Appliance-Benutzerhandbuch

Arcserve Unified Data Protection

Version 10.0

arcserve

Appliance-Benutzerhandbuch

Arcserve Unified Data Protection

Version 10.0

**Das Inhaltsverzeichnis wird im linken Fensterbereich angezeigt. Wenn Sie alle Themen anzeigen möchten, klicken Sie auf das oben verfügbare 

-Symbol.**

arcserve

Rechtliche Hinweise

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

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

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

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

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

Der Hersteller dieser Dokumentation ist Arcserve.

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

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

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 nur auf Englisch verfügbar.

Produktdokumentation

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

Das Knowledge Center von Arcserve UDP umfasst die folgende Dokumentation:

- **Arcserve UDP Lösungshandbuch**

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

- **Arcserve UDP Versionshinweise**

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

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

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

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

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

Kapitel 2: Einführung in die Arcserve 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 in die führende Arcserve Unified Data Protection-Software integriert, die bereits in der neuesten Hardware vorinstalliert ist. Die Appliance bietet eine vollständige und integrierte Datenschutzlösung für alle Benutzer, die nicht nur Ihren derzeitigen Anforderungen entspricht, sondern auch in Zukunft die sich stetig wandelnden Anforderungen für Sicherung, Archivierung und Notfallwiederherstellung erfüllt.

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. Weitere Informationen zur Appliance-Garantie finden Sie unter Appliance-Garantie.

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 unterstützten Betriebssystemen finden Sie unter 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, wichtige Geschäftsinformationen zu schützen und wiederherzustellen. Arcserve Unified Data Protection Agent for Linux verfolgt Änderungen an einem Knoten auf Blockebene und sichert dann nur die geänderten Blöcke in einem Zuwachssicherungsprozess. Dadurch können Sie häufige Sicherungen durchführen, die Größe jeder Zuwachssicherung (und des Sicherungsfensters) wird reduziert und die Sicherung wird aktueller. Arcserve Unified Data Protection Agent for Linux bietet auch die Möglichkeit, Dateien oder Ordner wiederherzustellen und eine Bare-Metal-Recovery (BMR) aus einer einzigen Sicherung auszuführen. 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 wird unter dem Standardinstallationspfad in 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:\Program Files (x86)\Arcserve" installiert, nachdem Sie es mithilfe der Datei "InstallASBU.iso" geladen und installiert haben. Mithilfe der in der Arcserve Appliance installierten Komponenten können Sie das Ziel von Arcserve UDP auf einem Band sichern. Weitere Informationen zu unterstützten Betriebssystemen finden Sie unter 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 Continuous Availability

Arcserve Continuous Availability 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 unterstützten Betriebssystemen finden Sie unter Kompatibilitätsmatrix.

Arcserve Continuous Availability 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 Continuous Availability ist nicht in der Anwendung vorinstalliert. Weitere Informationen zum Installieren und Konfigurieren von Arcserve Continuous Availability 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.

Inhalt der Box

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

- 10000-Serie
- 9000-Serie
- X-Serie

In der Box der Appliance 10000 Series enthaltene Gegenstände

Die folgenden Gegenstände sind in der Verpackung mit dem 10048DR-10576DR-Zubehör enthalten:

- Schnellstarthandbuch, Arcserve Appliance, ZUERST-LESEN-BLATT
- Arcserve QR-Flyer (mit QR-Code zu Handbüchern)
- 1 x Arcserve 10000-Server-Hardware-Installationshandbuch
- 2 x Netzkabel (C13 zu NEMA 5-15P). Zusätzlich zum standardmäßigen US-Netzkabel wird der Packung ein Paar Netzkabel für das Zielland beigefügt.
- 1 x Schienen-Kit/Halterungensatz
- 1 x Beutel mit Schrauben der Größe 3,5 für HDD
- 1 x Beutel mit Schrauben der Größe 2,5 für HDD
- CABLE, FLEXBOOT,CAT6,NETWORK,3FT,BLUE CABLE, FLEXBOOT,CAT6,NETWORK,7FT,BLACK

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)

In der Box der Appliance Serie X enthaltene Gegenstände

Arcserve Appliance Serie X umfasst folgende Komponenten:

- **Appliance Serie Compute Node:**
  - MICROSOFT
  - WIN SVR EMB STD 2019 16-CORE

  Zubehör-Box Compute Node:
  - Windows 4-Core Erweiterungslizenzen (10 Stück)
  - HARDWARE-EINRICHTUNGSHANDBUCH, ARCSERVE R740
  - SCHNELLSTARTHANDBUCH, ARCSERVE, INFODATEI UPD APPLIANCE
  - Dell Sicherheitsdokumentation
  - Netzkabel (2 Stück) US- oder landesspezifisch, falls bestellt
  - Rackmount-Schienen-Kit
  - Kabelverwaltungsarm
  - Optionale Komponenten, falls bestellt:
    - SFPs
    - SAS-Kabel
    - DAC-Kabel

  Hinweis: An der Vorderseite des Arrays wird Folgendes angebracht: lackierte Blende Arcserve ME4084 und Aufklebergruppe.
- **Appliance Serie X Storage Node**

  Die Box für das 5U-Speichersystem enthält Folgendes:
  - Dokumentation
  - 5U-Gehäuse für den Appliance-Speicher
  - Zwei Netzkabel
  - Separat verpackte Festplatten (nur 5U-Gehäuse)
  - Fibre Channel- oder iSCSI SFP+-Transceiver oder -Kabel (eines pro Host-Port)
  - Hostkabel (1 pro Host-Port des Controllermoduls)
  - Verlängerungskabel (1 pro Erweiterungsmodul)

- Optionales Gehäuse-Blendenset mit einem Schlüssel (1 pro 5U-Gehäuse)
- Passendes Rackmount-Kit für 5U-Speichersystemgehäuse

ME4084 Zubehörboxen:

- HARDWARE-EINRICHTUNGSHANDBUCH, ARCSERVE ME4084
- Rackmount-Schienen-Set
- C19 bis C20, PDU-Stil, 2,5 m Netzkabel (2 Stück)
- Serielles Kabel
- 12 Gbit HD-Mini-auf-HD-Mini-SAS-Kabel, 2M (4 Stück)
- Speicher-Array – Dokumentation mit den Zulassungsinformationen
- Dokumentation zum Einrichten des Speicher-Arrays
- Dokumentation mit Sicherheits- und Umweltinformationen
- Schlüssel zum Entfernen der Blende
- Nicht verwendete Aufkleber für Laufwerksnummern

  Hinweis: Die Festplatten befinden sich in einer separaten Box unter dem Array.

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.

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 9000 und X sind je nach Ihren Anforderungen in unterschiedlichen Modellen verfügbar:

- Modell 10024BU - 10576DR
- Modelle 9012 - 9504 DR
- Modell X-Serie

Modell 10024BU-10576DR

Arcserve Appliance Modell 10024BU - 10576DR

Arcserve Appliance Spezifikationen der 10000-Serie							
Appliance-Modell	**10048DR**	**10072D-R**	**10144D-R**	**10192D-R**	**10288D-R**	**10384DR**	**10576D-R**
Effektive Kapazität (TB)1	48	72	144	192	288	384	576
Nutzbare Kapazität	16 TB	24 TB	48 TB	64 TB	96 TB	128 TB	192 TB
Maximal nutzbare Kapazität unter Verwendung des Erweiterungskits	40 TB	40 TB	80 TB	80 TB	160 TB	160 TB	K/A
Formfaktor	2U						
Basis-RAM (DDR5 5600)	128 GB (4 x 32 GB)	256 GB (8 x 32 GB)					384 GB (12 x 32 GB)
Max. RAM	512 GB						
SAS 12G HDD Enterprise Grade 7,2k	6 x 4 TB	8 x 4 TB	8 x 8 TB	10 x 8 TB	8 x 16 TB	10 x 16 TB	14 x 16 TB
NVMe M.2	2 x 480 GB (RAID 1) für Betriebssystem und UDP						
SSD	2 x 3,2 TB für Hash (RAID 1)						
CPU	Dual Intel® Xeon® Silver 4510T 12C 2 G						
RAID-Controller	Broadcom 3916 mit CacheVault-Schreibcache-Schutz						
HDD-RAID-Konfiguration	RAID6						
Laufwerkschächte	14 x HDD, 2 x SSD						

Optionale RAM-Erweiterungs-Kits	✓	✓	✓	✓	✓	✓	✓
DIMM-Slots	16						
NIC	Insgesamt 4 Ports. 2 x 10 GbE onboard. 2 x 10 GbE Base-T über Broadcom BCM57416						
Verfügbare PCIe-Slots	3 (Low Profile)						
Remote-Hardware-Verwaltung	IPMI (Advance-Lizenz)						
Netzteile	2 x 1600 W, redundant, Titanium-Stufe (96 %), Hot-Swap-fähig						
HDD-Kit (optional)	8 x 4 TB (24 TB) RAM-Upgrade empfohlen	6 x 4 TB (16 TB)	6 x 8 TB (32 TB)	4 x 8 TB (16 TB)	6 x 16 TB (64 TB)	4 x 16 TB (32 TB) RAM-Upgrade empfohlen	X
RAM-Erweiterungs-Kit (optional)	Jedes Kit mit 128 GB (4 x 32) kann mehrfach bestellt werden. Max. 3 Kits		Jedes Kit mit 128 GB (4 x 32) kann mehrfach bestellt werden. Max. 2 Kits.				128 GB (4 x 32), maximal 1 Kit.
Broadcom Aero HBA 9500-8e PCIe Gen4	Optional						
Broadcom BCM57416 Dual Port 10 Gbit/s Base-T Adapter	Optional						
Intel X710 Std LP Dual Port 10G SFP+	Optional						
Broadcom BCM57414 Std LP Dual Port 25G SFP28	Optional						
QLogic 2692 mit zwei Ports und 16 Gb Fibre Channel-HBA	Optional						
Gewicht	Bruttogewicht: 28,12 kg (62 lbs)						

	Nettogewicht: 18,82 kg (41,5 lbs)
Packmaße	658 x 274 x 998 mm (25,9" x 10,8" x 39,3")
In-Rack-Maße	437 x 89 x 705 mm (17,2" x 3,5" x 27,75")

Hinweis: Die effektive Kapazität berücksichtigt die Deduplizierung der globalen Quelle und entspricht dem 3-fachen der nutzbaren Kapazität. Die tatsächliche Sicherungskapazität kann je nach Datentyp, Sicherungstyp, Ablaufplan und anderen Faktoren variieren.

