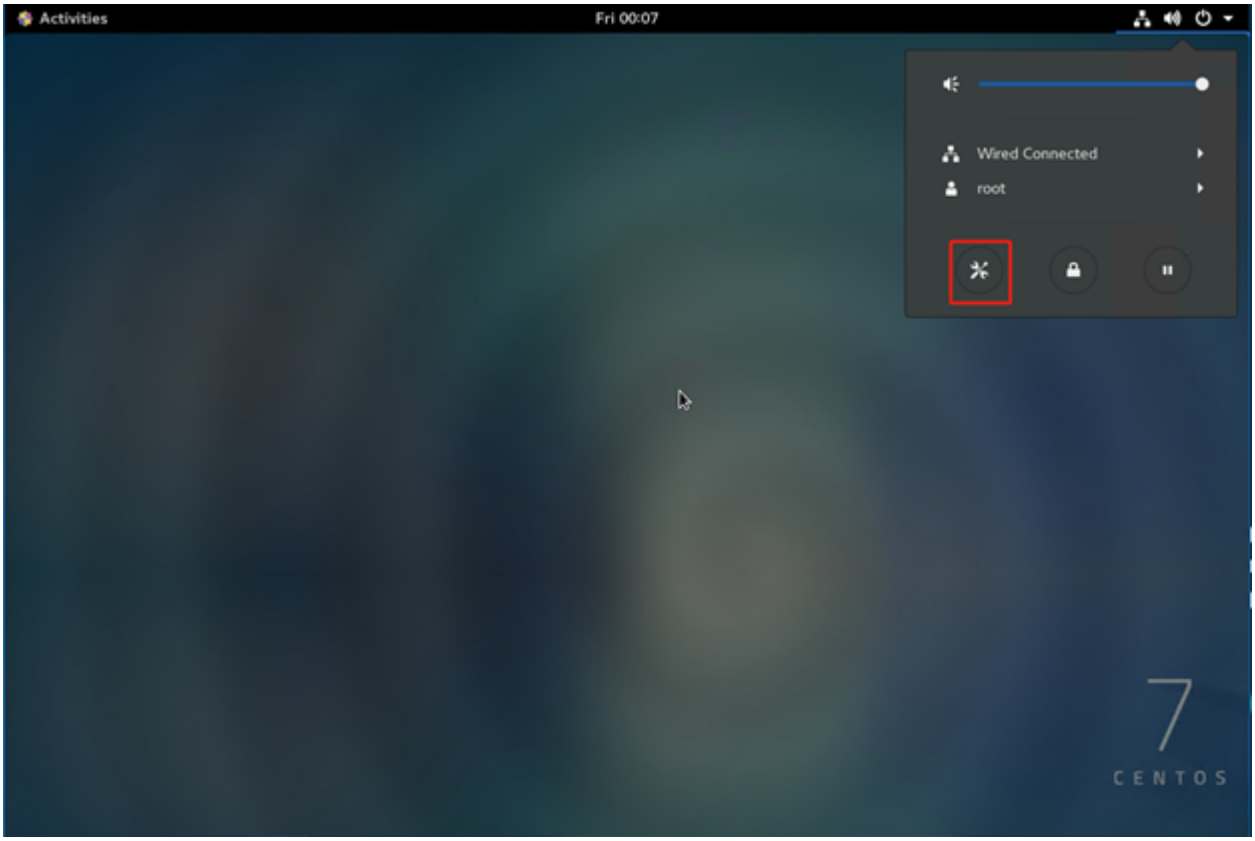
Sie haben die vorhandene Arcserve Appliance- erfolgreich in eine andere neue Arcserve Appliance- migriert.

Ändern der Eingabequelle des vorinstallierten Linux-Sicherungsservers

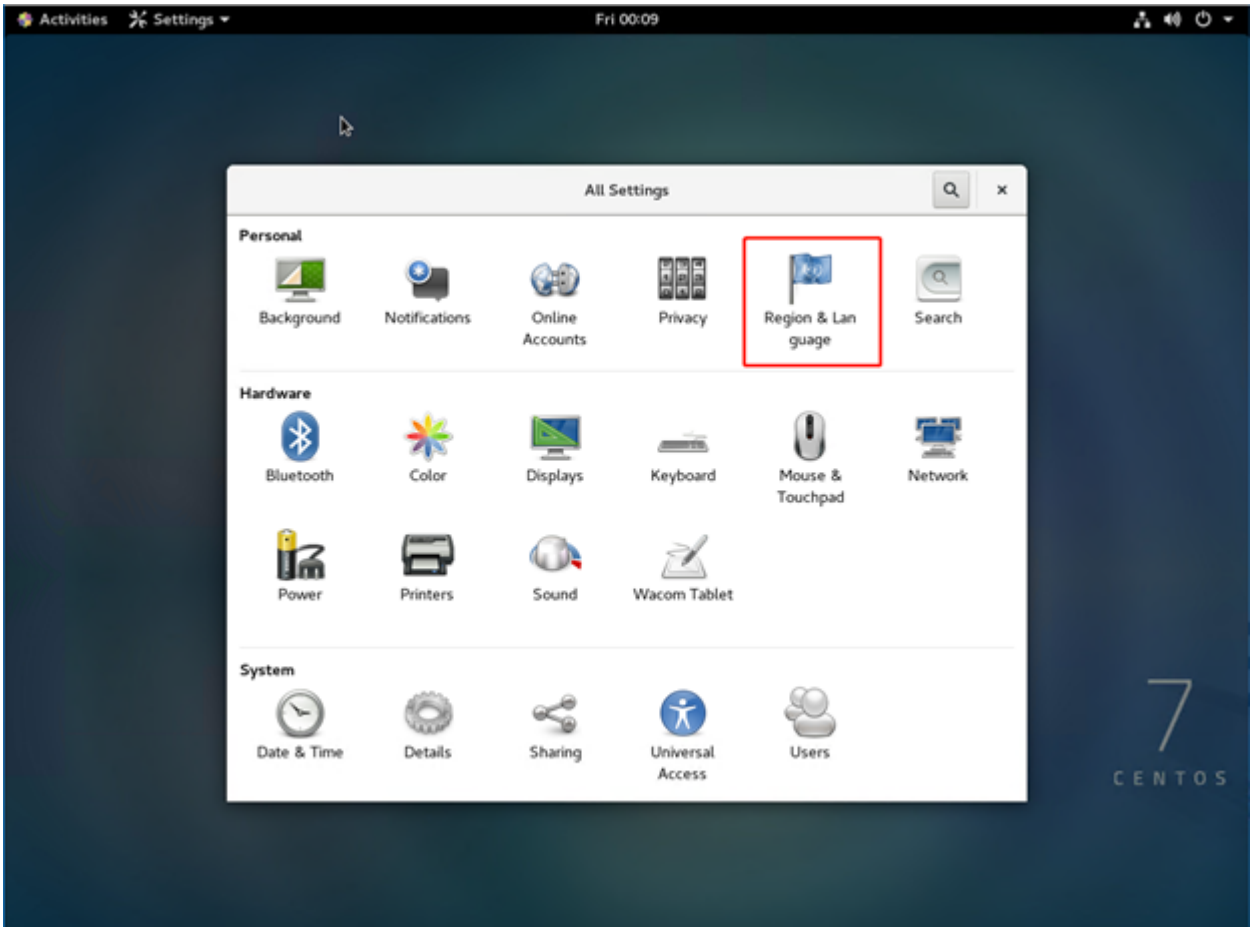
Sie können die Tastatur des vorinstallierten Linux-Sicherungsservers ändern.

Befolgen Sie diese Schritte:

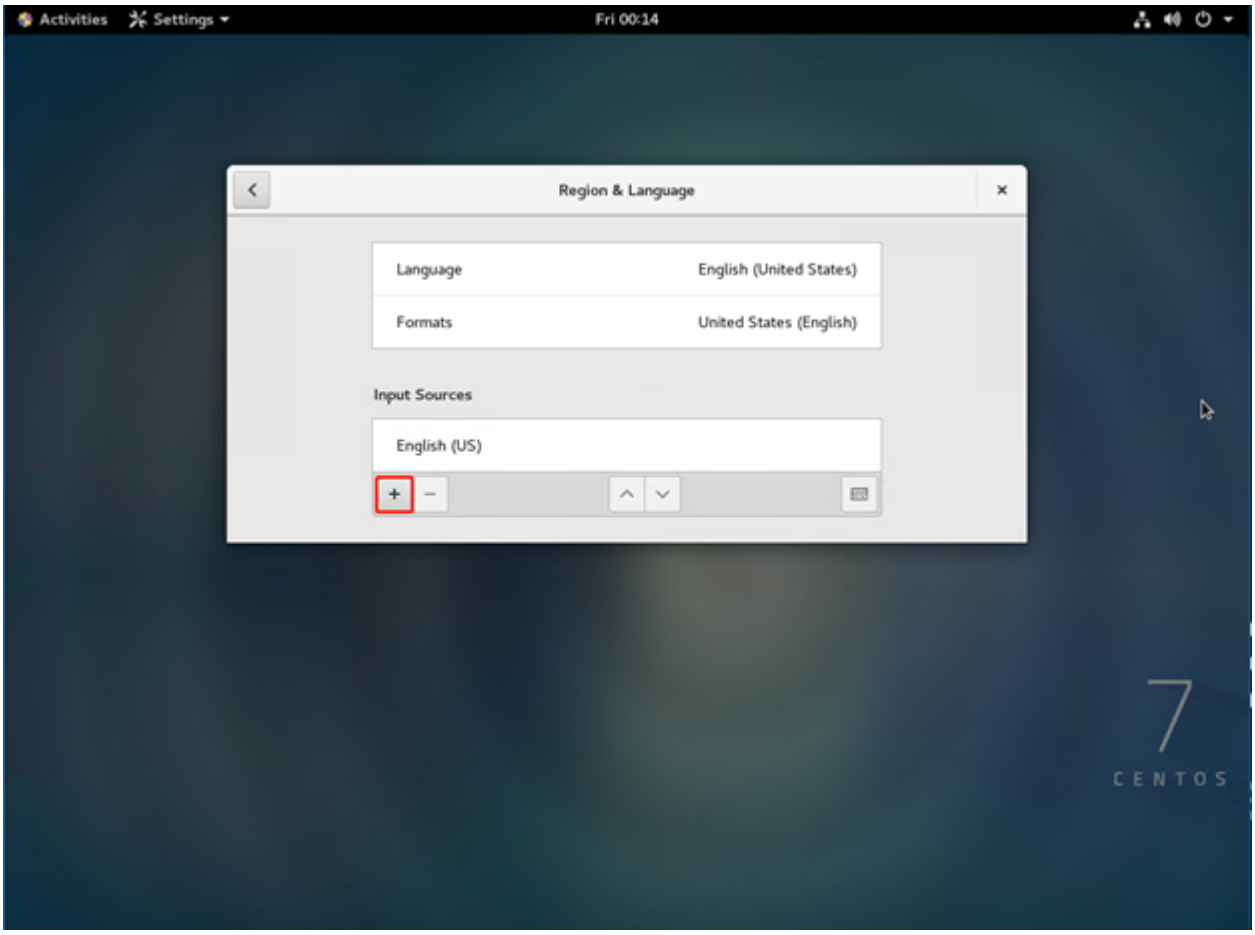
1. Melden Sie sich bei Arcserve Appliance als Administrator an.
2. Klicken Sie auf **Einstellungen**.



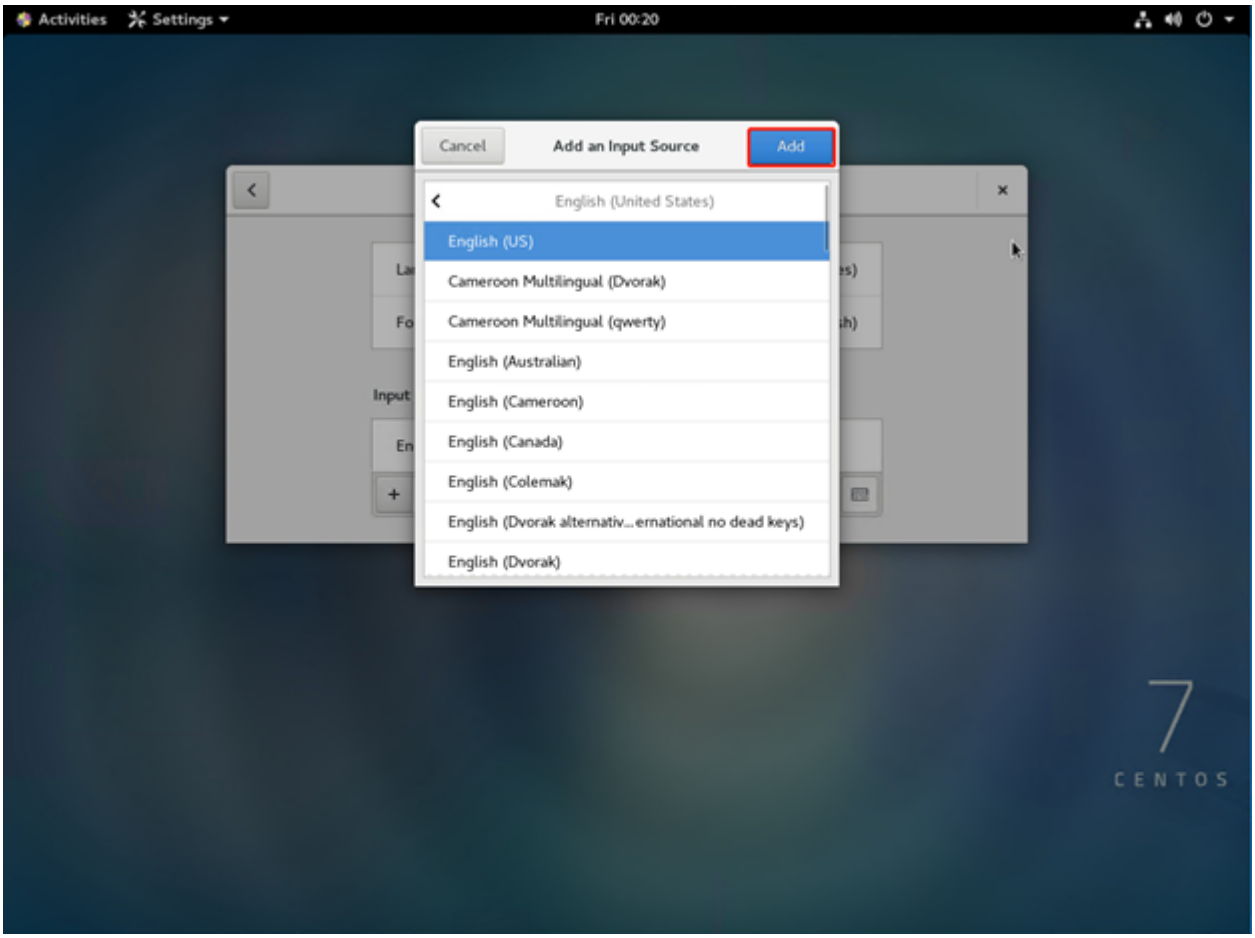
3. Klicken Sie auf **Region & Sprache**.



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



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



6. Klicken Sie auf **Hinzufügen**.

   Die Eingabequelle wurde erfolgreich hinzugefügt.

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

Sie können Arcserve Appliance per Remote-Zugriff überwachen.

Dieser Abschnitt enthält folgende Themen:

Arbeiten mit IPMI

Dieser Abschnitt enthält folgende Themen:

So ändern Sie das IPMI-Kennwort

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

Befolgen Sie diese Schritte:

1. Starten Sie Ihr System.

   Der Bildschirm "Bootup" wird angezeigt.

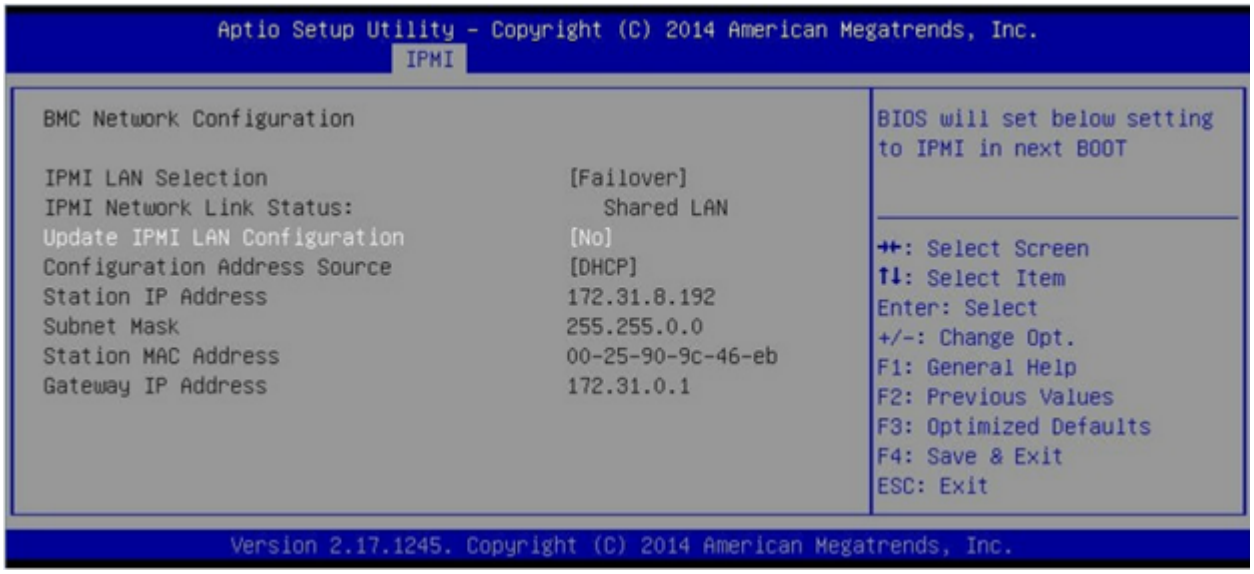
2. Drücken Sie den Schlüssel **Löschen** .

   Der BIOS-Setup-Bildschirm wird angezeigt.

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

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

   Hinweis: Standardmäßig ist die Konfigurationsadressquelle auf DHCP eingestellt.



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

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

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

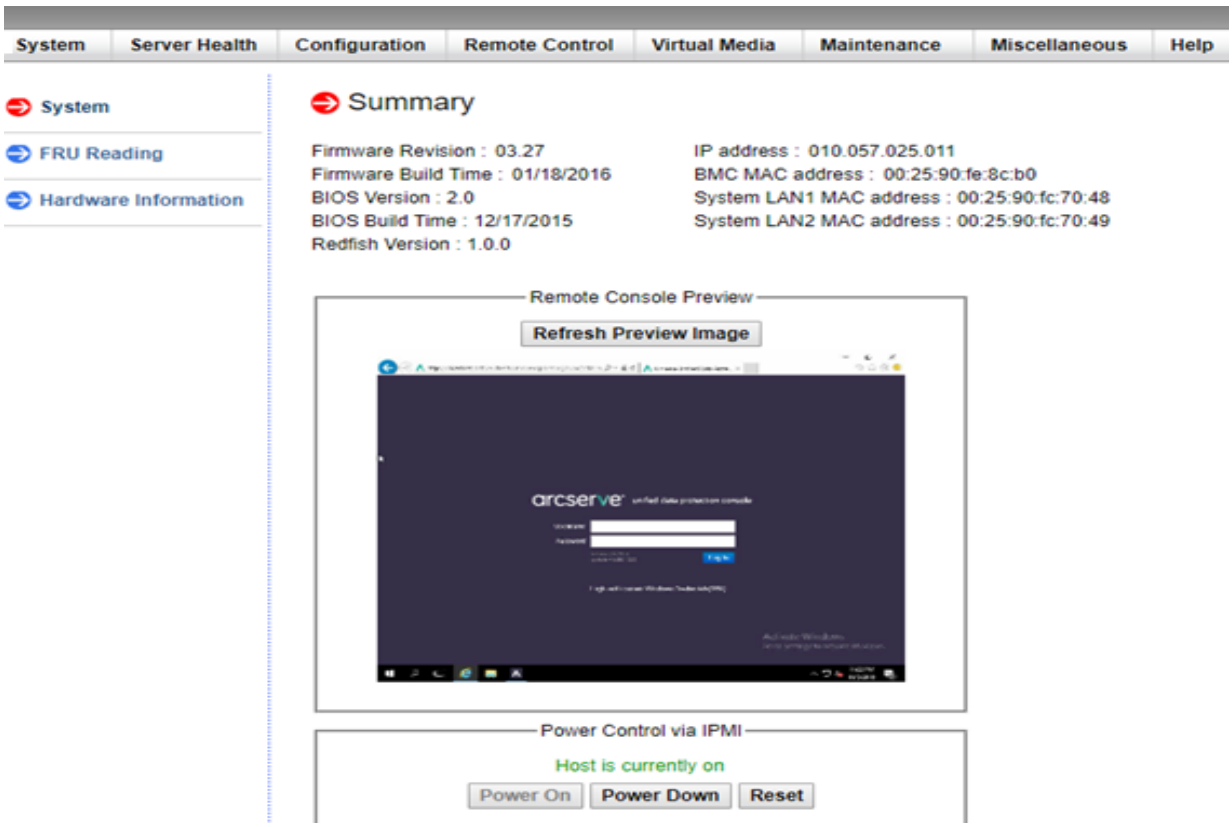
7. Geben Sie im Feld Benutzername Ihren Benutzernamen ein.

   Standard: ADMIN

8. Geben Sie im Feld Kennwort Ihr Kennwort ein.

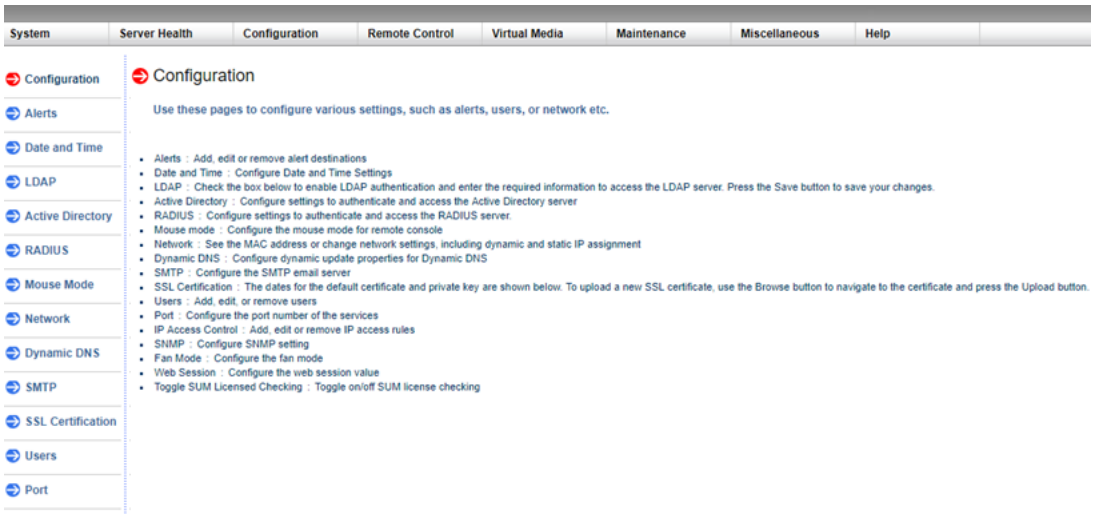
   Standard: ARCADMIN

   Die Startseite (IPMI-Hauptbildschirm) wird angezeigt.



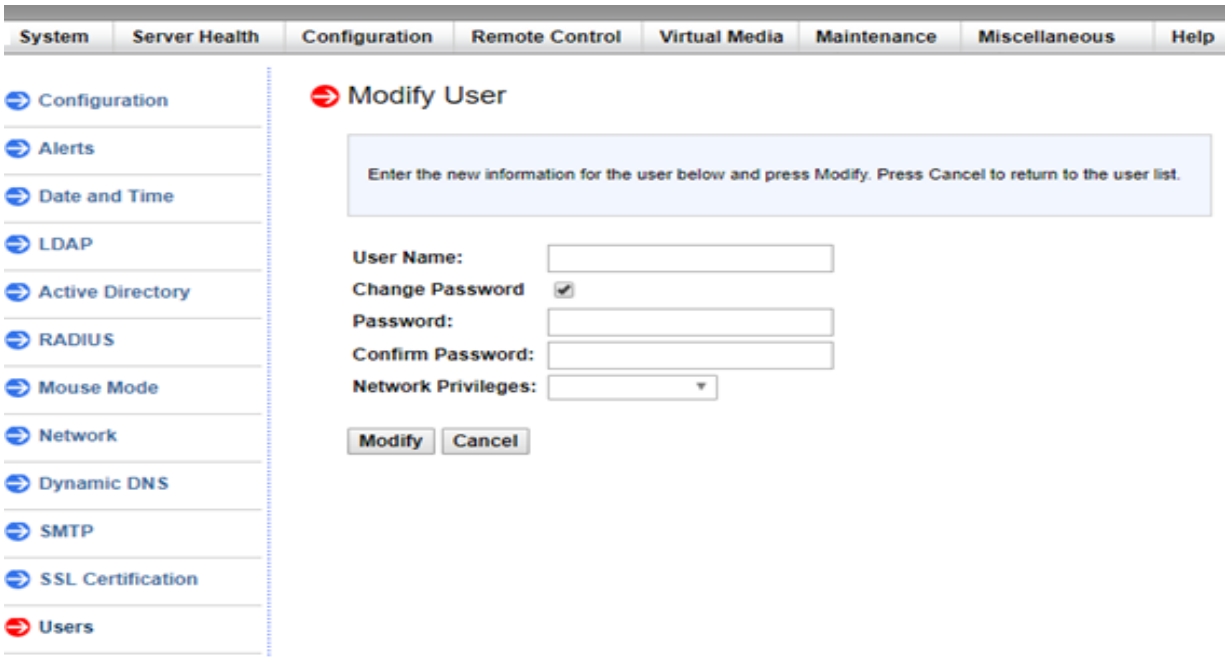
9. Klicken Sie in der oberen Leiste auf die Option **Konfiguration.**

   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**.

    Das Fenster "Benutzer ändern" wird angezeigt.



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

    Das Kennwortfeld wird aktiviert.
15. Geben Sie das neue Kennwort ein und bestätigen Sie es.
16. Klicken Sie auf **Ändern**, um die Änderungen zu speichern.

Ihr IPMI-Kennwort wurde erfolgreich geändert.

So aktualisieren Sie die IPMI-Firmware

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

Befolgen Sie diese Schritte:

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.

Arbeiten mit dem integrierten Dell Remote Access Controller (iDRAC)

Dieser Abschnitt enthält folgende Themen:

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

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

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

Befolgen Sie diese Schritte:

So melden Sie sich bei iDRAC an:

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

   Die Anmeldeseite von iDRAC wird angezeigt.

2. Geben Sie folgende Informationen ein:

   Benutzername: Root

   Kennwort: ARCADMIN

3. Klicken Sie auf **Anmelden**.

Überwachen des Systemstatus und Verwalten der Systeminformationen:

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

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

So Starten Sie die virtuelle Konsole:

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

Die Seite "Virtuelle Konsole" wird angezeigt.

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

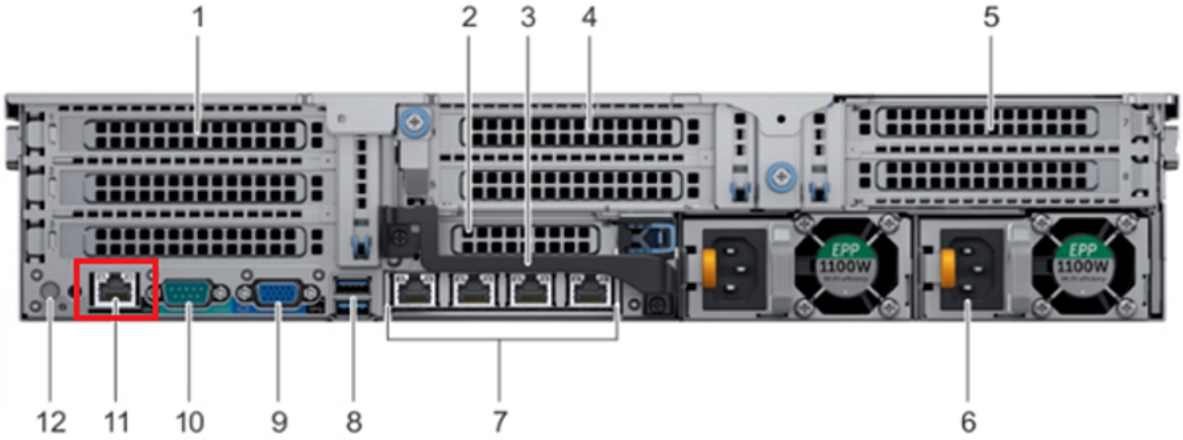
Suchen der IP-Adresse des integrierten Dell Remote Access Controller (iDRAC)

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

Rückseite der 9012-9048 für iDRAC9 anzeigen

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

Rückseite der 9072DR-9504 DR für iDRAC9 anzeigen

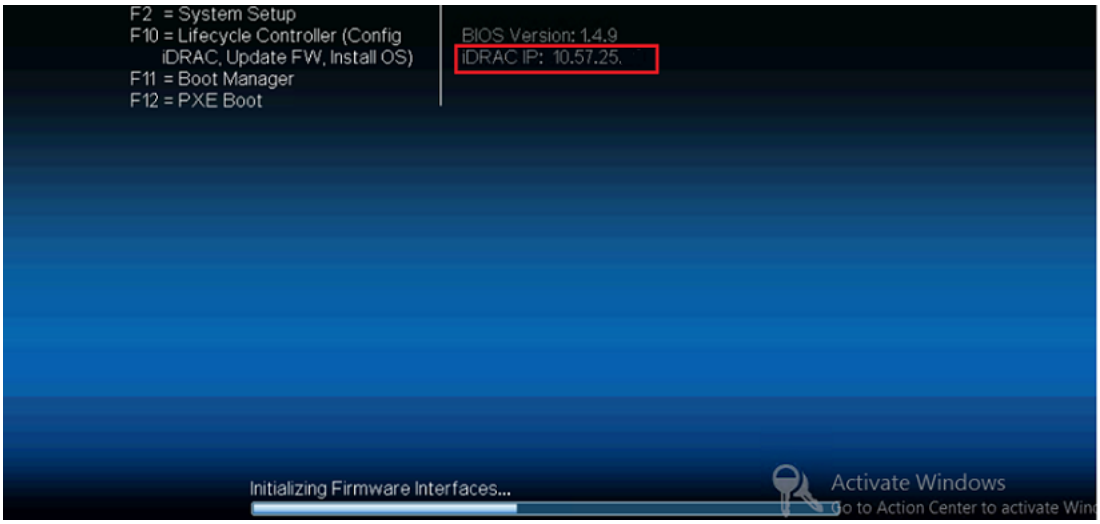


iDRAC9 dedicated network port on
rear panel of Arcserve Appliance 9072DR-9504DR series models

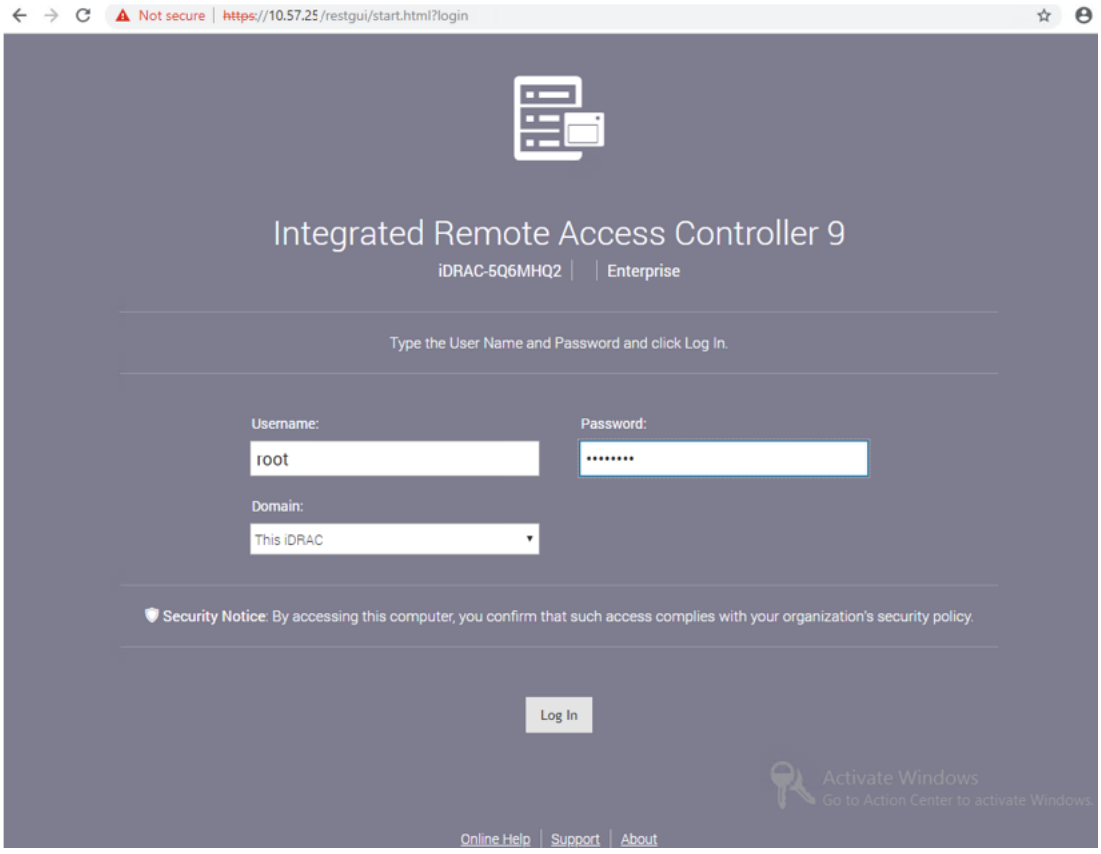
Sie finden die IP-Adresse des iDRAC auf der Appliance.

Befolgen Sie diese Schritte:

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



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



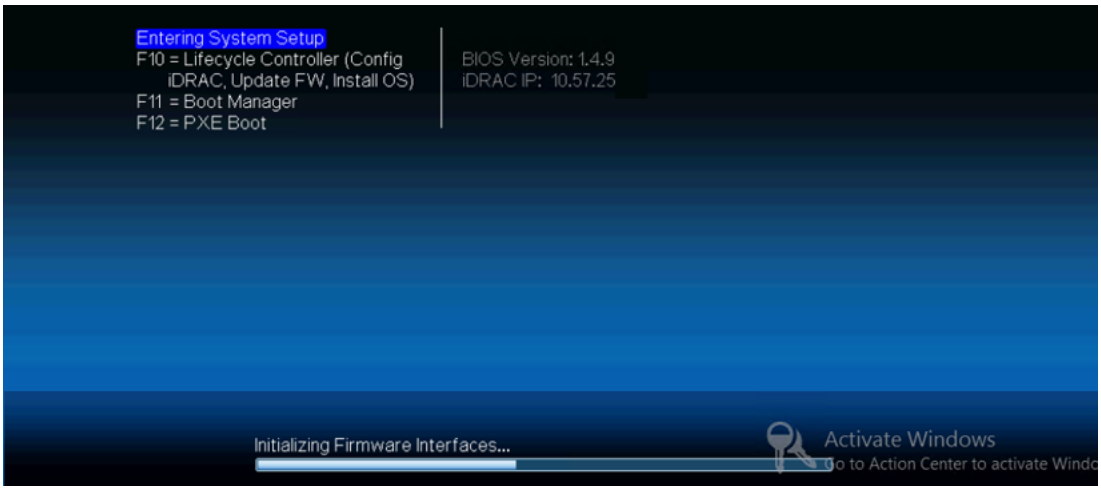
Die Anmeldeseite von iDRAC wird angezeigt.

Konfigurieren der DHCP- oder statischen IP-Adresse des iDRAC

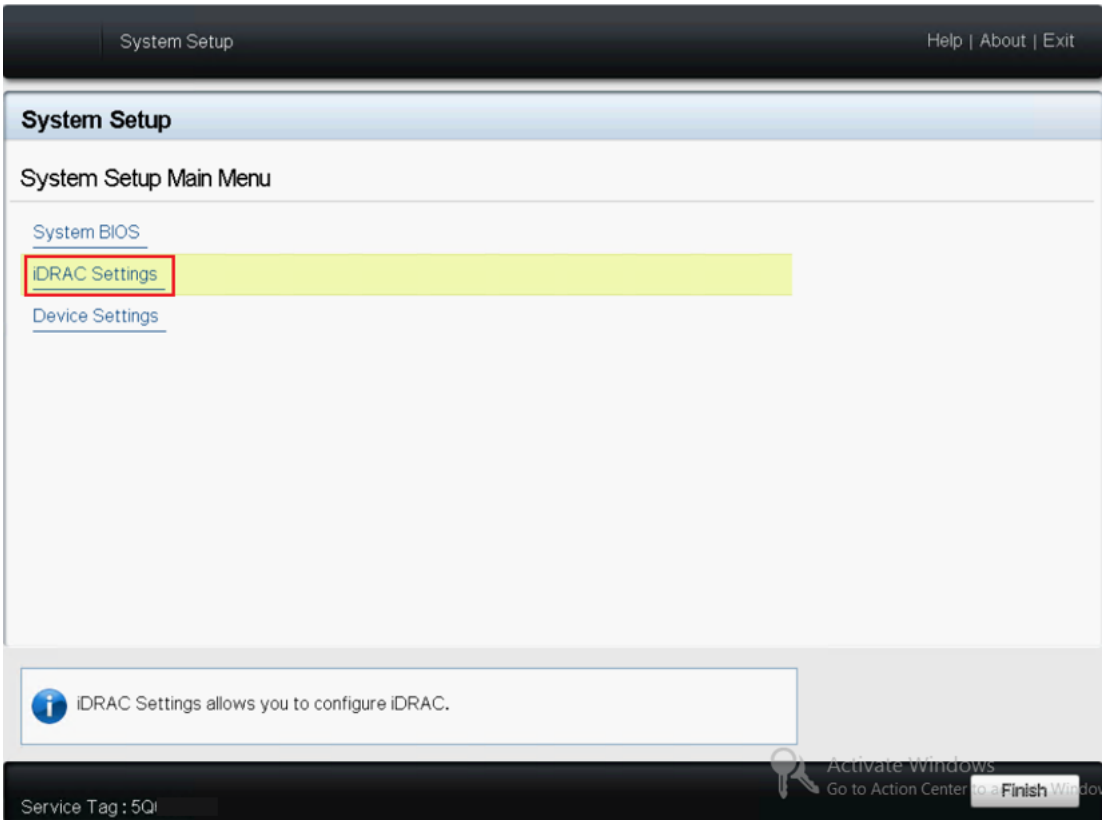
Sie können den DHCP-Netzwerk-Modus für iDRAC festlegen.

Befolgen Sie diese Schritte:

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

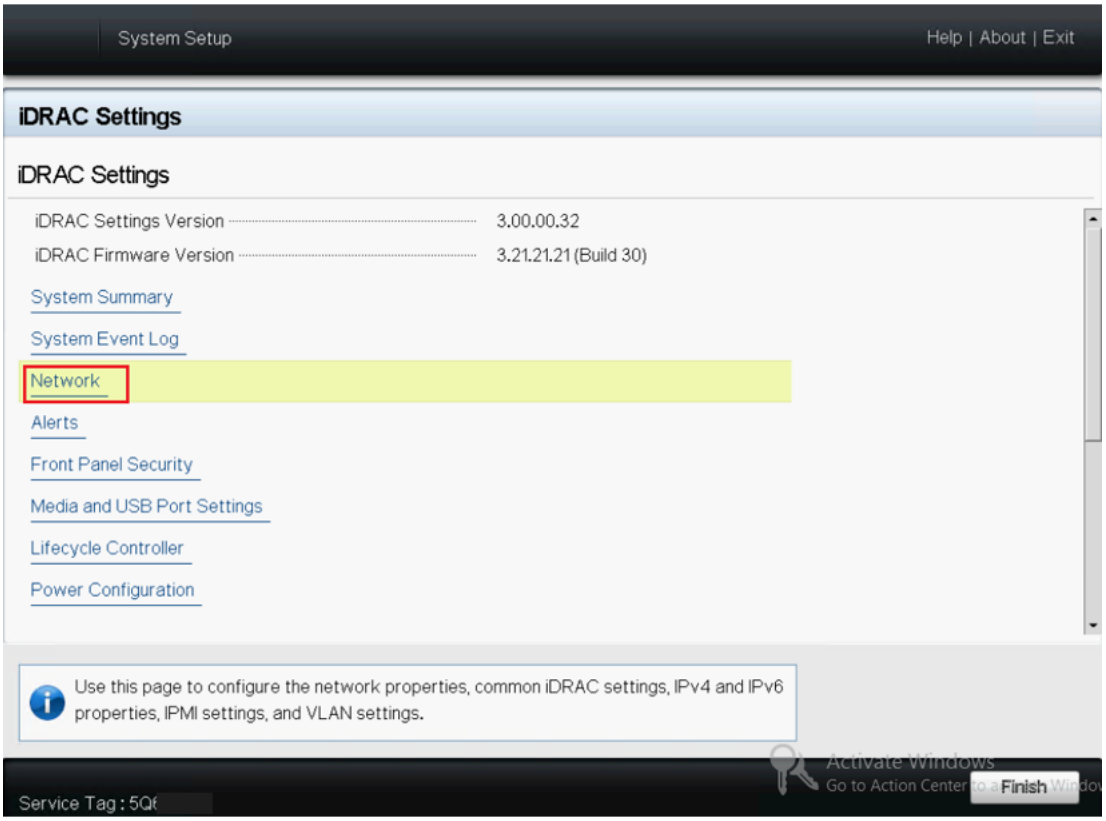


2. Klicken Sie im Bildschirm des Hauptmenüs des System-Setups auf i**DRAC Einstellungen**.

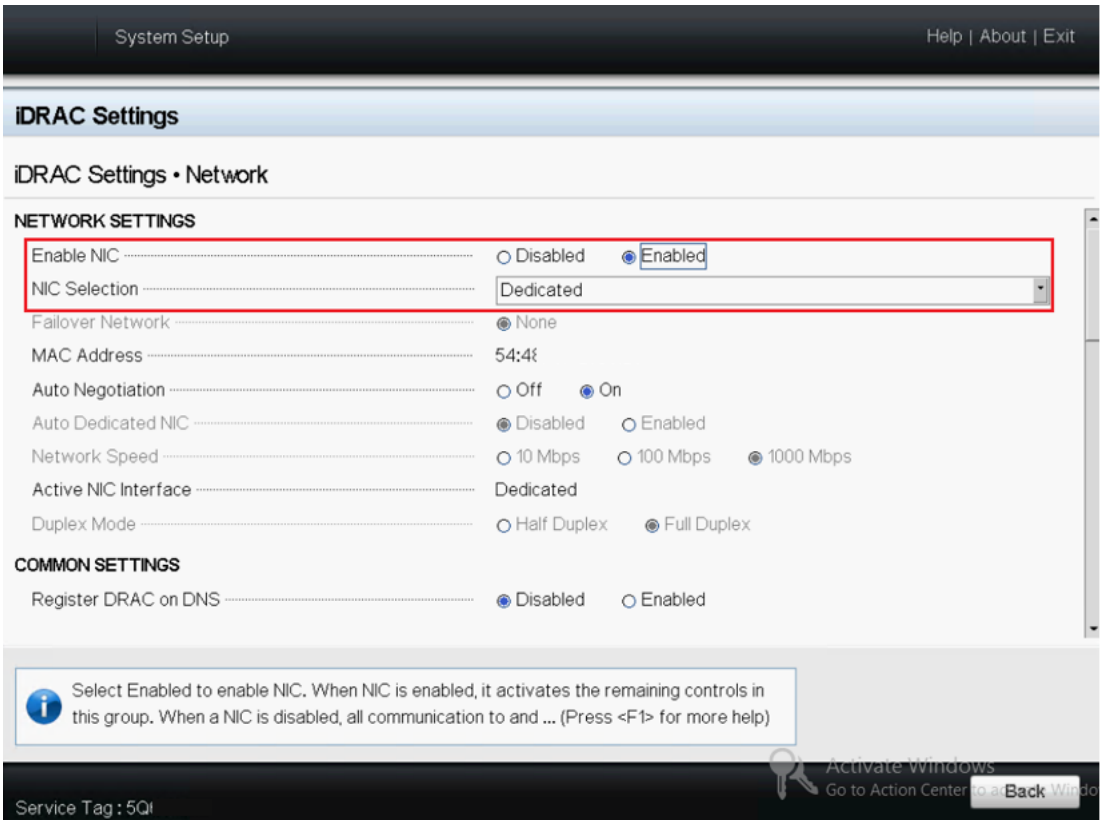


3. Klicken Sie in den Optionen der iDRAC Einstellungen auf**Netzwerk**.

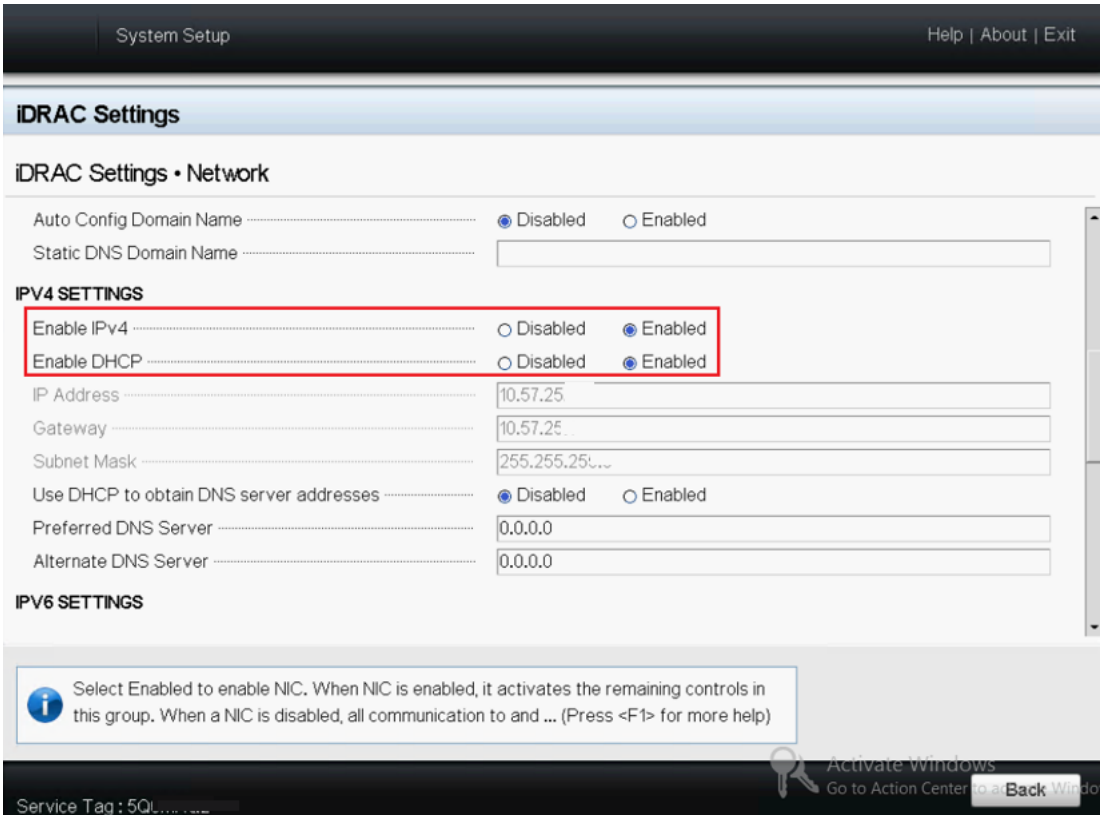
Die Felder für die Netzwerk-Einstellungen werden angezeigt.