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 (Werkseinstellungen)	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, redundante Stromversorgung (1 + 1), 550 W			Dual, Hot-Plug, redundante Stromversorgung (1 + 1), 750 W							
iDRAC Enterprise	1										

Modell Serie X

Arcserve Appliance Modell Serie X

Arcserve Appliance Serie X – Spezifikationen					
Appliance-Modell	**X1000DR**	**X1500DR**	**X2000DR**	**X2500DR**	**X3000DR**
Effektive Kapazität (TB) [1]	1.056	1.584	2.112	2.640	3.168
Maximale effektive Kapazität mit Erweiterungs-Kits (TB) [1]	3.168				
Hinweis: Die effektive Kapazität berücksichtigt die Deduplizierung der globalen Quelle und ist etwa dreimal so groß wie die nutzbare Kapazität der Festplatten. SSDs sind nicht eingeschlossen. Die tatsächliche Sicherungskapazität kann abhängig von Faktoren wie Datentypen, Sicherungstyp, Ablaufplan usw. variieren.					
Disk Imaging- und Disaster Recovery-Software	Arcserve UDP Premium Edition, enthalten				
Tape Integration Software	Arcserve Backup, enthalten				
Continuous Availability mit automatisiertem Failover	Arcserve Continuous Availability, optional				
Compute Node					
CPU	Dual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)				
Standard-RAM	1.024 GB (16 x 64) DDR4-3200 RDIMM				
Max. RAM	2,048 GB				
DIMM-Slots	24				
NVMe-SSD	2 x 1.6TB (RAID-1) und 6 x 4TB (RAID-5)				
Laufwerkschächte	24 x 2,5-Zoll-Enterprise-NVMe-SSD				
Externer SAS 12Gbps HBA-Controller	2x enthalten				
Intel X550 Quad-Port 10G Base-T-Adapter	Enthalten				
Broadcom 57414 Dual-Port 25Gb SFP28-Adapter	Optional				
Intel X710 Dual-Port 10G SFP + FC-Adapter	Optional				
QLogic 2692 mit zwei Ports und 16 Gb Fibre Channel-HBA	Optional				
Remote-Hardware-Verwaltung	iDRAC Enterprise, enthalten				
Netzteile	Dual, Hot-Plug, redundante Stromversorgung (1 + 1),				

	1100 W				
Wärmeableitung	4100 BTU/h				
Gewicht	34 kg (75 lb)				
Formfaktor	2U				
Maße im Rack (ohne Blende, Vorderseite und Netzteilgriffe)	67,9 cm x 43,4 cm x 8,7 cm (26,7" x 17,1" x 3,4")				
Äußere Abmessungen (einschließlich Blende, Vorderseite und Griffen des Netzteils)	75,19 cm x 48,2 cm x 8,7 cm (29,6" x 19,0" x 3,4")				
Packmaße	97 cm x 66 cm x 30 cm (38" x 26" x 12")				
Storage Node					
16 TB SAS 12G Hot-Plug-Festplatte	28	42	56	70	84
Minimale verwendbare Kapazität	352	528	704	880	1056
Lineare Erweiterung mit optionalen Kits	✓	✓	✓	✓	
RAID-Ebene	RAID-ADAPT				
RAID-Controller	Dual-SAS-12-Gb-Controller mit 8 Ports				
Hotspare-Speicherplatz auf Festplatten	Bis zu 64 TB				
Netzteile	Dual, redundant (1 + 1), 2200 W				
Wärmeableitung	7507 BTU				
Gewicht	Von 64 kg (141 lbs) bis 135 kg (298 lbs)				
Formfaktor	5U				
Äußere Abmessungen (einschließlich Blende, Vorderseite und Griffen des Netzteils)	97,47 cm x 48,30 cm x 22,23 cm (38,31" x 19,01" x 8,75")				

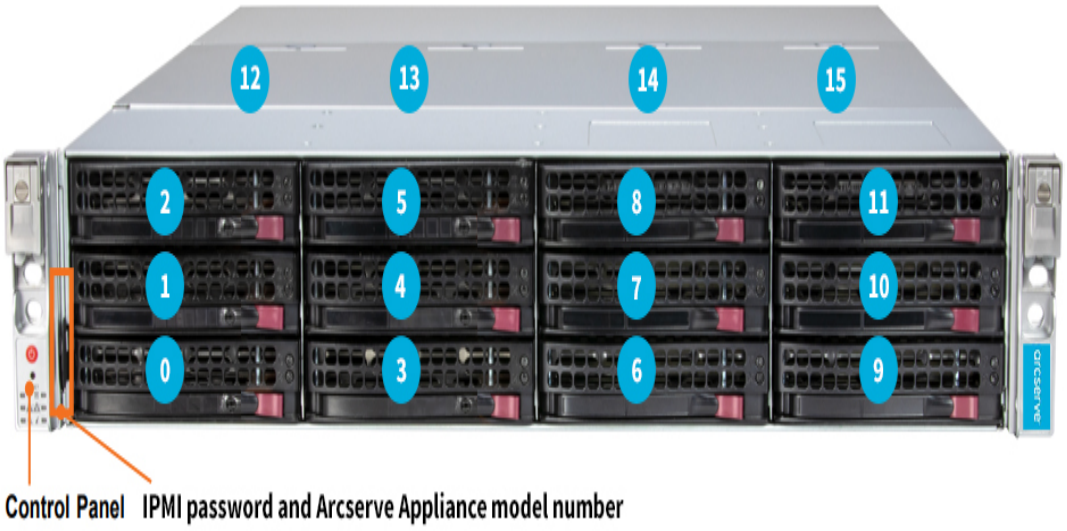
Steuerelemente und Anzeigen

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 10024BU - 10048BU
- Vorderseite 10048DR - 10576DR
- Vorderseite 9012 - 9048
- Vorderseite 9072DR - 9504 DR
- Vorderseite der Serie X
- Rückseite 10024BU - 10048BU
- Rückseite 10048DR - 10576DR
- Rückseite 9012 - 9048
- Rückseite der 9072DR - 9504DR
- Rückseite Serie X
- Draufsicht 10024BU - 10048BU

Vorderseite 10048DR-10576DR

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



Steuerelement/Anzeige	Beschreibung
0–5	3,5"-SAS-HDDs. Weitere Informationen finden Sie unter Laufwerksträger-LED.
6–11	3,5"-SAS-HDDs. Weitere Informationen finden Sie unter Laufwerksträger-LED.
12–13	3,5"-SAS-HDDs. Weitere Informationen finden Sie unter Laufwerksträger-LED.
14–15	2,5"-SAS-SSDs. Weitere Informationen finden Sie unter Laufwerksträger-LED.
Bedienfeld	Umfasst den Netzschalter, den Reset-Schalter und die LED-Anzeigen. Weitere Informationen finden Sie unter Bedienfeld.
IPMI-Kennwort und Arcserve Appliance-Modellnummer	Enthält das IPMI-Kennwort und die Arcserve Appliance-Modellnummer

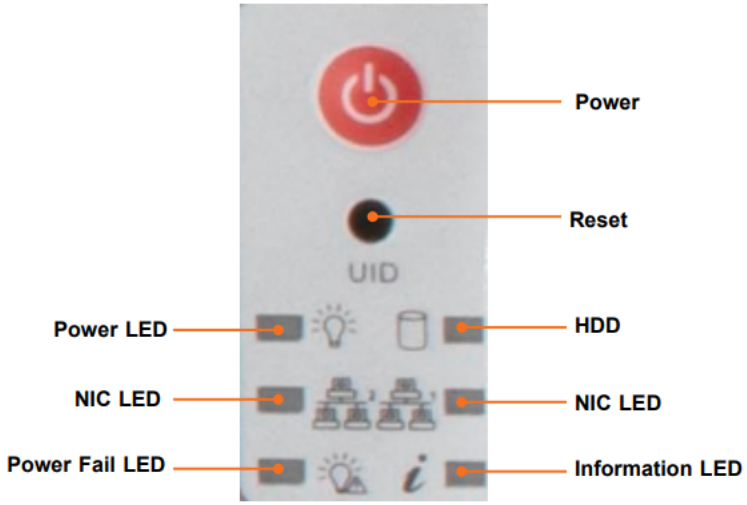
Laufwerksträger-LED

Jeder Laufwerksträger verfügt über zwei LEDs: eine Aktivitäts- und eine Status-LED. Für RAID-Konfigurationen mit einem Controller wird die Bedeutung der Statusanzeige in der folgenden Tabelle beschrieben:

	Farbe	Blinkmuster	Geräteverhalten
Aktivitäts-LED	Blau	Leuchtet dauerhaft	SAS-/ NVMe-Laufwerk im Ruhezustand installiert
	Blau	Blinkt	E/A-Aktivität
	Aus		SATA-Laufwerk im Ruhezustand installiert
Status-LED	Rot	Leuchtet dauerhaft	Ausfall des Laufwerks mit RSTe-Unterstützung
	Rot	Blinkt mit 1 Hz	Laufwerk mit RSTe-Unterstützung wird rekonstruiert
	Rot	Zweimaliges Blinken und eine Unterbrechung mit 1 Hz	Hotspare für Laufwerk mit RSTe-Unterstützung

	Rot	Zweimaliges Blinken und eine Unterbrechung mit 1 Hz	Einschalten des Laufwerks mit RSTe-Unterstützung
	Rot	Blinkt mit 4 Hz	Identifizieren von Laufwerken mit RSTe-Unterstützung
	Grün	Leuchtet dauerhaft	NVMe-Laufwerk kann sicher entfernt werden
	Gelb	Blinkt mit 1 Hz	NVMe-Laufwerk nicht entfernen

Bedienfeld



Steuerelement/Anzeige	Beschreibung
Netzschalter	Mit dem Haupt-Netzschalter erhält der Server Strom über die primäre Stromversorgung bzw. wird vom Strom getrennt, er bleibt jedoch im Standby-Modus.
Reset-Taste	Hiermit wird das System neu gestartet.
Netz-LED	Zeigt an, dass die Netzteile des Systems mit Strom versorgt werden. Diese LED leuchtet, wenn das System normal funktioniert.
HDD	Wenn diese LED blinkt, weist dies auf Aktivität der Speicherlaufwerke hin.
NIC-LEDs	Wenn diese LED blinkt, weist dies auf Netzwerkaktivität der LANs hin.
Stromausfall-LED	Zeigt an, dass ein Netzteilmodul ausgefallen ist.
Informations-LED	Weist den Bediener auf verschiedene Zustände hin. Wei-

	tere Informationen finden Sie unter Informations-LED.

Informations-LED

Die folgende Tabelle beschreibt den Status der Informations-LED:

Farbe, Status	Beschreibung
Rot, dauerhaft	Eine Überhitzungs-Bedingung ist aufgetreten.
Rot, blinkend mit 1 Hz	Lüfterausfall; auf nicht betriebsbereiten Lüfter überprüfen
Rot, blinkend mit 0,25 Hz	Stromausfall; auf nicht betriebsbereites Netzteil überprüfen
Blau, dauerhaft	UID wurde lokal aktiviert, um den Server in einer Rack-Umgebung zu finden.
Blau, blinkend	UID wurde mithilfe des BMC aktiviert, um den Server in einer Rack-Umgebung zu finden.