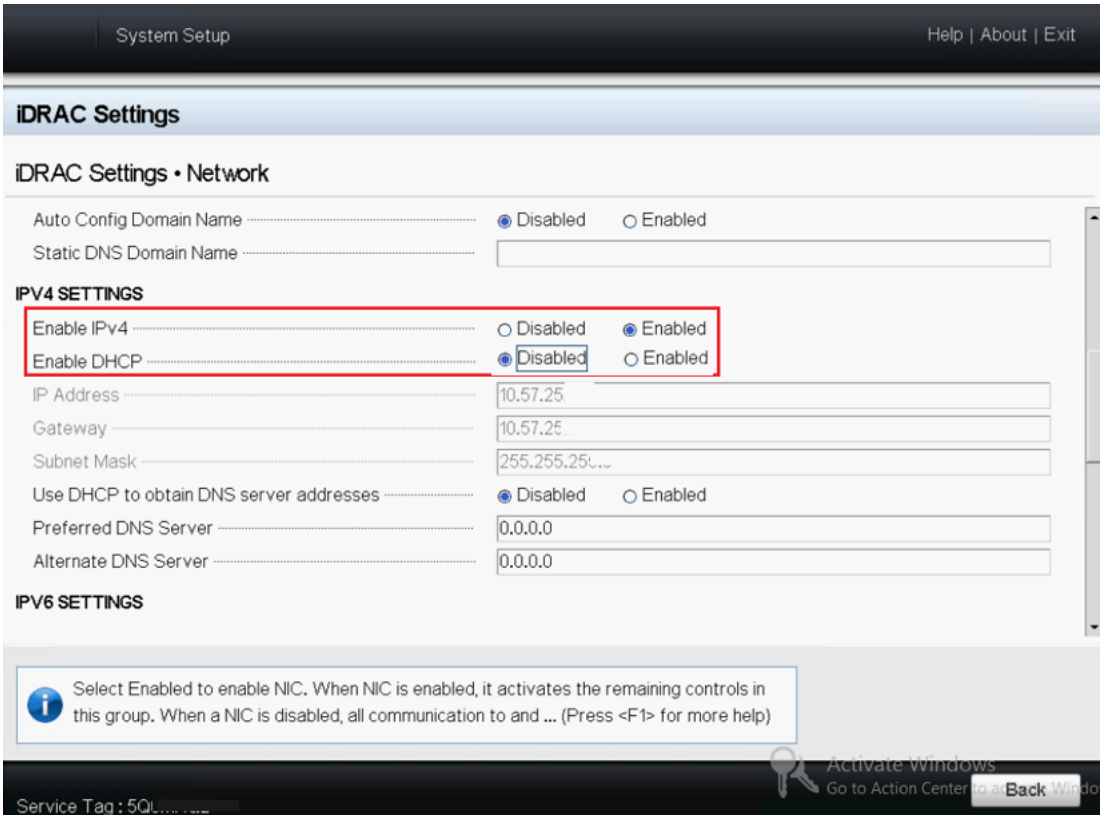
4. Wählen Sie **Aktiviert** für **NIC-Einstellung aktivieren** aus, und wählen Sie **Dedizierte** für **NIC-Auswahl** aus, um verwenden die dedizierte Netzwerkschnittstelle zu verwenden.



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

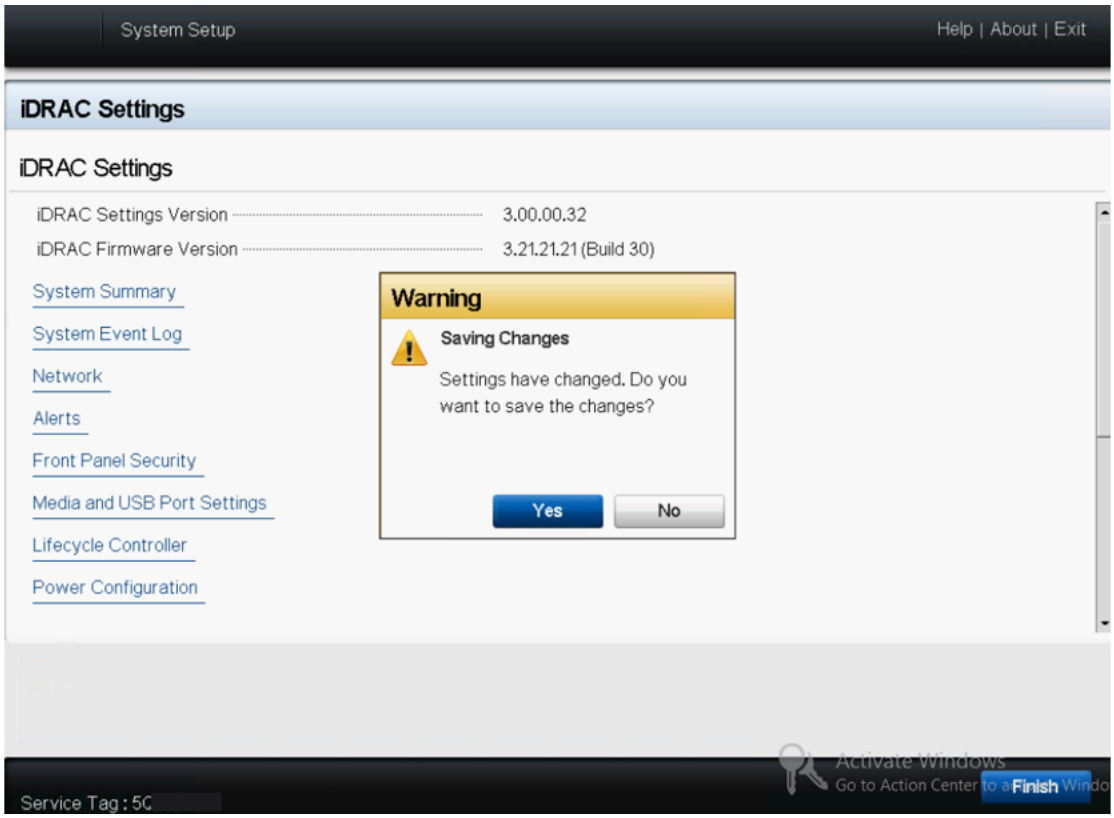


Hinweis: Wenn Sie die statische IP-Adresse für das dedizierte iDRAC-Netzwerk festlegen möchten, legen Sie für **IPv4 aktivieren** die Option **Aktiviert** und für **DHCP aktivieren Deaktiviert** aus. Legen Sie IP-Adresse, Gateway und Subnetzmaske entsprechend der Netzwerkkonfiguration fest.

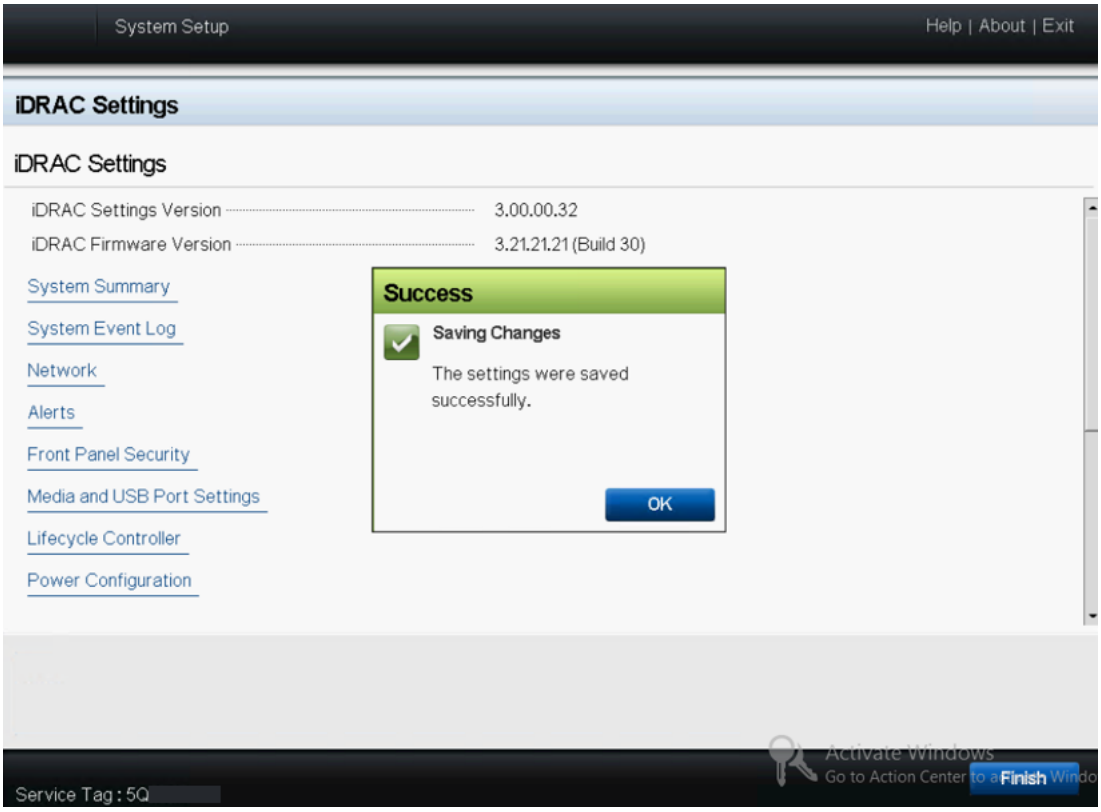


6. Klicken Sie auf **Zurück**, klicken Sie auf **Fertig stellen**, und klicken Sie dann auf **Ja** im Dialogfeld **Warnung**.

Die Netzwerkinformationen werden gespeichert.

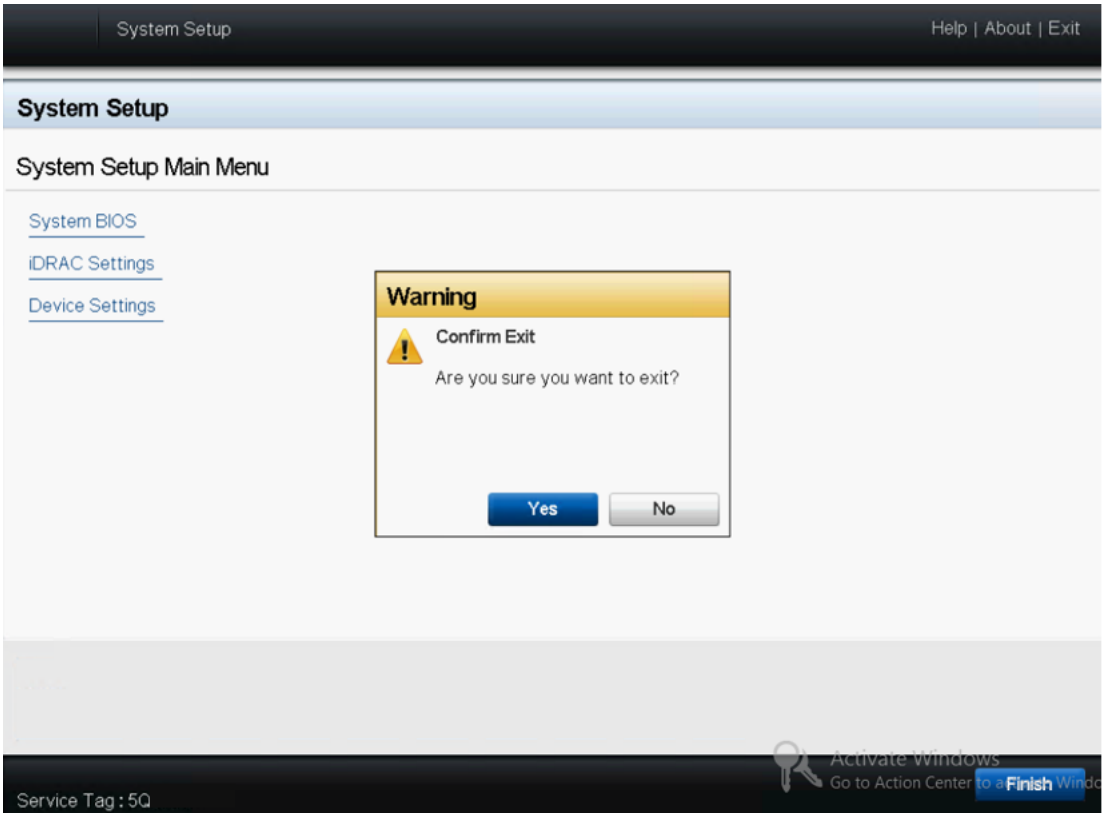


7. Klicken Sie im Dialogfeld **Erfolg** auf **OK**.



Sie haben die Konfiguration der iDRAC DHCP abgeschlossen.

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



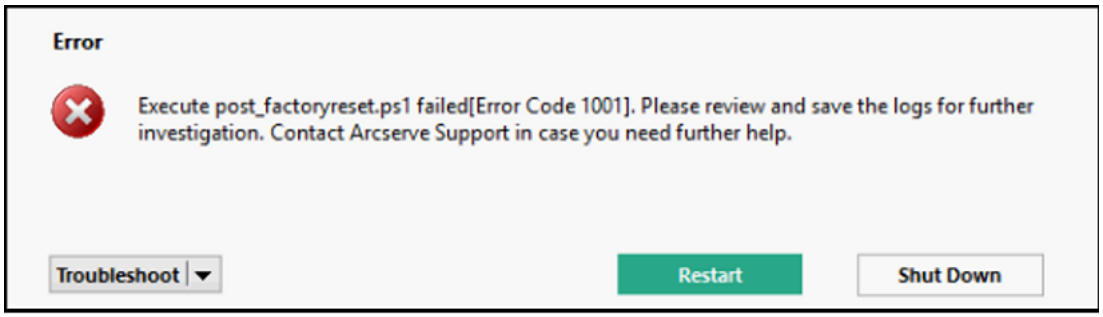
Der DHCP-Netzwerk-Modus für iDRAC-Initialisierung ist nun konfiguriert.

Kapitel 8: Wiederherstellen oder Reparieren derArcserve Appliance

Dieser Abschnitt enthält folgende Themen:

Debuggen und auf Werkseinstellungen zurücksetzen

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



Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

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

   Folgende Optionen werden angezeigt:

   Befehlszeile

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

   Anzeigen von Protokollen

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

   "Auf Werkseinstellungen zurücksetzen" erneut starten

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

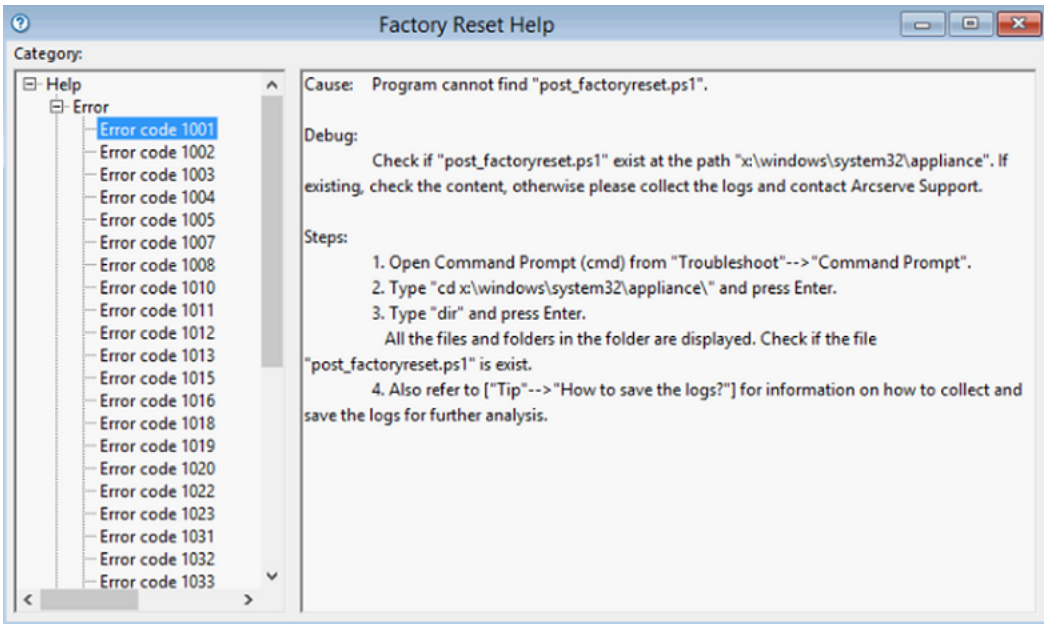
   Hilfe

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

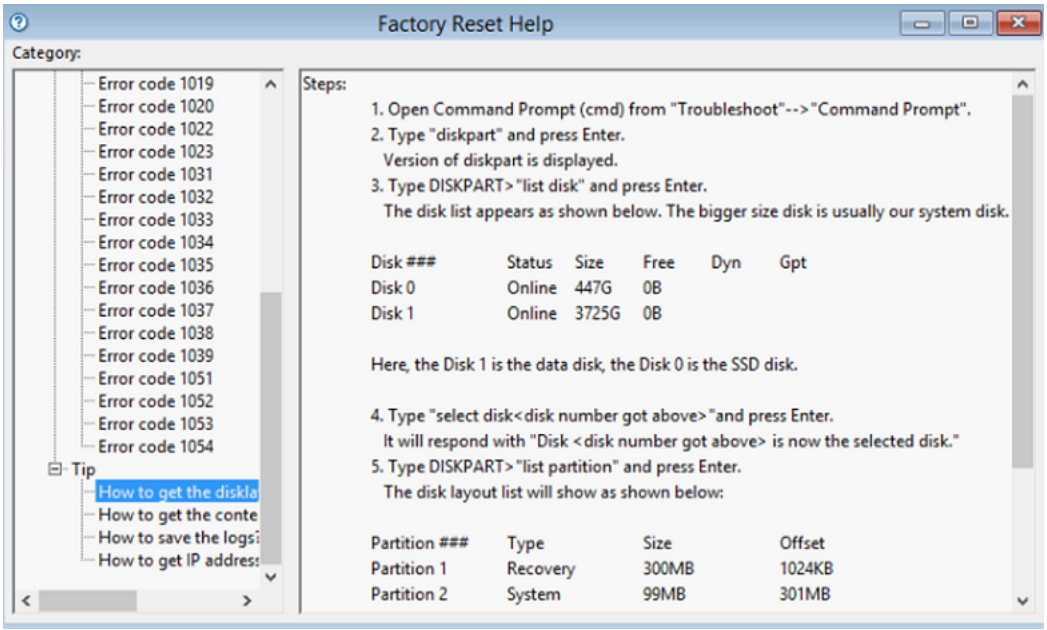
Werkseinstellungen abgerufen wird oder wie Sie die Protokolle speichern.

2. Klicken Sie in den angezeigten Optionen auf **Hilfe**.

Der Bildschirm zeigt mehrere Fehlercodes mit Details an.



3. Navigieren Sie für den in der Fehlermeldung angezeigten Fehlercode zu **Tipp**, und folgen Sie den Anweisungen, wie im rechten Fenster angezeigt.



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

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

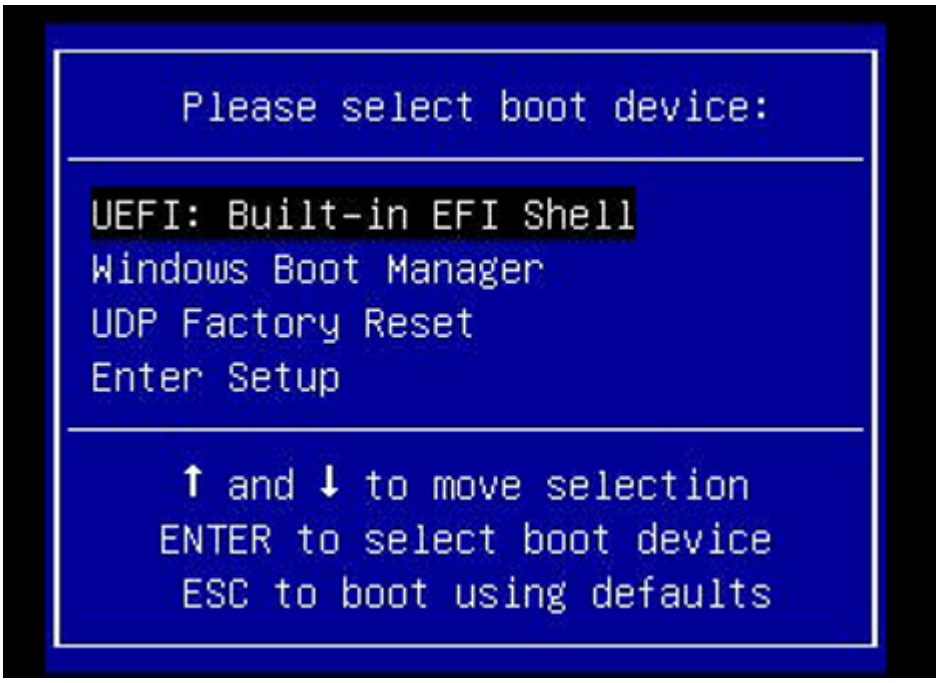
Sie können die UDP-Werkeinstellung auf dem Startmenü der Serie Arcserve Appliance anwenden. Mit den UDP-Werkeinstellungen können Sie dieArcserve Appliance in den ursprünglichen Zustand ohne Konfiguration zurücksetzen.

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

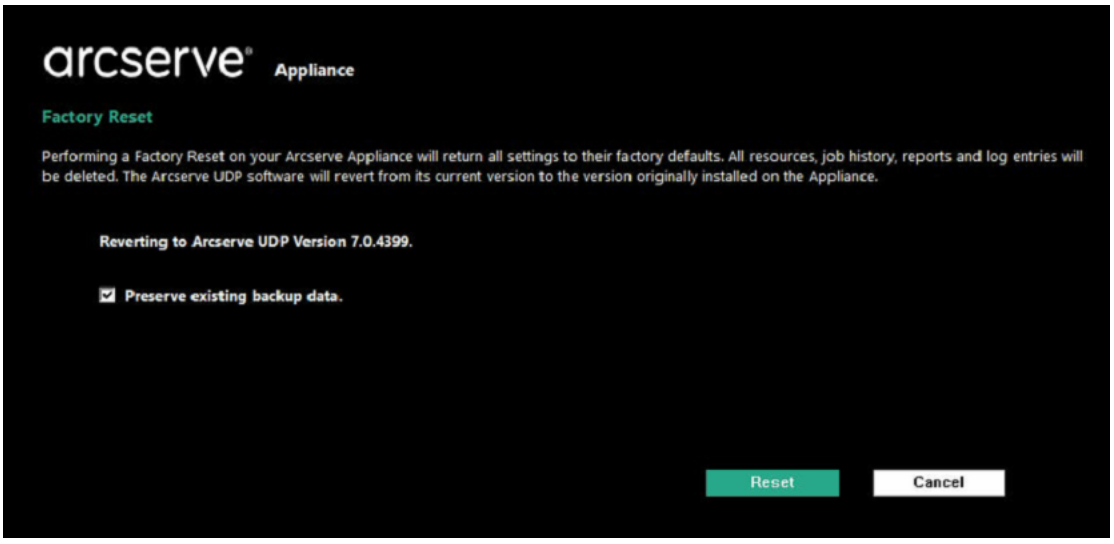
Befolgen Sie diese Schritte:

1. Drücken Sie F11, um das Startmenü aufzurufen.

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



Es wird eine Seite zum Zurücksetzen auf Werkseinstellungen angezeigt.

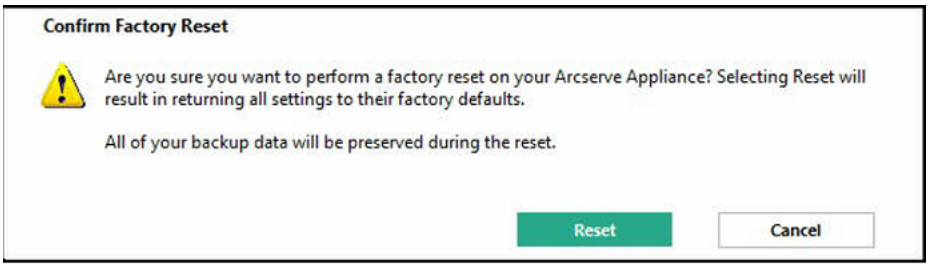


Hinweise:

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

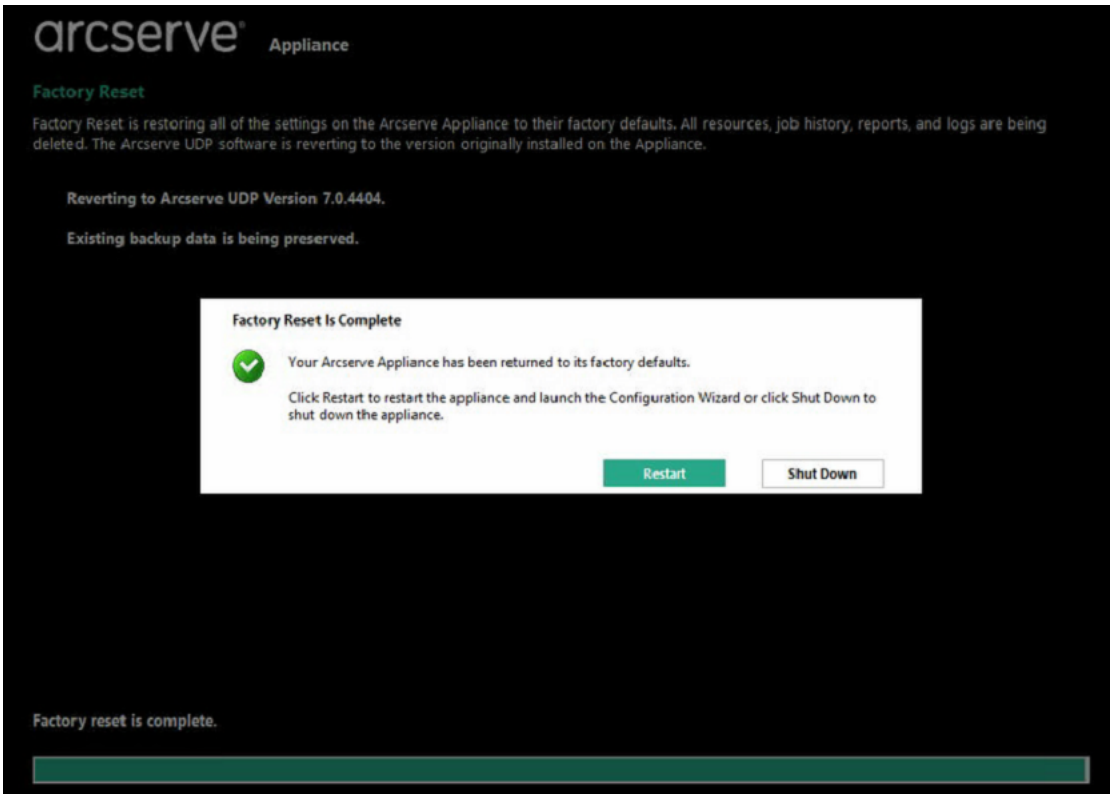
1. Klicken Sie auf **Zurücksetzen**.

Ein Bestätigungsdialogfeld wird angezeigt.



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

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



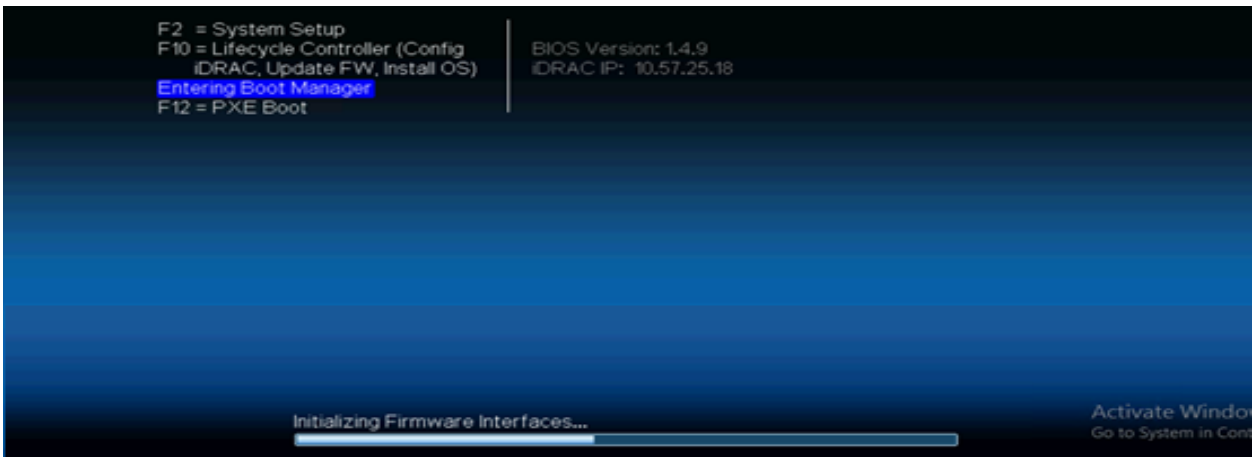
Anwenden von Arcserve UDP-Werkseinstellungen unter Verwendung der Startoption für Geräte der 9012-9504DR Serie

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

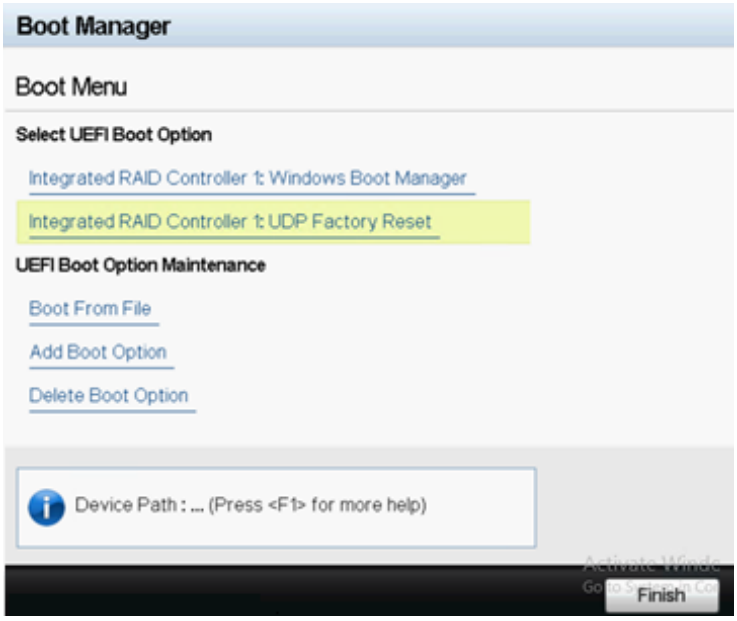
Hinweis: Sie können auch die Option „Sicherungsdaten beibehalten“ auswählen, während Sie das Gerät auf die UDP-Werkeinstellungen zurücksetzen.

Befolgen Sie diese Schritte:

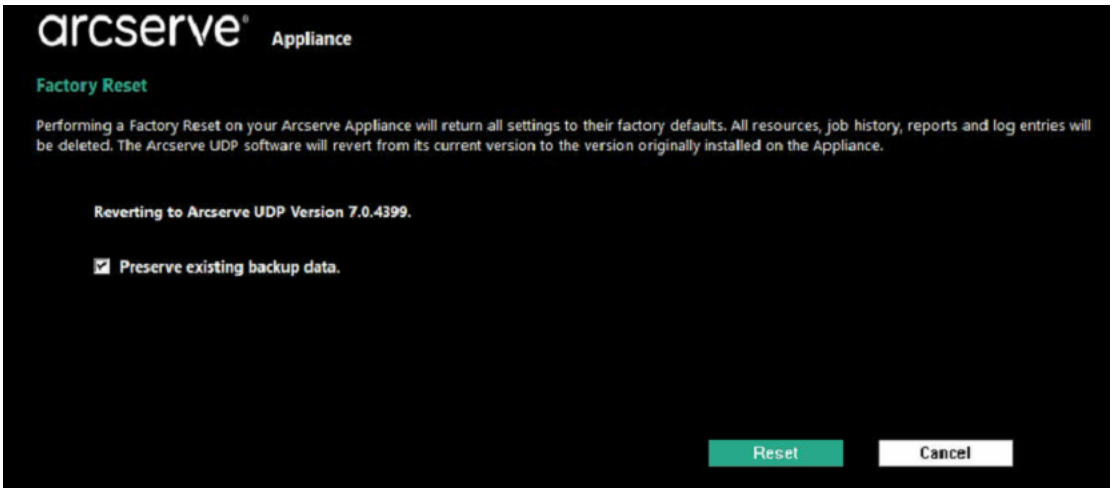
1. Drücken Sie F11 auf der Tastatur, um das Startmenü aufzurufen.



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



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.

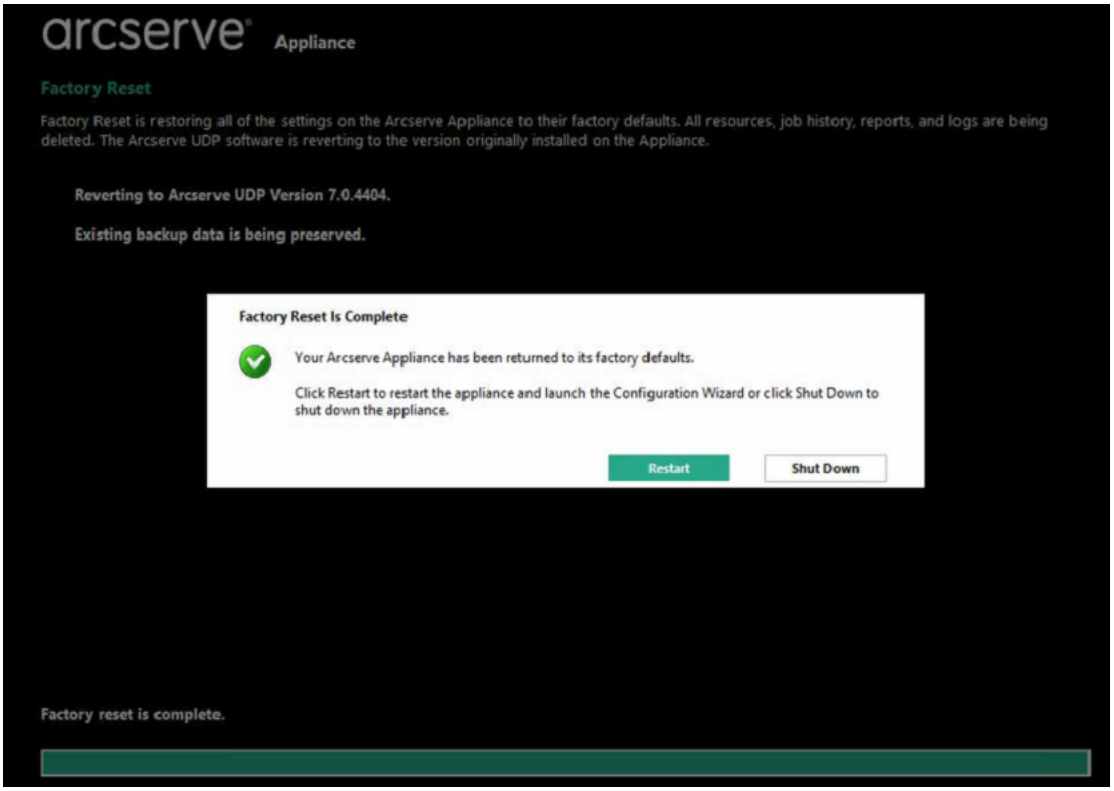
3. Klicken Sie auf **Zurücksetzen**.

Ein Bestätigungsdialogfeld wird angezeigt.

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

4. Nachdem die Appliance auf die Werkseinstellungen zurückgesetzt wurde, können Sie eine der folgenden Aktionen durchführen:

   - Klicken Sie auf **Neustart**, um die Appliance neu zu starten.
   - Klicken Sie auf **Herunterfahren**, um die Appliance zu schließen.



Löschen der Konfiguration und Zurücksetzung der Appliance auf Werkseinstellungen

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

Befolgen Sie diese Schritte:

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

   Alle gesicherten Daten werden standardmäßig beibehalten.

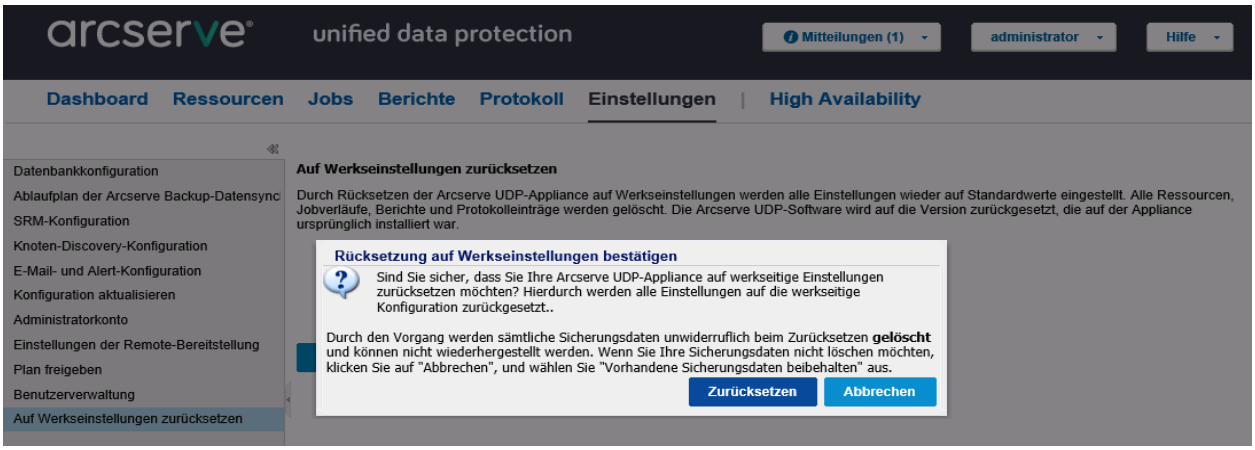
   Hinweise:

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

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

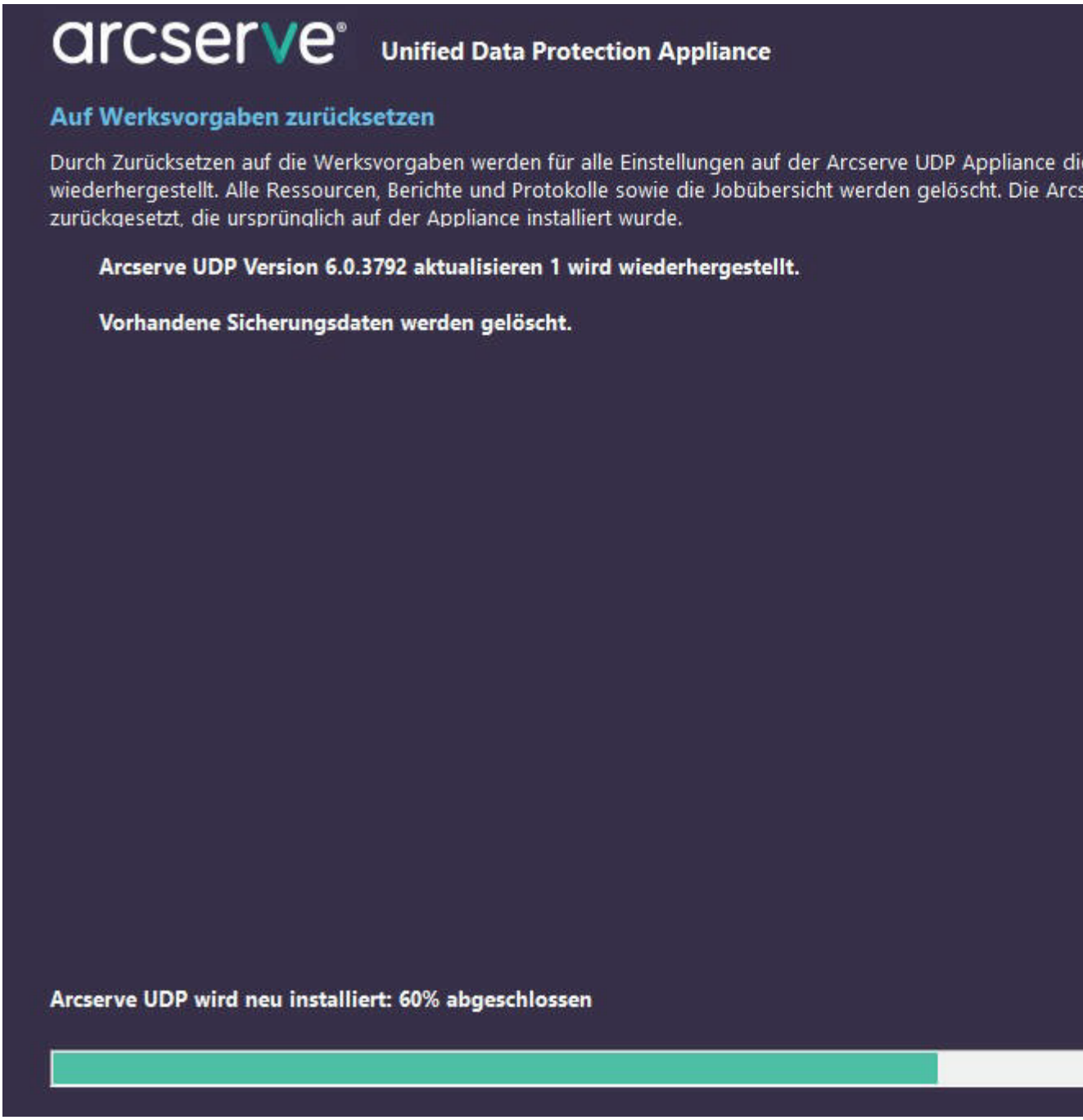
2. Klicken Sie auf **Auf Werkseinstellungen zurücksetzen**.

   Ein Bestätigungsdialog wird angezeigt.



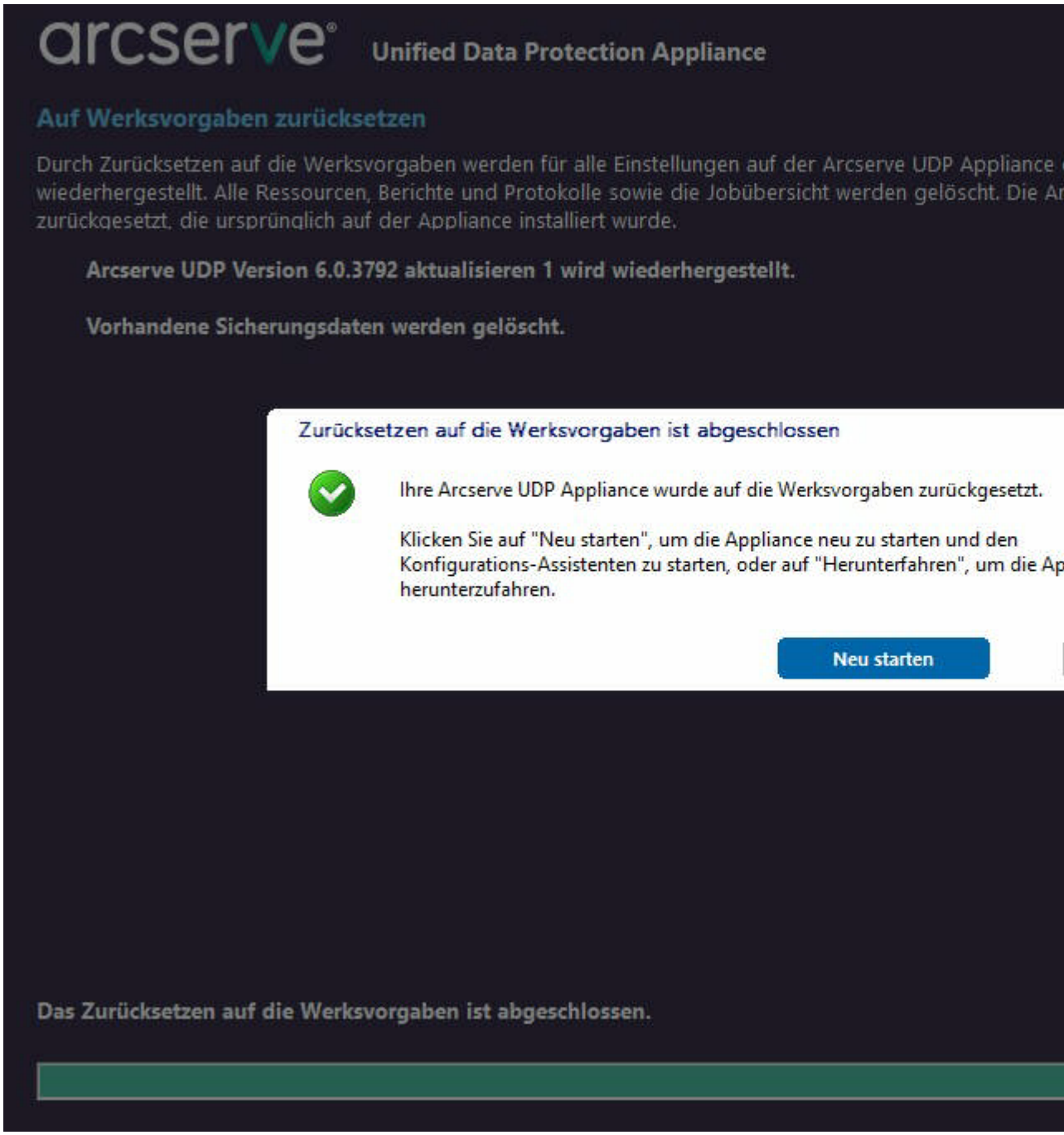
3. Klicken Sie im Bestätigungsdialog auf **Zurücksetzen**, um die Zurücksetzung auf Werkseinstellungen zu starten.

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



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.


arcserve
Unified Data Protection Appliance
Auf Werksvorgaben zurücksetzen
Durch Zurücksetzen auf die Werksvorgaben werden für alle Einstellungen auf der Arcserve UDP Appliance
wiederhergestellt. Alle Ressourcen, Berichte und Protokolle sowie die Jobübersicht werden gelöscht. Die Ar
zurückgesetzt, die ursprünglich auf der Appliance installiert wurde.
Arcserve UDP Version 6.0.3792 aktualisieren 1 wird wiederhergestellt.
Vorhandene Sicherungsdaten werden gelöscht.
Zurücksetzen auf die Werksvorgaben ist abgeschlossen
Ihre Arcserve UDP Appliance wurde auf die Werksvorgaben zurückgesetzt.
Klicken Sie auf "Neu starten", um die Appliance neu zu starten und den
Konfigurations-Assistenten zu starten, oder auf "Herunterfahren", um die Ap
herunterzufahren.
Neu starten
Das Zurücksetzen auf die Werksvorgaben ist abgeschlossen.

Festplatte entfernen und ersetzen

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

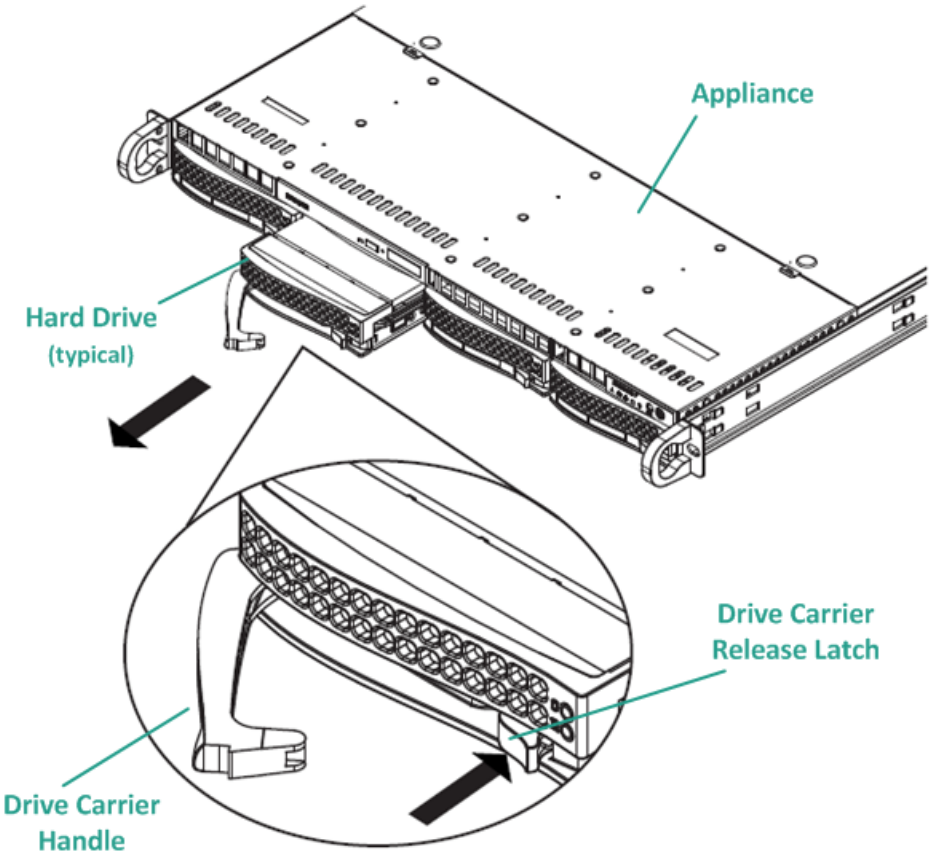
Die Arcserve Appliance enthält vier Festplattenträger, die von links nach rechts mit 0, 1, 2 und 3 gekennzeichnet sind. Wenn Sie mehr als eine Festplatte ersetzen, sollten Sie die Ersatzfestplatten kennzeichnen, sodass Sie wissen, welche Festplatte in den einzelnen Festplattenträgern platziert werden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

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

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

Befolgen Sie diese Schritte:

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

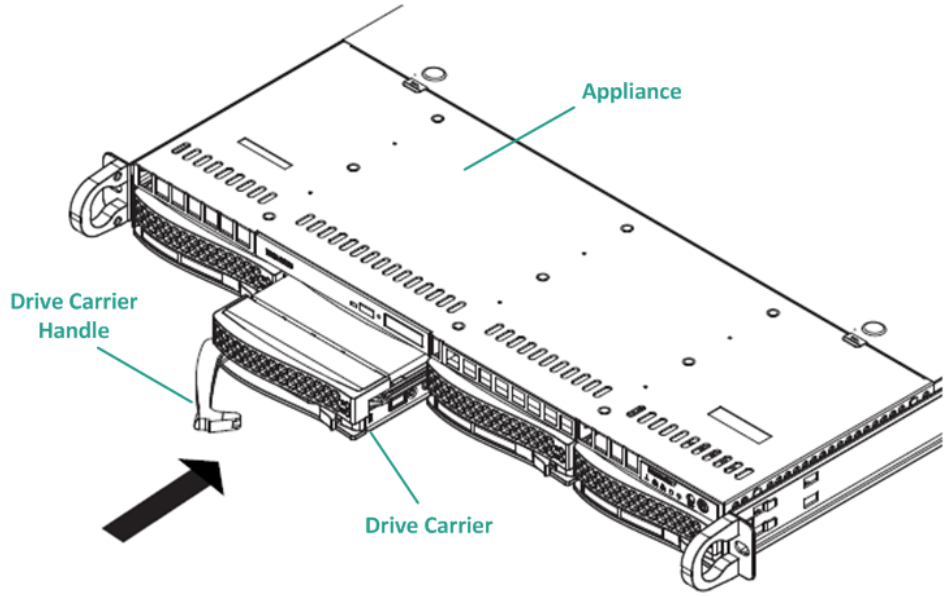


3. Ziehen Sie den Laufwerksträger am Griff vorne aus der Appliance. Die Festplatten sind in Laufwerk montiert, um ihren Ausbau und Austausch aus der Appliance zu vereinfachen. Diese Träger tragen außerdem zu einem ausreichenden Luftstrom für die Laufwerkschächte bei.

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

4. Entfernen Sie die alte Festplatte aus dem Laufwerkträger, und installieren Sie die neue Festplatte. Achten Sie dabei sorgfältig darauf, dass die Austausch-Festplatte richtig ausgerichtet sind: mit der Beschriftung nach oben und den sichtbaren Komponenten auf der Unterseite.

5. Schieben Sie den Laufwerksschacht in die Appliance, bis sie vollständig montiert ist, und fixieren Sie ihn durch Schließen des Laufwerksträger-Griffs.



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

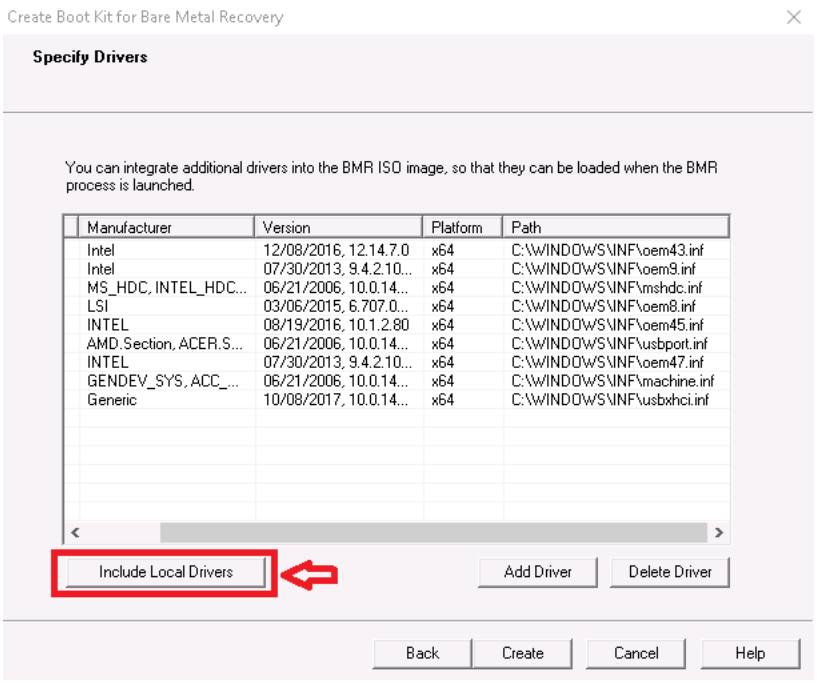
Durchführen einer Bare Metal Recovery (BMR), ohne Daten beizubehalten

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

Befolgen Sie diese Schritte:

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

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

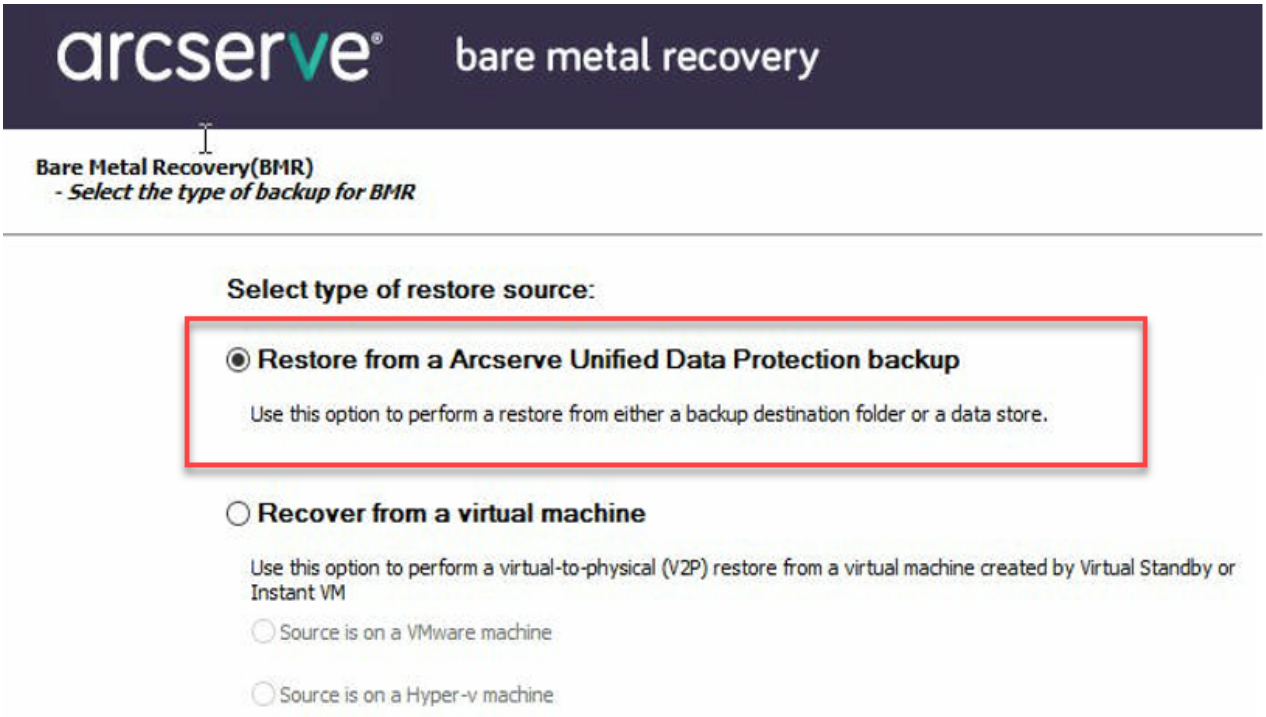


2. Starten Sie die Arcserve Appliance mit dem BMR-ISO-Image oder dem USB-Stick.

Das **Arcserve Bare-Metal-Recovery** Setup wird angezeigt.

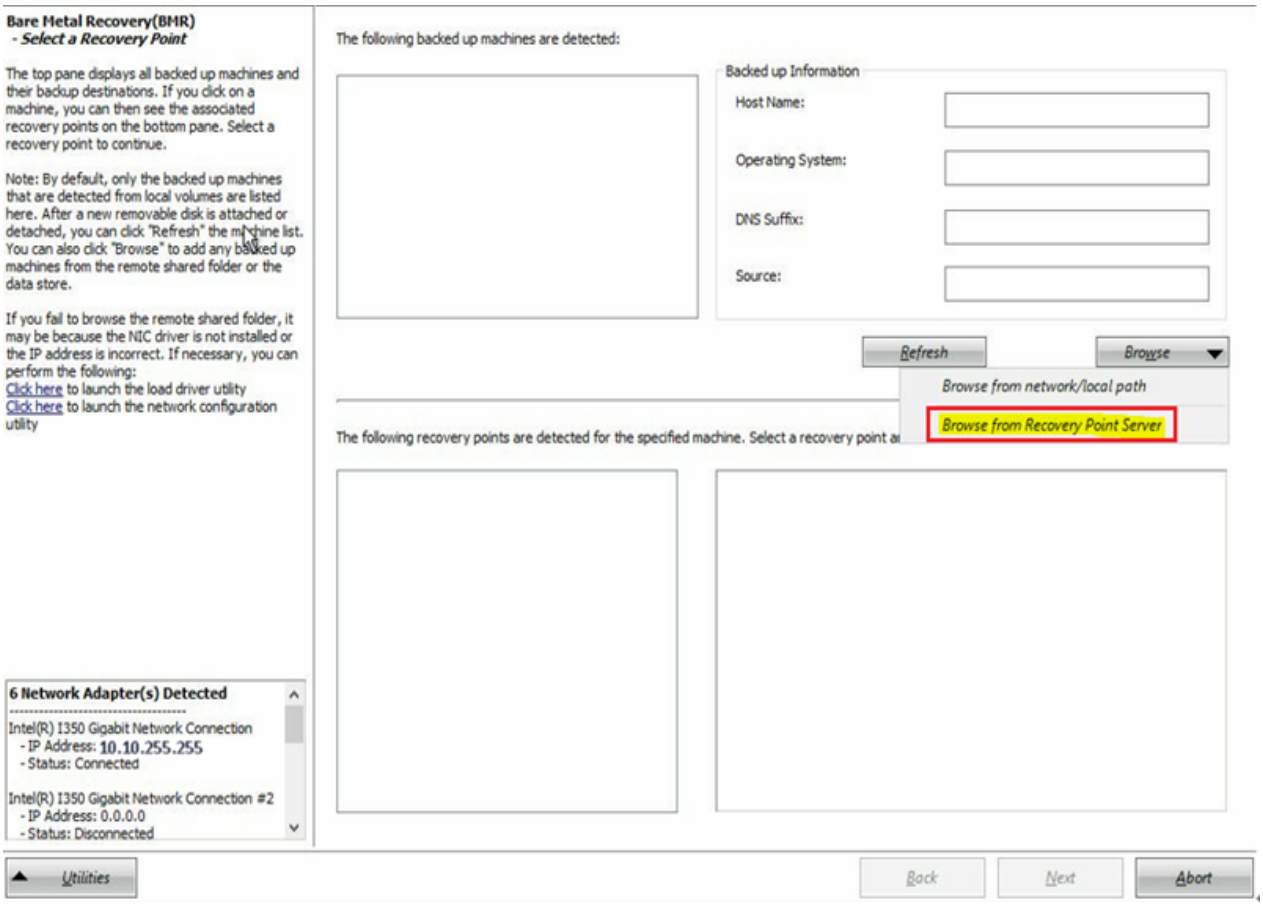
3. Wählen Sie die erforderliche Sprache aus, und klicken Sie auf **Weiter**.

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



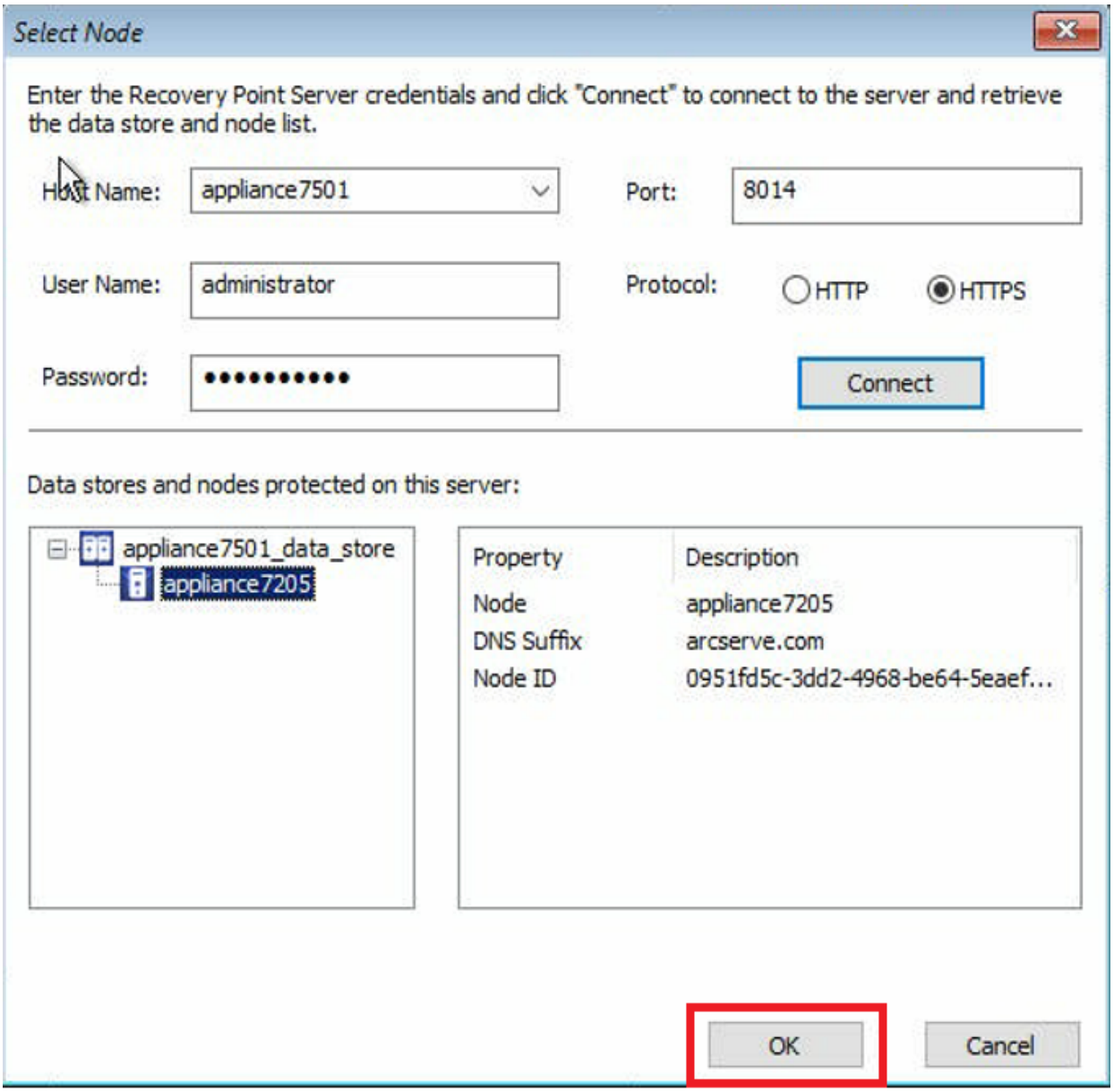
Das Fenster **Assistent zum Auswählen eines Wiederherstellungspunkts** wird angezeigt.

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



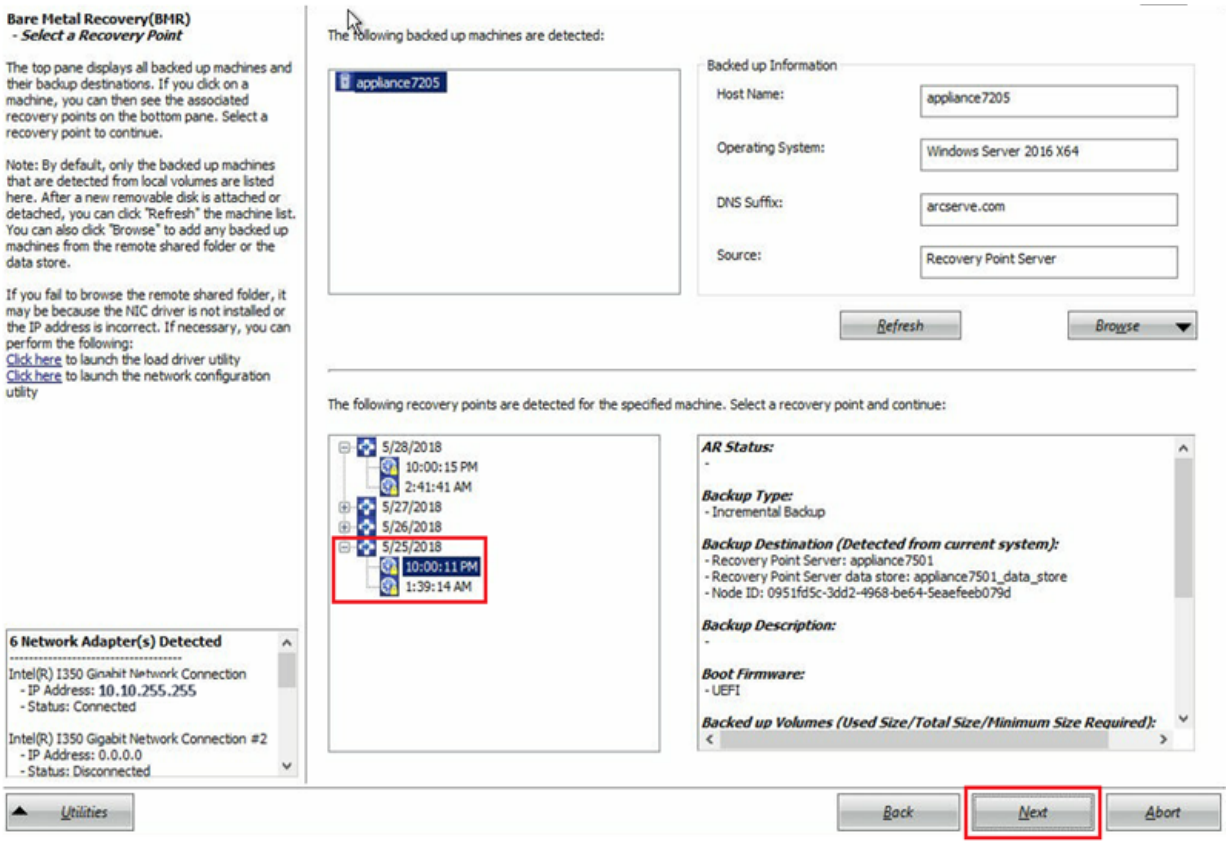
Das Fenster **Knoten auswählen** wird angezeigt.

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**.



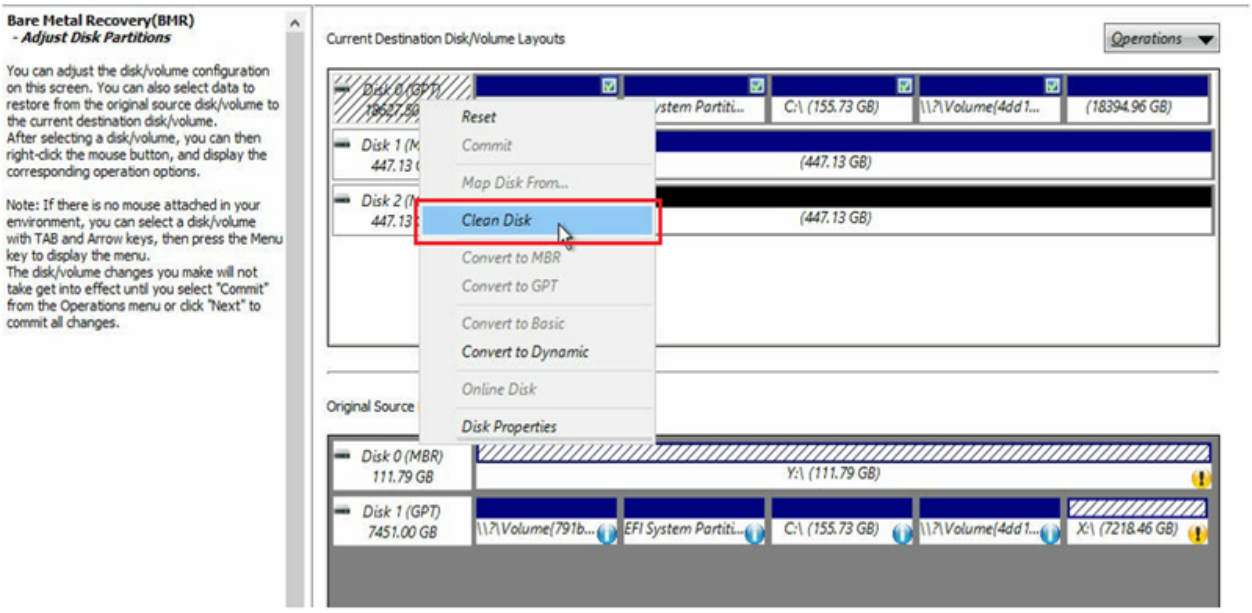
10. (Optional) Geben Sie das Sitzungskennwort ein, wenn Sie dazu aufgefordert werden, und klicken Sie dann auf **OK**.

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

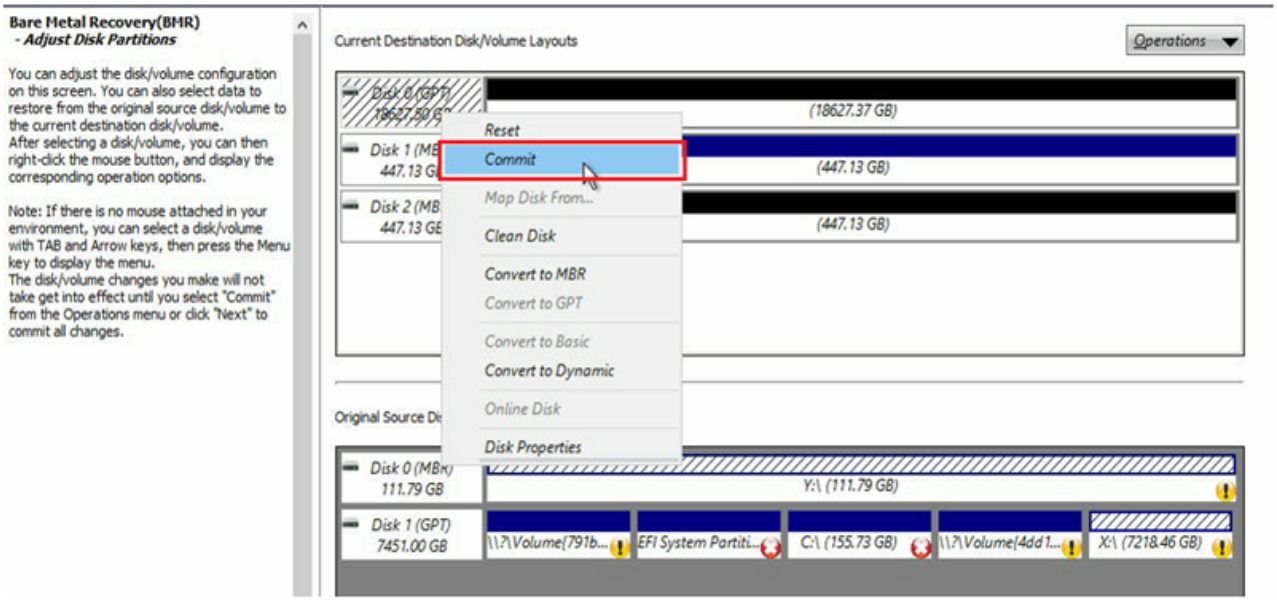
11. Wählen Sie **Erweiterter Modus** aus, und klicken Sie auf **Weiter**.

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**.

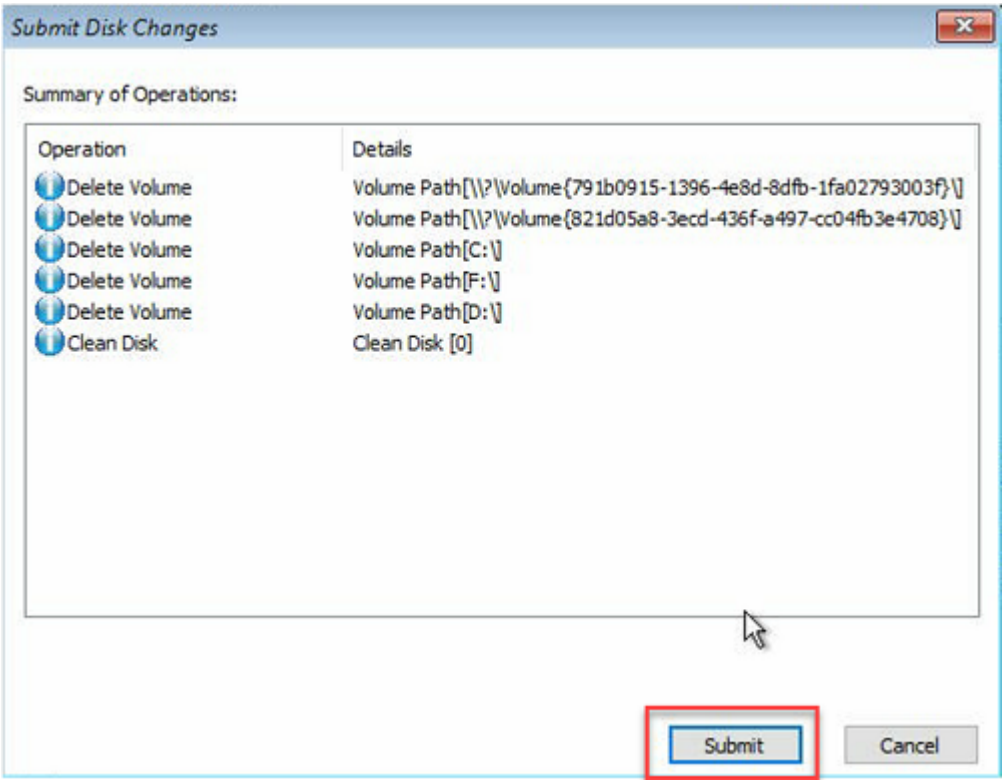


13. Klicken Sie nach der Reinigung der Festplatte mit der rechten Maustaste auf denselben Datenträger, und klicken Sie auf **Commit**.

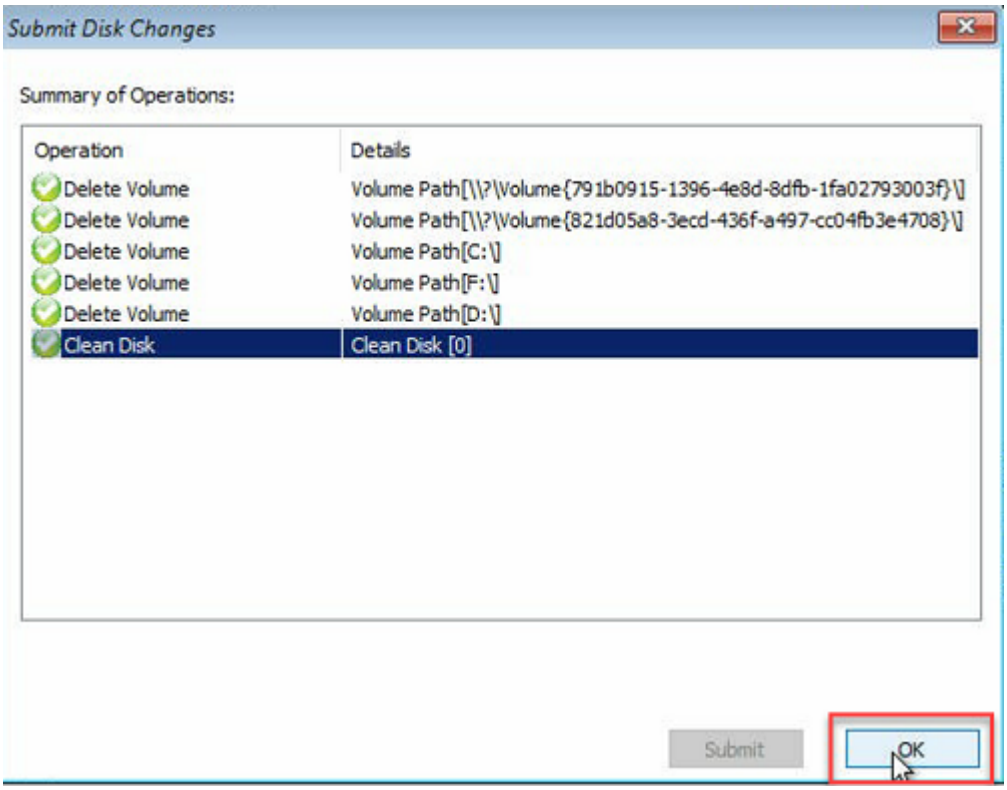


Das Fenster **Datenträgeränderungen übergeben** wird angezeigt.

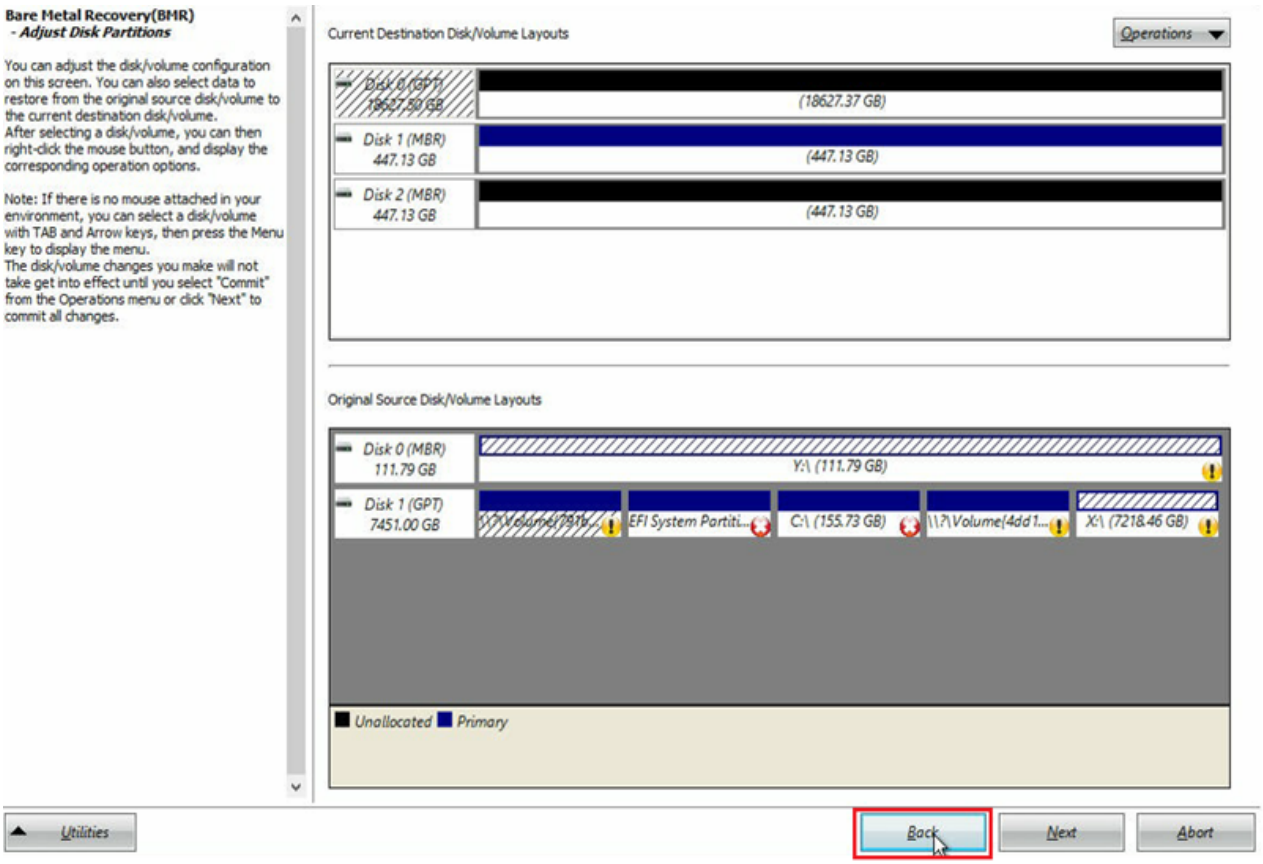
14. Klicken Sie auf **Übergeben**.



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

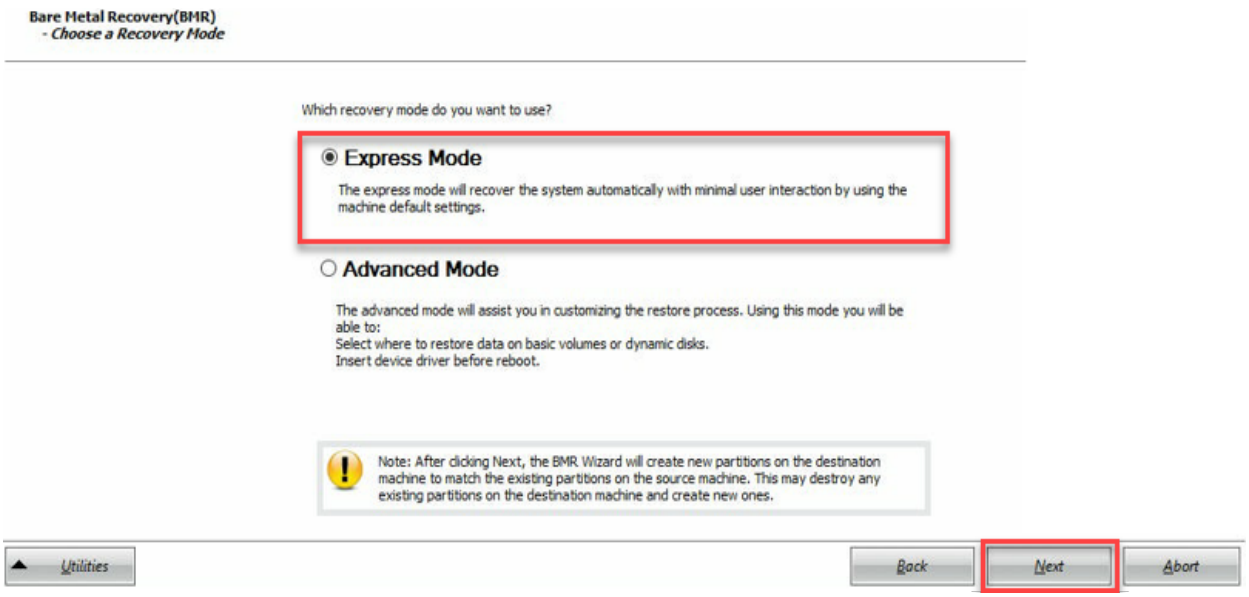


16. Klicken Sie im Dialogfeld **Bare-Metal-Recovery (BMR) – Datenträgerpartitionen anpassen** auf **Zurück**.



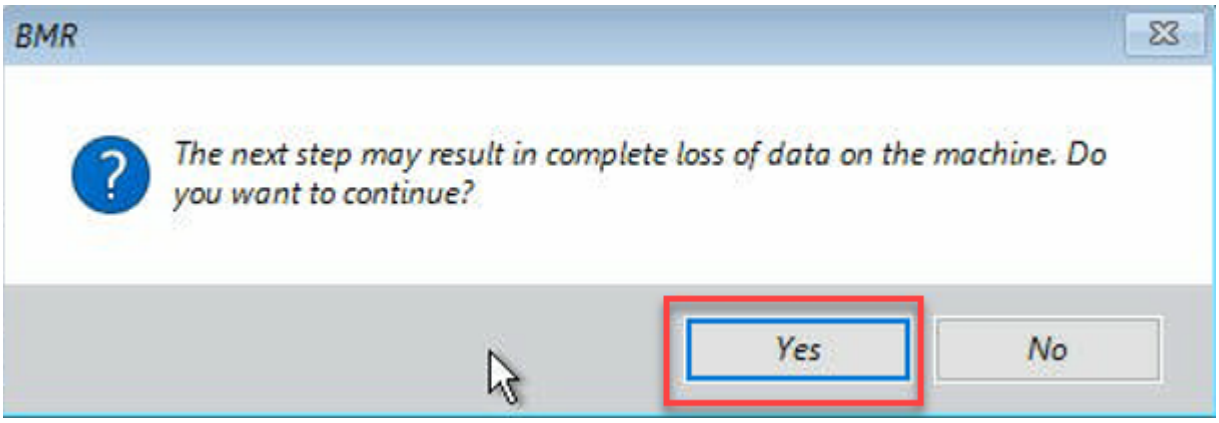
Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungsmodus auswählen** wird angezeigt.

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



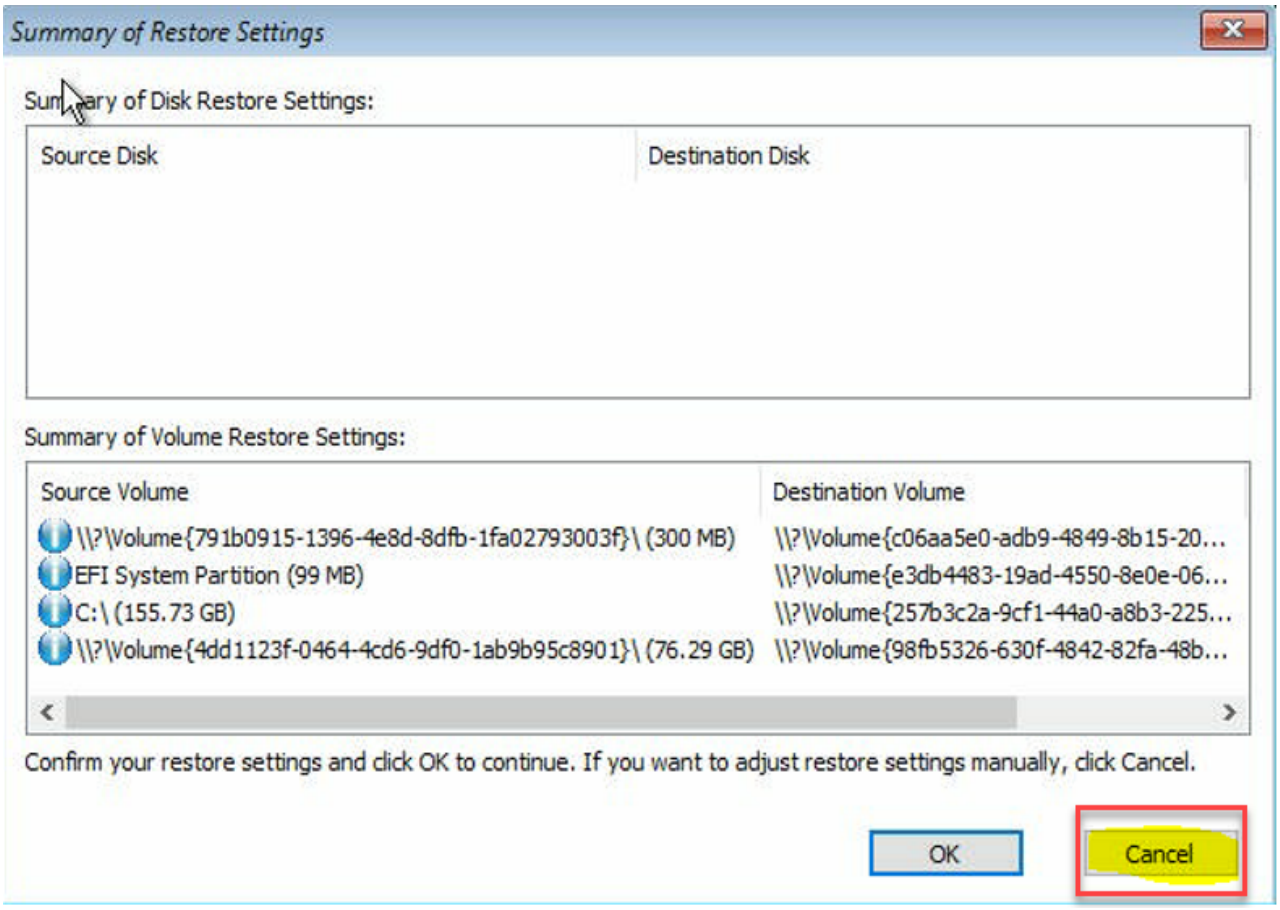
Das Dialogfeld **BMR** wird angezeigt.