Vorderseite 9012 - 9048

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	K/A	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	K/A	Hier können Sie Laufwerke installieren, die auf Ihrem System unterstützt werden. Weitere Informationen über Laufwerke finden Sie unter Link.
3	Optisches Laufwerk (optional)	K/A	Ein optionales schlankes SATA DVD-ROM-Laufwerk oder ein DVD+/-RW-Laufwerk.
4	VGA-Anschluss		Hier können Sie ein Anzeigegerät an das System anschließen.
5	USB-Port (optional)		Der USB-Anschluss ist USB 2.0-kompatibel.
6	Rechtes Bedienfeld	K/A	Enthält den Netzschalter, USB-Port, iDRAC Direct micro-Port und die iDRAC-Direktstatus-LED.
7	Informationsetikett	K/A	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.

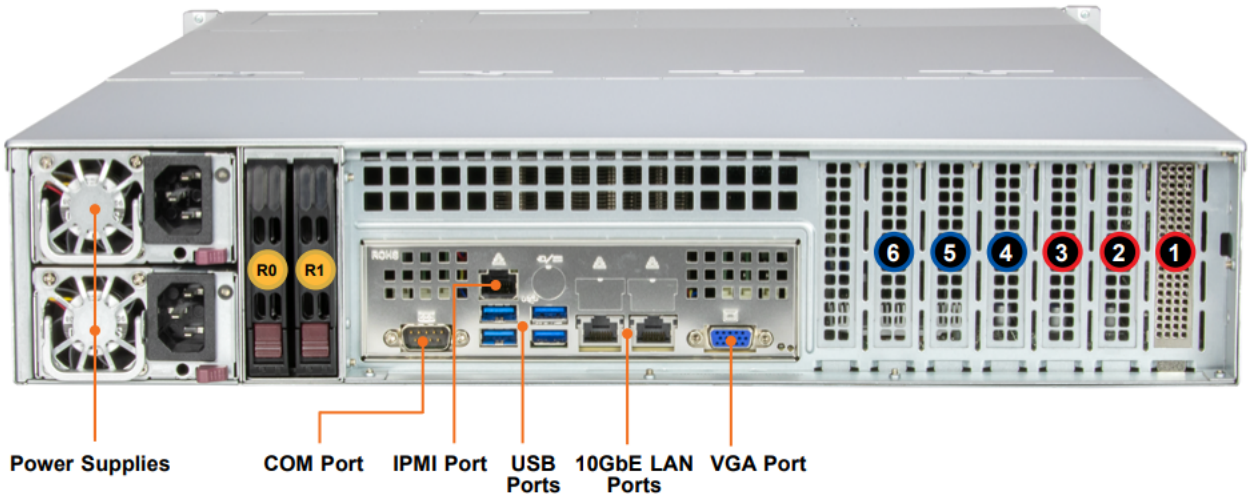
Nummer	Steuerelement/Anzeige	Symbol	Beschreibung
1	Linkes Bedienfeld	NA	Enthält den Systemstatus und System-ID, Status-LED und die Anzeige für iDRAC Quick Sync 2 (drahtlos).
2	Laufwerksteckplätze	NA	Hier können Sie Laufwerke installieren, die auf Ihrem System unterstützt werden. Weitere Informationen 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.

Vorderseite der Serie X

Weitere Informationen zur Vorderseite finden Sie unter Appliance Installation Serie X – Compute Node und Appliance Installation Serie X – Storage Node.

Rückseite 10048DR-10576DR

Die Rückseite der Arcserve Appliance umfasst Erweiterungskartensteckplätze, Netzteilmodule, LED zur Geräteerkennung, LAN-Ports, USB-Ports, VGA-Ports, BMC-LAN-Port und COM-Port. In der folgenden Tabelle werden diese Elemente beschrieben.



Steuerelement/Anzeige	Beschreibung
R0, R1	Nicht verwendbar
1	Hardware-RAID-Controller
2	Cache-Vault für Hardware-RAID-Controller
3	10 GbE Base-T
4	Erweiterungssteckplatz für optionale Karten (Low Profile)
5	Erweiterungssteckplatz für optionale Karten (Low Profile)
6	Erweiterungssteckplatz für optionale Karten (Low Profile)
Netzteile	Zwei redundante 1600-W-Netzteile. Weitere Informationen finden Sie unter Netzteil-LEDs.
COM-Port	Serieller Port (RS-232)
IPMI-Port	Dedizierter IPMI-LAN-Port
USB-Ports	Vier USB 3.0-Ports
VGA-Anschluss	Ein Videoport
LAN-Ports	Zwei RJ45 10 GbE LAN-Ports

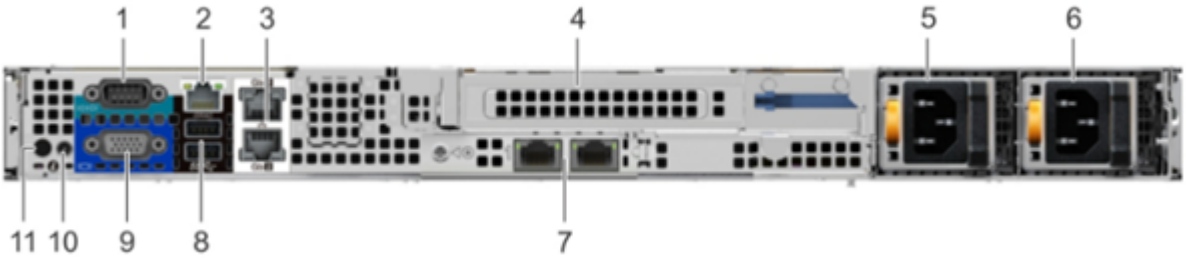
Hinweis: Sie finden die Seriennummer auf der Rückseite des Servers in der Nähe des VGA-Ports und auf der IPMI-Oberfläche.

Netzteil-LEDs

Stromversorgungszustände	Grüne LED	Gelbe LED
Netzteil wird nicht mit Strom versorgt	AUS	AUS
Kritische Ereignisse beim Netzteil, die zu einer Abschaltung führen/Fehler/OCP/OVP/Lüfterausfall/OTP/UVP	AUS	Gelbe LED
Warnungsereignisse für das Netzteil, wobei das Netzteil in Betrieb bleibt: hohe Temperaturen, Überspannung, Unterspannung usw.	AUS	Geld blinkend mit 1 Hz
Wechselstrom anliegend und nur 12 VSB AN (NETZTEIL AUS)	Grün blinkend mit 1 Hz	AUS
Eingeschaltet und OK	Grün	AUS
Netzkabel nicht angeschlossen und im redundanten Modus	AUS	Gelb

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.

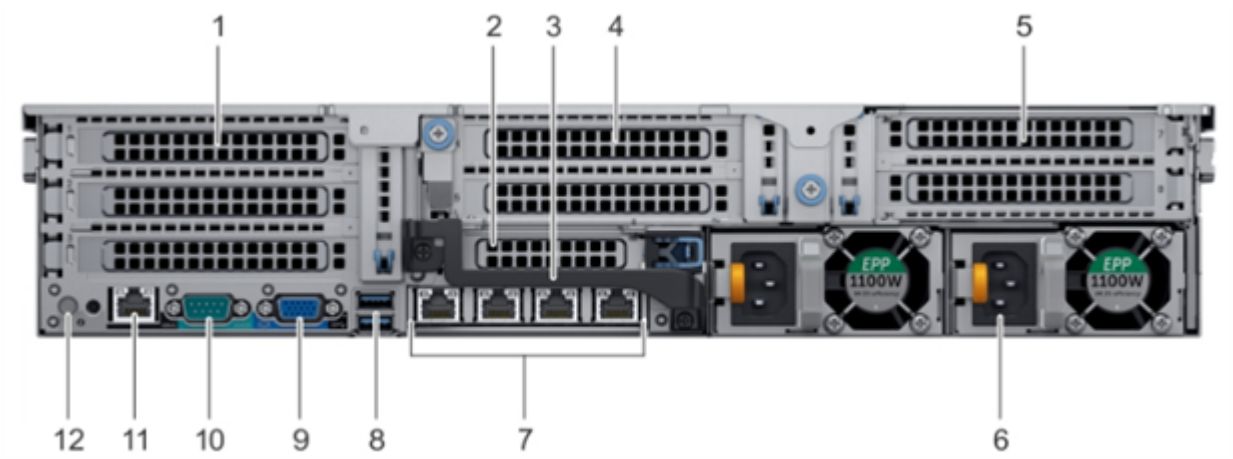


Nummer	Steuerelement/Anzeige	Symbol	Beschreibung
1	Serieller Port		Über diesen Port können Sie ein Peripheriegerät an das System anschließen. Weitere Informationen finden Sie unter link.
2	Dedizierter iDRAC9-Netzwerkport		Verwenden Sie den iDRAC9 dedizierte Netzwerkport, um sicher auf den eingebetteten 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 Sys-

			tem 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.
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 Höhe)	NA	Der PCIe-Erweiterungssteckplatz (Riser 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.

Rückseite Serie X

Weitere Informationen zur Rückseite finden Sie unter Appliance Installation Serie X – Compute Node und Appliance Installation Serie X – Storage Node.

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 #	Port-typ	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 Global Deduplication-Datenspeicherdienst (GDD) von Arcserve UDP RPS. Ein Arcserve UDP-GDD-Datenspeicher verwendet 3 freie Ports, die mit "5000" beginnen. Sie werden benötigt, wenn der Datenspeicher mit GDD aktiviert oder die Wiederherstellungsaufgabe verwendet wird.

6052	TCP	Arcserve Backup-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	Arcserve Backup	CA.ARCserve.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	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.
8014	TCP	Arcserve UDP-Server	httpd.exe	Gibt den Standard-Port für HTTP/HTTPS-Kommunikation zwischen dem Arcserve UDP-Server und den

				Arcserve UDP-Konsolen an. * Gibt den freigegebenen Standard-Port und den einzigen Port an, den Sie öffnen müssen, wenn Sie den Arcserve UDP-Server als Replikationsziel verwenden. Öffnen Sie nicht die Ports 5000–5060, da diese von Datenspeichern mit aktivierter globaler Deduplizierung verwendet werden. **Hinweis:** Sie können den standardmäßigen Kommunikationsport während der Installation der Arcserve UDP-Komponenten ändern.
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.
18005			CA.ARCserve.CommunicationFoundation.WindowsService.exe	Zum Herunterfahren von Tomcat, das von Arcserve UDP Server oder Agent 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
41523	TCP	CASDiscovery	CASDSCSVC.EXE	Arcserve-Discovery-Dienst
41524	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.