18. Klicken Sie auf **Ja**.



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

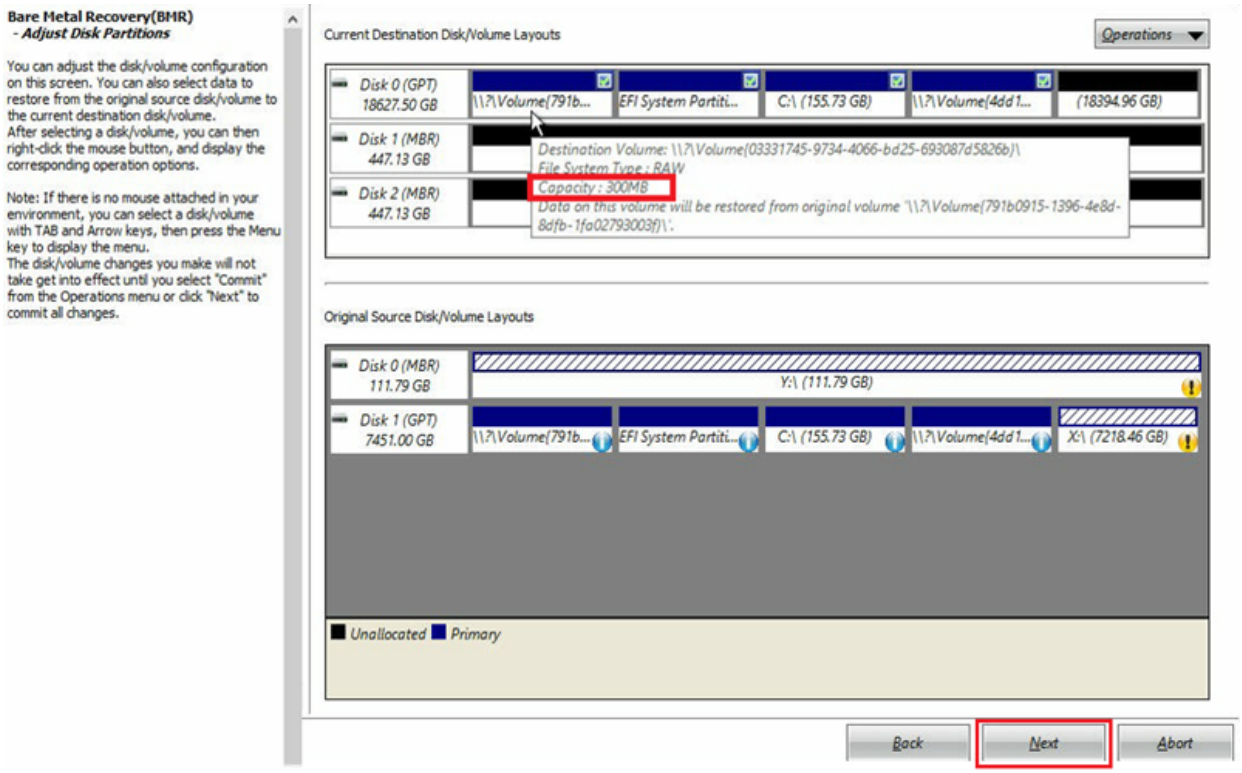
19. Klicken Sie auf **Abbrechen**.



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

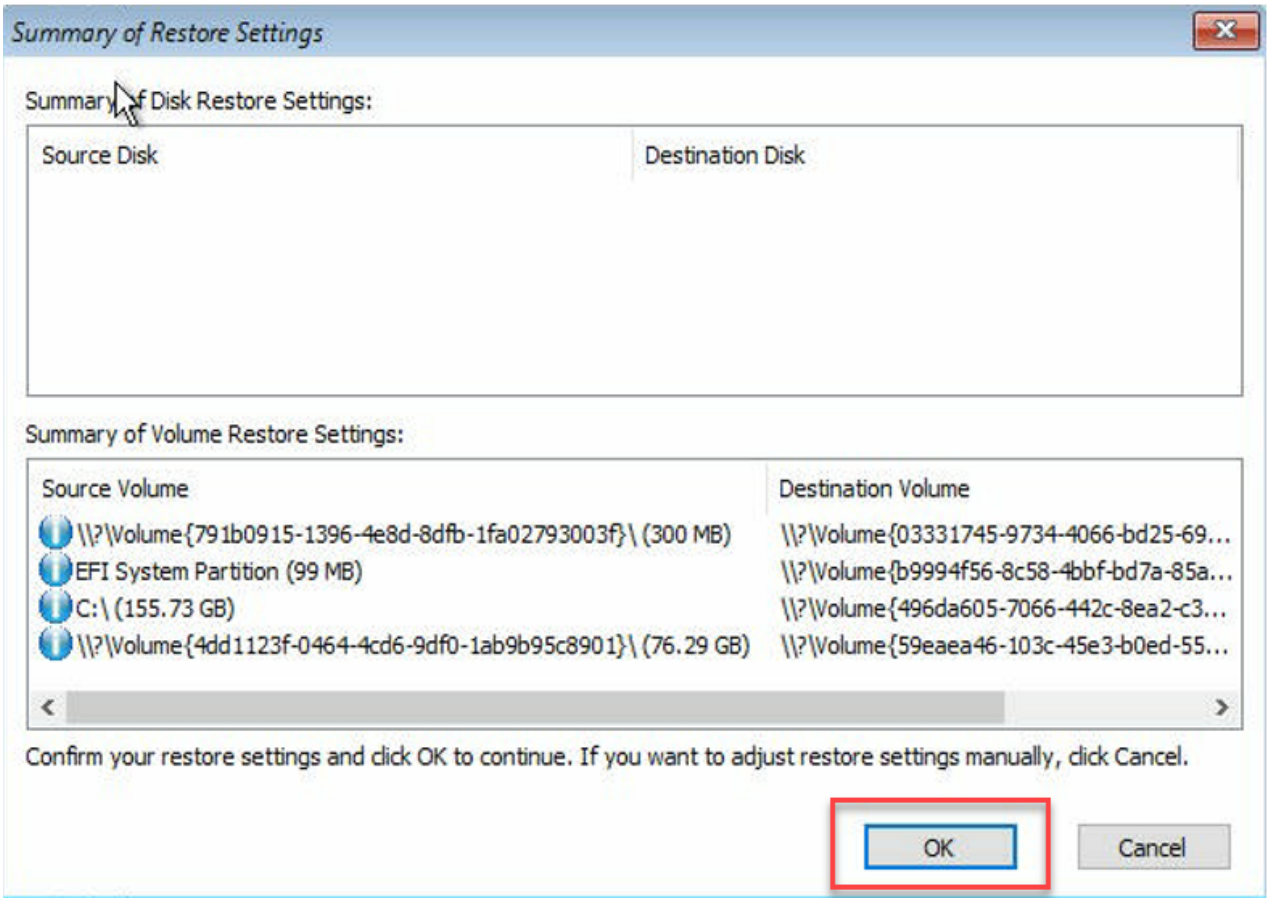
20. Vergleichen und überprüfen Sie, ob die Kapazität der ersten vier Partitionen auf der Registerkarte **Aktuelle Zieldatenträger/Volume-Layouts** dem größten verfügbaren GPT-Datenträger auf der Registerkarte **Ursprüngliche Quelldatenträger/Volume-Layouts** entspricht, und klicken Sie auf**Weiter**.

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



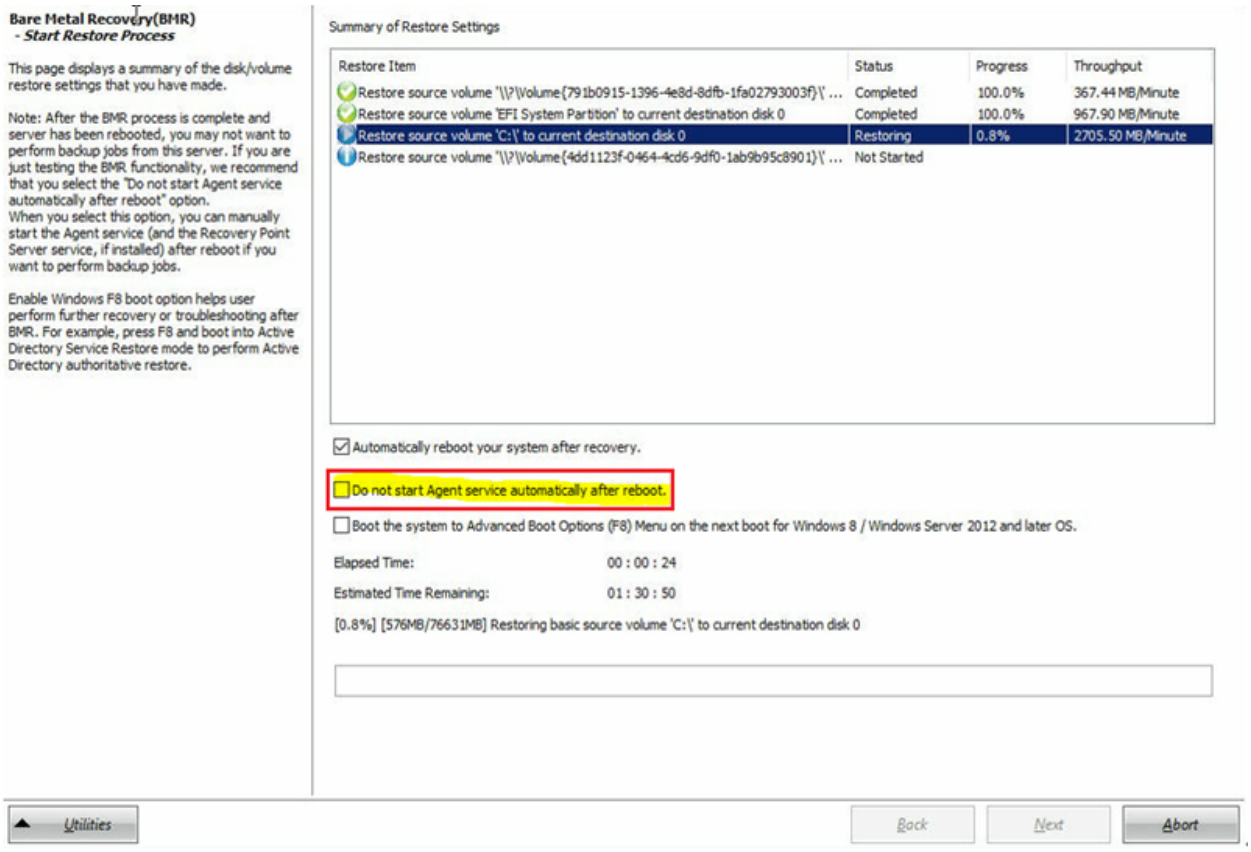
Das Dialogfeld **Übersicht über die Wiederherstellungseinstellungen** wird angezeigt.

21. Klicken Sie auf **OK**.



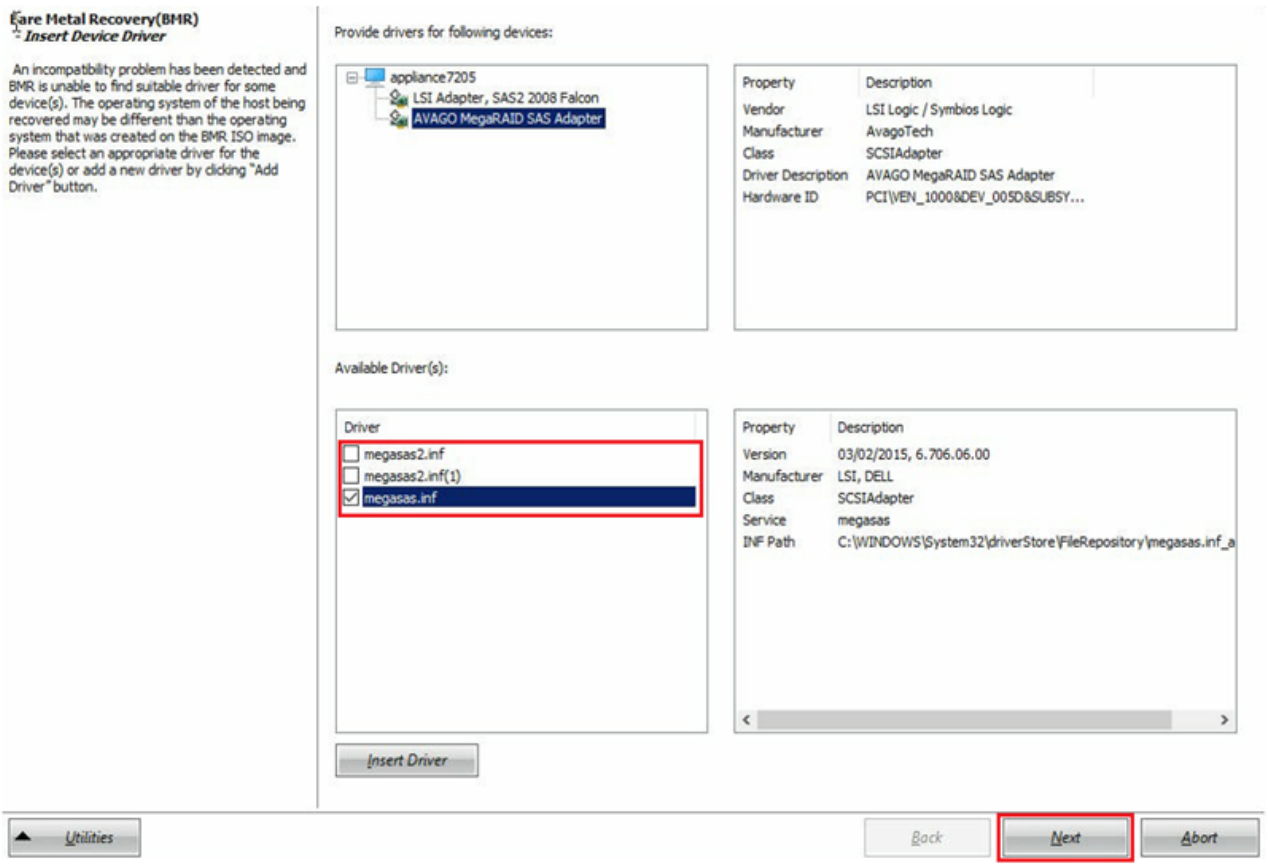
Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungsprozess starten** wird angezeigt.

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

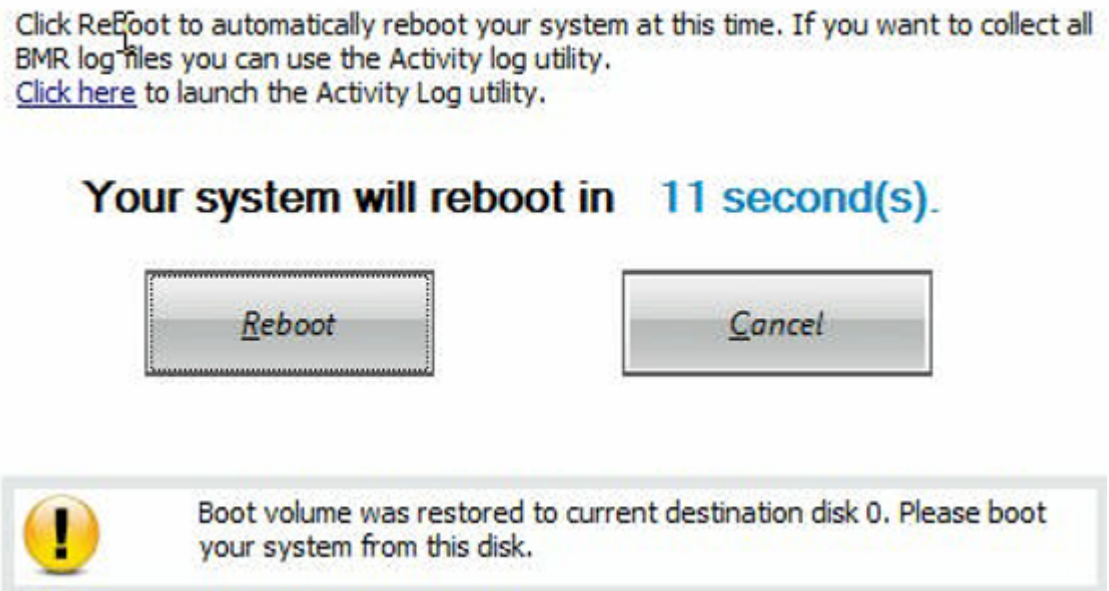


Das Dialogfeld **Bare-Metal-Recovery (BMR) – Gerätetreiber einfügen** wird angezeigt.

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



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



Der BMR-Prozess wurde erfolgreich abgeschlossen.

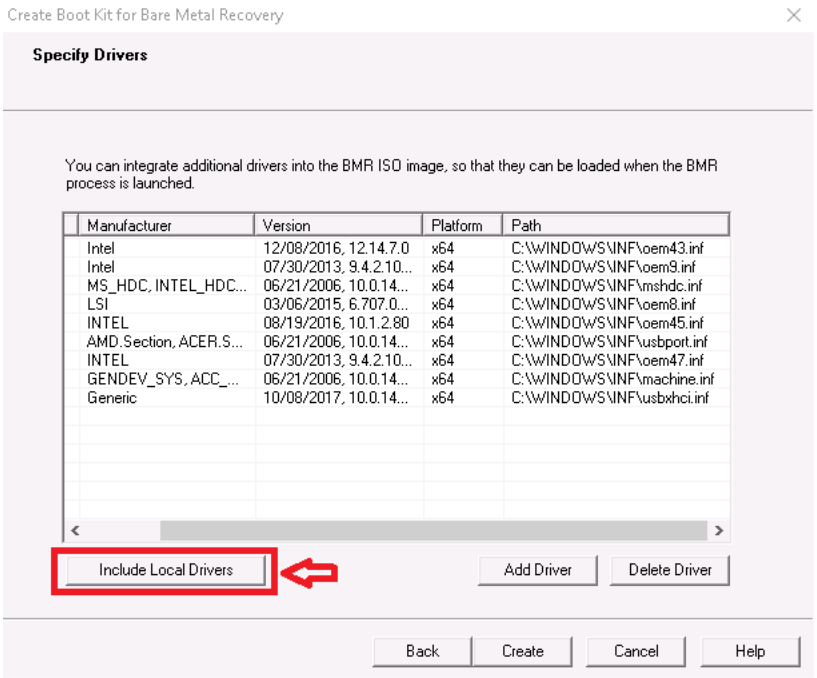
Durchführen einer Perform Bare Metal Recovery (BMR) und Beibehalten der Daten

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

Befolgen Sie diese Schritte:

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

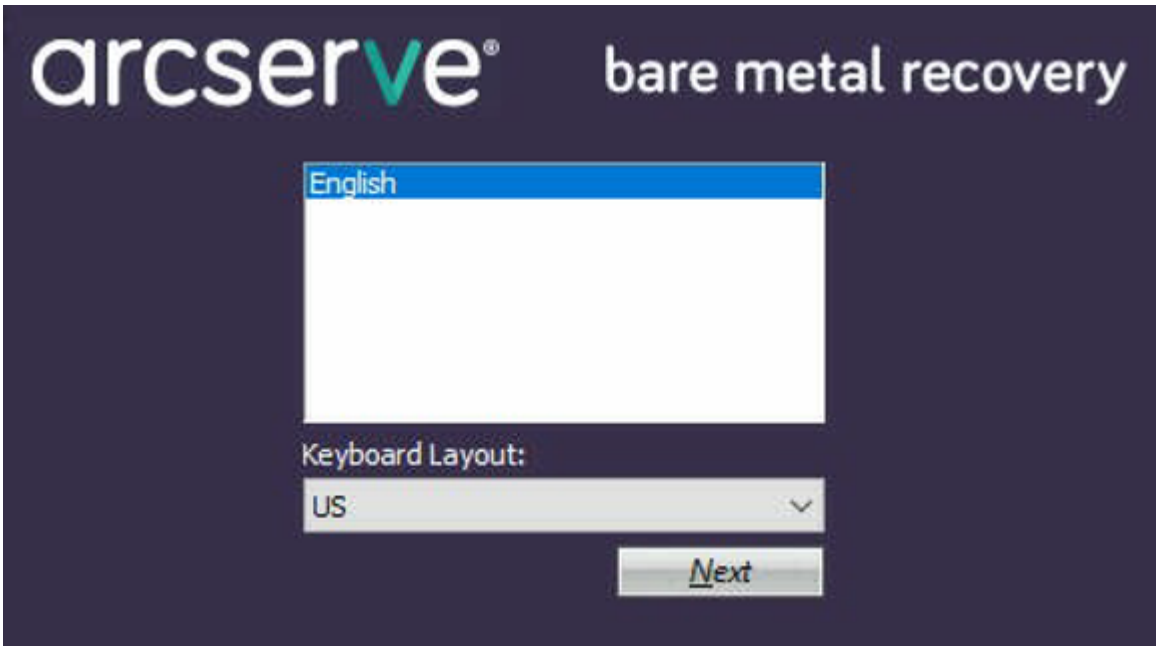
   Hinweis: Sie müssen die lokalen Treiber für das ISO-Image mit einschließen. Um die lokalen Treiber einzuschließen, aktivieren Sie die Option **Lokale Treiber einschließen** im Fenster **Bootkit für Bare-Metal-Recovery erstellen**. Weitere Informationen zum Erstellen des Bootkits finden Sie unter diesem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



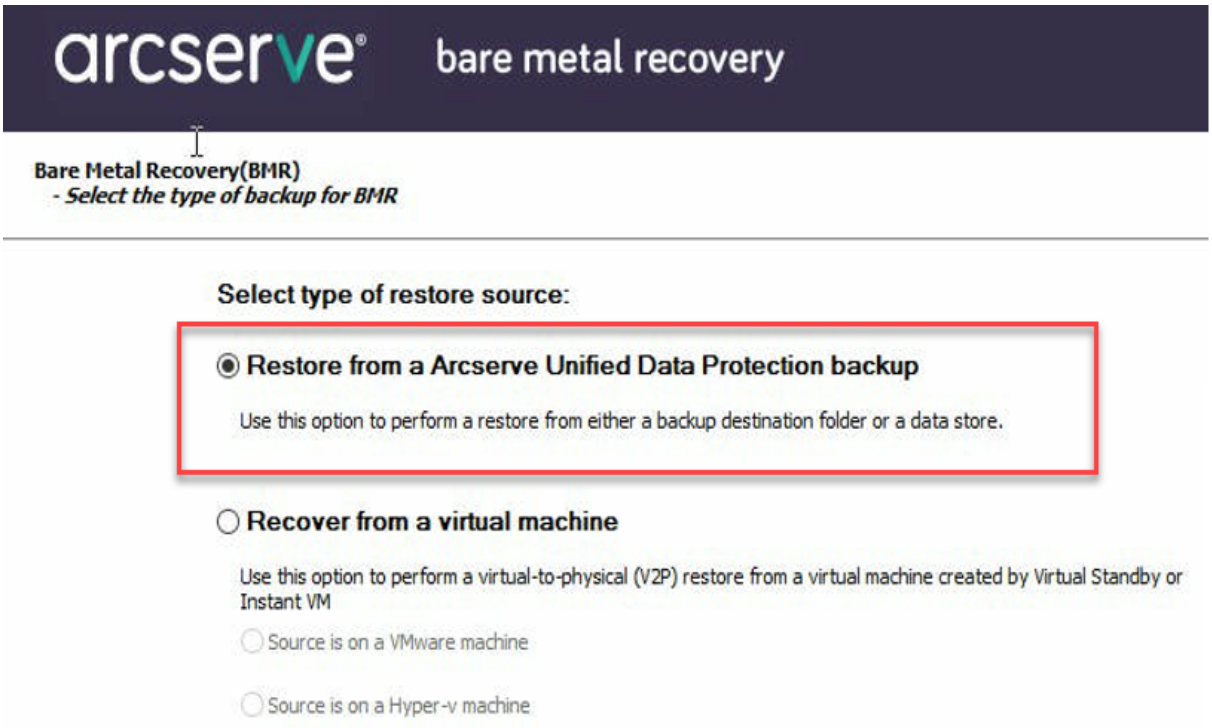
2. Starten Sie die Arcserve Appliance mit dem BMR-ISO-Image oder dem USB-Stick.

   Das **Arcserve Bare-Metal-Recovery** Setup wird angezeigt.

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

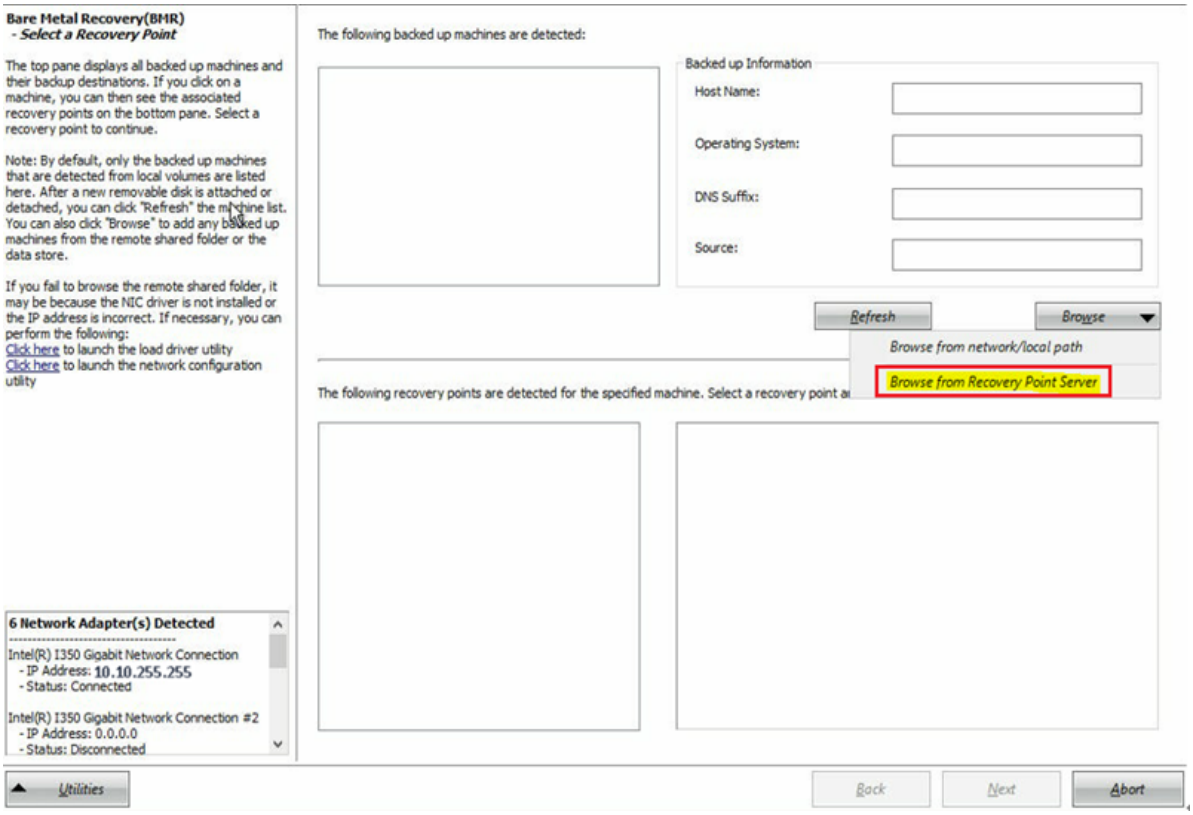


4. Wählen Sie die Option **Wiederherstellung von einer Arcserve Unified Data Protection-Sicherung** aus, und klicken Sie auf **Weiter**.



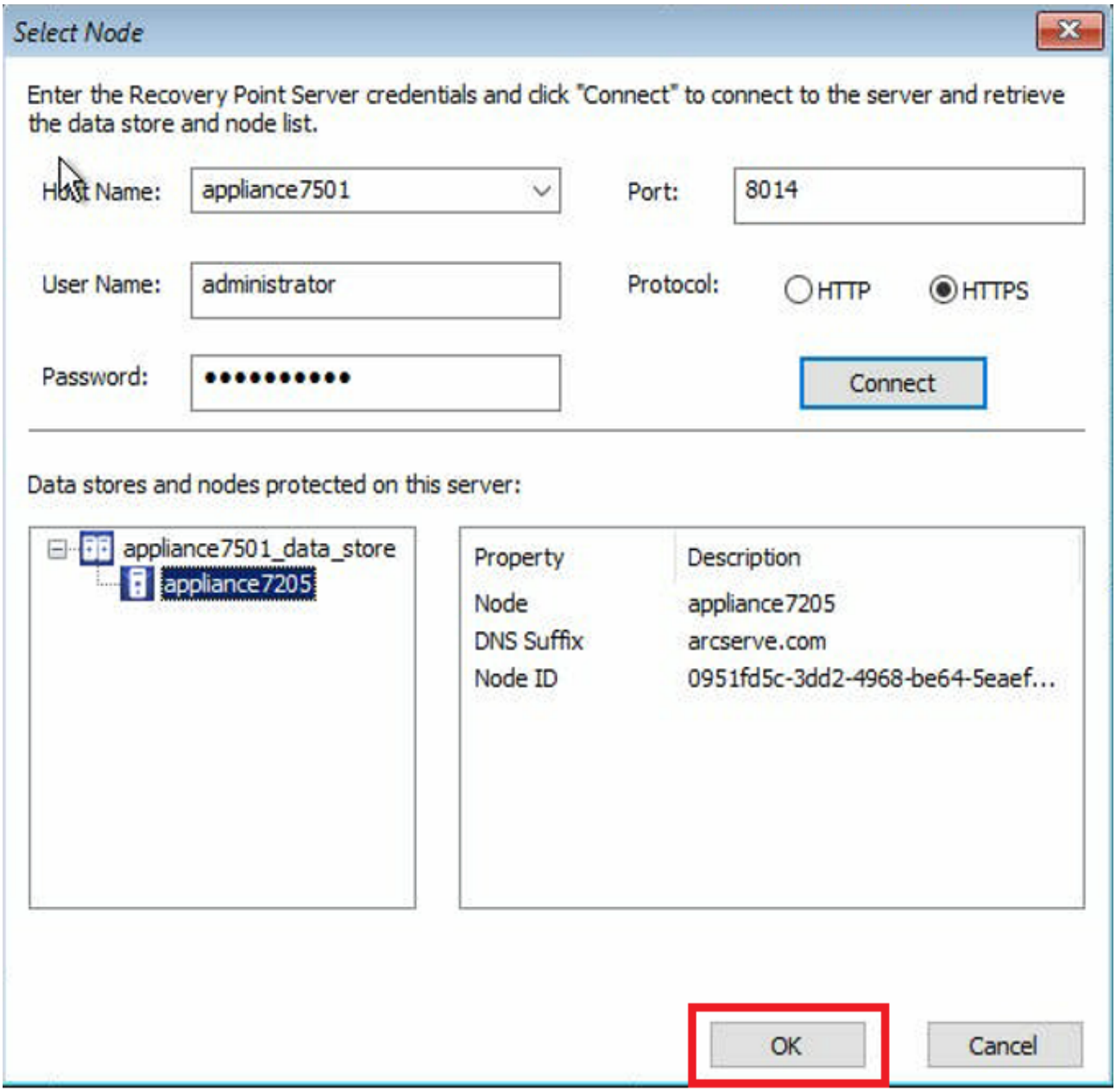
Das Fenster **Assistent zum Auswählen eines Wiederherstellungspunkts** wird angezeigt.

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



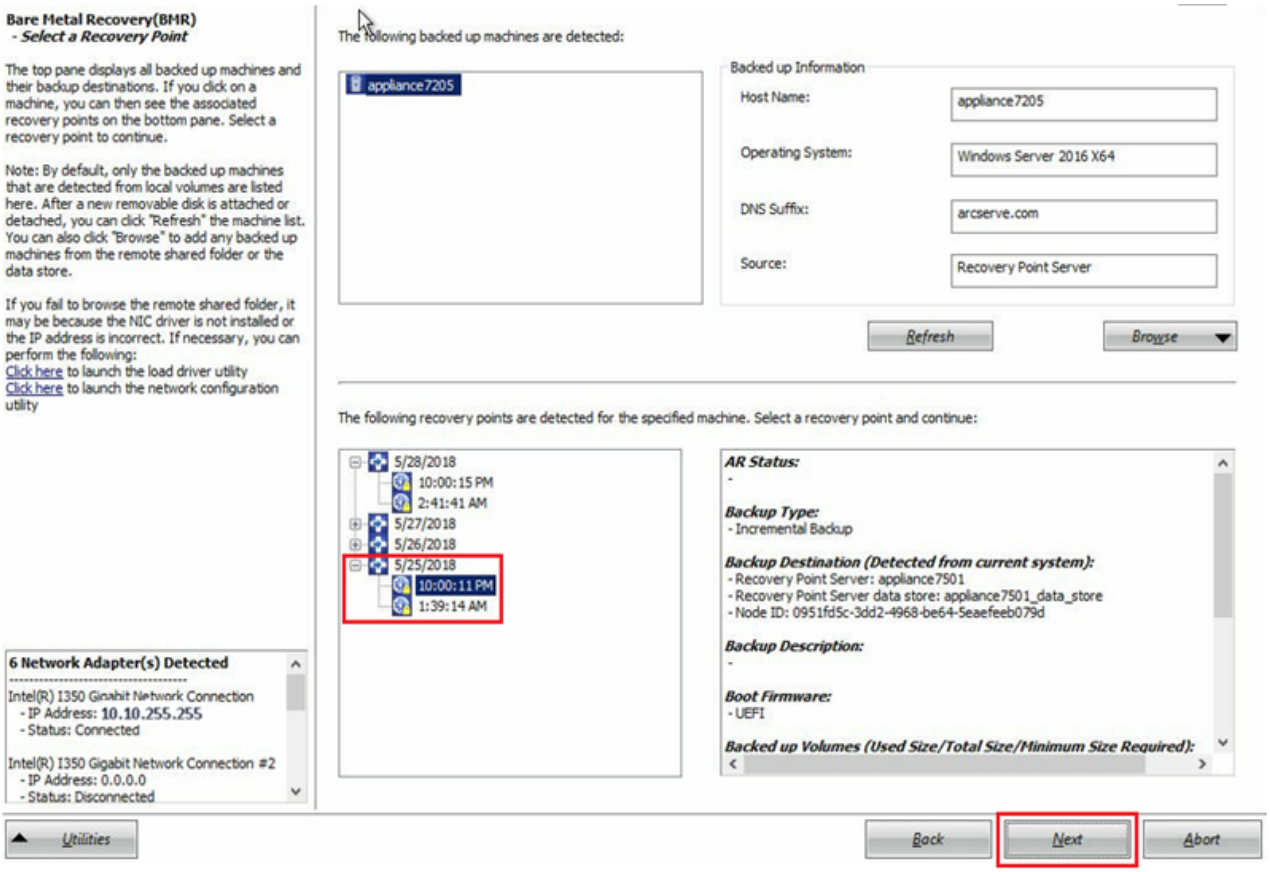
Das Fenster **Knoten auswählen** wird angezeigt.

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.

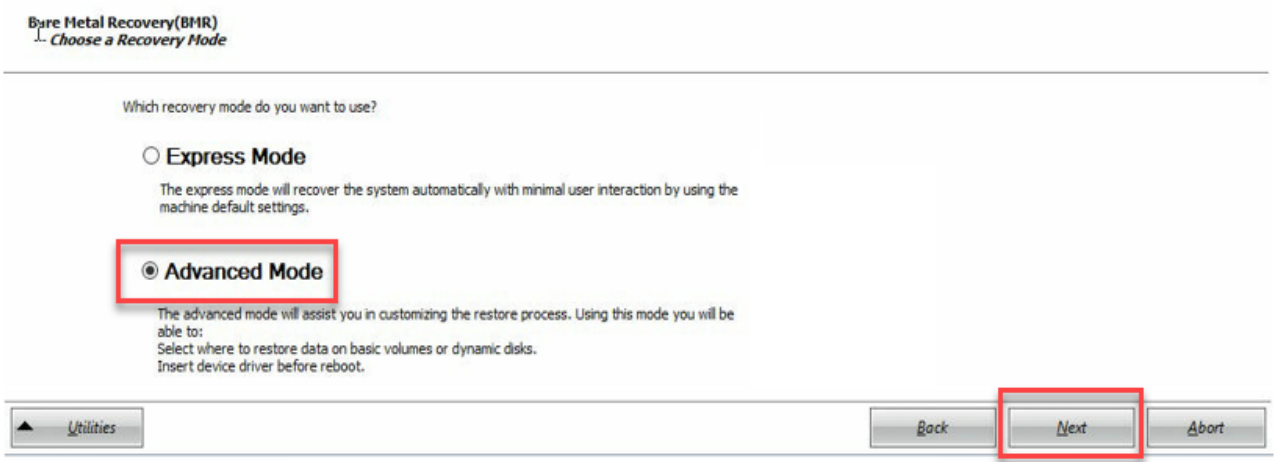
9. Wählen Sie den gewünschten Wiederherstellungspunkt aus, und klicken Sie auf **Weiter**.



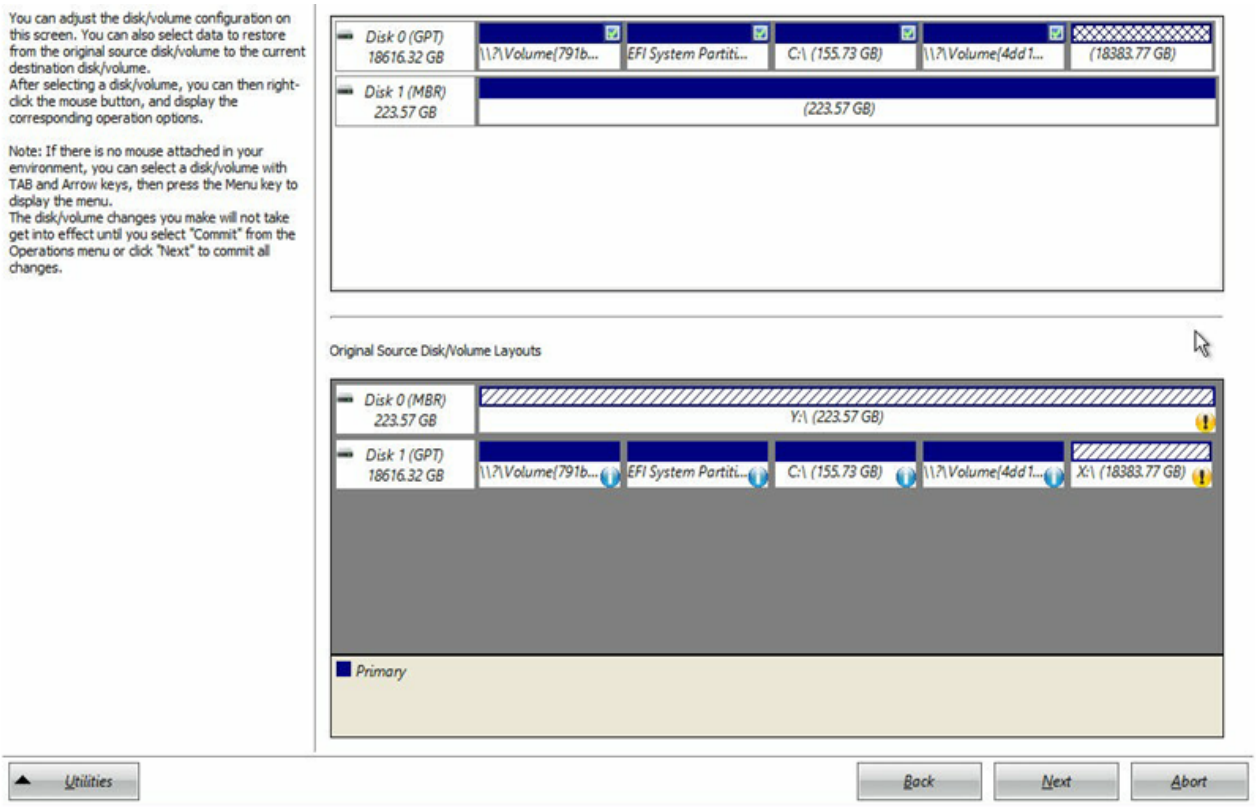
10. (Optional) Geben Sie das Sitzungskennwort ein, wenn Sie dazu aufgefordert werden, und klicken Sie dann auf **OK**.

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

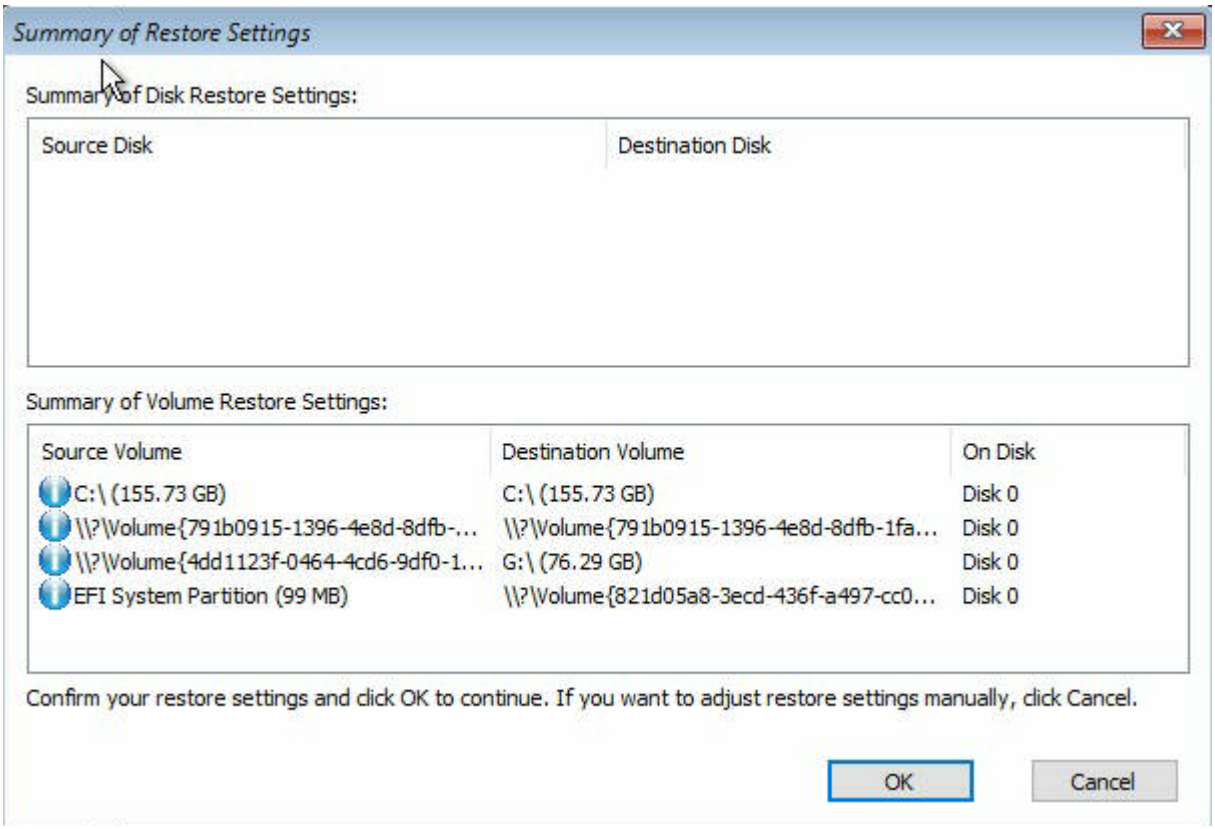
11. Wählen Sie **Erweiterter Modus** aus, und klicken Sie auf **Weiter**.