Kapitel 3: 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 die Version 10.0 oder der Aktualisierung von Arcserve Backup auf die Version 19.0 ist der ursprüngliche Lizenzschlüssel auf der Arcserve Appliance nicht mehr funktionsfähig. Um die neuen Lizenzschlüssel für Arcserve UDP 10.0 und Arcserve Backup 19.0 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 auf Arcserve Appliance

Das Upgrade von Arcserve Appliance v9.1 auf Arcserve UDP 10.0 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

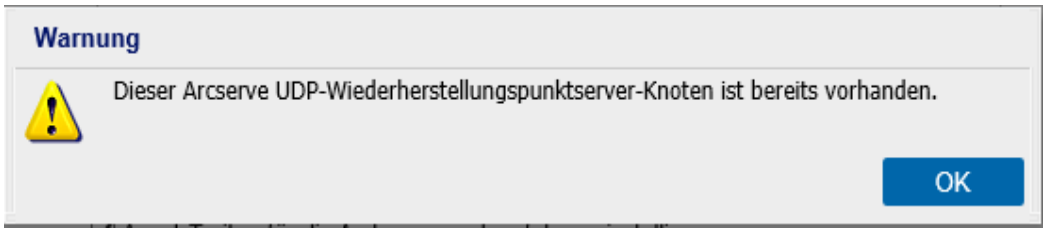
Aktualisieren Sie diese Arcserve Appliance und beachten Sie anschließend die beschriebene Aktualisierungssequenz, um die Umgebung zu aktualisieren.

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 4: 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

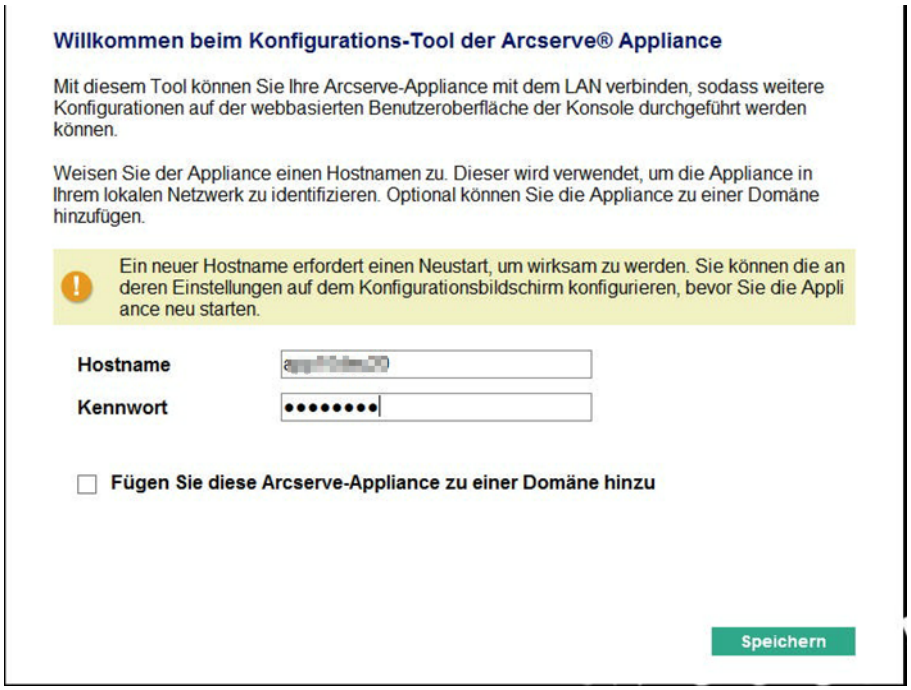
   Geben Sie einen Hostnamen für die Appliance ein. Das Zuweisen eines Namens erleichtert die Identifizierung der Appliance im Netzwerk.

   Kennwort

   Gibt das Administratorkennwort an.

   Fügen Sie diese Arcserve Appliance zu einer Domäne hinzu

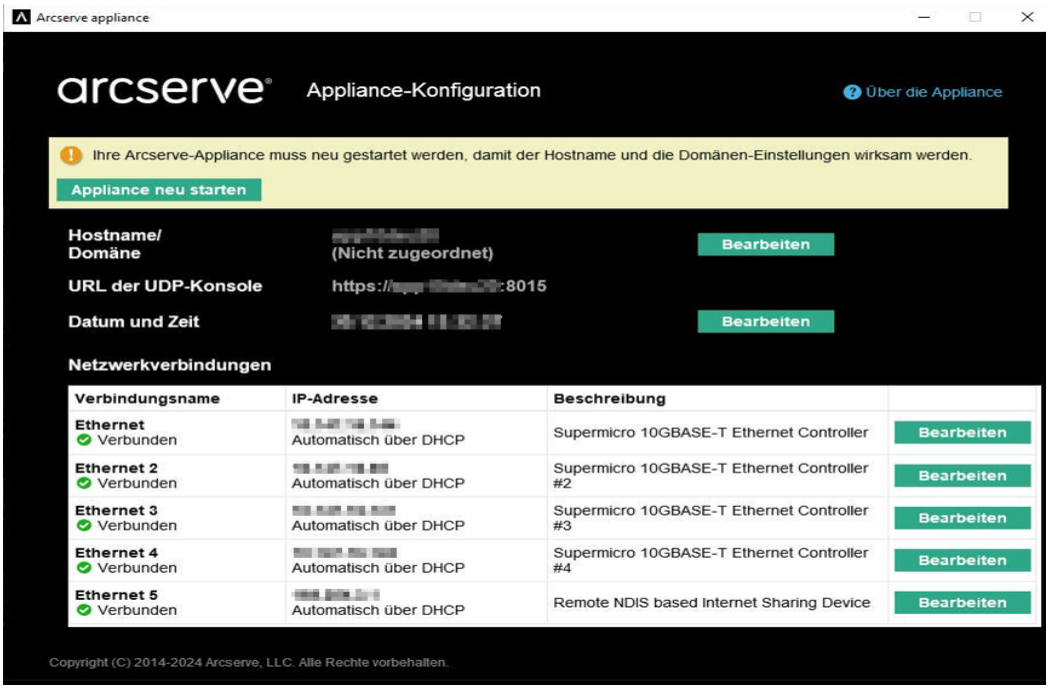
   Aktivieren Sie das Kontrollkästchen, um die Appliance als Mitglied einer Domäne in Ihrem Netzwerk aufzunehmen. Geben Sie die Werte in die Felder "Domäne", "Benutzername" und "Kennwort" an, die angezeigt werden, wenn die Option aktiviert ist.



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.

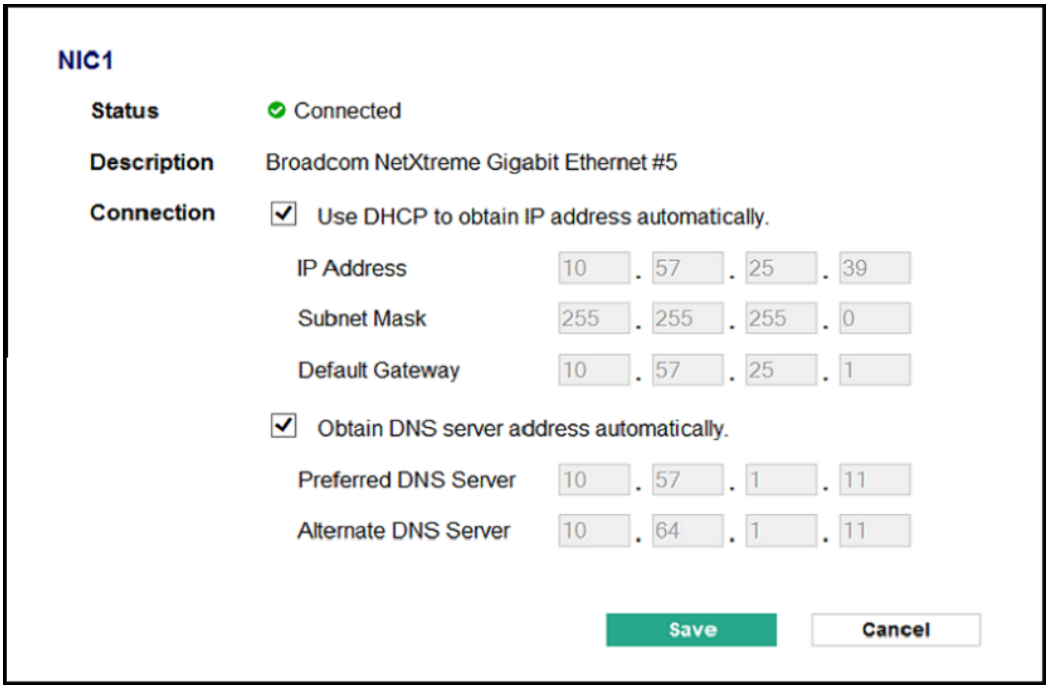
4. Klicken Sie auf **Speichern**.

   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.

Wichtig! Überprüfen Sie, ob in der Eingabeaufforderung ein Skript wie *acrun.-bat* ausgeführt wird. Bevor Sie mit dem Neustart fortfahren, warten Sie unbedingt, bis dieses Skript abgeschlossen ist.

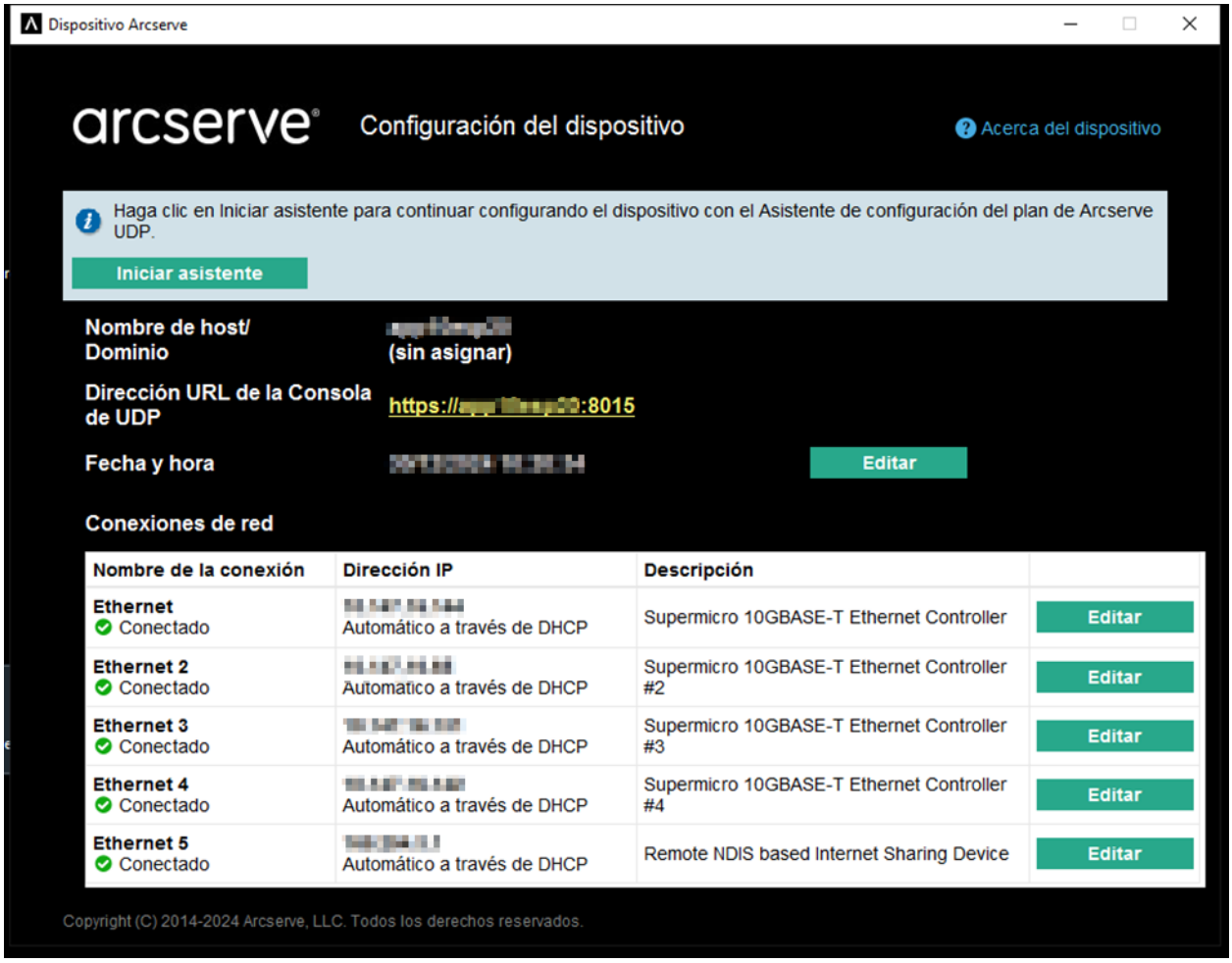
7. Um die Änderungen zu übernehmen, klicken Sie auf **Appliance neu starten**, um die Appliance neu zu starten.

   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 der Arcserve 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: Wenn die Appliance in einer Domäne konfiguriert ist, schließen Sie die Konfiguration des Appliance-Assistenten mit der Administrator-Anmeldung ab, da ein Domänenbenutzer den Appliance-Assistenten nicht konfigurieren kann.

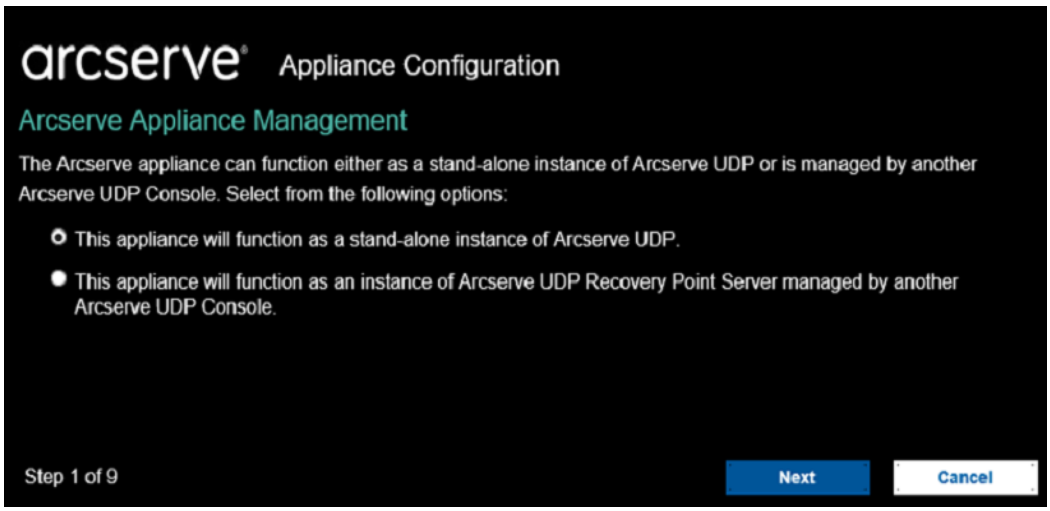
Alle Schritte desArcserve Appliance-Konfigurationsassistenten sind optional. Sie können sie überspringen, indem Sie auf **Abbrechen** klicken und direkt die UDP-Konsole öffnen und Pläne erstellen.

Befolgen Sie diese Schritte:

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

   Der Unified Data Protection-Assistent wird zuerst geöffnet, und das Dialogfeld für das Arcserve Appliance-Management 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 im Dialogfeld für die Verwaltung der Arcserve Appliance 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 Datenspeicher-Dialogfeld 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.

Hinweise:

- Der Standardwert für die Blockgröße der Deduplizierung beträgt 16 KB. Sie können die Blockgröße der Deduplizierung jedoch entsprechend Ihren Anforderungen konfigurieren.

  Um die Blockgröße der Deduplizierung zu konfigurieren, gehen Sie wie folgt vor:

  a. Navigieren Sie zu folgendem Speicherort:

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

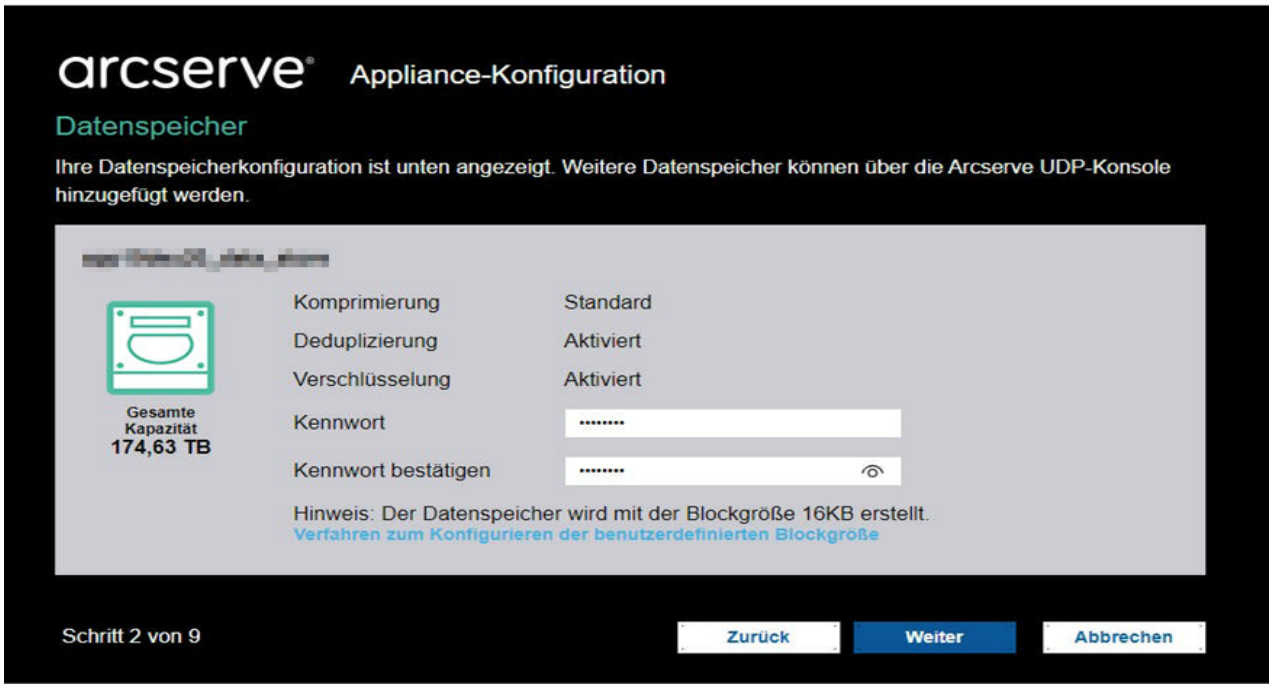
  b. Öffnen Sie die Datei **ApplianceDefaultSetting.properties**, und bearbeiten Sie dann *deduplicationBlockSize*.

- Sie müssen die Blockgröße der Deduplizierung konfigurieren, bevor Sie das Verschlüsselungskennwort für den Datenspeicher angeben und auf die Schaltfläche **Weiter** klicken.

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 im Datenspeicher-Dialogfeld das Verschlüsselungskennwort für den Datenspeicher ein, geben Sie es zur Bestätigung erneut ein, und klicken Sie dann 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.

5. Geben Sie im Dialogfeld "E-Mail und Alert" die folgenden E-Mail- und Alert-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.

Von

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

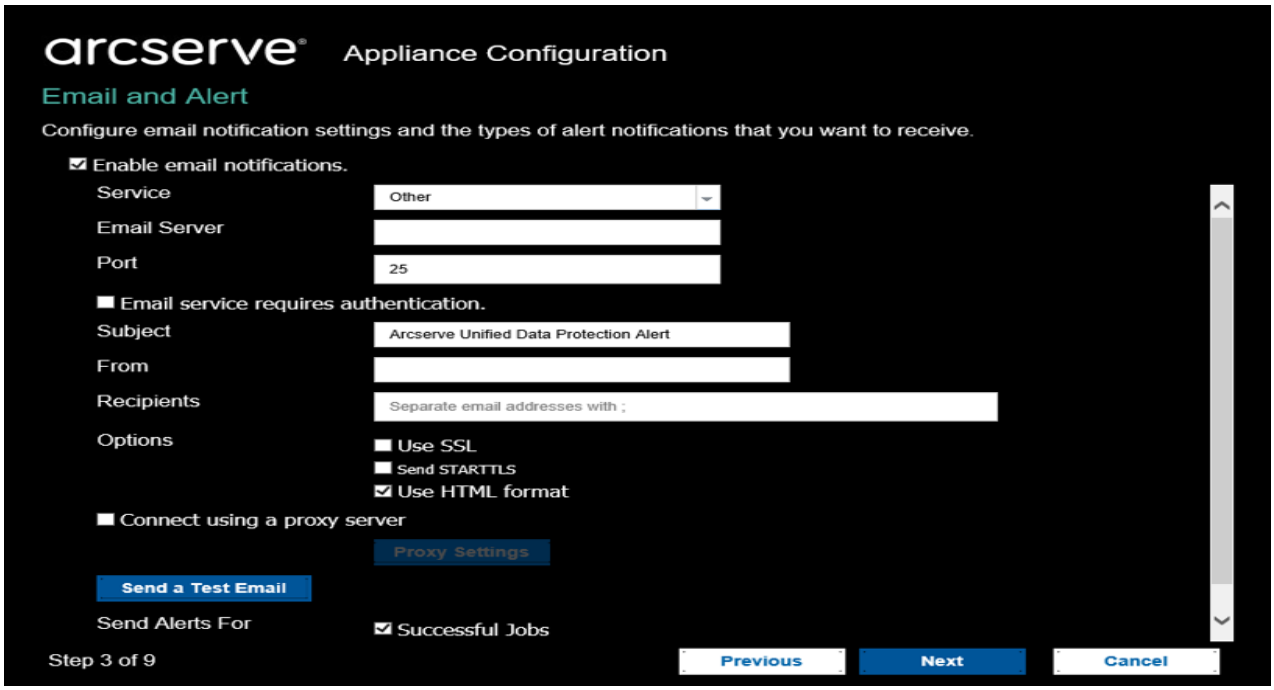
Gibt die Verschlüsselungsmethode für den Kommunikationskanal an.