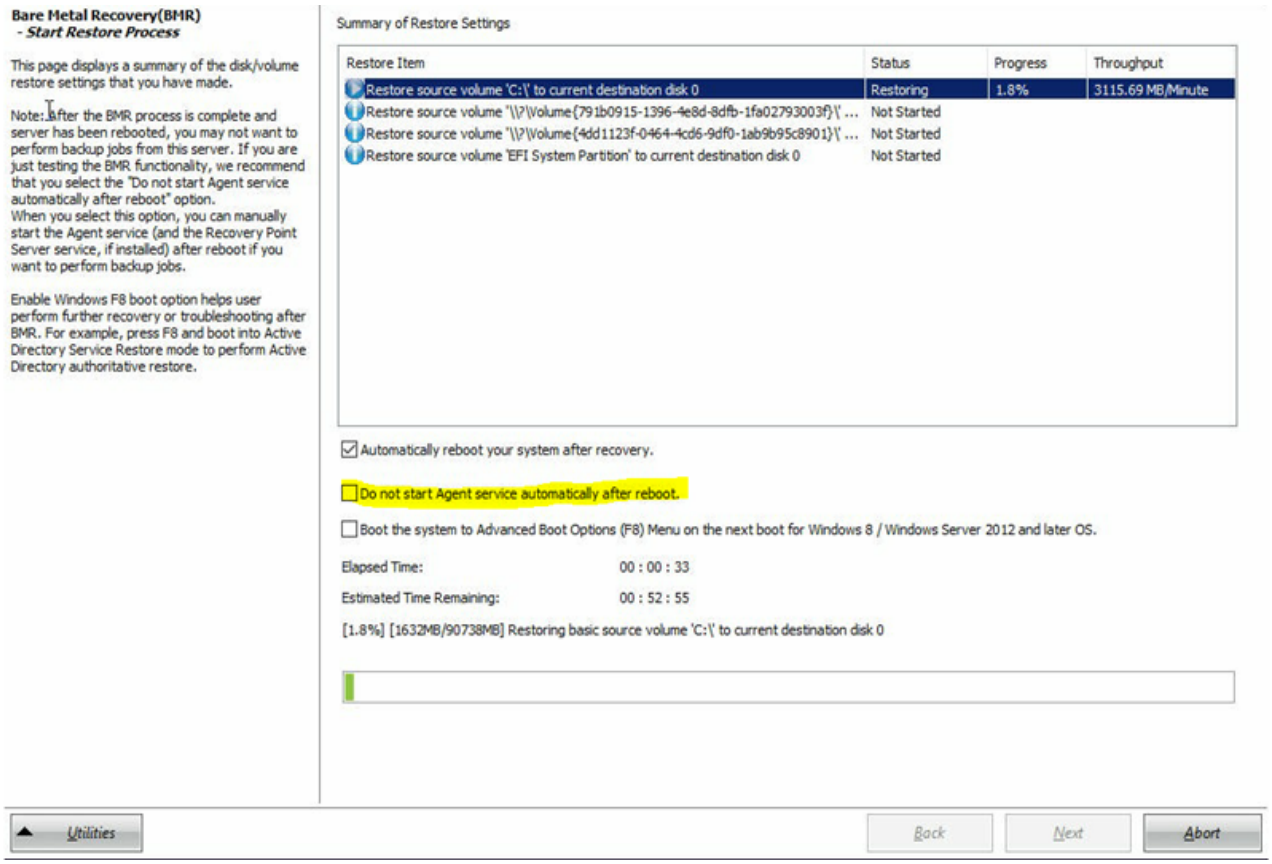
12. Klicken Sie im Dialogfeld **Bare Metal Recovery (BMR)-Daten-trägerpartitionen anpassen** auf **Weiter**.



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.

Kapitel 9: Durchführung einer Kapazitätserweiterung der Appliance

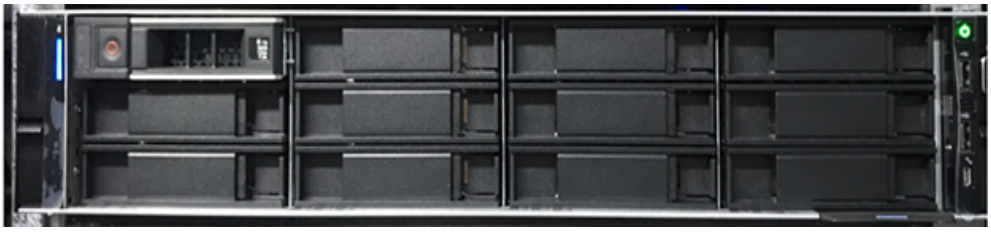
Dieser Abschnitt enthält folgende Themen:

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

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

Befolgen Sie diese Schritte:

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



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

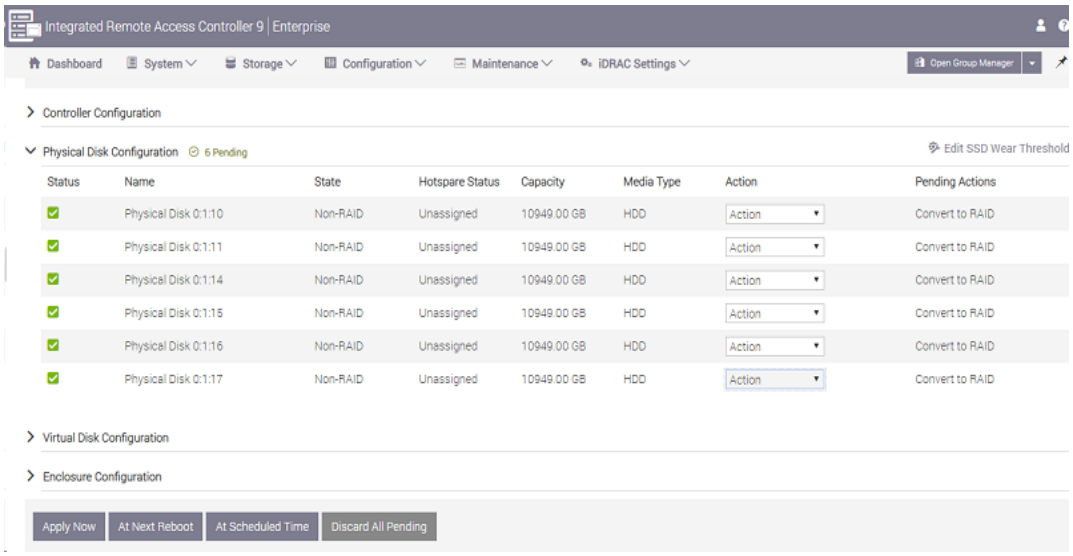
    Ein Dialogfeld wird mit der folgenden Fehlermeldung angezeigt:

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

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

    c. Klicken Sie auf **OK**.

    Unter Ausstehende Aktionen wird der Status In Raid konvertieren angezeigt.



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

Jetzt anwenden

Die Aktion zur Konvertierung in Raid wird sofort gestartet.

Beim nächsten Neustart

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

Geplante Zeit

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

Alle ausstehenden verwerfen

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

e. Navigieren Sie zu **Wartung**, **Jobwarteschlange**.

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

3. Gehen Sie folgendermaßen vor, um einen virtuellen Datenträger zu erstellen:

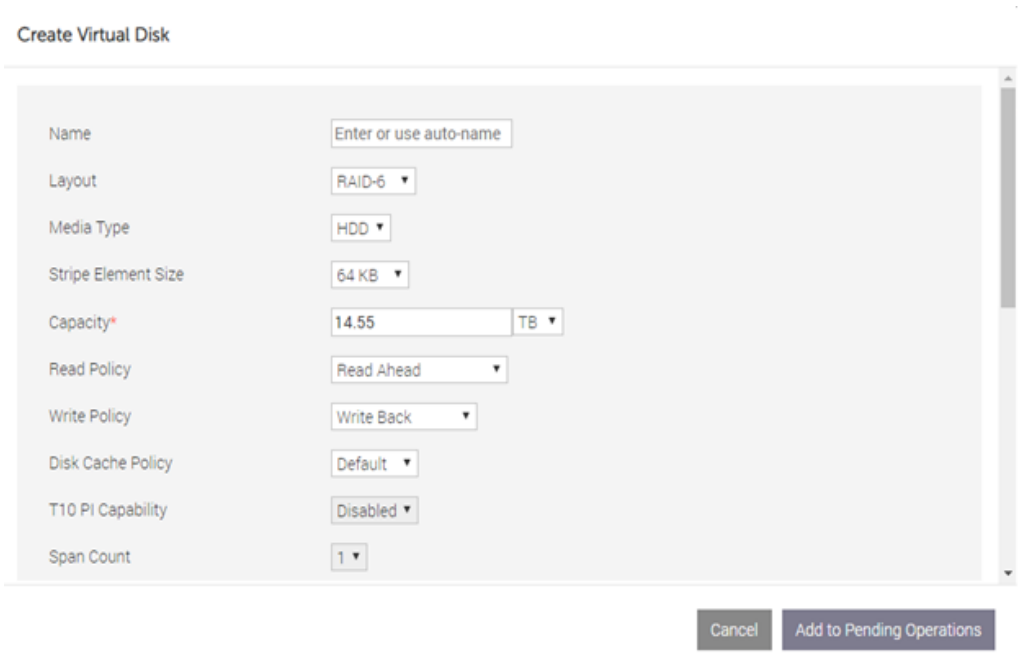
a. Navigieren Sie zu "Konfiguration, "Speicherkonfiguration“ und "Virtuelle Datenträgerkonfiguration".

b. Klicken Sie unter **Virtuelle Datenträgerkonfiguration** auf **Virtuellen Datenträger erstellen**.

c. Wählen Sie **RAID-6** als **Layout** aus.

d. Wählen Sie unter **Physischen Datenträger auswählen** den Datenträger aus, der in RAID konvertiert werden soll.

e. Klicken Sie auf **Zu ausstehende Vorgängen hinzufügen**.



f. Navigieren Sie zu "Konfiguration" und "Speicherkonfiguration".

g. Klicken Sie auf eine der folgenden Optionen, um den ausstehenden Vorgang abzuschließen:

Jetzt anwenden

Der Vorgang zum Erstellen eines virtuellen Datenträgers wird sofort gestartet.

Beim nächsten Neustart

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

Geplante Zeit

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

Alle ausstehenden verwerfen

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

h. Navigieren Sie zu **Wartung**, **Jobwarteschlange**.

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

i. Navigieren Sie **zu Computerverwaltung** und **Datenträgerverwaltung**.

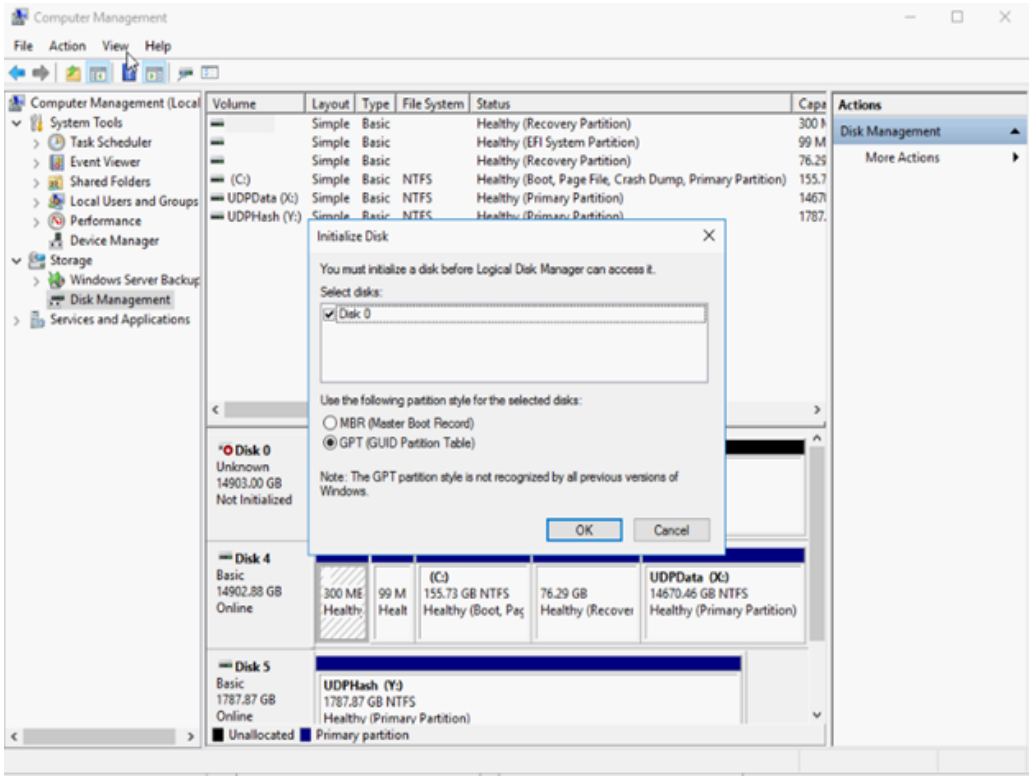
j. Doppelklicken Sie auf den neuen virtuellen Datenträger, den Sie hinzugefügt haben.

Das Fenster "Datenträger initialisieren" wird angezeigt.

k. Wählen Sie die **GPT-Datenträger (GUID-Partitionstabelle)** aus, und klicken Sie auf **OK**.

l. Wählen Sie im Fenster **Datenträgerverwaltung** den virtuellen Datenträger aus, und wenden Sie die folgenden Eigenschaften an:

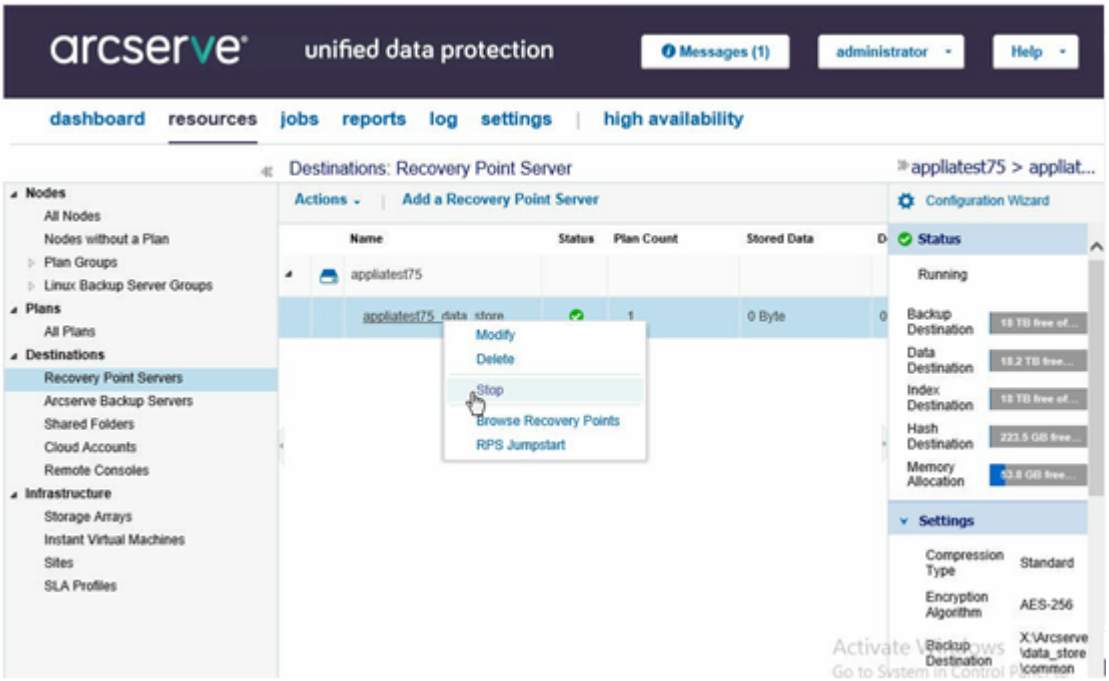
- Einen Laufwerksbuchstaben zuweisen
- NTFS als Dateisystem angeben
- Formatieren des Datenträgers



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

      Die Seite Arcserve Appliance-Konfiguration wird geöffnet.
   c. Klicken Sie auf **UDP Konsole starten**.

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



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

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

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

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

as_gddmgr.exe –DataPath Display <Name des Datenspeichers>

Dem Datenspeicher wurde erfolgreich ein neuer erweiterter Datenpfad hinzugefügt.

h. Navigieren Sie in der UDP-Konsole zu **Ressourcen**, **Ziele** und **Recovery Point Server**.

i. Klicken Sie mit der rechten Maustaste auf den Datenspeicher, und klicken Sie auf **Starten**.

j. Nehmen Sie die Pläne wieder auf, die Sie zuvor in der UDP-Konsole unterbrochen haben.

Die Datenkapazität von Arcserve Appliance wurde erfolgreich erweitert.

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

Dieser Abschnitt enthält folgende Themen:

Appliance-Infield-Erweiterung für alle verfügbaren Modelle

Modell	Aktuelle Kapazitäten\TB	Erweiterungs-Shelf-Kapazität	Aktuelle SSD – GB	Neue SSD REQ – GB	Freie Steckplätze	Add-on-Karten	BESCHREIBUNG
8100	4, 6	8 (6 x 2-TB-Festplatten)	120	8 TB – 140	2, 3	LSI SAS 9200 – 8E HBA Qlogic Dual-Port HBA Quad-Port 1G Netzwerkkarte Dual-Port 10G SPF + Dual-Port 10G Kupfer Infield-Erweiterung – (MegaRAID SAS 9380-8e)	1. Modell 8100 unterstützt nur 8-TB-Infield-Erweiterung. 2. 8100 - 8 TB Erweiterungs-Shelf mit integrierter und vorkonfigurierter SSD 240 GB. 3. 8100 verfügt über 2 und 3 als optionale Steckplätze. Ein freier Steckplatz ist obligatorisch für die Appliance-Infield-Erweiterung/MegaRAID SAS 9380-8e. 4. Wenn beide optionalen Steckplätze

							mit Zusatzkarten befüllt sind, müssen Sie mindestens einen (vorzugsweise Steckplatz 3) Steckplatz freigeben, damit die Erweiterung möglich ist. 5. Der SAS-Anschluss wird zwischen der Appliance und dem Erweiterungs-Shelf verwendet. 6. 8100 – Erweiterungs-Shelf enthält RAID 6. 7. Erweiterungs-Shelf enthält zwei Netzteile. 8. Befolgen Sie nach Anschluss der Erweiterungs-Shelf die Anweisungen zum **Hinzufügen eines Datenpfads** im Erweiterungs-

							leitfaden. 9. 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-Festplatten) ODER 16 (6 x 4-TB-Festplatten)	220	8 TB – NA 16 TB – 280	2, 3	LSI SAS 9200 – 8E HBA Qlogic Dual-Port HBA Quad-Port 1G Netzwerkkarte Dual-Port 10G SPF + Dual-Port 10G Kupfer Infield-Erweiterung (MegaRAID SAS 9380-8e)	1. Modell 8200 unterstützt 8-TB- oder 16-TB-Infield-Erweiterung. Clients können jeweils nur ein Erweiterungs-Shelf anschließen. 2. 8200 - 16 TB Erweiterungs-Shelf mit integrierter und vorkonfigurierter SSD 480 GB. 3. 8200 verfügt über 2 und 3 als optionale Steckplätze. Ein freier Steckplatz ist obligatorisch für die Appliance-Infield-

							Erweiterung/MegaRAID SAS 9380-8e. 4. Wenn beide optionalen Steckplätze mit Zusatzkarten befüllt sind, müssen Sie mindestens einen (vorzugsweise Steckplatz 3) Steckplatz freigeben, damit die Erweiterung möglich ist. 5. Der SAS-Anschluss wird zwischen der Appliance und dem Erweiterungs-Shelf verwendet. 6. Erweiterungs-Shelf enthält RAID 6. 7. Erweiterungs-Shelf enthält zwei Netzteile. 8. Befolgen Sie nach Anschluss der Erweiterungs-

							Shelf die Anweisungen zum **Hinzufügen eines Datenpfads** im Erweiterungsleitfaden. 9. Wenn eine neue SSD erforderlich ist, folgen Sie den Anweisungen unter **HASH-Ziel zu neuer SSD migrieren** im Erweiterungshandbuch.
8300	16, 20, 24, 28, 32, 36, 40	8 (6 x 2-TB-Festplatten) ODER 16 (6 x 4-TB-Festplatten) ODER 40 (12 x 4-TB-Festplatten)	480	8 TB – NA 16 TB – 560 40 TB – 790	2, 5, 6	LSI SAS 9200 – 8E HBA Qlogic Dual-Port HBA Quad-Port 1G Netzwerkkarte Dual-Port 10G SPF + Dual-Port 10G Kupfer Infield-Erwei-	1. Modell 8300 unterstützt 8-TB-, 16-TB- oder 40-TB-Infield-Erweiterung. Clients können jeweils nur ein Erweiterungs-Shelf anschließen. 2. 8300 – 16-TB-/40-TB-Erweiterungs-Shelf enthält eingebaute und vorkonfigurierte SSD 1,9 TB.

						terung (MegaRAID SAS 9380-8e)	3. 8300 verfügt über 2, 5 und 6 als optionale Steckplätze. Ein freier Steckplatz ist obligatorisch für die Appliance-Infield-Erweiterung/MegaRAID SAS 9380-8e. 4. Wenn beide optionalen Steckplätze mit Add-on-Karten gefüllt sind, müssen Sie mindestens einen Steckplatz frei machen, um die Infield-Erweiterung verwenden zu können, vorzugsweise Steckplatz 2. 5. Der SAS-Anschluss wird zwischen der Appliance und dem Erweiterungs-Shelf verwendet. 6. Erweiterungs-Shelf enthält

							RAID-6 (6 x 4-TB-Festplatten). 7. Erweiterungs-Shelf enthält zwei Netzteile. 8. Befolgen Sie nach Anschluss der Erweiterungs-Shelf die Anweisungen zum **Hinzufügen eines Datenpfads** im Erweiterungsleitfaden. 9. Wenn eine neue SSD erforderlich ist, folgen Sie den Anweisungen unter **HASH-Ziel zu neuer SSD migrieren** im Erweiterungshandbuch. (Nur für Appliance 8300: Beim Verbinden mit einem 40-TB-Appliance-Erweiterungs-

							Shelf bleibt eine 2-TB-SSD frei, die Sie in der Base-Appliance und nicht im Erweiterungs-Shelf platzieren müssen. Nähere Informationen hierzu finden Sie im Erweiterungshandbuch).
8400	32,40,48,56,64,72,80	8 (6 x 2-TB-Festplatten) ODER 16 (6 x 4-TB-Festplatten) ODER 40 (12 x 4-TB-Festplatten)	1200	8 TB – NA 16 TB – NA 40 TB – NA	2, 5, 6	LSI SAS 9200 – 8E HBA Qlogic Dual-Port HBA Quad-Port 1G Netzwerkkarte Dual-Port 10G SPF + Dual-Port 10G Kupfer Infield-Erweiterung (MegaRAID SAS 9380-8e)	1. Modell 8400 unterstützt 8-TB-, 16-TB- oder 40-TB-Infield-Erweiterung. Clients können jeweils nur ein Erweiterungs-Shelf anschließen. 2. 8400 – erfordert keine zusätzliche SSD. 3. 8400 verfügt über 2, 5 und 6 als optionale Steckplätze. Ein freier Steckplatz ist obligatorisch für die Appliance-

							Infield-Erweiterung/MegaRAID SAS 9380-8e. 4. Wenn beide optionalen Steckplätze mit Zusatzkarten befüllt sind, müssen Sie mindestens einen (vorzugsweise Steckplatz 2) Steckplatz freigeben, damit die Erweiterung möglich ist. 5. Der SAS-Anschluss wird zwischen der Appliance und dem Erweiterungs-Shelf verwendet. 6. Erweiterungs-Shelf enthält RAID 6. 7. Erweiterungs-Shelf enthält zwei Netzteile. 8. Befolgen Sie nach Anschluss der Erweiterungs-

							Shelf die Anweisungen zum **Hinzufügen eines Datenpfads** im Erweiterungsleitfaden.

In der Box enthaltene Gegenstände

Folgende Gegenstände sind in der Box enthalten:

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

- Appliance-Erweiterungs-Shelf

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

- CVPM02-Modul (CacheVault Power Module02) und Kabel

- MegaRAID SAS 9380-8e RAID-Controller

- SAS-Kabel

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

- SSD (optional)

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

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

Befolgen Sie diese Schritte:

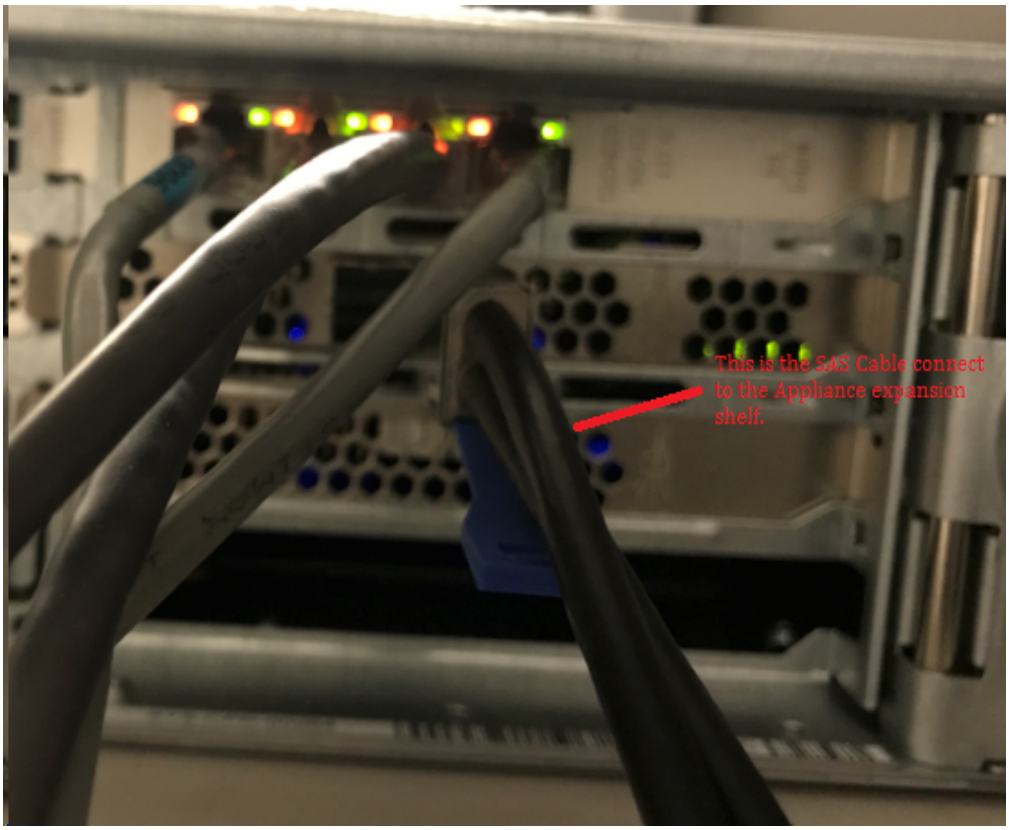
1. Bereiten Sie das Appliance-Erweiterungs-Shelf vor und platzieren Sie es in der Nähe des Appliance-Servers.
2. Verbinden Sie das *CacheVault Power Module02 (CVPM02)* mit dem *MegaRAID Controller 9380-8e*.

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

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

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

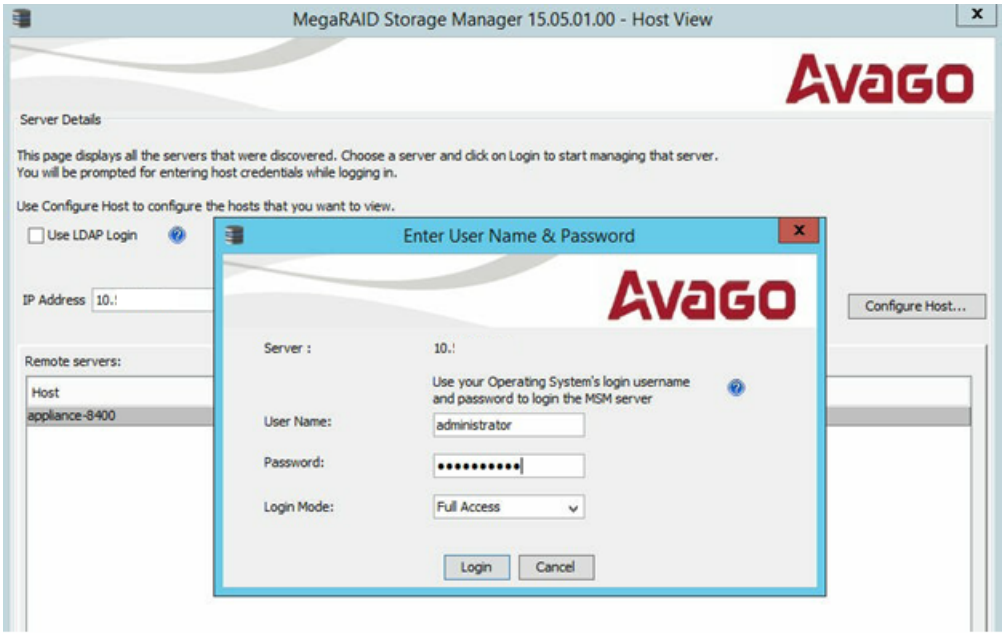
7. Sichern Sie die *MegaRAID Controller 9380-8e*-Halterung am Gehäuse des Systems.
8. Ersetzen Sie die Abdeckung des Appliance-Server-Gehäuses.
9. Verbinden Sie den *MegaRAID Controller 9380-8e* auf dem Appliance-Server und den *MegaRAID Controller* in der Appliance-Erweiterungs-Shelf mit dem SAS-Kabel.



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

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

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

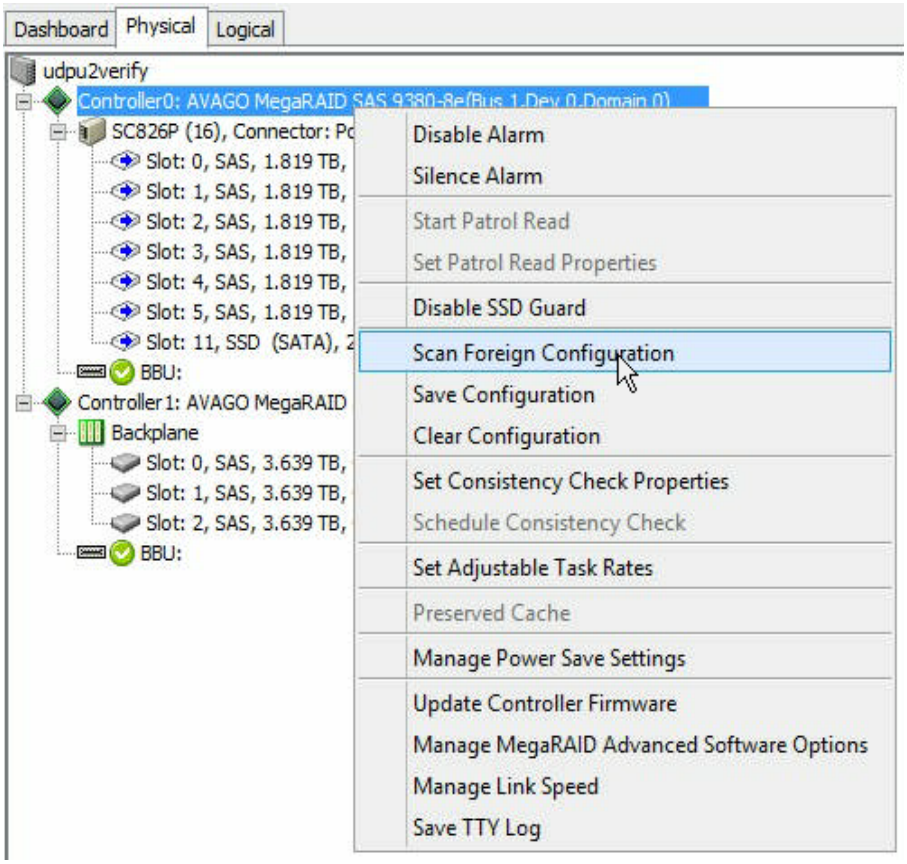


14. Gehen Sie folgendermaßen vor, um den RAID-Controller über den MegaRAID Storage Manager zu überprüfen:

    a. Navigieren Sie zur Registerkarte **Physisch**, auf der die beiden Controller aufgeführt sind.

    b. Wählen Sie **Controller 9380-8e** aus, und stellen Sie sicher, dass alle an den Controller 9380-8e angeschlossenen Datenträger online und verfügbar sind.

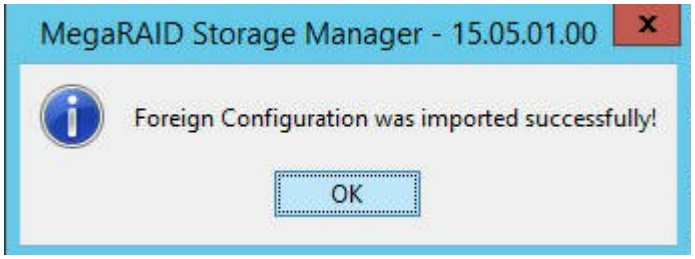
    Hinweis: Wenn es Datenträger gibt, die nicht online sind, klicken Sie mit der rechten Maustaste, und wählen Sie **Scan Foreign Configuration**.



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

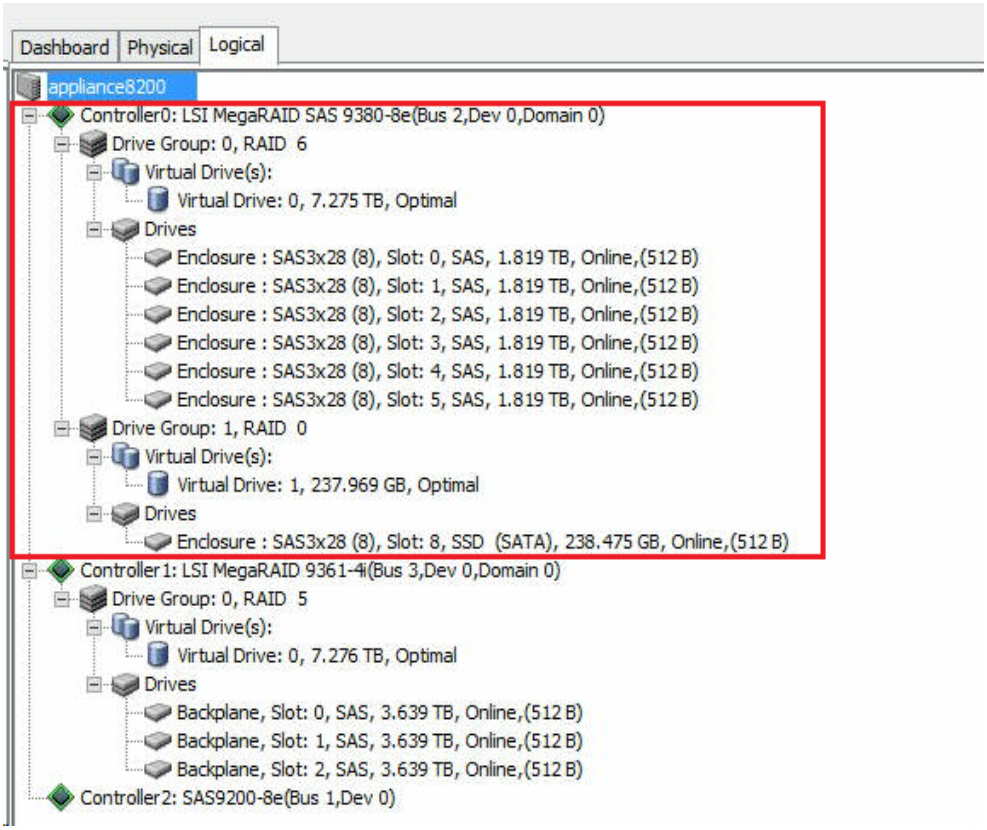
d. Klicken Sie auf **Ja**, um den Importprozess zu starten.

e. Klicken Sie auf **OK**.



Alle Laufwerke im Erweiterungs-Shelf sind nun online.

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

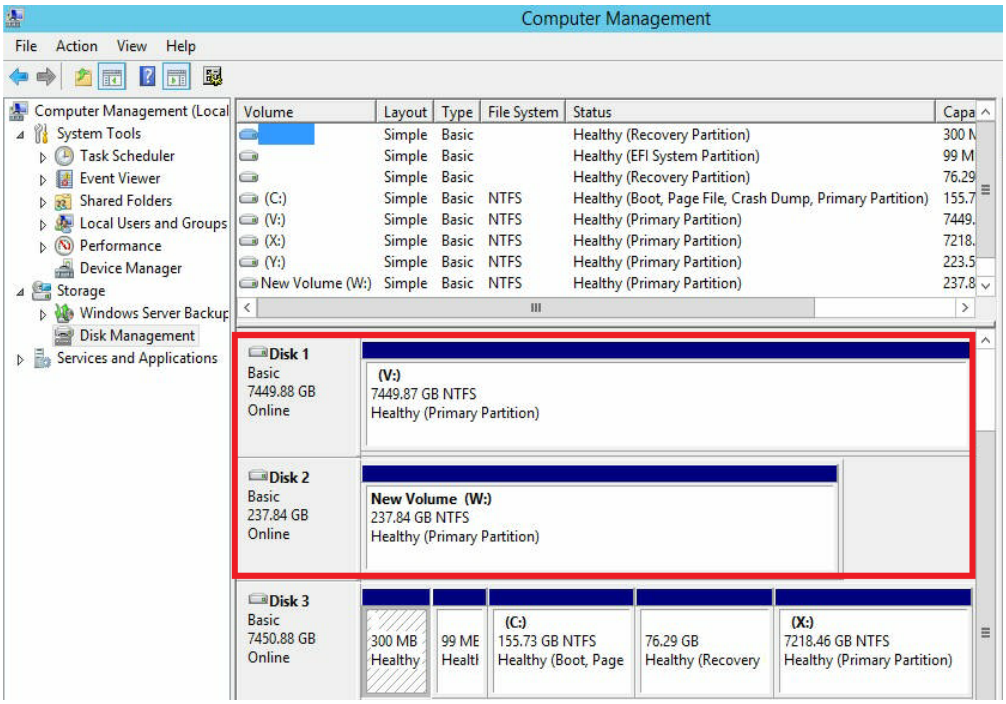


16. Öffnen Sie die Computerverwaltung, und navigieren Sie zur Datenträgerverwaltung, und führen Sie folgende Schritte aus:

    a. Formatieren Sie den als Appliance-Erweiterungs-Shelf montierten Datenträger als NTFS, und weisen Sie einen Laufwerksbuchstaben zu. Zum Beispiel "V:".

    b. Formatieren Sie die SSD als NTFS , und weisen Sie einen Lauf-

werksbuchstaben zu. Zum Beispiel "B:".



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

So ändern Sie den Arcserve UDP-Datenspeicher

Dieser Abschnitt enthält folgende Themen:

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

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

Befolgen Sie diese Schritte:

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

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

as_gddmgr.exe –DataPath Display <Name des Datenspeichers>

Migrieren eines Hash-Ziels zur neuen SSD

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

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

Befolgen Sie diese Schritte:

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

Überprüfen die Gesamtkapazität des Datenspeichers auf der Arcserve UDP-Konsole

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

Fortsetzen aller Pläne von der Arcserve UDP-Konsole

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

Kapitel 10: Arbeiten mit Netzwerkkonfiguration

Dieser Abschnitt enthält folgende Themen:

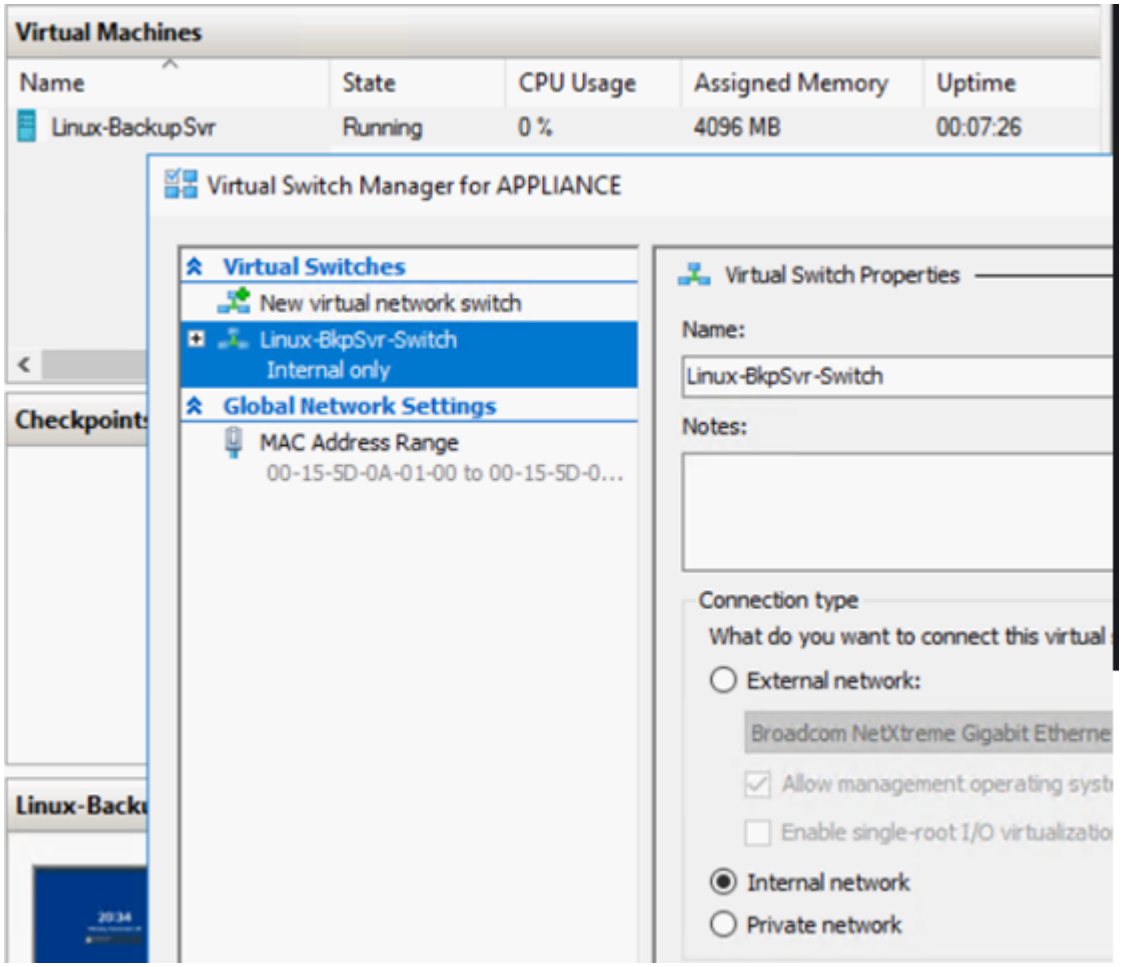
Funktionsweise der Netzwerkkonfigurationsdetails

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

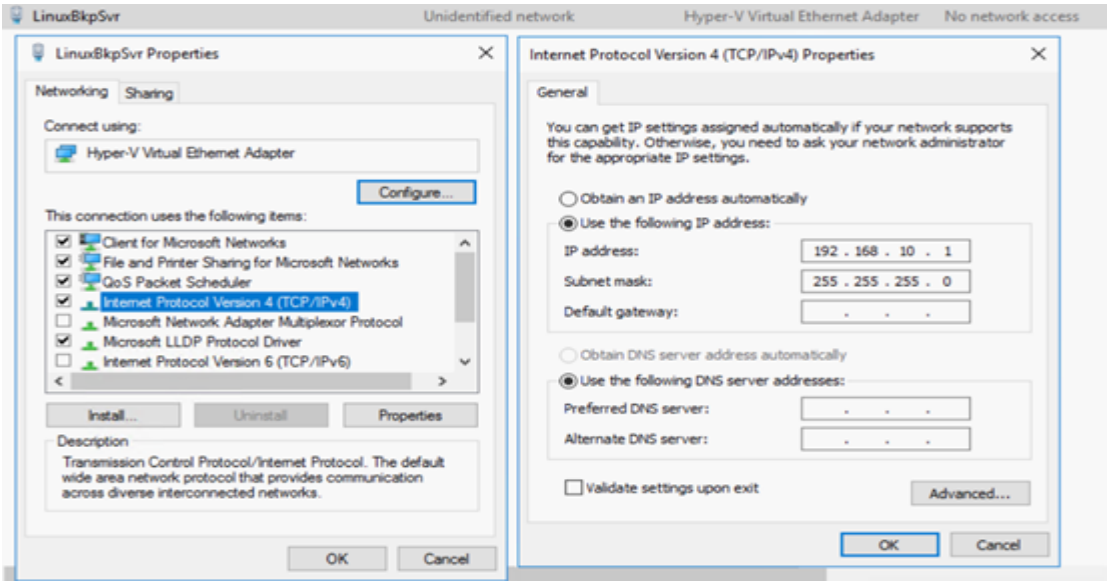
- Der Benutzer muss den Hostnamen des integrierten Linux nicht ändern.
- Der Benutzer speichert eine IP-Adresse für den Linux-Sicherungsserver im Netzwerk.
- Der Linux-Sicherungsserver kann eine Verbindung zu jedem beliebigen Rechner im öffentlichen Netzwerk herstellen.
- Jeder Rechner im öffentlichen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

Netzwerkkonfigurationsdetails:

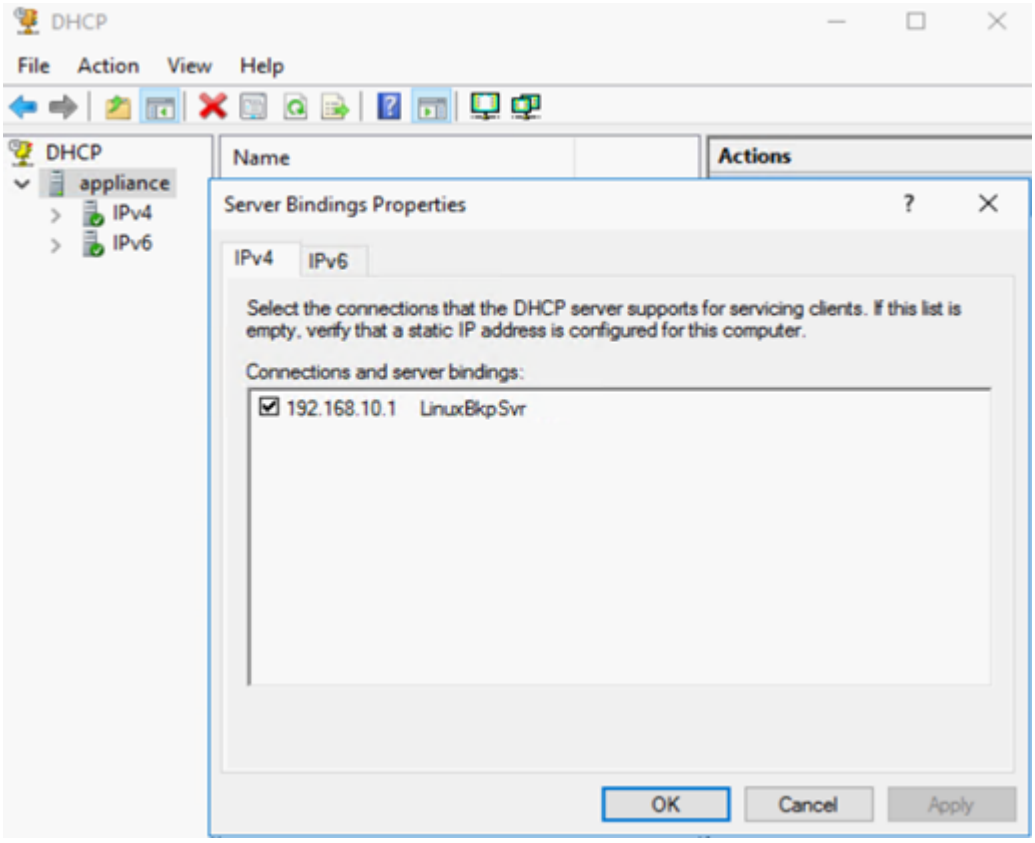
- Auf dem Hyper-V-Manager gibt es einen rein internen virtuellen Switch (*Linux-BkpSvr-Switch*), der nur von Linux-BackupSvr verwendet wird.



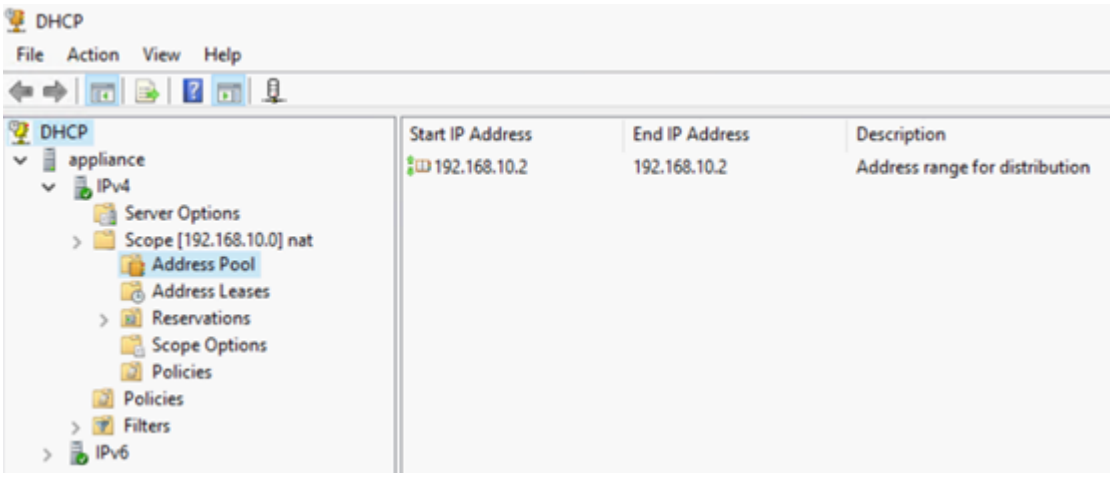
- Unter *Systemsteuerung\Netzwerk und Internet\Netzwerkverbindungen* wird ein "Hyper-V-Adapter für virtuelles Ethernet" namens "LinuxBkpSvr" angezeigt. Die IPv4-Adresse für diesen Switch wurde standardmäßig auf "192.168.10.1" festgelegt, wie unten gezeigt.



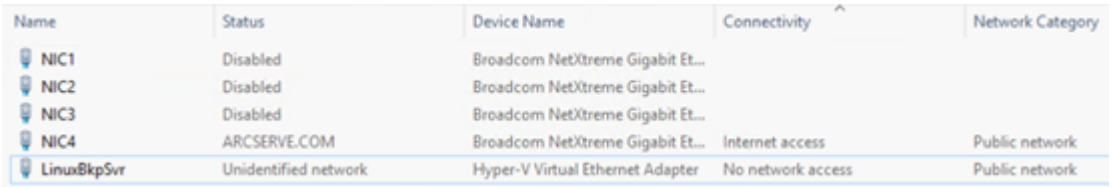
- Sie haben in der Standardeinstellung DHCP-Server auf dem Appliance-Rechner konfiguriert. Der DHCP-Server funktioniert nur auf dem virtuellen Hyper-V-Adapter.

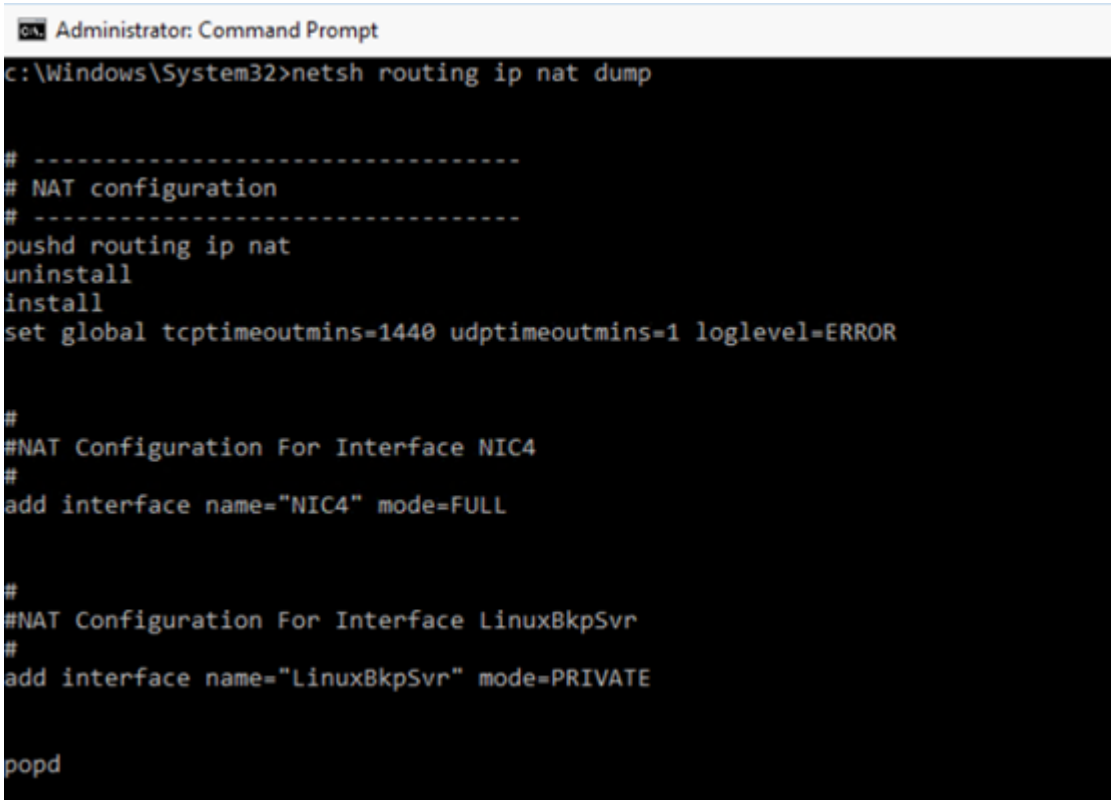


- Standardmäßig stellt nur eine 192.168.10.2 im Adresspool sicher, dass der integrierte Linux-Sicherungsserver die IP 192.168.10.2 erhält.

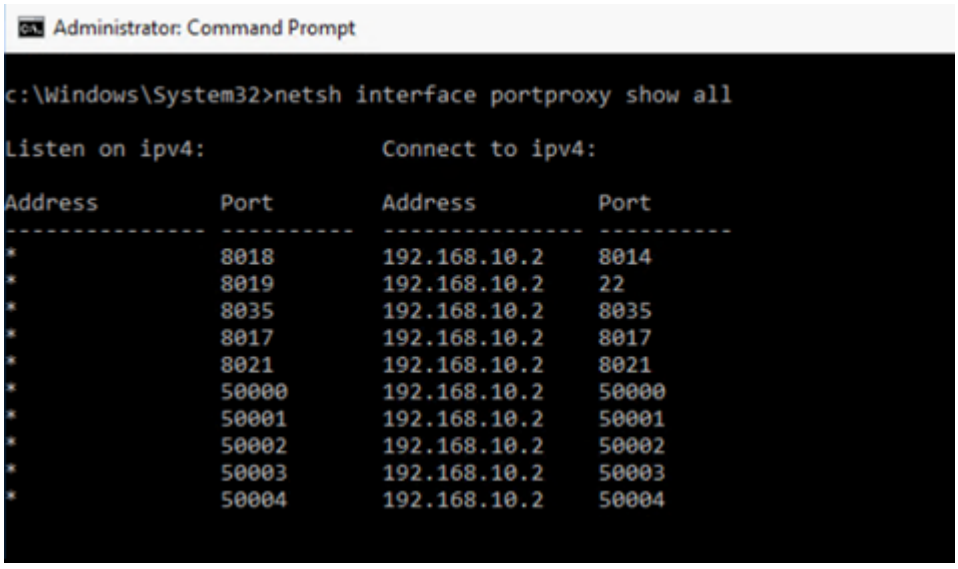


- NAT wurde auf dem Appliance-Rechner konfiguriert.





- 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.

```
[root@Linux-BackupSvr network-scripts]# cat ifcfg-eth0
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=eth0
UUID=9ae68090-5e77-4396-b6c4-a5d6d83ab62f
DEVICE=eth0
ONBOOT=yes
ZONE=
[root@Linux-BackupSvr network-scripts]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.2  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::c08c:d0dc:bf67:8afa  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:0a:01:00  txqueuelen 1000  (Ethernet)
        RX packets 20955  bytes 28503433 (27.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19202  bytes 1534457 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 14  bytes 1600 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 1600 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Konfiguration des NIC-Teaming-Prozesses

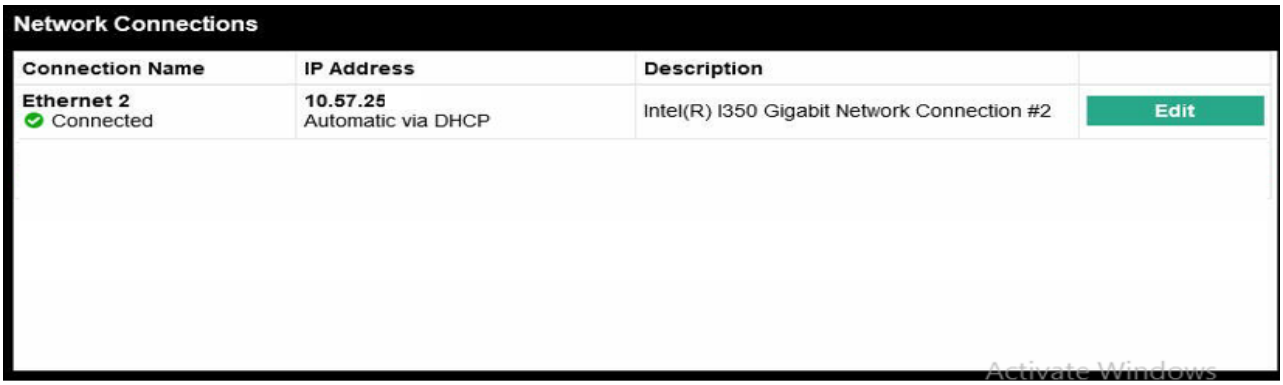
Die Arcserve Appliance enthält integrierte Ethernet-Ports. Um diese Ports verwenden zu können, muss das Ethernet-NIC-Teaming konfiguriert werden. NIC-Teaming ermöglicht die Platzierung mehrerer Netzwerkadapter in einem Team für Bandbreitenaggregation und Netzwerkverkehr-Failover, um im Falle eines Netzwerkkomponentenausfalls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

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

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

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

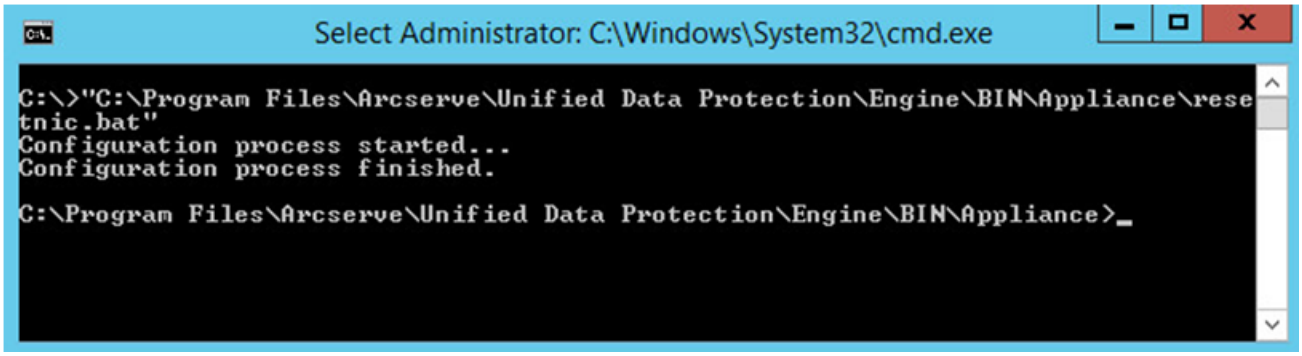
   Hinweis: Wenn eine DHCP- oder statische IP-Adresse verwendet wird, können Sie die IP-Adresse für das NIC-Team im Fenster "Netzwerkverbindungen" konfigurieren. Stellen Sie sicher, dass dem NIC-Team eine gültige IP-Adresse zugewiesen wurde und dass es in Ihrem Netzwerk verfügbar ist.



2. Führen Sie folgenden Befehl aus:

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

   Die Konfiguration wird abgeschlossen und die folgende Meldung wird angezeigt.



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

Deaktivieren des DHCP-Servers

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

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

1. Öffnen Sie die Datei *C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Configuration\Appliance.properties*.
2. Ändern Sie die Datei in *DHCP_ENABLE=false*. Die Datei *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

Konfigurieren der IP-Adresse für den vorinstallierten Linux-Sicherungsserver

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

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

1. Öffnen Sie die Datei *C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Configuration\Appliance.properties*.
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.

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

     DHCP_ENABLE=true

     AdapterName=LinuxBkpSvr

     Appliance_IPAddress=192.168.100.1

     Linux_IPAddress=192.168.100.2
3. Speichern Sie die Datei.
4. Löschen Sie die Datei *C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\dhcpdone.flag*.

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

   Hinweis:

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

6. Führen Sie folgenden Befehl über die Befehlseingabeaufforderung aus:

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

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

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

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

Weitere Informationen zum Lastenausgleich zwischen Servern finden Sie unter 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>

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

So überprüfen Sie den Netzwerkstatus auf der Appliance

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

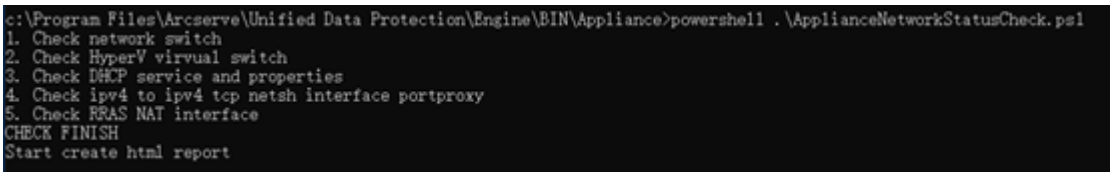
Das Tool ApplianceNetworkStatusCheck.ps1 ist in Arcserve Appliance Server UDP V7.0 Update1 verfügbar.

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

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

   C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance
3. Führen Sie ApplianceNetworkStatusCheck.ps1 aus, um einen Bericht zu generieren:

   #Powershell.\ ApplianceNetworkStatusCheck.ps1

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

Kapitel 11: Sicherheitsmaßnahmen

Dieser Abschnitt enthält folgende Themen:

Allgemeine Sicherheitsmaßnahmen

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

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

  A급 기기 (업 무 용 방 송 통 신 기 자 재)

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

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

- Überprüfen Sie den Kasten, in dem die Appliance ausgeliefert wurde, und stellen Sie sicher, dass keine sichtbaren Anzeichen von Beschädigungen zu erkennen sind. Wenn Beschädigungen erkennbar sind, bewahren Sie das gesamte Verpackungsmaterial auf und wenden Sie sich sofort an den Arcserve-Support unter https://www.arcserve.com/support.
- Suchen Sie einen geeigneten Aufstellungsort für das Rackelement, in dem die Appliance installiert wird. Er sollte sich in einem sauberen, staubfreien Bereich befinden, der gut gelüftet und aufgeräumt ist. Vermeiden Sie Bereiche, in denen Wärme, Elektrorauschen oder elektromagnetische Felder generiert werden.
- Das Rack muss auch in der 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 von der Appliance entfernt werden, auf einem Tisch, damit Sie nicht versehentlich auf die Komponenten treten.
- Tragen Sie während der Arbeit an der Appliance keine losen Kleidungsstücke wie Krawatten oder Ärmel ohne Knöpfe, die mit elektrischen Stromkreisen in Kontakt kommen oder in einen Lüfter gezogen werden können.
- Entfernen Sie jeglichen Schmuck und alle Gegenstände aus Metall vom Körper, da es sich um ausgezeichnete metallische Leiter handelt, die zu Kurzschlüssen führen und Sie verletzen können, wenn Sie in Kontakt mit Leiterplatten (PCBs) oder mit stromführenden Bereichen kommen.
- Nach dem Zugriff auf das Innere der Appliance schließen Sie die Appliance und fixieren sie mit den Halteschrauben am Rack, nachdem Sie sichergestellt haben, dass alle Verbindungen hergestellt wurden.

Sicherheitsmaßnahmen zur Elektrik

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

- Sie müssen die Position des Netzschalters der Appliance sowie die Positionen des Not-Aus-Schalters für den Raum, des Trennschalters und der Steckdose kennen. Bei einem Unfall im Zusammenhang mit der Elektrik können Sie dann die Appliance schnell von der Stromversorgung trennen.
- Arbeiten Sie bei der Arbeit mit Hochspannungskomponenten nicht allein.
- Die Appliance sollte stets von der Stromversorgung getrennt sein, wenn wichtige Systemkomponenten, wie z. B. das Serverboard, Arbeitsspeichermodule, das DVD-ROM-Laufwerk und das Diskettenlaufwerk ausgebaut oder eingebaut werden (nicht erforderlich für hot-swap-fähige Laufwerke). Beim Trennen der Stromversorgung sollten Sie zuerst die Appliance über das Betriebssystem ausschalten und dann die Netzkabel von allen Netzteilmodulen in der Appliance abziehen.
- Beim Arbeiten in der 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-Batterie: **ACHTUNG** – Wenn die interne Batterie falsch herum installiert wird, besteht Explosionsgefahr, da die Pole umgekehrt werden. Diese Batterie darf nur durch eine Batterie des gleichen oder eines ähnlichen Typs, der vom Hersteller empfohlen wird, ersetzt werden. Entsorgen Sie verbrauchte Akkus gemäß den Anweisungen des Herstellers.

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

FCC-Konformität

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

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

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

Vorsichtsmaßnahmen gegen elektrostatische Entladungen (ESD)

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

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

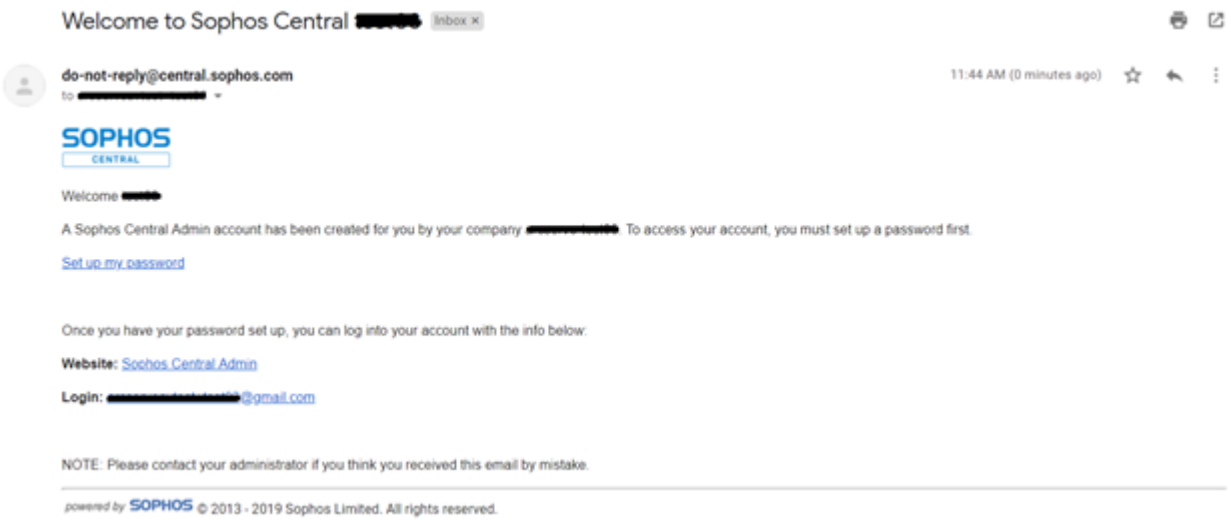
Kapitel 12: Aktivieren von Sophos auf der Arcserve Appliance

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

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

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

   Hinweis: Wenn Sie mehr als ein Kundenkonto beantragen, erhalten Sie die entsprechende Anzahl von Willkommens-E-Mails für jedes Konto separat von Sophos, um das Passwort entsprechend einzurichten.
   Wenn Sie bereits über ein vorhandenes Kundenkonto verfügen und weiterhin dasselbe Kundenkonto verwenden möchten, um einen weiteren Arcserve Appliance Sophos zu aktivieren, erhalten Sie solche Willkommens-E-Mails nicht an die E-Mail-Adresse, die mit diesem Kundenkonto verknüpft ist. Sie erhalten eine E-Mail von Arcserve, die eine Zip-Datei und Anweisungen zum Aktivieren von Sophos enthält.



2. Es stehen zwei Methoden zum Aktivieren von Sophos auf der Arcserve Appliance zur Verfügung.

Hinweis: Um weitere Arcserve Appliance Sophos zu aktivieren, wiederholen Sie die Schritte von Methode 1 bzw. Methode 2 nach Bedarf.

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

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

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

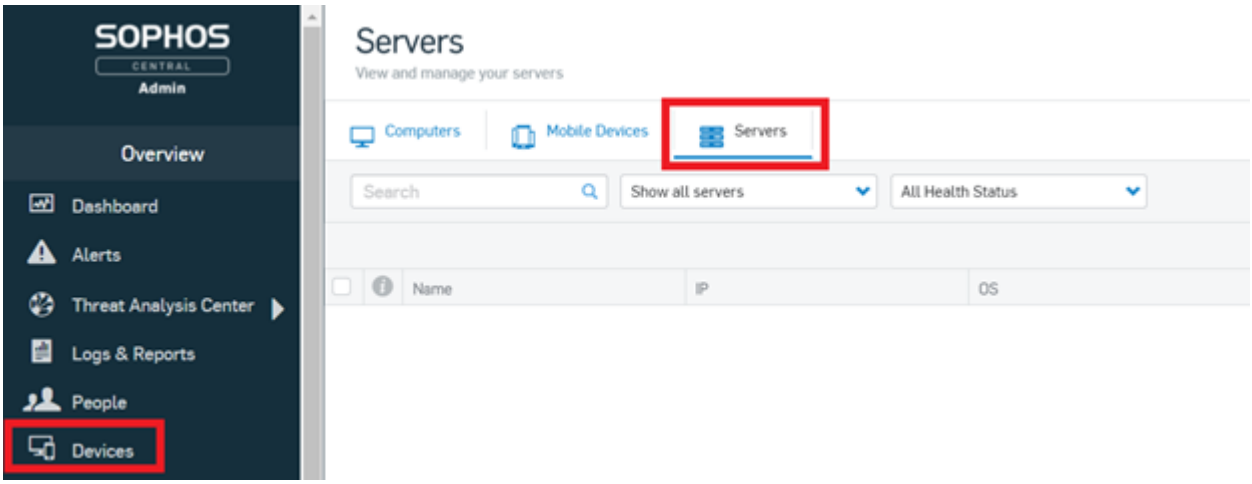
- **Config.xml:** Die Konfigurationsdatei.
- **Registration.txt:** Die Registrierungsdatei.
- **Arcserve_Appliance_Sophos_Activation.ps1:** Powershell-Skript zum Aktivieren von Sophos.

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

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

   #powershell .\ Arcserve_Appliance_Sophos_Activation.ps1
5. Um die geschützte Arcserve Appliance anzuzeigen, melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Kennwort bei der Sophos Central-Seite an, und navigieren Sie dann zu „Geräte > Server“.

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



Sophos wird auf der Appliance aktiviert.

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

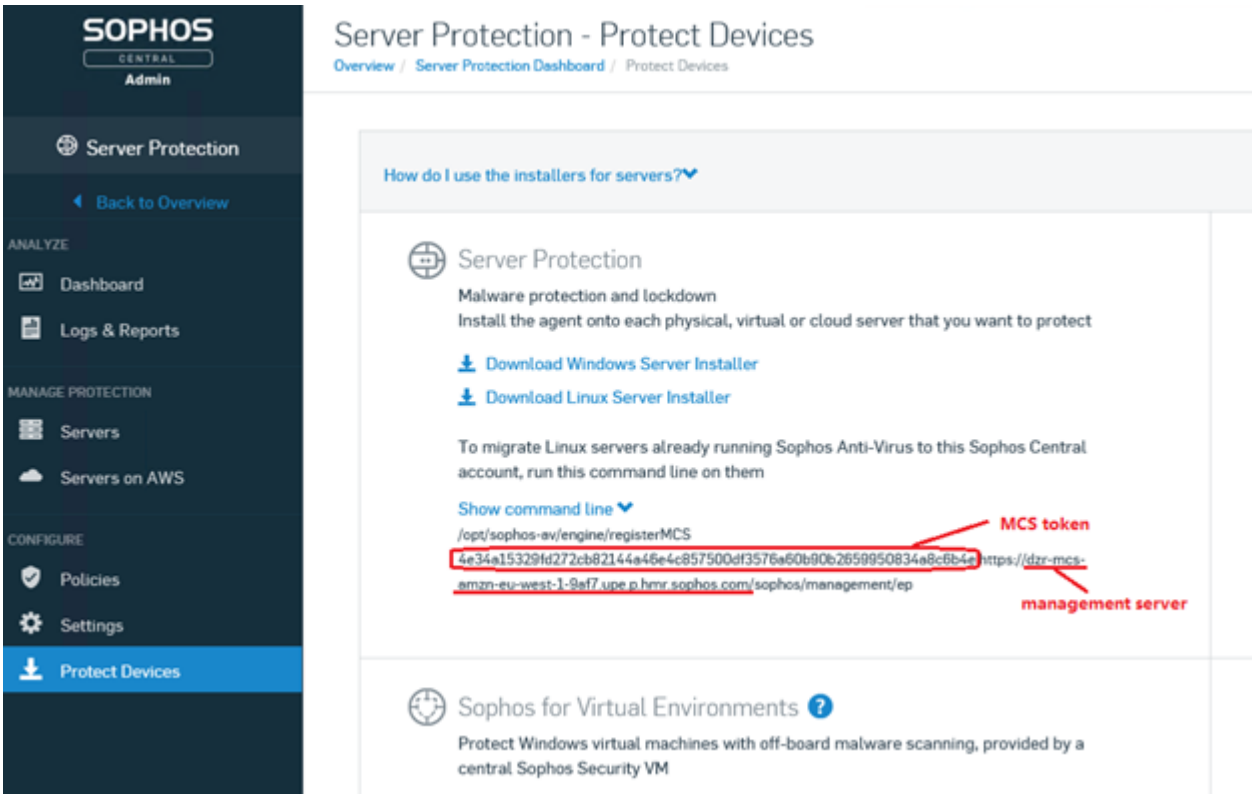
Dieser Abschnitt enthält Informationen zum Aktivieren von Sophos auf der Arcserve Appliance mithilfe des Skripts Customer_Boot.ps1.

Befolgen Sie diese Schritte:

1. Um sich bei der Sophos Central-Seite anzumelden, öffnen Sie https://cloud.sophos.com, und verwenden Sie Ihre E-Mail-Adresse und Ihr Kennwort.

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

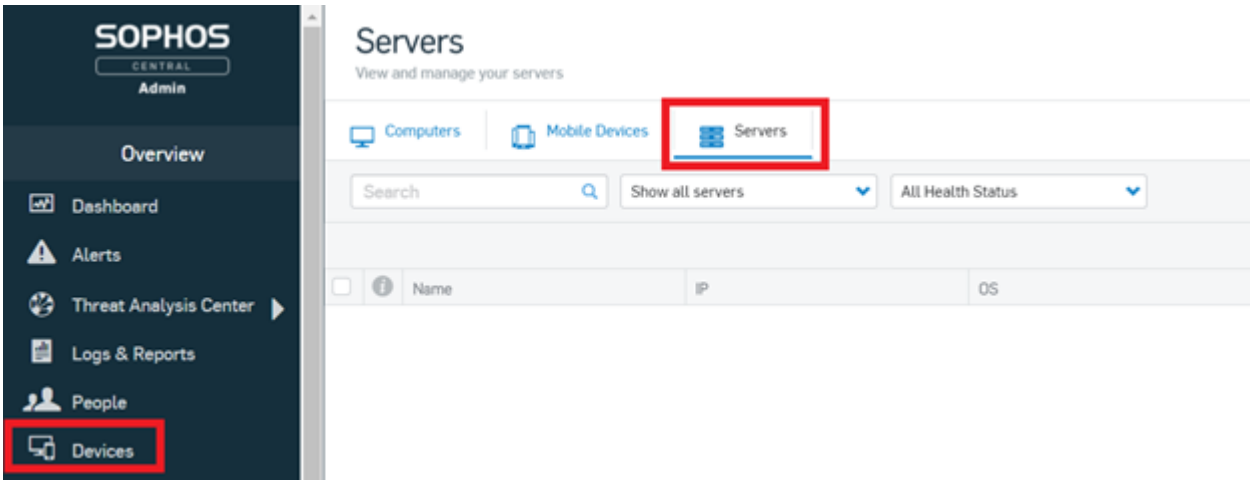
2. Navigieren Sie zur Seite „Schutzgeräte“ unter „Serverschutz“, und klicken Sie auf den Link „Befehlszeile anzeigen“.



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

   #cd “C:\Program Files\Arcserve\Appliance\Sophos\Customer_Boot”
6. Führen Sie Customer_Boot.ps1 aus.

   #powershell .\Customer_Boot.ps1
7. Geben Sie die Werte des MCS-Tokens und des Verwaltungsservers basierend auf der Eingabeaufforderung für die Befehlszeile ein, und warten Sie dann, bis die Befehlsausführung abgeschlossen ist.
8. Um die geschützte Arcserve Appliance anzuzeigen, melden Sie sich bei der Sophos Central-Seite an, und navigieren Sie dann zu „Geräte > Server“.



Sophos wird auf der Appliance aktiviert.

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

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

- Schützt Daten und Systemsicherungen vor Ransomware und anderen Angriffen
- Endpunktschutz, der signaturbasierte und signaturlose Malware-Erkennung kombiniert.
- Tief lernendes neuronales Netzwerk
- Anti-Exploit-Technologie
- CyptoGuard Anti-Ransomware- und WipeGuard-Technologien und mehr, um die breiteste Palette von Endpunktbedrohungen zu stoppen

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

Befolgen Sie diese Schritte:

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

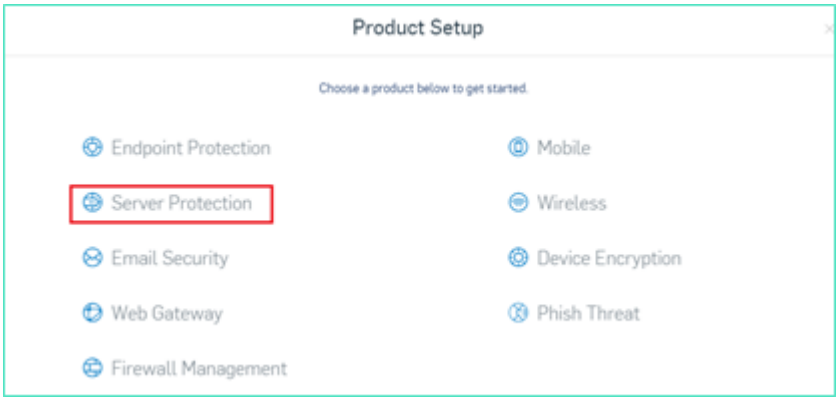
tRequest@Arcserve.com, und fügen Sie alle relevanten Details hinzu. Sie erhalten eine automatisch generierte E-Mail-Bestätigung.

Nachdem Sie Ihre E-Mail-ID bestätigt haben, verarbeitet Arcserve Ihre Anfrage, erstellt ein Konto auf der Sophos Central und sendet eine E-Mail mit Anweisungen zum Erstellen eines Kennworts.

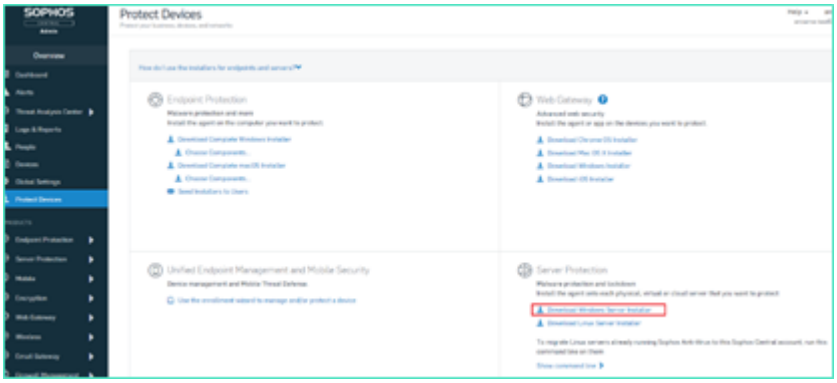
3. Um ein Passwort für Ihr neues Konto auf Sophos Central zu erstellen, folgen Sie den Anweisungen in der E-Mail.
4. Melden Sie sich bei Arcserve Appliances als Administrator oder als Benutzer mit lokalen Administratorrechten an.

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

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



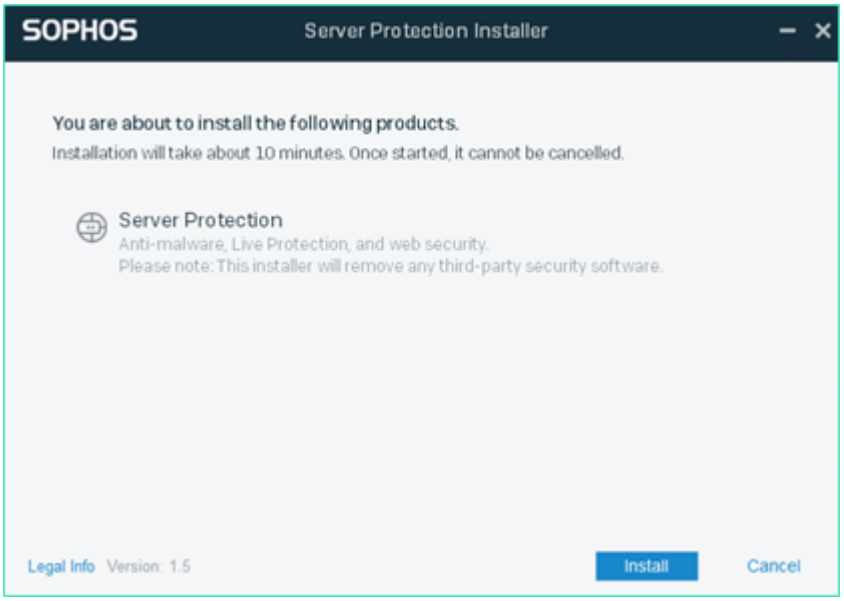
7. Klicken Sie im Abschnitt „Serverschutz“ auf **Windows Server Installer herunterladen**, und speichern Sie dann das Installationsprogramm **SophosSetup.exe** in einem Ordner auf der Appliance.



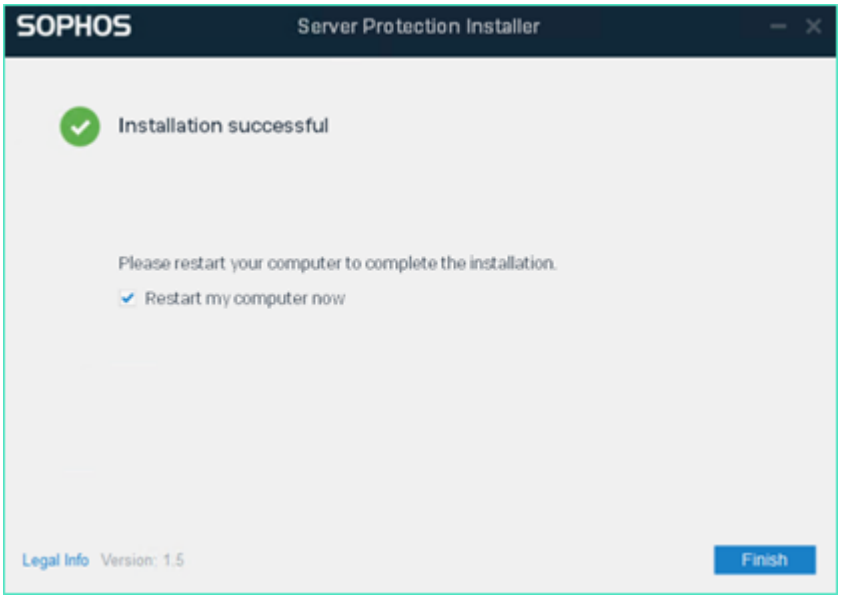
8. Um das Installationsprogramm zu starten, öffnen Sie den Ordner, und doppelklicken Sie dann auf **SophosSetup.exe**.

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

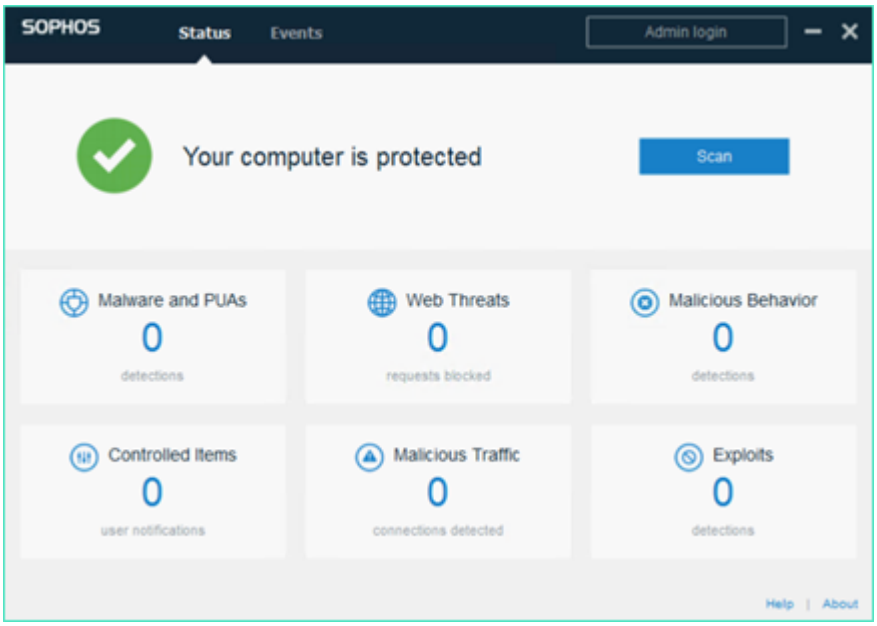
9. Klicken Sie auf **Installieren**.



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



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



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

12. Um auf Sophos Central zuzugreifen, klicken Sie auf **Admin Login**. Es ermöglicht Ihnen, Sophos Intercept X Advanced Server zu verwalten, Warnungen und Richtlinien festzulegen usw.

Hinweise:

- Es ist erforderlich, dass Sie über Internetzugang in der Appliance verfügen, um "Sophos Intercept X Advanced" und alle dazugehörigen Updates zu installieren. Sophos Intercept X ist Cloud-basiert, und es sind keine Offline-Installationsprogramme verfügbar.
- Wenn Sie bereits eine andere Appliance erworben haben und über ein Sophos-Konto über Arcserve verfügen, verwenden Sie dasselbe Konto für alle Arcserve Appliances.
- Wenn Sie bereits ein Sophos-Konto über einen anderen Kauf haben, z. B. direkt von Sophos, geben Sie eine andere E-Mail-Adresse für ein separates Konto bei Sophos Central an.
- Wenn die Sophos-Installation aus irgendeinem Grund fehlschlägt, befolgen Sie die Anweisungen auf dem Bildschirm oder per E-Mail, die zusammen mit der Fehlermeldung bereitgestellt werden.
- Um Updates für Sophos Intercept X Advanced for Server wie Malwaredefinitionsupdates und Versionsaktualisierungen zu erhalten, benötigen Sie eine gültige und aktive Wartung für Ihre Appliance.

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

Kapitel 12: Aktualisieren der Firmware für Arcserve Appliance 9000 Series

Dieser Abschnitt enthält folgende Themen:

Upgrade der BIOS-Firmware für Arcserve Appliance 9000 Series

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

Anzeigen der BIOS-Firmwareversion

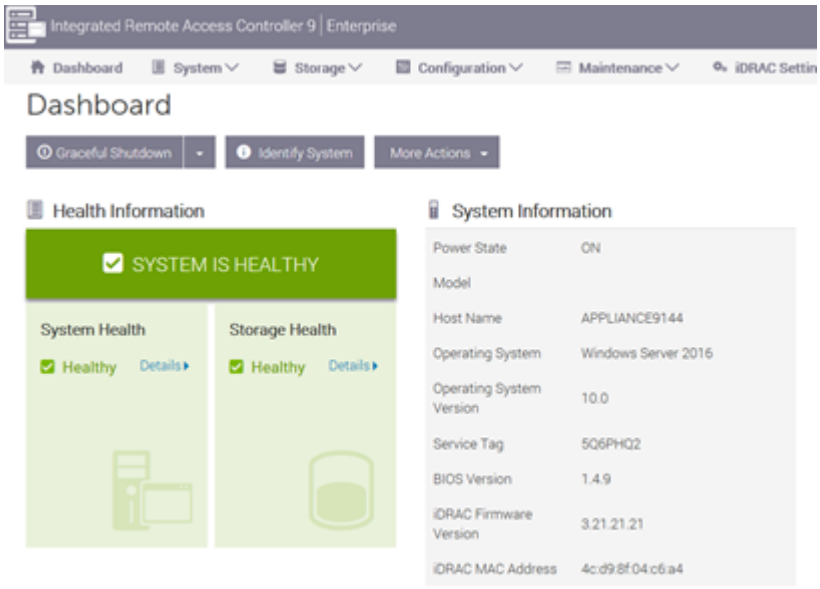
Verwenden Sie eine der folgenden Methoden, um die BIOS-Firmwareversion anzuzeigen:

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

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

Befolgen Sie diese Schritte:

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

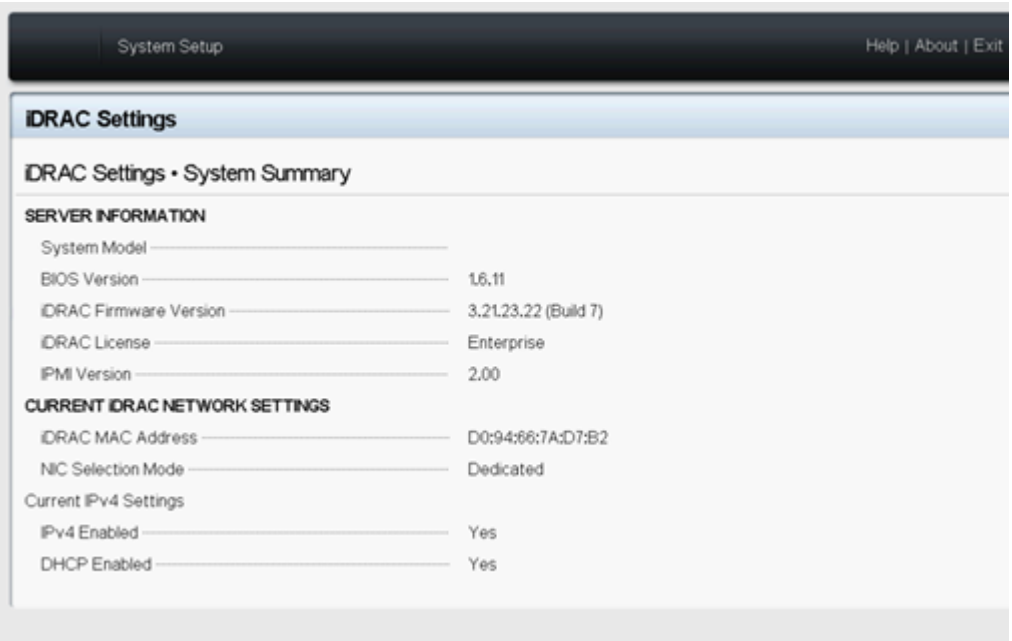


Auf der Seite iDRAC-Dashboard werden die Systeminformationen angezeigt, die die BIOS-Firmwareversion enthalten.

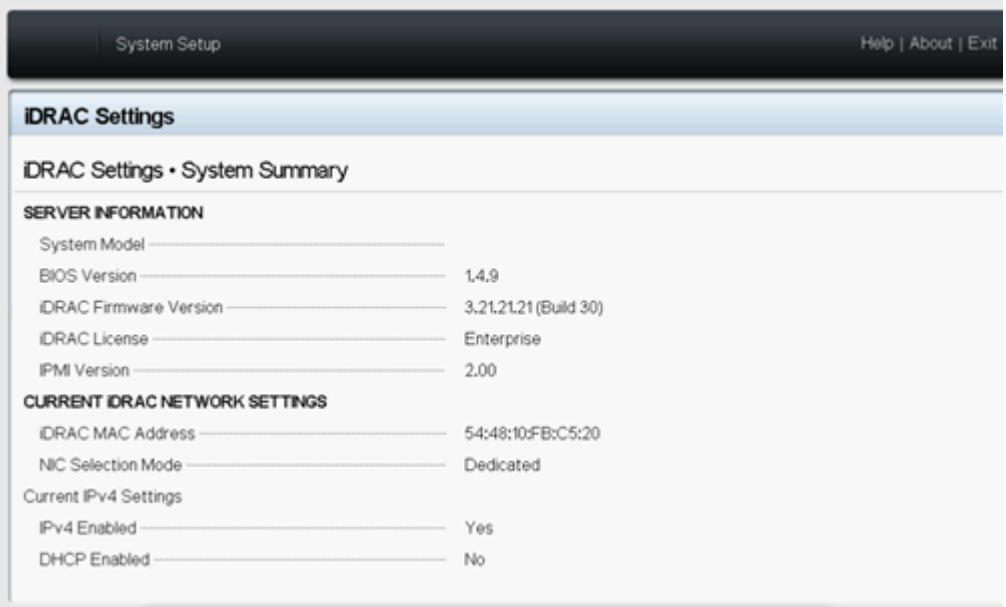
Methode 2: BIOS-Firmware-Version von BIOS Arcserve Appliance 9000 Series anzeigen

Befolgen Sie diese Schritte:

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



Auf der Seite wird die Firmware-Version angezeigt.



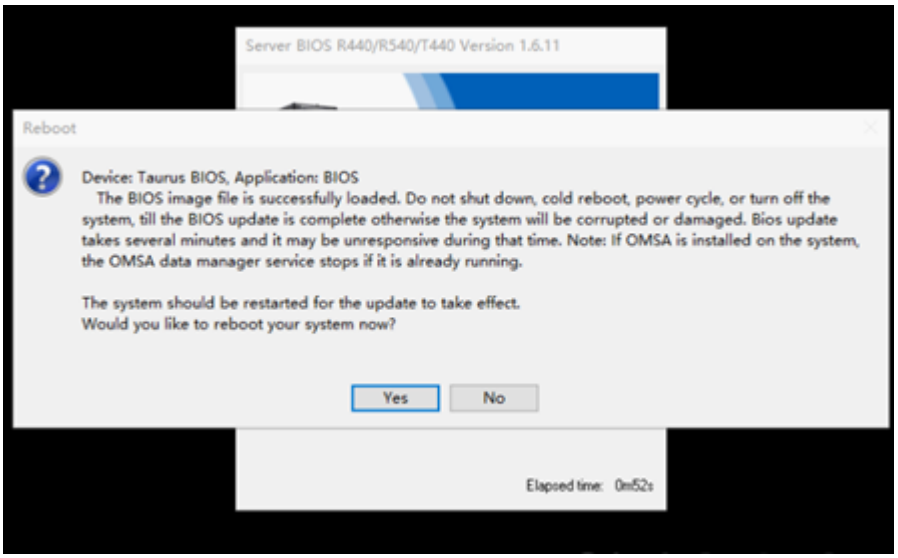
Herunterladen des aktualisierten Pakets für BIOS

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

BIOS aktualisieren

Befolgen Sie diese Schritte:

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



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

Überprüfen des aktualisierten BIOS

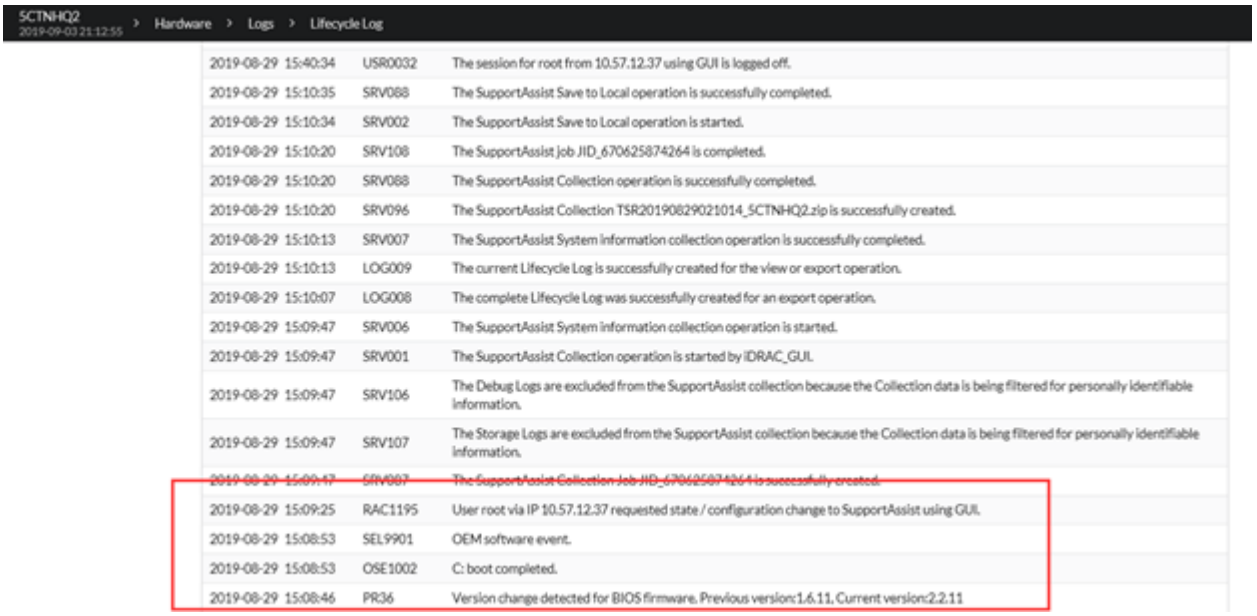
Verwenden Sie eine der folgenden Methoden:

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

Überprüfen des aktualisierten BIOS mithilfe von Systemprotokollen

Befolgen Sie diese Schritte:

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



Überprüfen des aktualisierten BIOS über iDRAC Web Interface oder BIOS

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

Aktualisieren der iDRAC-Firmware für Arcserve Appliance 9000 Series

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

Anzeigen der iDRAC-Firmwareversion

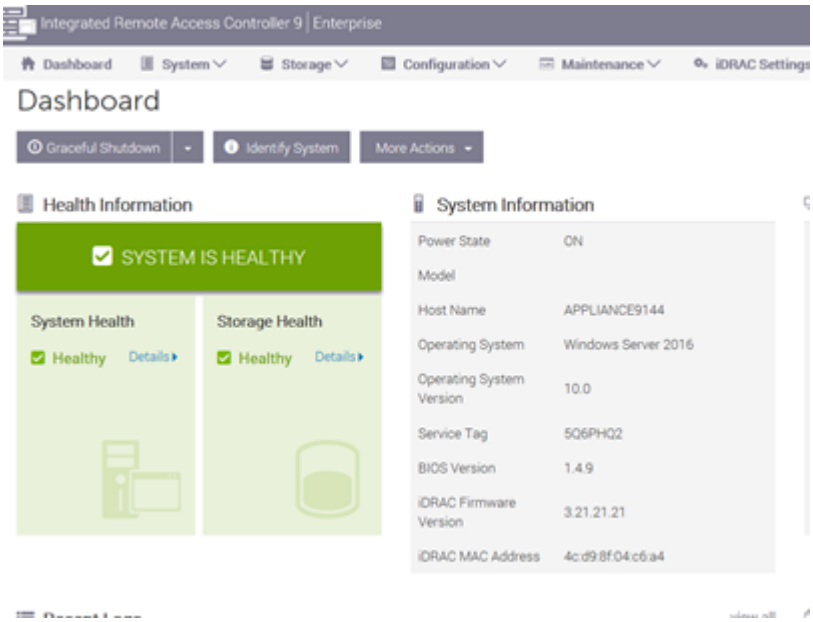
Verwenden Sie eine der folgenden Methoden, um die iDRAC-Firmwareversion anzuzeigen:

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

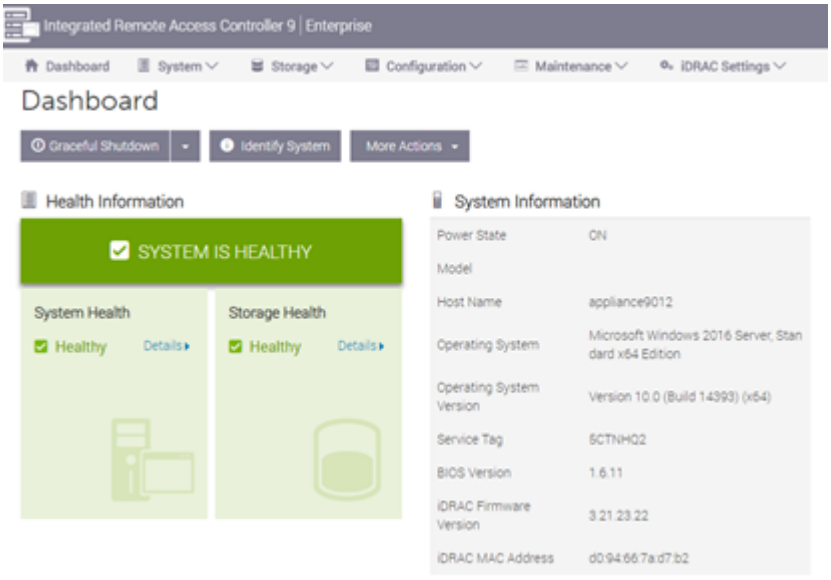
iDRAC-Firmwareversion von iDRAC Web Interface anzeigen

Befolgen Sie diese Schritte:

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



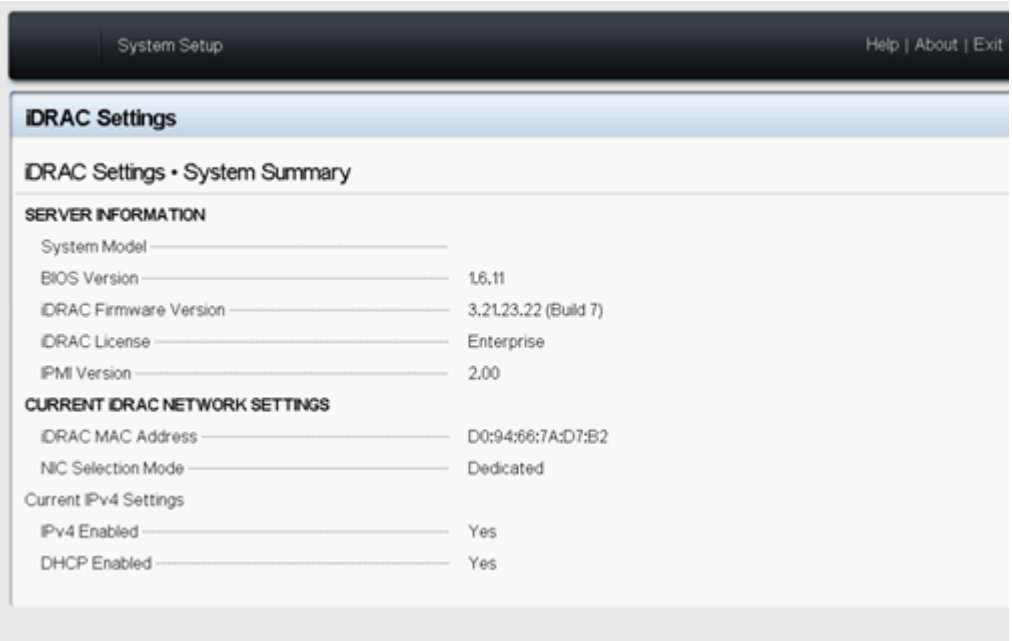
Das iDRAC-Dashboard zeigt die Systeminformationen an, die die iDRAC-Firmwareversion enthalten.



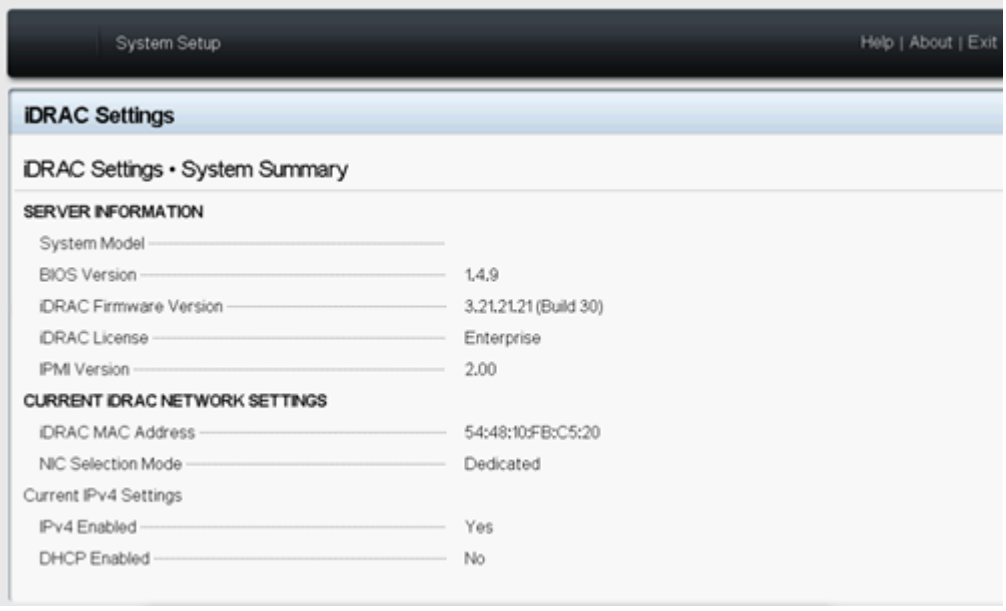
Methode 2: iDRAC-Firmwareversion von BIOS Arcserve Appliance 9000 Series anzeigen

Befolgen Sie diese Schritte:

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



Auf der Seite wird die Firmware-Version angezeigt.



Herunterladen des aktualisierten Pakets für iDRAC

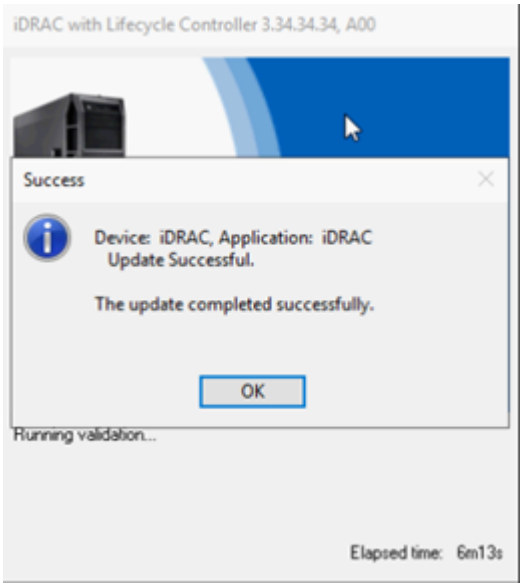
Sie können das neueste iDRAC-Firmwarepaket eines bestimmten Modells der Arcserve Appliance 9000 Series von der Dell-Website herunterladen oder den Arcserve-Support kontaktieren.

iDRAC aktualisieren

Befolgen Sie diese Schritte:

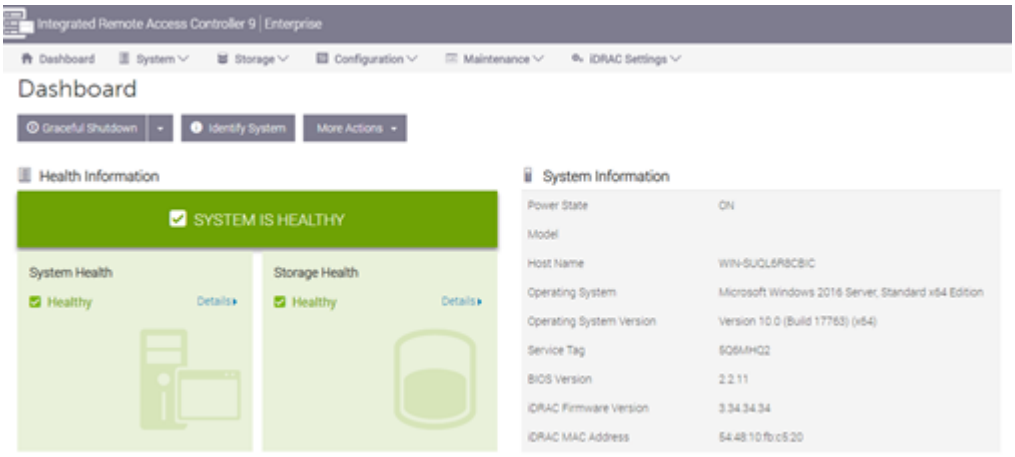
1. Kopieren Sie das Upgradepaket auf den lokalen Datenträger der Arcserve Appliance 9000 Series.
2. Starten Sie das Upgradepaket, und folgen Sie dann den Anweisungen, um das Upgrade abzuschließen.

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



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

jetzt abgeschlossen.



Überprüfen des aktualisierten BIOS

Verwenden Sie eine der folgenden Methoden:

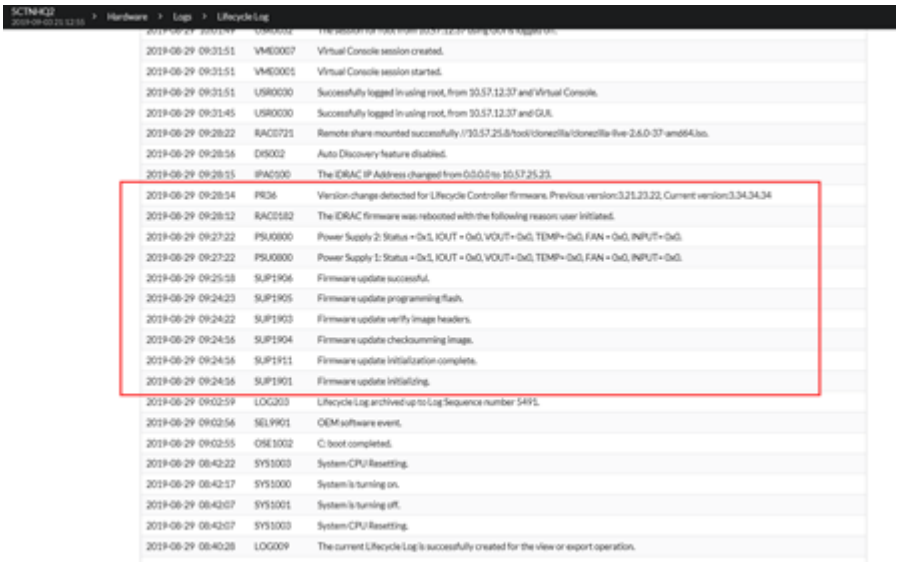
- Überprüfen des aktualisierten iDRAC mithilfe von Systemprotokollen
- Überprüfen des aktualisierten iDRAC von iDRAC Web Interface oder BIOS

Überprüfen des aktualisierten iDRAC mithilfe von Systemprotokollen

Befolgen Sie diese Schritte:

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

Aktualisierungsvorgangs keine Fehler aufgetreten sind.



Überprüfen des aktualisierten iDRAC von iDRAC Web Interface oder BIOS

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

Kapitel 13: Fehlerbehebung

Dieser Abschnitt enthält folgende Themen:

Linux-Sicherungsserver kann über die Konsole keine Verbindung herstellen

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 Arcserve Applianceaus duplizierten Knoten anderer Appliance-Berichte

Problem

Beim Sichern der Appliance B von der Appliance A aus erhalte ich die folgende Fehlermeldung im Aktivitätsprotokoll:

"Die folgenden Knoten sind dupliziert: Appliance_B, Appliance_A. Daher haben sie dieselbe Agenten-ID, was zu unerwarteten Ergebnissen führen kann. Das Problem duplizierter Knoten kann entstehen, wenn der Knoten mit einem anderen Knotennamen (z. B. dem DNS-Namen oder der IP-Adresse) hinzugefügt wurde oder wenn einige Rechner durch Klonen voneinander eingerichtet wurden."

Fall 1: Appliance B wird als RPS zur UDP-Konsole von Appliance A hinzugefügt.

Beispiel: Auf Appliance B können Sie die Appliance mit dem UDP-Assistenten konfigurieren und Folgendes wählen: "Diese Appliance funktioniert als Instanz des Arcserve UDP Recovery Point Server, der von einer anderen Arcserve UDP-Konsole verwaltet wird."

Lösung

1. Halten Sie den Datenspeicher auf dem Appliance-B-Knoten vom RPS-Bereich der UDP-Konsole aus an.
2. 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 Agent-Knoten zur UDP-Konsole von Appliance A hinzugefügt.

Beispiel: Ein Plan schützt Appliance B über eine agentenbasierte Sicherungsaufgabe auf der UDP-Konsole von Appliance A.

1. Melden Sie sich bei Appliance B an, und löschen Sie den Registrierungsschlüssel der Knoten-ID, die sich unter [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve Unified Data Protection\Engine] befindet.
2. Starten Sie den Arcserve UDP Agent-Dienst von Appliance B aus neu.
3. Gehen Sie in der UDP-Konsole zum Bereich "Knoten", "Alle Knoten", und aktualisieren Sie den Knoten von Appliance B aus.

Linux-Sicherungsserver kann nicht mit einem Knoten im Netzwerk kommunizieren

Problem

Linux-Sicherungsserver kann nicht mit einem Knoten im Netzwerk kommunizieren

Lösung

Wenn der Appliance-Windows-Server nicht mit einem Knoten im Netzwerk kommunizieren kann, kann der Linux-Sicherungsserver auch nicht mit einem Knoten kommunizieren.

Befolgen Sie diese Schritte:

1. Überprüfen Sie, ob der Knoten vom Appliance-Windows-Server aus verfügbar ist.
2. Navigieren Sie zu folgendem Speicherort, um zu überprüfen, ob der Netzwerkadapter LinuxBkpSvr vorhanden ist, wie im Folgenden dargestellt:

   ```
   Bedienfeld > Netzwerk und Internet > Netzwerkverbindungen
   ```

3. Wenn LinuxBkpSvr nicht verfügbar ist, navigieren Sie zum folgenden Speicherort, und überprüfen Sie, ob die Flag-Datei adapterNameChanged.flag vorhanden ist:

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

   Falls vorhanden, entfernen Sie die Datei adapterNameChanged.flag.

4. Navigieren Sie zum folgenden Speicherort, und starten Sie Routing und RAS-Management:

   ```
   Server-Manager > Tools > Routing und Remote-Zugriff
   ```

5. Überprüfen Sie, ob alle verfügbaren Netzwerkschnittstellen und LinuxBkpSvr zum NAT hinzugefügt werden, wie im Folgenden dargestellt.

   Wenn alle Netzwerkschnittstellen und LinuxBkpSvr bereits aufgelistet sind, überprüfen Sie, ob die verschiedenen physischen Netzwerkschnittstellen mit anderen Sub-Netzwerk verbunden sind. Diese Aktion löst das Kommunikationsproblem des Linux-Sicherungsservers.

   Wenn alle Netzwerkschnittstellen und *LinuxBkpSvr* aufgeführt sind, fahren Sie mit dem nächsten Schritt fort.

6. Löschen Sie die Datei *dhcpdone.flag* von folgendem Speicherort:

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

7. Geben Sie mithilfe der Befehlszeile den Ordner *c:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance* ein, und führen Sie resetdhcp.ps1 (siehe unten) aus.

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

   Wenn das Skript erfolgreich ausgeführt wird, wird das Kommunikationsproblem für den Linux-Sicherungsserver gelöst.

Linux-Sicherungsserver kann das Netzwerk-DNS-Suffix nicht abrufen

Wenn Sie die statische IP-Adresse auf den Appliance-Server festlegen, kann nach dem Neustart des Netzwerkdiensts das Netzwerk-DNS-Suffix nicht ordnungsgemäß vom Linux-Sicherungsserver abgerufen werden. Dies führt zu Kommunikationsproblemen zwischen dem Linux-Sicherungsserver und der UDP-Konsole. Sie können dann aufgrund der Kommunikationsprobleme diesen Linux-Sicherungsserver nicht mehr verwenden, um den Linux-Knoten zu schützen.

Problem

Der Status des Linux-Sicherungsservers wird auf der UDP-Konsole als getrennt angezeigt. Der **Aktualisierungsknoten** kann den Linux-Sicherungsserver nicht erfolgreich aktualisieren, und das gelbe Warnsymbol ändert sich nicht in Grün. Dies tritt auf, wenn die statische IP-Adresse auf den Appliance-Server festgelegt ist, aufgrund dessen der Linux-Sicherungsserver dann das DNS-Netzwerksuffix nicht ordnungsgemäß abrufen kann.

Lösung

Um dieses Problem zu lösen, können Sie die Datei "file/etc/resolv.conf" direkt auf dem Linux-Rechner mit dem richtigen DNS-Suffix aktualisieren.

Standardzeitzone auf der Appliance

Problem

Die Standardzeitzone ist (UTC-08:00) Pacific Time (USA und Kanada), unabhängig davon, welche Region Sie auswählen, wenn Sie die Appliance erstmalig in Betrieb nehmen.

Lösung

Navigieren Sie zum **Arcserve Backup Appliance-Assistenten**, klicken Sie auf **Bearbeiten**, und legen Sie **Datum und Uhrzeit** fest, um die Zeitzone zu ändern.

Lizenzfehler, auch wenn Lizenzen verfügbar sind

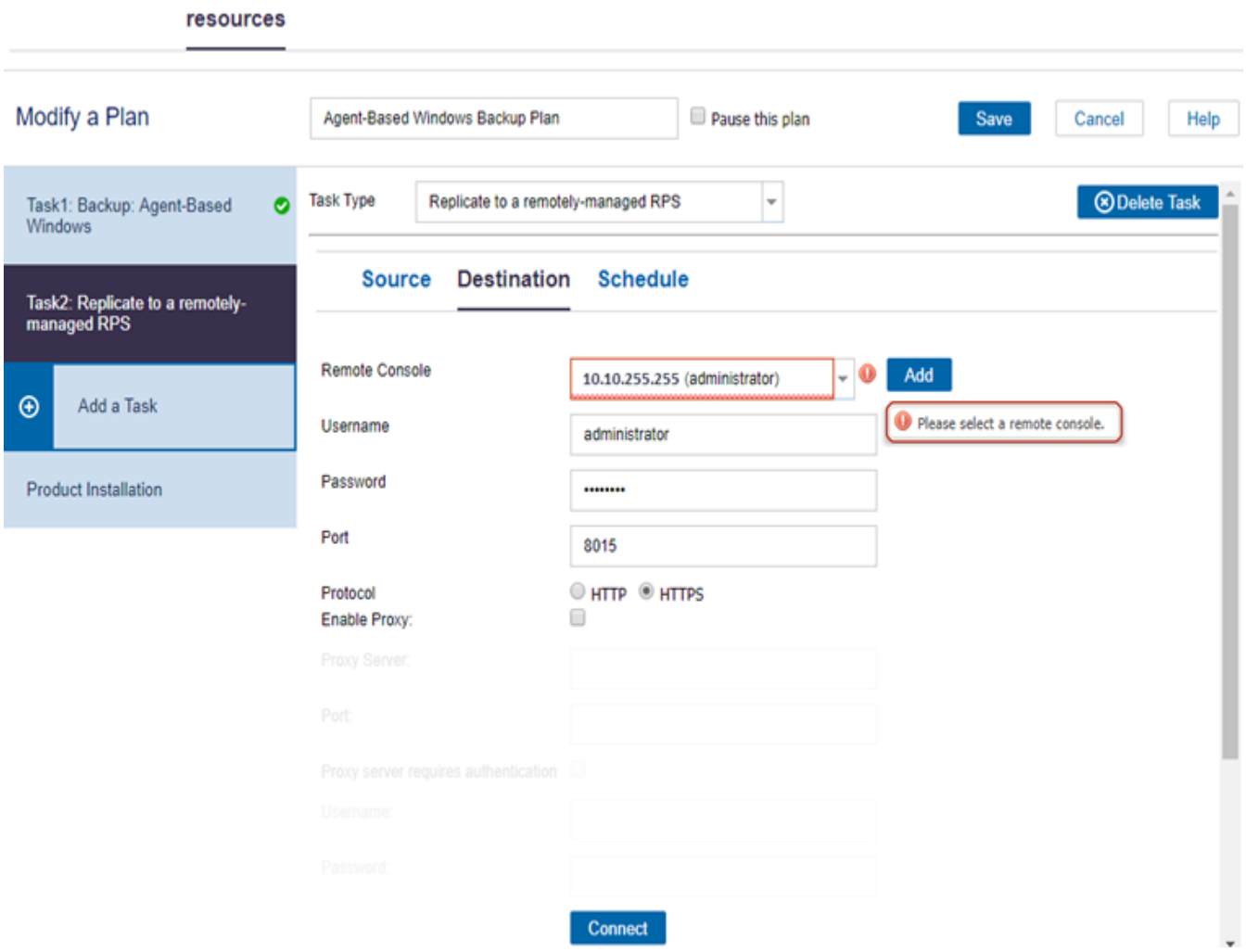
Weitere Informationen zu lizenzbezogenen Fehlern in der Appliance bei verfügbaren Lizenzen finden Sie über den Link.

ARCserve UDP-Konsole zeigt beim Hinzufügen einer replizierten Remote-Konsole zu einer remote verwalteten RPS-Task einen Fehler an

Wenn Sie bei Arcserve UDP-Appliance v6.5 Update1 einen Task *Zu einem remote verwalteten RPS replizieren* hinzufügen und den Hostnamen/die IP eines anderen Appliance-Rechners als Recovery Point Server (RPS) in das Feld *Remote-Konsole* eingeben, wird folgende Fehlermeldung in der Arcserve UDP-Konsole angezeigt.

Hinweis: Dieser Fehler wird in einerArcserve Appliance mit der Standardversion Arcserve UDP v6.5 Update 3 oder höher behoben.

Fehlermeldung: *Wählen Sie eine Remote-Konsole aus.*



Dieses Problem entsteht durch die Verwendung derselben GUID auf der lokalen und der Remote-Konsole.

Gehen Sie folgendermaßen vor, um den remote verwalteten RPS-Task auf einer anderen Appliance zu unterstützen:

1. Löschen Sie die GUID auf der lokalen Appliance aus dem folgenden Registrierungspfad:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Management\Console\GUID

2. Löschen Sie die GUID aus der Datenbank mithilfe der folgenden Befehle in PowerShell:

```
$database = 'arcserveUDP'
$server = 'localhost\arcserve_app'
$sqlconn = New-Object System.Data.SqlClient.SqlConnection
$sqlconn.ConnectionString = "Data Source=$server;Initial Catalog=$database;Integrated Security=SSPI;"
$sqlconn.Open()
$sqlcmd = New-Object System.Data.SqlClient.SqlCommand
$sqlcmd.Connection = $sqlconn
$sqlcmd.CommandText = "delete from as_edge_configuration where ParamKey='ConsoleUuid'"
$sqlcmd.ExecuteNonQuery()
$sqlconn.Close()
```

3. Starten Sie den UDP Management Service auf dem lokalen Appliance-Rechner.

4. Führen Sie die folgenden Schritte in der UDP-Konsole des lokalen Rechners aus:

   a. Wählen Sie **Alle Knoten** in der Knotenansicht.

   b. Klicken Sie mit der rechten Maustaste, und klicken Sie auf **Aktualisieren**.

   c. Klicken Sie auf **OK**, um alle Knoten zu aktualisieren.

5. Wählen Sie alle RPS-Knoten in der Ansicht "Recovery Point Servers" aus, klicken Sie mit der rechten Maustaste, und klicken Sie auf **Aktualisieren**, um alle RPS-Knoten zu aktualisieren.

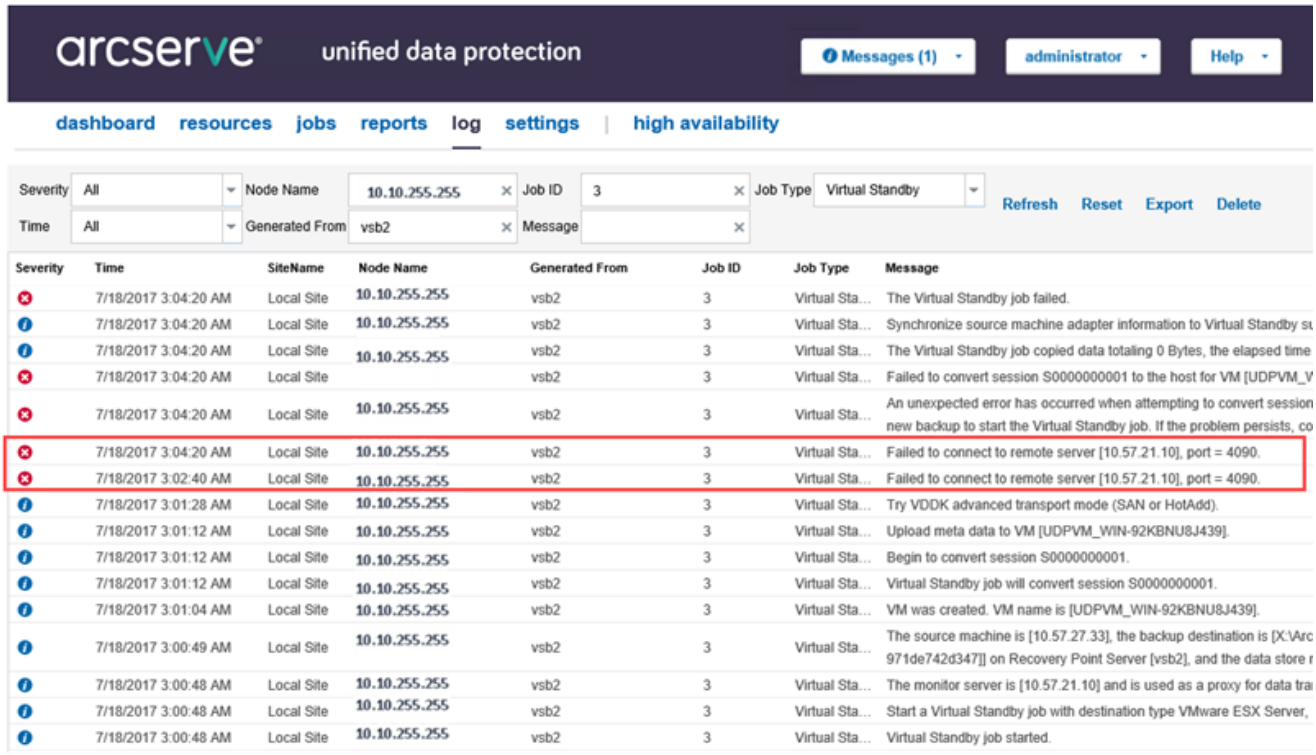
Der Task *Zu einem remote verwalteten RPS replizieren* wird zwischen zwei Appliance-Rechnern erfolgreich unterstützt.

Die VSB-Task kann nicht mit einer anderen Appliance als Überwachungsserver durchgeführt werden

Wenn Sie auf Arcserve Appliance v6.5 Update1 einen VSB-Task durchführen und eine andere Appliance als Monitor verwenden, schlägt der VSB-Task fehl, und im Aktivitätsprotokoll wird die folgende Fehlermeldung angezeigt.

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

Fehlermeldung: *Verbindung zum Remote-Server fehlgeschlagen [IP], port = 4090.*



Dieses Problem entsteht dadurch, dass dieselbe GUID sowohl auf der Monitor-Appliance als auch auf dem Arcserve UDP-RPS-Appliance-Rechner vorhanden ist.

Gehen Sie folgendermaßen vor, um den VSB Task zu unterstützen:

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

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

2. Löschen Sie die GUID auf der lokalen Appliance mit dem folgenden Registrierungspfad:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\GUID

3. Starten Sie alle UDP-Dienste auf Arcserve UDP-RPS-Appliance mit dem folgenden Befehl in der Befehlszeile:

   C:\Program Files\Arcserve\Unified Data Protection\Management\BIN> cmdutil.exe /startall

4. Gehen Sie von der UDP-Konsole des lokalen Rechners aus folgendermaßen vor:

   a. Wählen Sie in der Pläneansicht die Option *Alle Pläne* aus.

   b. Klicken Sie mit der rechten Maustaste, und klicken Sie auf **Jetzt bereitstellen**.

   c. Klicken Sie auf **OK**, um alle Pläne bereitzustellen.

Die Aufgabe "Virtual Standby" wird jetzt unterstützt.

Kapitel 14: Best Practices

In diesem Abschnitt werden die folgenden Themen behandelt:

Best Practices für die Netzwerkkonfiguration

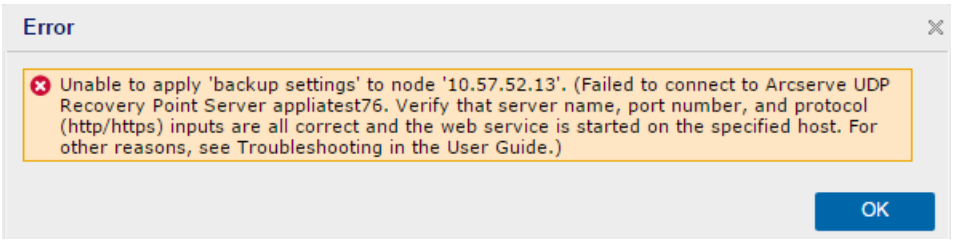
- Wenn mehrere Netzwerkschnittstellen in der Produktionsumgebung verbunden sind, stellen Sie sicher, dass die einzelnen Netzwerkadapter mit unterschiedlichen Subnetzwerken verbunden sind.
- Wenn in der zu schützenden Produktionsumgebung kein Linux-Knoten vorhanden ist, empfehlen wir, VM Linux-BackupSvr, den DHCP-Server-Dienst und den RRAS auf der Appliance anzuhalten.

  Weitere Informationen finden Sie unter Deaktivieren des DHCP-Servers.
- Wenn sowohl der Appliance als auch die Agent-Knoten auf dem gleichen Subnetzwerk online sind, tritt ein Verbindungsproblem zwischen der Appliance und einen Agent-Knoten auf, wenn mehrere Netzwerkschnittstellen mit dem gleichen Subnetzwerk in der Appliance verbunden sind.

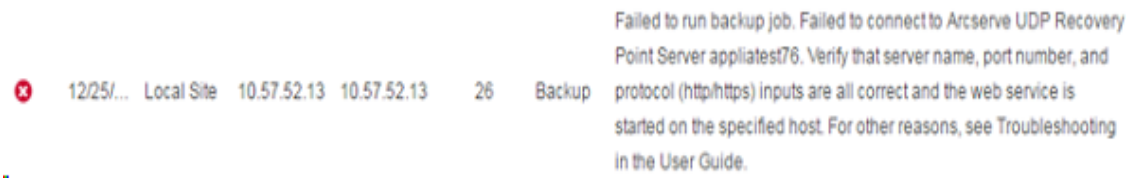
  Problem

  Wenn die Appliance und die Agent-Knoten auf dem gleichen Subnetzwerk online sind, können die folgenden Symptome auftreten:

  - In der Arcserve UDP-Konsole wird bei der Bereitstellung des Plans 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:\Windows\system32>ping 10.57.52.13

Pinging 10.57.52.13 with 32 bytes of data:
Reply from 10.57.52.13: bytes=32 time<1ms TTL=127
Reply from 10.57.52.13: bytes=32 time=1ms TTL=127
Reply from 10.57.52.13: bytes=32 time<1ms TTL=127
Reply from 10.57.52.13: bytes=32 time<1ms TTL=127
```

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

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

Pinging appliatest76 [10.57.52.47] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.57.52.47:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Lösung

Um das Verbindungsproblem zwischen der Appliance und dem Agent-Knoten zu beheben, führen Sie einen der folgenden Schritte aus:

- Wenn kein Linux-Knoten in der Produktionsumgebung verfügbar ist, halten Sie den DHCP-Server-Dienst und RRAS-Dienst auf der Appliance an, und überprüfen Sie, ob das Problem behoben wurde.

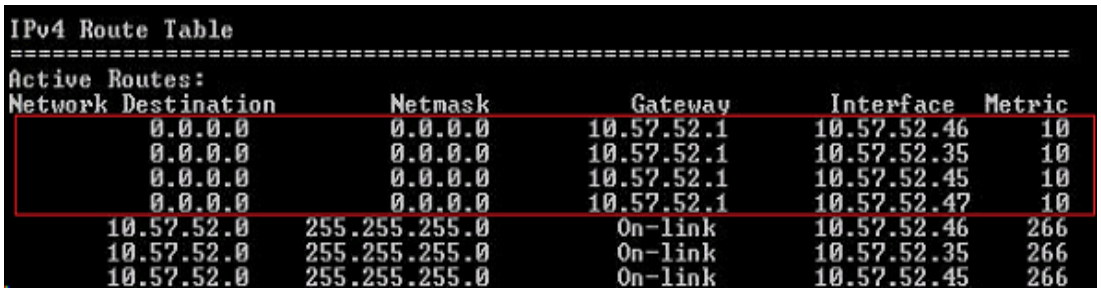
  Weitere Informationen finden Sie unter Deaktivieren des DHCP-Servers.

- Gehen Sie auf der Appliance und auf dem Agent-Knoten folgendermaßen vor:

  Schritte auf der Appliance:

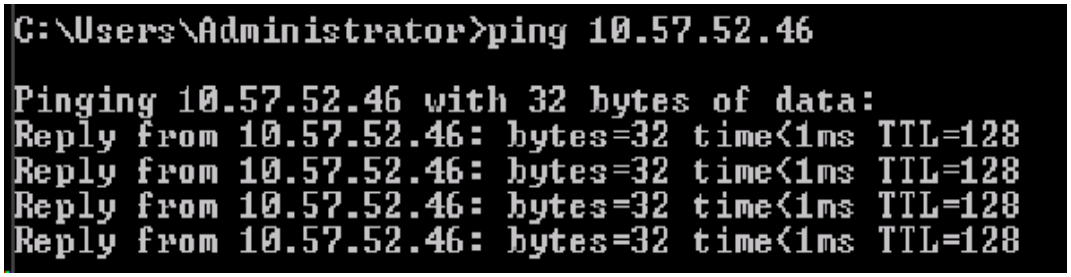
  1. Führen Sie *ipconfig /all* in der DOS-Befehlseingabeaufforderung aus, um die verfügbaren IPv4-Adressen auf der Appliance zu erhalten:
  2. Führen Sie *Route Print* in der DOS-Befehlseingabeaufforderung aus, um die IPv4-Routentabelle abzurufen, und zeichnen Sie die Reihenfolge für alle verfügbaren IPv4-Adressen auf der App-

liance auf:



Schritte auf dem Agent-Knoten:

1. 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:



2. Ändern Sie die Datei *C:\Windows\System32\drivers\etc\hosts*, um einen Datensatz für das Paar *oben abgerufene IPv4/Appliance-Hostname* hinzuzufügen und die Datei zu speichern.

Best Practices für Windows-Defender mit PowerShell-cmdlets

Sie können die Defender-cmdlets mithilfe der folgenden Befehle abrufen:

- *PS C:\> (Get-MpPreference).ExclusionPath*

  Ruft den Ausschlusspfad von Defender ab.

- *PS C:\> (Get-MpPreference).ExclusionProcess*

  Ruft Ausschlussprozesse von Defender ab.

- *PS C:\> Add-MpPreference –ExclusionPath "full_path_of_the_folder_or_file"*

  Ordner oder Dateien der Ausschlussliste werden ausgeschlossen.

- *PS C:\> Add-MpPreference –ExclusionProcess "full_path_of_executable_programs"*

  Dateien, die durch die Prozesse geöffnet wurden, werden ausgeschlossen.