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.



6. Klicken Sie auf **Weiter**.

   Das Dialogfeld Replikation zum Remote-RPS wird geöffnet.

7. Geben Sie im Dialogfeld "Replikation zum Remote-RPS" die folgenden Details an, wenn Sie möchten, dass die Appliance auf einem 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.

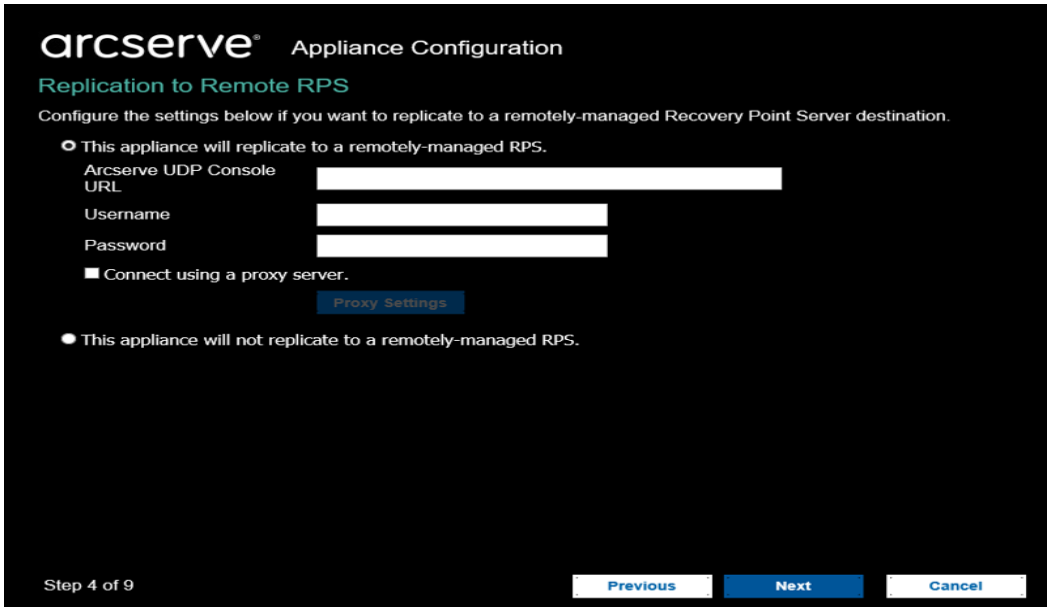
Benutzername und Kennwort

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.

Hinweis: 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.



8. 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.

9. Geben Sie im Dialogfeld "Plan erstellen" die folgenden Details an, um einen Plan zu erstellen:

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.

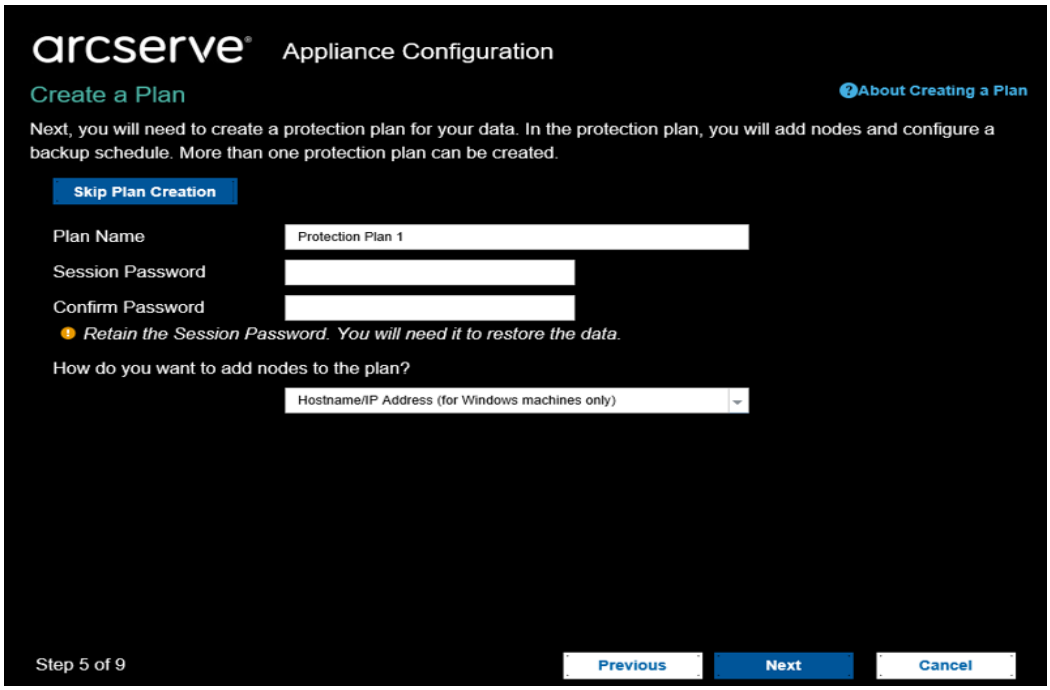
- Von einem vCenter/ESX-Server importieren

  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.



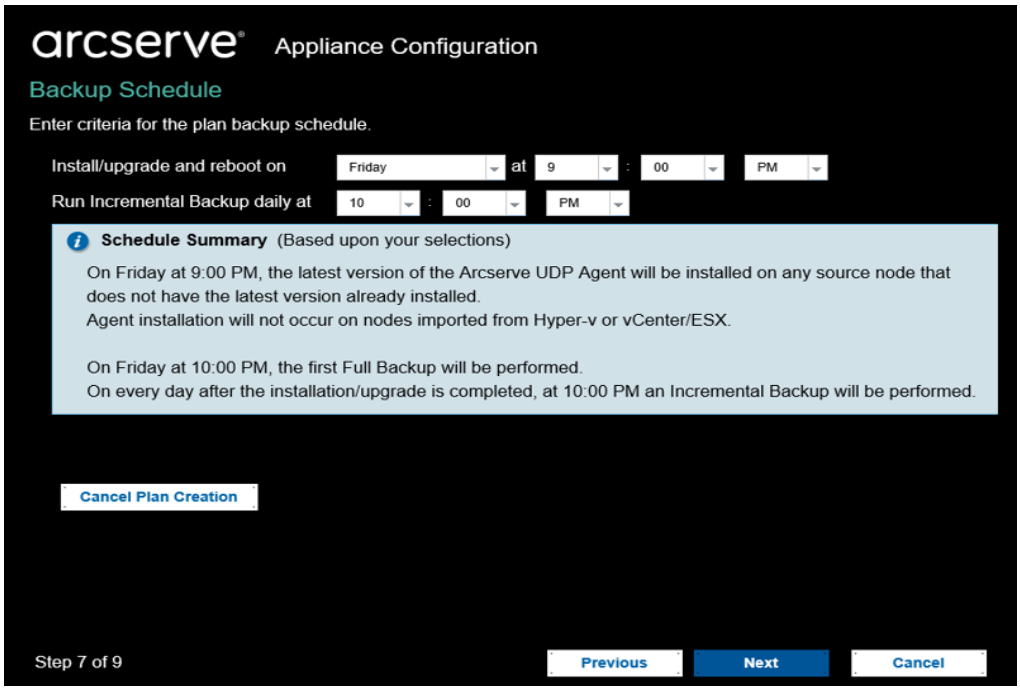
10. Nachdem die Knoten zu Ihrem Plan hinzugefügt wurden, klicken Sie auf **Weiter**.

    Das Dialogfeld Sicherungsablaufplan wird geöffnet.

11. Geben Sie im Dialogfeld "Sicherungsablaufplan" den folgenden Ablaufplan 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**.



12. Klicken Sie auf **Weiter**.

    Das Dialogfeld Bestätigung des Plans wird geöffnet.

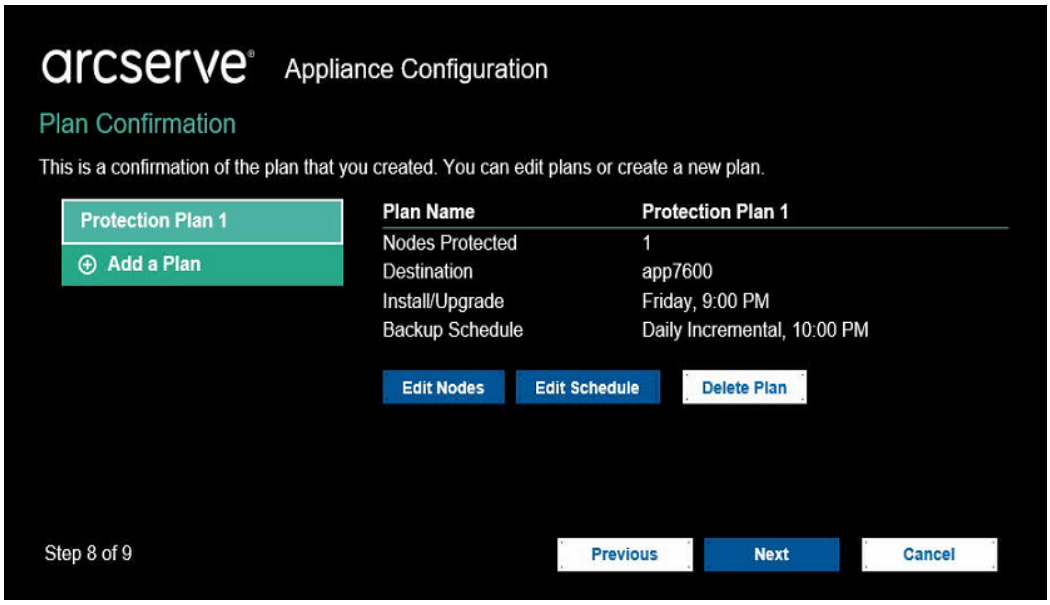
13. Überprüfen Sie im Dialogfeld "Bestätigung des Plans" die Details Ihres Plans. Sie können die Knoten oder den Ablaufplan ändern, indem Sie auf "Knoten bearbeiten" bzw. "Ablaufplan bearbeiten" klicken, oder Sie können einen Plan hinzufügen oder löschen.

    Knoten bearbeiten

    Fügen Sie die Quellknoten hinzu, die Sie schützen möchten.