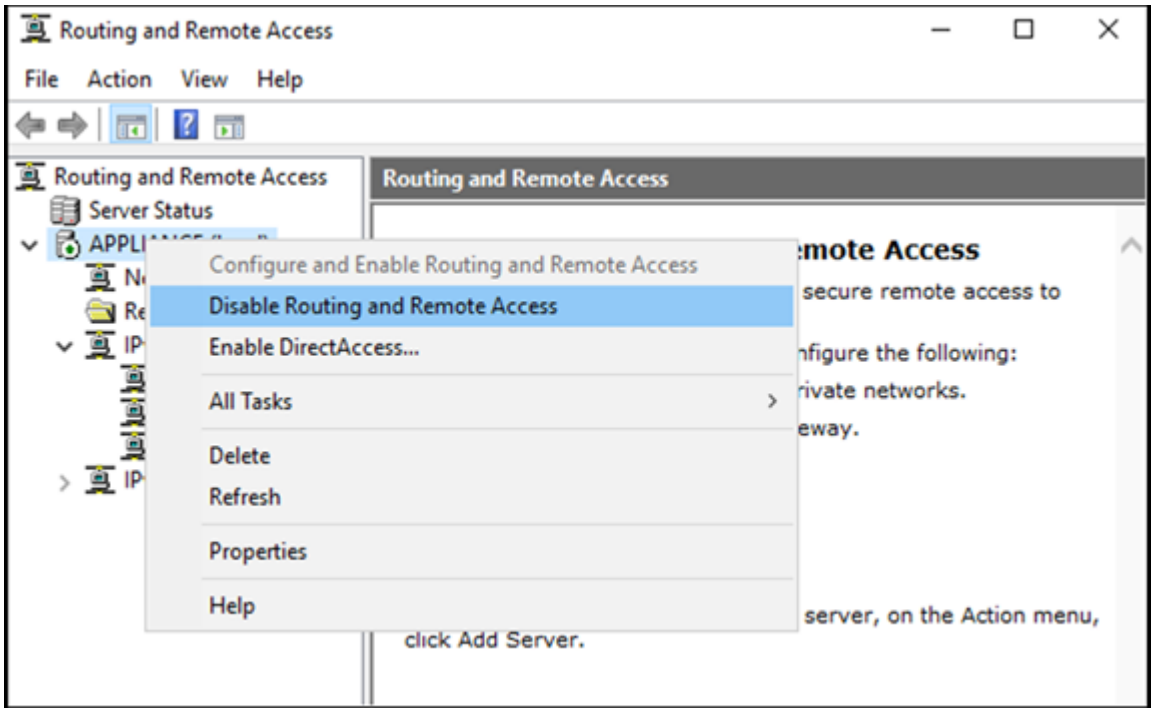
- *PS C:\> Remove-MpPreference –ExclusionPath "full_path_of_the_folder"*

  Entfernt einen Ordner aus der Ausschlussliste.

Konfigurieren des vorinstallierten Linux-Sicherungsservers für externes Netzwerk

Befolgen Sie diese Schritte:

1. Deaktivieren Sie den DHCP-Server. Weitere Informationen finden Sie unter Deaktivieren des DHCP-Servers.
2. Öffnen Sie zum Deaktivieren von RRAS "Routing und RAS", und klicken Sie auf **Routing und RAS deaktivieren**.

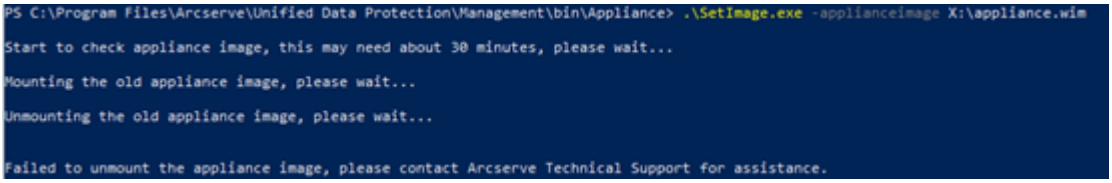


3. Gehen Sie wie folgt vor, um Linux-Sicherungsservernetzwerk auf ein externes Netzwerk festzulegen:
   a. Öffnen Sie den **Hyper-V**-Manager.
   b. Erstellen Sie einen neuen externen virtuellen Netzwerk-Switch.
   c. Ändern Sie die Einstellung des VM-Netzwerkadapters für den Linux-Sicherungsserver, um den neu erstellten externen virtuellen Netzwerk-Switch zu verwenden.
   d. Überprüfen Sie die Netzwerkeinstellung des Linux-Sicherungsservers, und stellen Sie sicher, dass die IP-Adresse und das DNS über den externen virtuellen Netzwerk-Switch abgerufen werden.
   e. Entfernen Sie den ursprünglichen Linux-Sicherungsserver aus der UDP-Konsole.
   f. Fügen Sie den Linux-Sicherungsserver mit Angabe der folgenden Informationen erneut zur UDP-Konsole hinzu:
      - **Hostname:** Linux-BackupSvr
      - **Port:** 8014

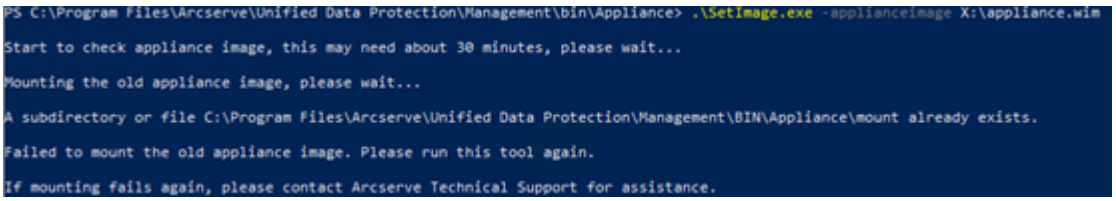
Bewährte Methoden zum Ersetzen des Werkseinstellungs-Image wenn mit Sophos gesichert

Nachdem Sophos aktiviert wurde und auf Arcserve Appliance ausgeführt wurde, können Sie das Werkseinstellungs-Image standardmäßig nicht mit dem Set

Appliance Image Utility ersetzen. Andernfalls schlägt die Ausführung von SetImage.exe fehl, wie in der Abbildung unten gezeigt.

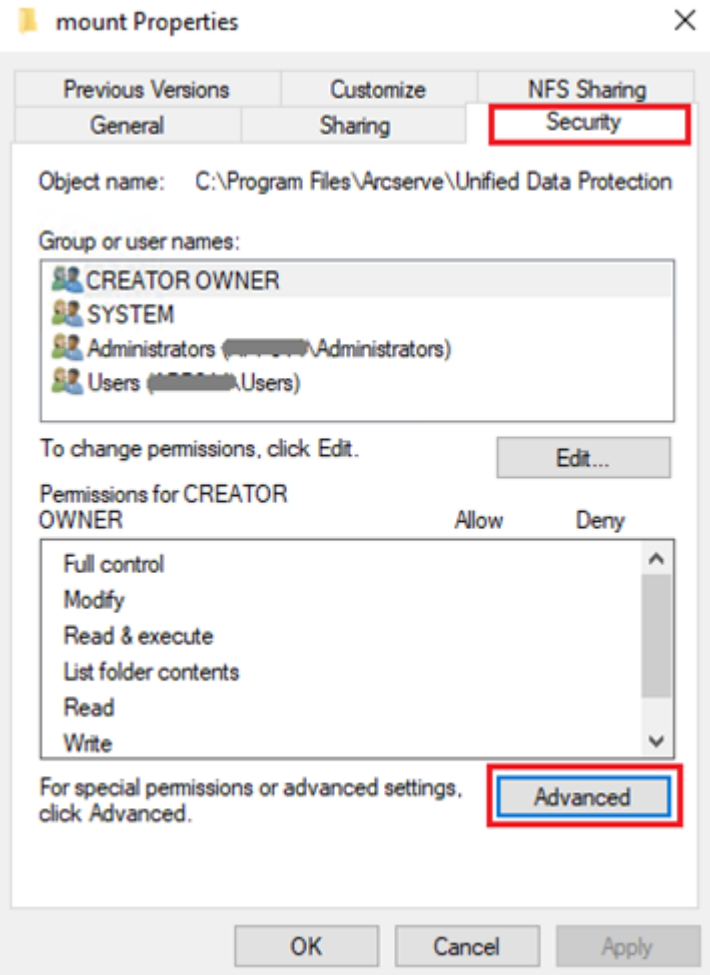


Bevor Sie den Befehl SetImage.exe ausführen, um das Werkseinstellungs-Image zu ersetzen, wenn Sophos auf Arcserve Appliance ausgeführt wird, überprüfen Sie, ob das Image bereits bereitgestellt wurde.
Wie in der Abbildung angegeben, wird die folgende Eingabeaufforderung angezeigt: *Ein Unterverzeichnis oder eine Datei C:\Programmdateien\Arcserve\Unified Data Protection\Management\BIN\Appliance\mount ist bereits vorhanden.*



Führen Sie die folgenden Schritte aus, um die Bereitstellung des Bildes aufzuheben:

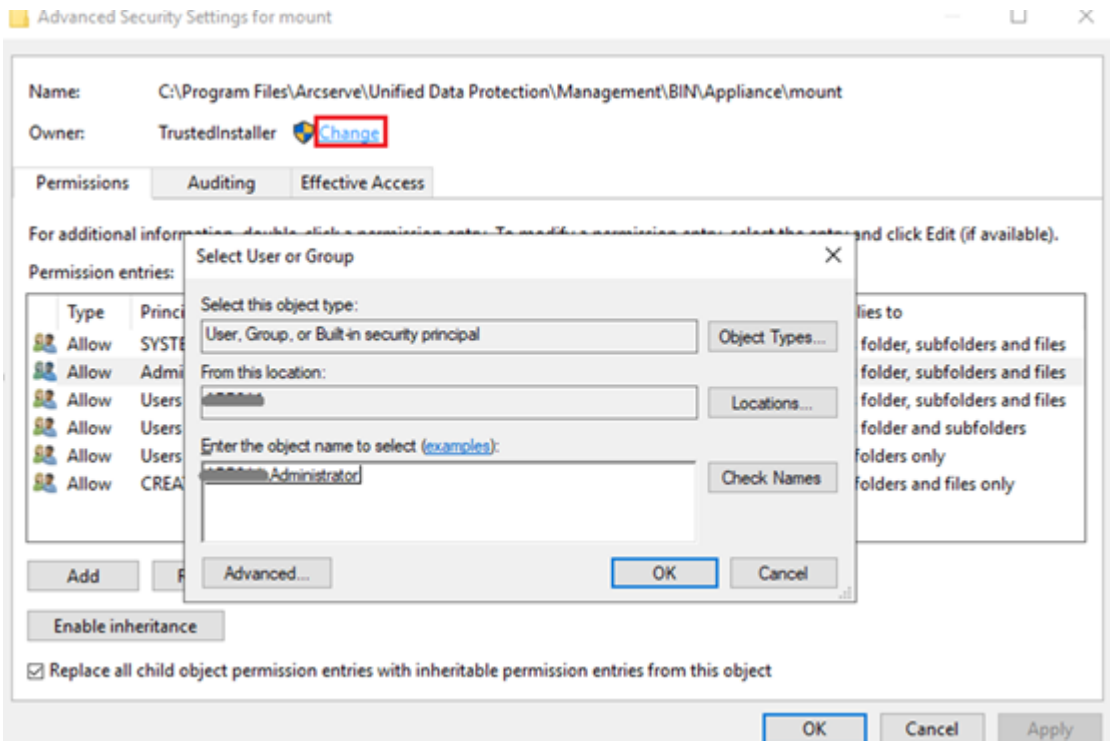
1. Um den Ordner zu suchen, öffnen Sie Windows-Explorer, und wechseln Sie zu C:\Programmdateien\Arcserve\Unified Data Protection\Management\BIN\Appliance\mount. Klicken Sie mit der rechten Maustaste auf den Ordner, und klicken Sie dann auf „Eigenschaften > Registerkarte Sicherheit > Erweitert“.



2. Um den Besitzer des Bereitstellungsordners in einen lokalen Administrator zu ändern, klicken Sie auf den Link **Ändern**.

Aktivieren Sie auf der Seite „Erweiterte Sicherheitseinstellungen“ die folgenden Optionen, um die Kontrolle über die Unterordner innerhalb des Ordners zu übernehmen und die Unterordnerberechtigungen durch die Einstellungen aus dem übergeordneten Ordner zu ersetzen:

- Ersetzen des Besitzes für Untercontainer und Objekt
- Ersetzen Sie alle untergeordneten Objektberechtigungseinträge durch vererbbare Berechtigungseinträge von diesem Objekt



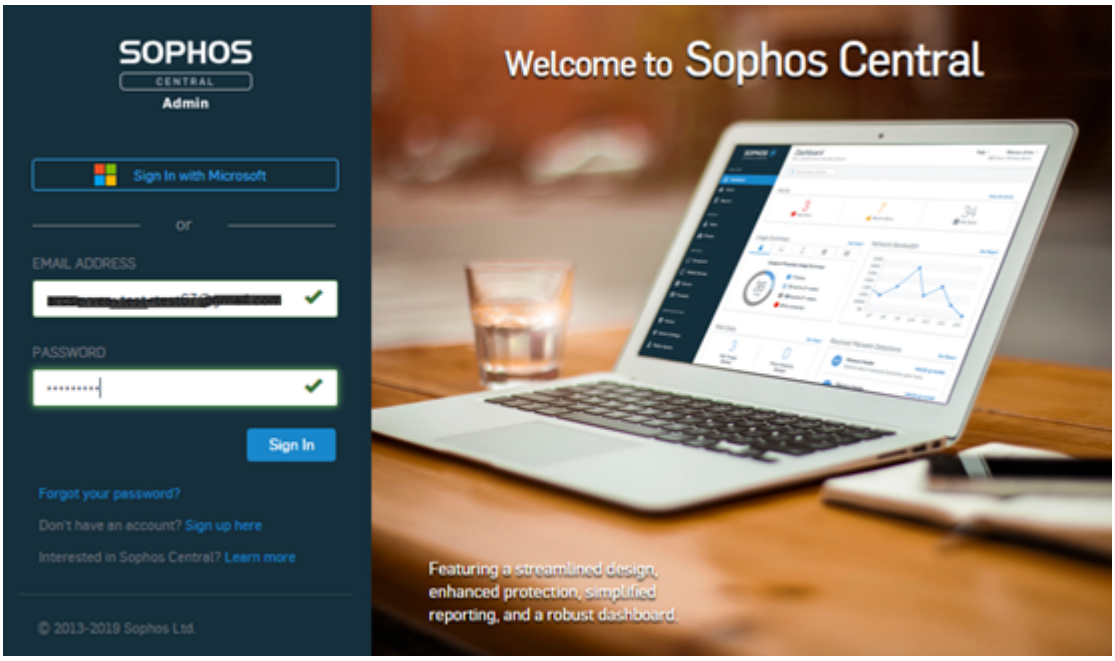
Wenden Sie alle Änderungen an. Stellen Sie für Bereitstellungsordner, Unterordner und Dateien sicher, dass der Besitzer in einen lokalen Administrator geändert wird.

3. Um die Bereitstellung des Bildes aufzuheben, führen Sie den folgenden Befehl mithilfe der Eingabeaufforderung aus:

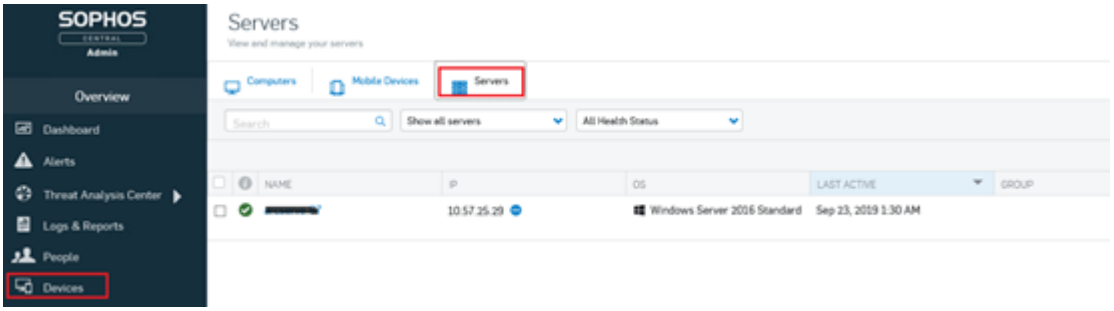
```
C:\>DISM /unmount-image /mountdir:"C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\mount" /discard
```

Führen Sie die folgenden Schritte aus, um den Befehl SetImage.exe auszuführen, um das Werkseinstellungs-Image zu ersetzen, wenn Sophos auf Arcserve Appliance ausgeführt wird:

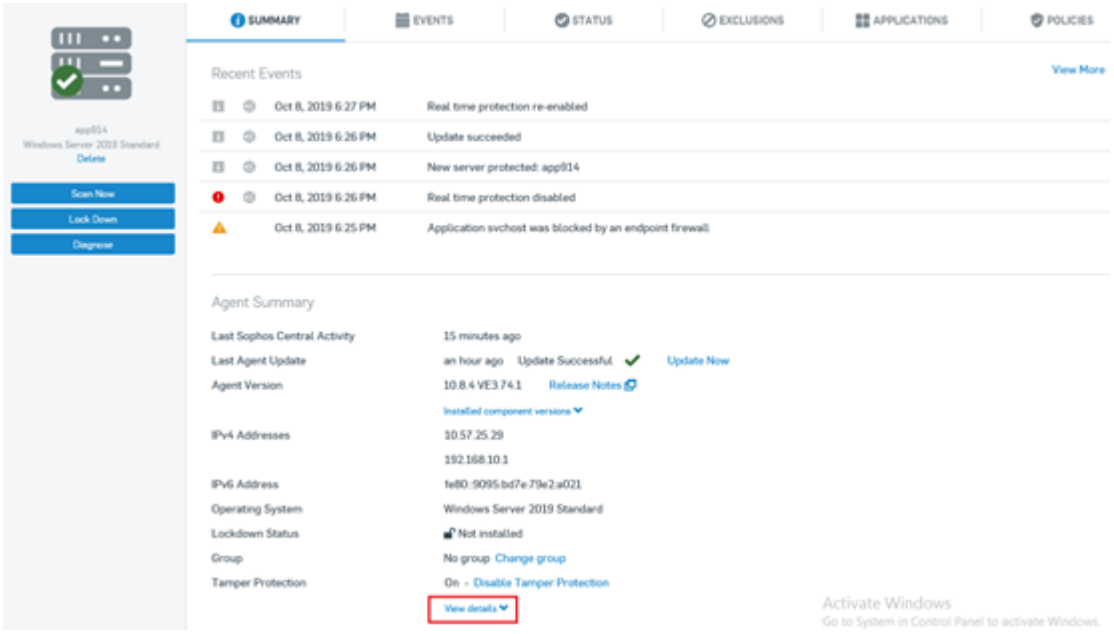
1. Melden Sie sich als Administrator beim Arcserve Appliance-System an. Verwenden Sie Ihre E-Mail-Adresse und Ihr Kennwort, um auf die Sophos Central Admin-Seite https://cloud.sophos.com/manage/ zuzugreifen.



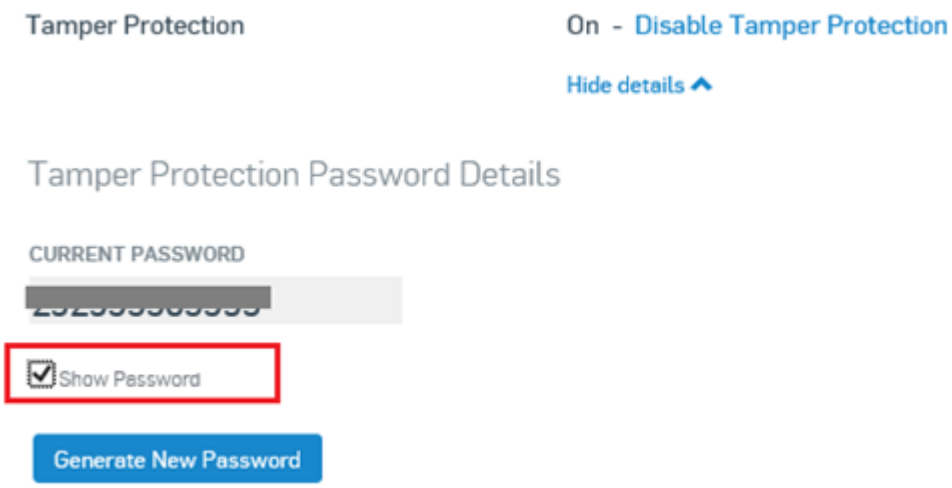
2. Navigieren Sie zu Geräte > Server, und klicken Sie dann auf den Servernamen Ihrer Arcserve Appliance.



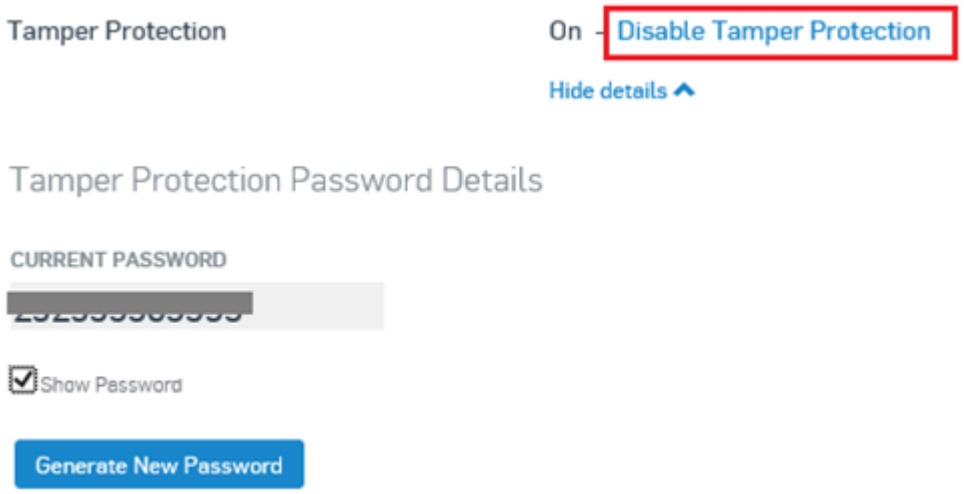
3. Klicken Sie auf der Registerkarte ZUSAMMENFASSUNG für das Feld „Manipulationsschutz“ auf **Details anzeigen**.



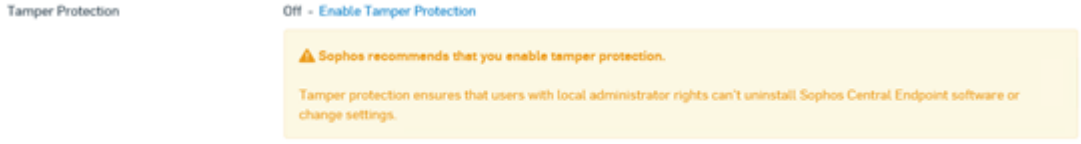
4. Aktivieren Sie unter „Kennwort anzeigen“ das Kontrollkästchen. Notieren Sie sich das Kennwort, das im Textfeld angezeigt wird.



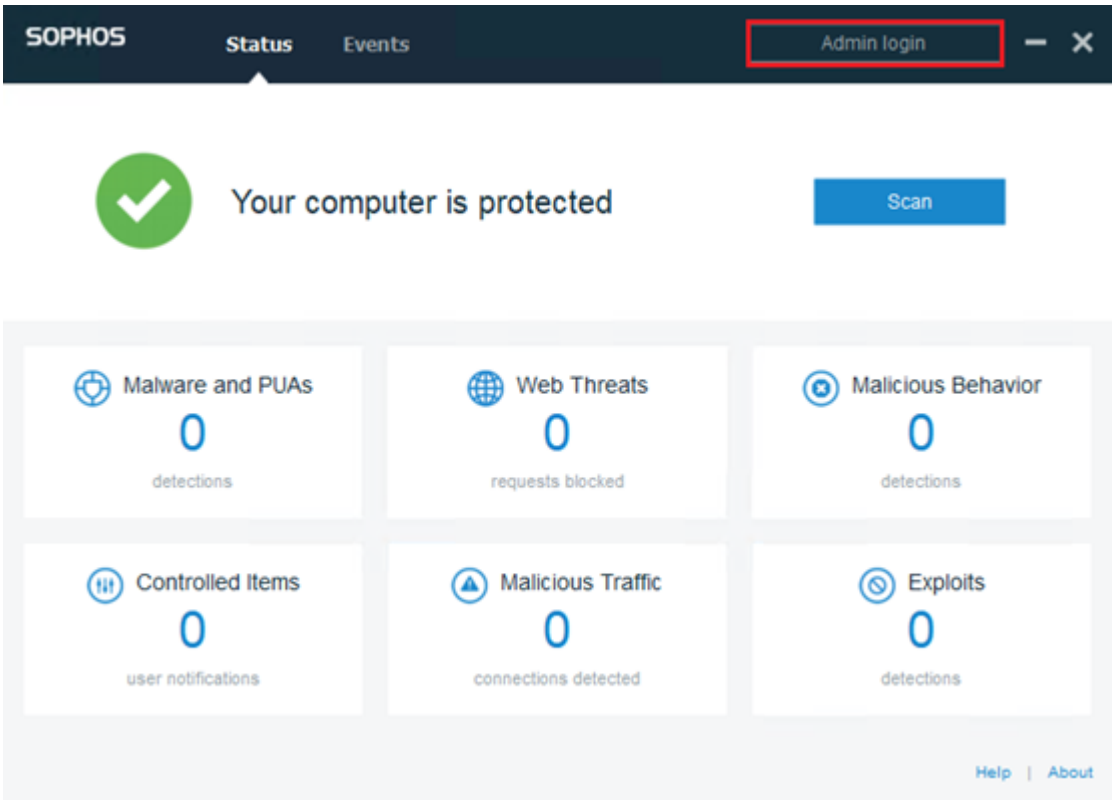
5. Klicken Sie auf **Manipulationsschutz deaktivieren**.



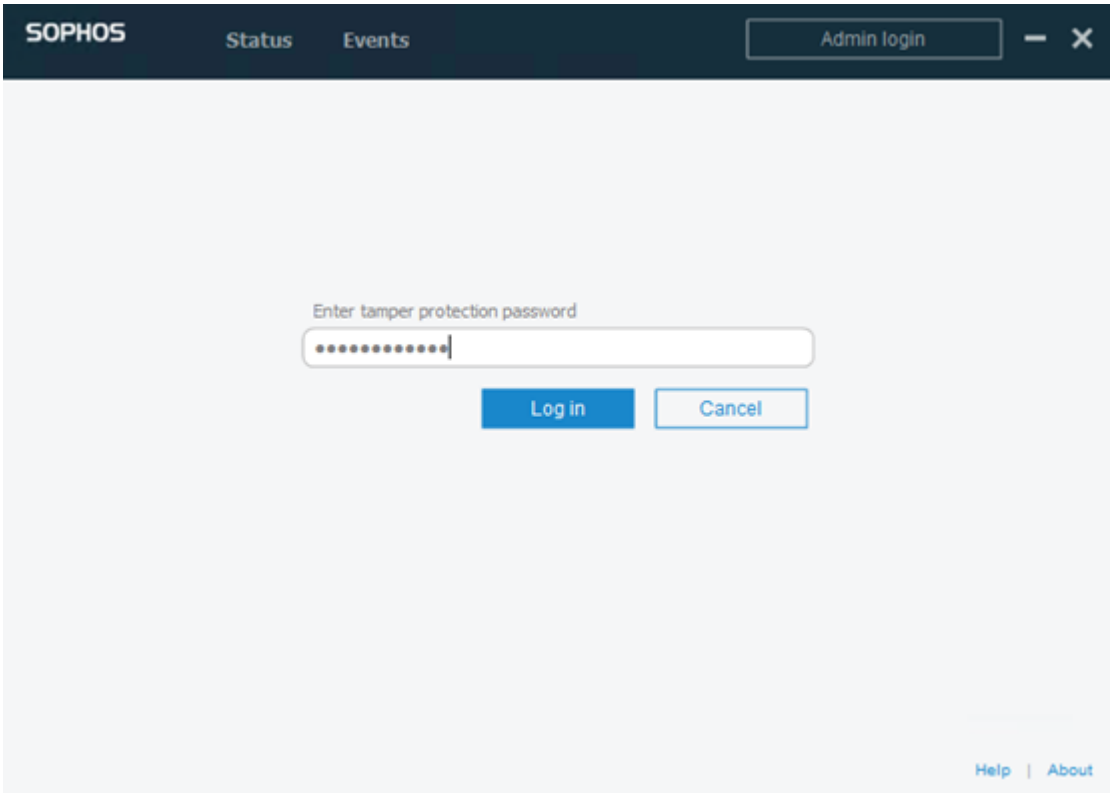
Der Manipulationsschutz wird deaktiviert.



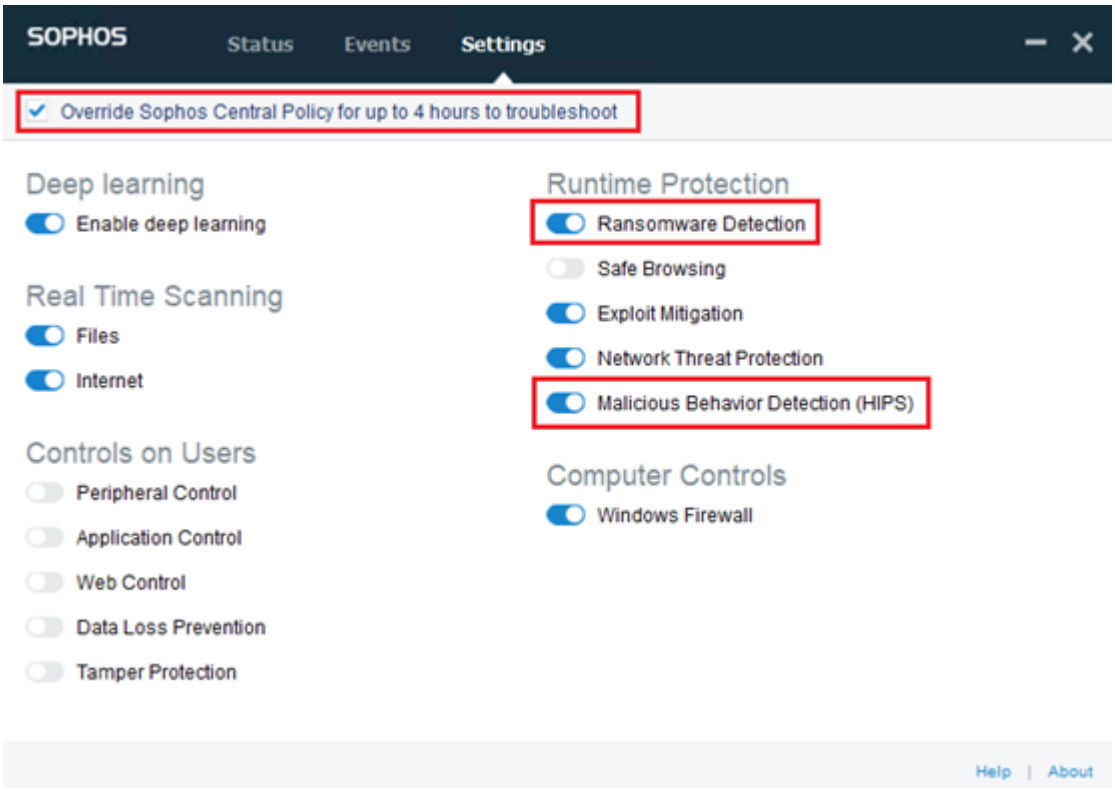
6. Starten Sie Sophos Endpoint, und klicken Sie dann auf **Admin Login**.



7. Geben Sie das in Schritt 4 notierte Kennwort für den Manipulationsschutz ein.



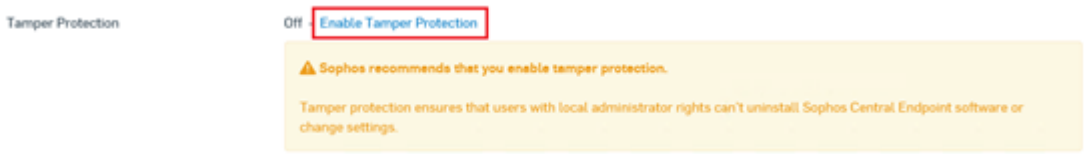
8. Aktivieren Sie auf der Registerkarte „Einstellungen“ die Option **Sophos-Zentralrichtlinie bis zu 4 Stunden lang zur Fehlersuche aufheben,** und deaktivieren Sie die Optionen **Ransomware-Erkennung** und **Erkennung von bösartigem Verhalten (HIPS)**.



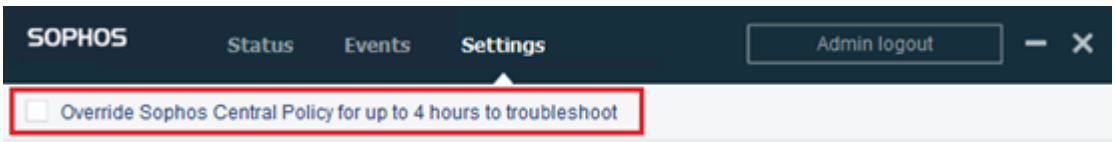
9. Um das Werkseinstellungs-Image zu ersetzen, führen Sie SetImage.exe aus. SetImage.exe wird erfolgreich ausgeführt.

Führen Sie die folgenden Schritte aus, um die Standardkonfiguration von Sophos nach der erfolgreichen Ausführung von SetImage.exe wiederherzustellen:

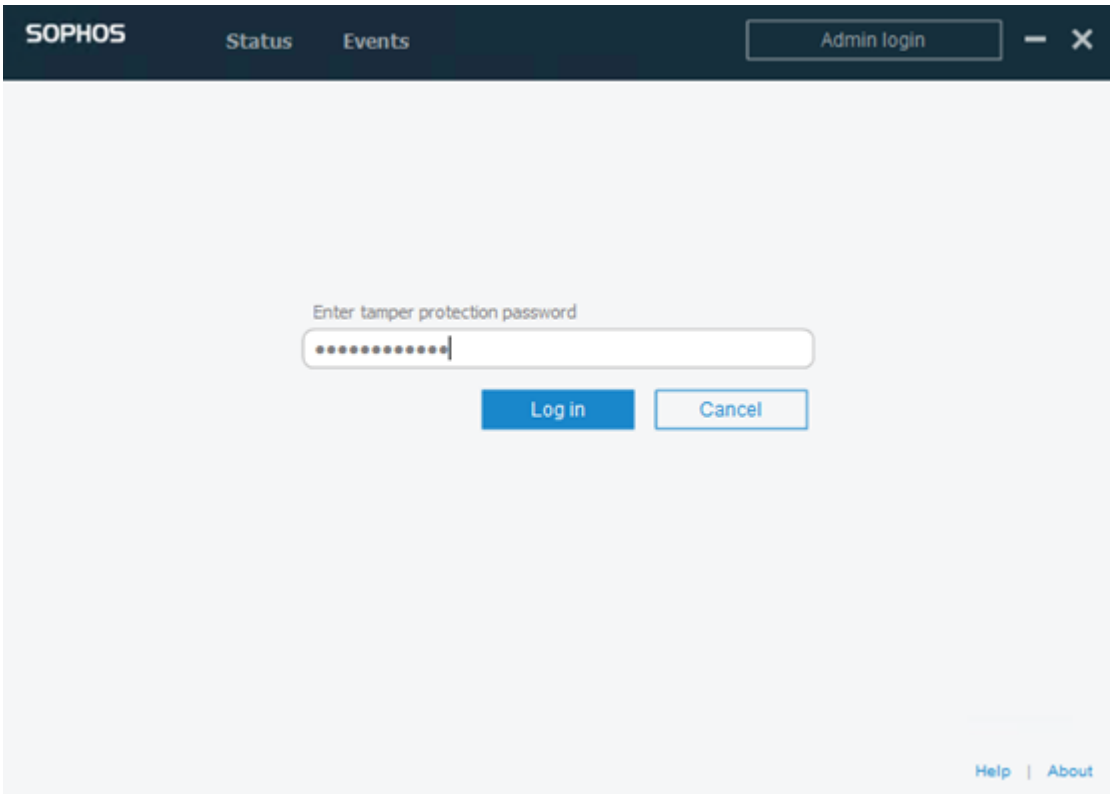
1. Um den Manipulationsschutz in Sophos Central Admin zu aktivieren, klicken Sie auf **Manipulationsschutz aktivieren**.



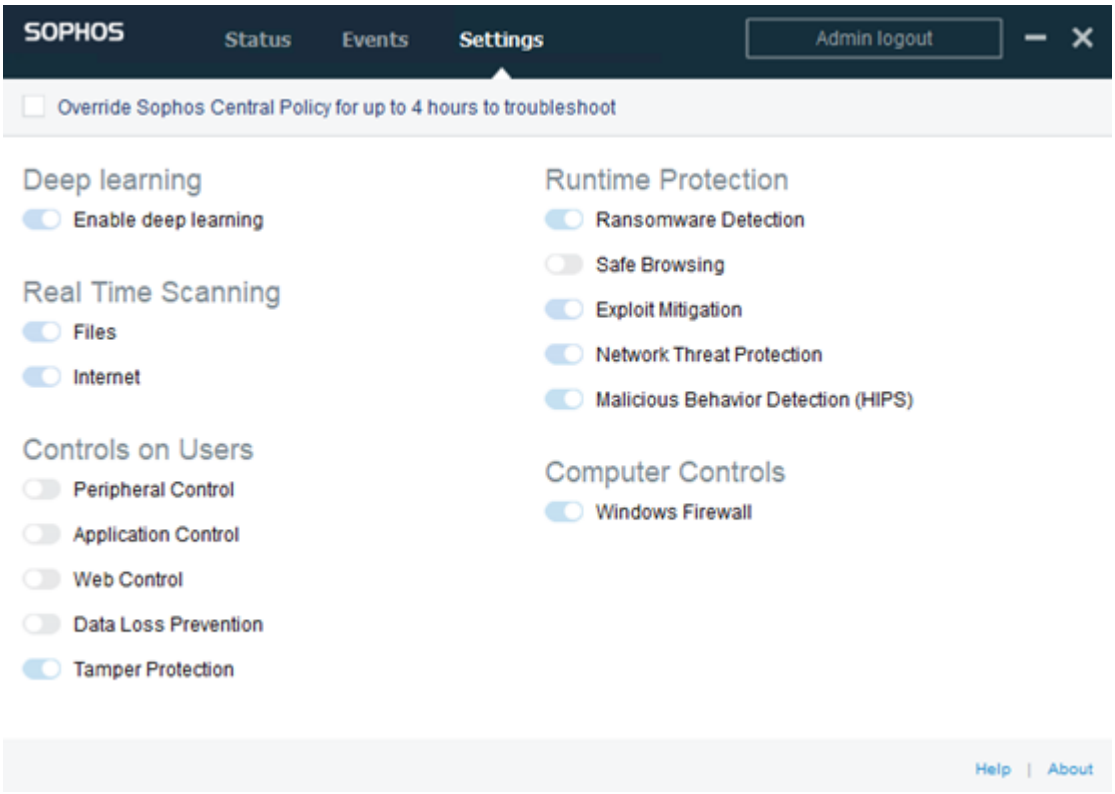
2. Deaktivieren das Kontrollkästchen **Sophos-Zentralrichtlinie bis zu 4 Stunden lang zur Fehlersuche aufheben**.



3. Um den Status der Sophos-Einstellungen zu überprüfen, warten Sie einige Minuten, und melden Sie sich dann mit dem Kennwort für den Manipulationsschutz bei Sophos Endpoint an.



Jetzt wurden die Sophos-Einstellungen auf die Standardeinstellungen wiederhergestellt.



Bewährte Verfahren zum Erstellen von Deduplizierungsdatenspeichern über Volumes hinweg

Mit as_gddmgr.exe, einem Befehlszeilentool, können Sie weitere Datenpfade über Volumes hinweg hinzufügen, um die Speicherkapazität des vorhandenen Deduplizierungsdatenspeichers zu erweitern.

Führen Sie die folgenden Schritte aus, um Deduplizierungsdatenspeicher über Volumes hinweg zu erstellen:

1. Melden Sie sich bei der Benutzeroberfläche der Arcserve UDP-Konsole an, und erstellen Sie dann einen Deduplizierungsdatenspeicher ohne erweiterten Datenpfad. Weitere Informationen finden Sie unter Hinzufügen von Datenspeichern.
2. Stoppen Sie den Datenspeicher. Weitere Informationen finden Sie unter Stoppen von Datenspeichern.
3. Öffnen Sie die Eingabeaufforderung, und geben Sie dann den folgenden Befehl ein, um die aktuelle Pfadkonfiguration des Datenspeichers anzuzeigen:

   as_gddmgr.exe -DataPath Display <Name des Datenspeichers>

   Der folgende Beispieldatenspeicher verfügt über einen primären Datenpfad auf X:\volume:

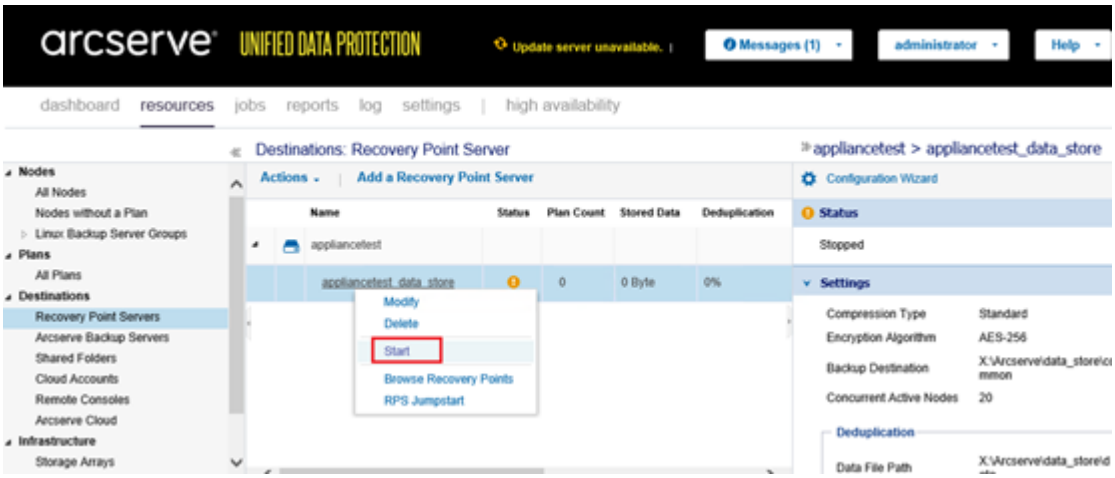
4. Um die Speicherkapazität des Deduplizierungsdatenspeichers zu erweitern, geben Sie den folgenden Befehl ein:

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

   Hinweis: Stellen Sie sicher, dass sich der primäre Pfad und alle erweiterten Pfade nicht auf demselben Volume befinden.

   Der folgende Beispieldatenspeicher verfügt über einen erweiterten Datenpfad auf W:\volume:

5. Wiederholen Sie Schritt 4 nach Bedarf.
6. Kehren Sie zur Benutzeroberfläche der Arcserve UDP-Konsole zurück, und starten Sie den Datenspeicher. Weitere Informationen finden Sie unter Starten von Datenspeichern.



Kapitel 15: Lizenzhinweise

Teile dieses Produkts enthalten Software von anderen Herstellern. Der nachfolgende Abschnitt enthält Informationen zur Software von anderen Herstellern.

Dieser Abschnitt enthält folgendes Thema:

PuTTY

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

Komponentenname	PuTTY
Kom-ponentenhersteller	Ursprünglich entwickelt von Simon Tatham
Komponentenversion	0.64
Rechtlicher Hinweis	htt-p://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html
Projektname	Appliance Rhodium
Komponententyp	Open Source
Quell-Code-URL	http://the.earth.li/~sgtatham/putty/0.64/
Erforderliche Plattform (en)	Windows 2012 R2, Windows 2016, Windows 2019
Komponenten-URL	http://the.earth.li/~sgtatham/putty/0.64/x86/
URL der Kom-ponentenversion	http://the.earth.li/~sgtatham/putty/0.64/x86/
Beschreibung	Auf dem Appliance-Rechner verwenden wir putty.exe zur Kommunikation mit dem Linux-Sicherungsserver, um das Systemgebietsschema und das UDP-Linux-Gebietsschema zu ändern.
Funktionen	Appliance
Lizenztext	htt-p://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html *PuTTY is copyright 1997-2019 Simon Tatham.* *Copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svyatoslav Kuzmich, Nico Williams, Viktor Dukhovni und CORE SDI S.A.* *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 KEINEM FALL SIND DIE COPYRIGHT-INHABER FÜR ANSPRÜCHE, KLAGEN ODER GEWÄHRLEISTUNGEN WEDER IM RAHMEN DES VERTRAGS, NOCH AUFGRUND VON UNRECHT ODER ANDEREN GRÜNDEN VERANTWORTLICH, DIE DURCH DIE SOFTWARE, DEREN NUTZUNG ODER ANDEREM UMGANG MIT DER SOFTWARE ODER IM ZUSAMMENHANG DAMIT ENTSTEHEN.
Copyright-Text	htt- p://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html *PuTTY is copyright 1997-2019 Simon Tatham.* *Copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svyatoslav Kuzmich, Nico Williams, Viktor Dukhovni und CORE SDI S.A.* *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 KEINEM FALL SIND DIE COPYRIGHT-INHABER FÜR ANSPRÜCHE, KLAGEN ODER GEWÄHRLEISTUNGEN WEDER IM RAHMEN DES VERTRAGS, NOCH AUFGRUND VON UNRECHT ODER ANDEREN GRÜNDEN VERANTWORTLICH, DIE DURCH DIE SOFTWARE, DEREN NUTZUNG ODER ANDEREM UMGANG MIT DER SOFTWARE ODER IM ZUSAMMENHANG DAMIT ENTSTEHEN.*
Verwendungszweck	Auf dem Appliance-Rechner verwenden wir putty.exe zur Kommunikation mit dem Linux-Sicherungsserver, um das Systemgebietsschema und das UDP-Linux-Gebietsschema zu ändern.
Änderungen erforderlich	Nein