    Bearbeiten eines Ablaufplans

    Ändert den Sicherungsablaufplan:

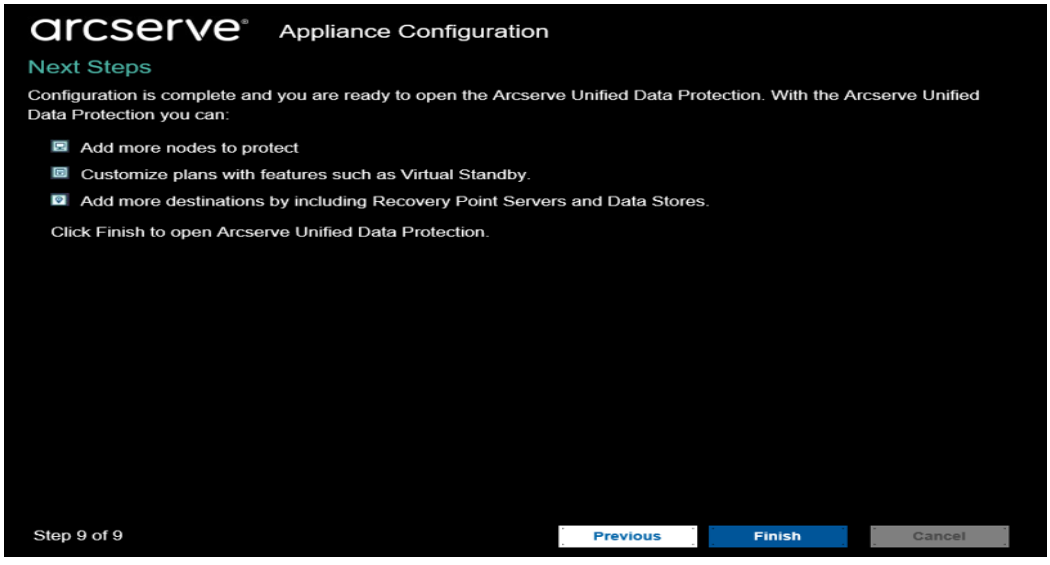


14. Klicken Sie nach der Überprüfung der Pläne auf **Weiter**.

    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.

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



Hinweis: Informationen zur Anmeldung bei der UDP-Konsole mit Domänen-Anmeldeinformationen finden Sie unter Zuweisen von Admin-Berechtigungen und Rollen zu einem Domänenbenutzer.

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 5: 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:

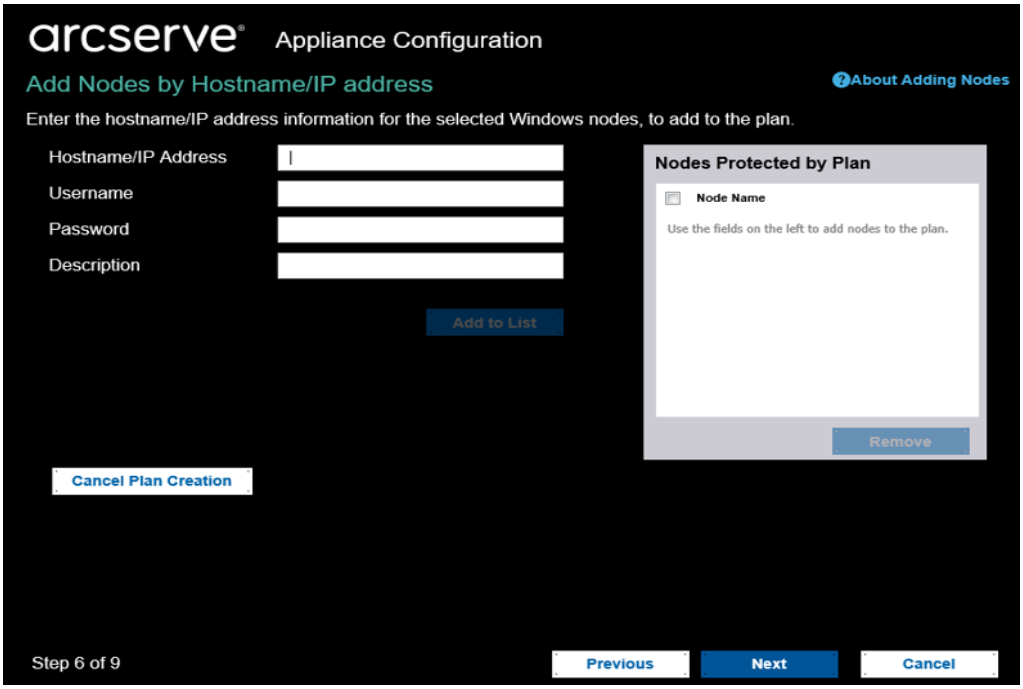
- Manuelle Eingabe der IP-Adresse oder des Hostnamens für den Knoten (Knoten nach Hostname/IP-Adresse hinzufügen)
- Erkennen von Knoten aus einem Active Directory (Knoten nach Active Directory hinzufügen)
- Importieren von VM-Knoten von ESX/vCenter-Servern (vCenter/ESX-Knoten hinzufügen)
- Importieren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

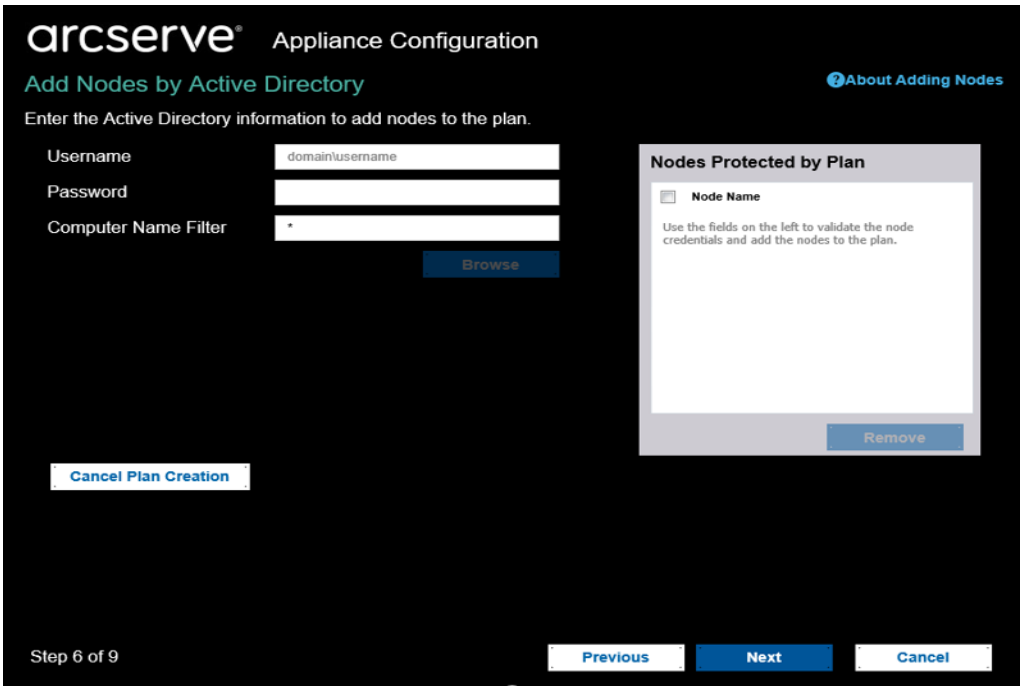
   Gibt das Benutzerkennwort an.

   Computernamenfilter

   Gibt den Filter zum Erkennen der Knotennamen an.

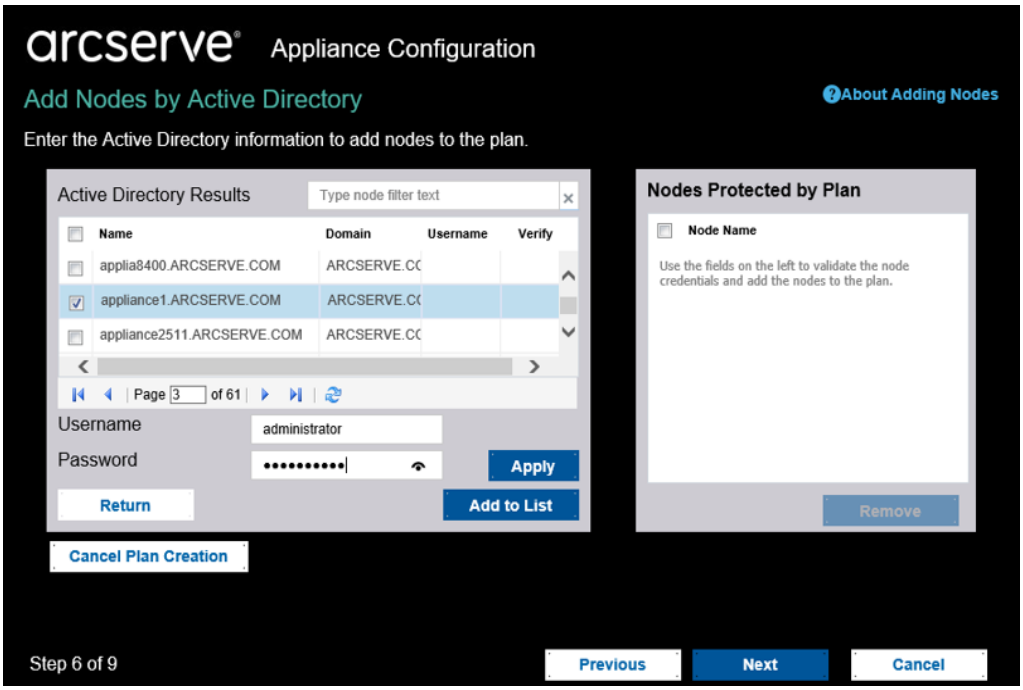
   Planerstellung abbrechen

   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

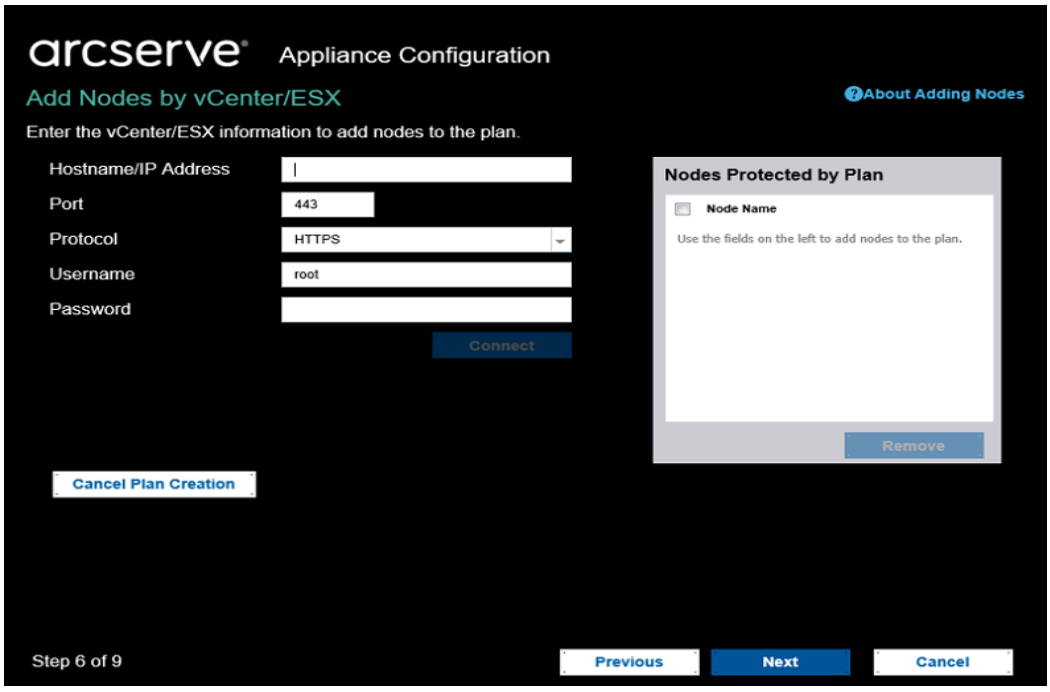
Gibt einen Benutzernamen auf dem Server an.

Kennwort

Gibt das Benutzerkennwort an.

Planerstellung abbrechen

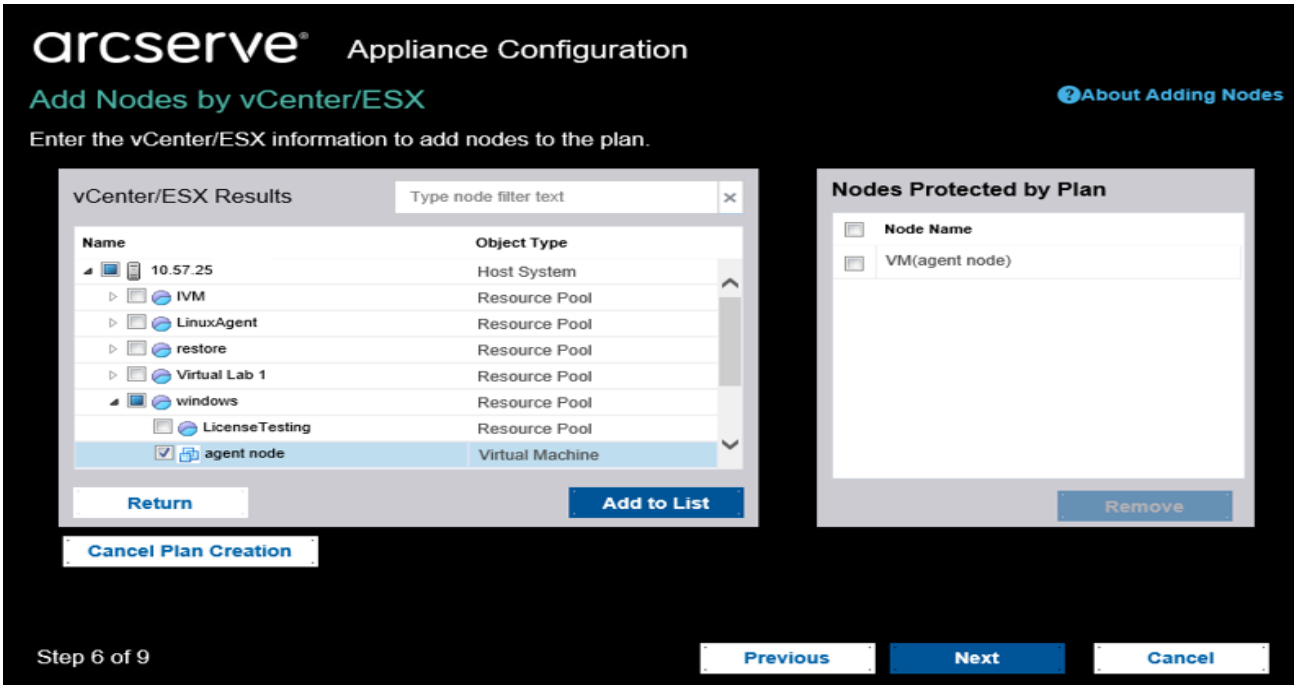
Bricht den gerade erstellten Plan ab.



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**.

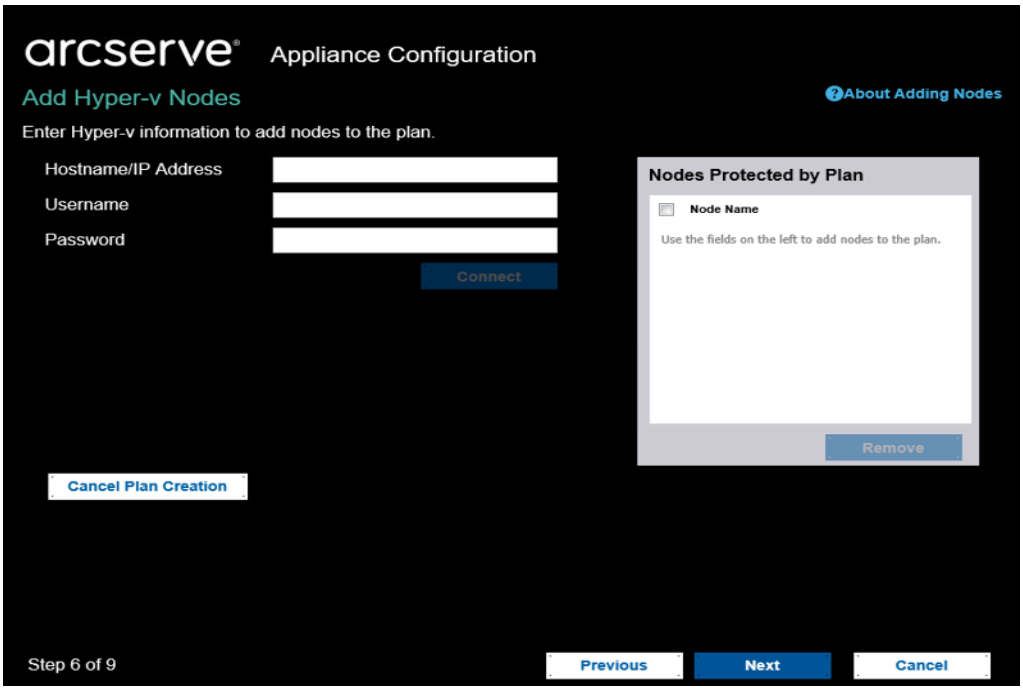
   Die Knoten werden zum Plan hinzugefügt.

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

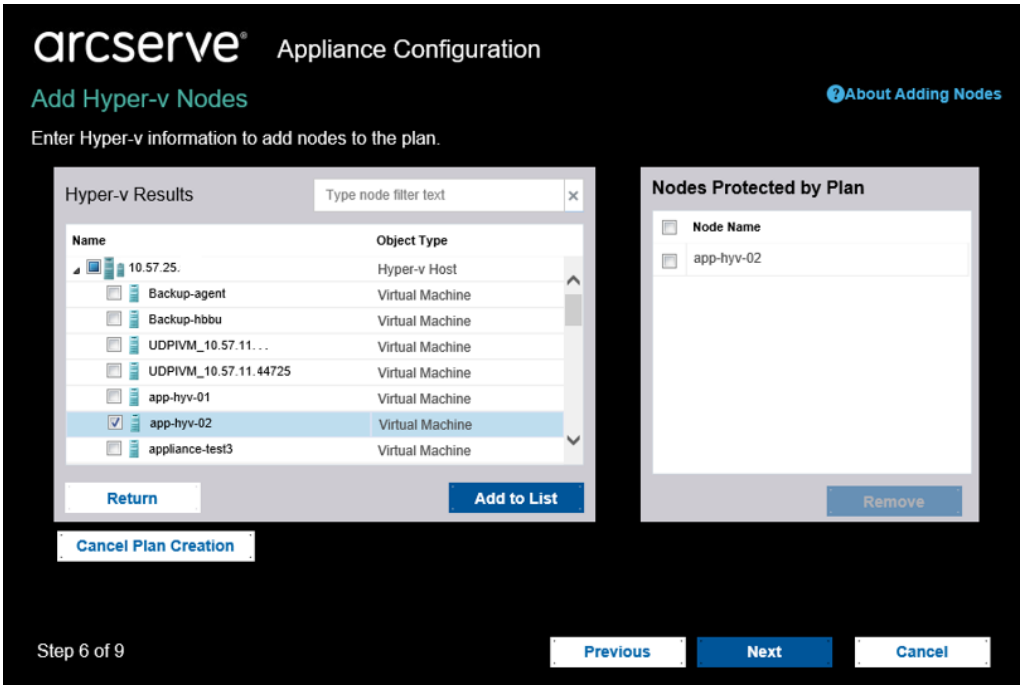
Gibt das Kennwort für den Benutzernamen an.

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 einem 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.

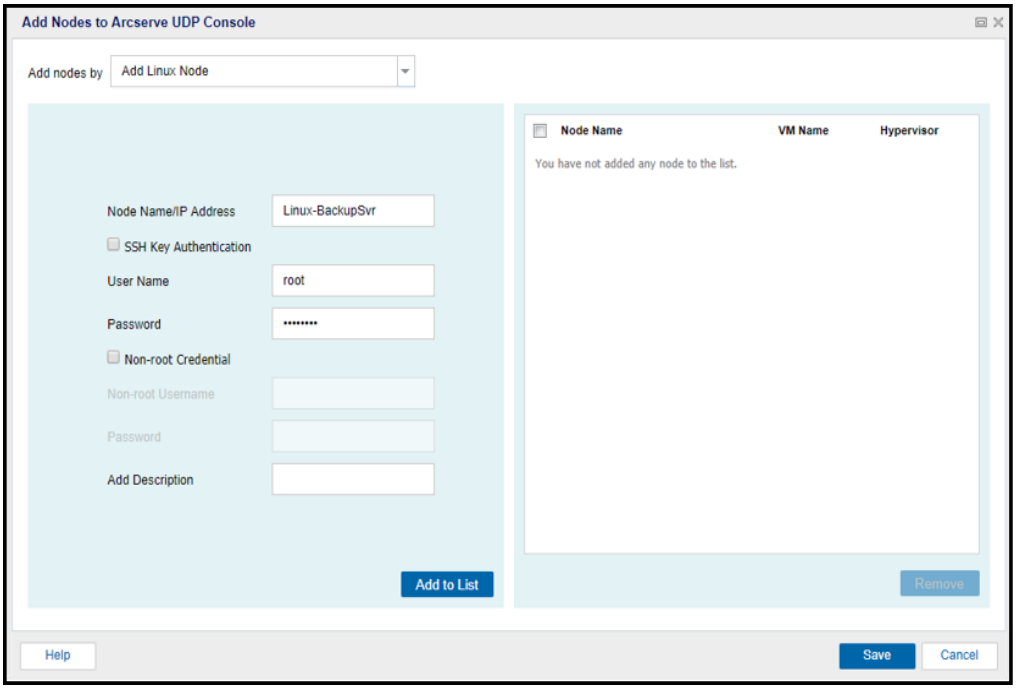
Erstellen eines Plans zur Sicherung von Linux-Sicherungsserver

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

Befolgen Sie diese Schritte:

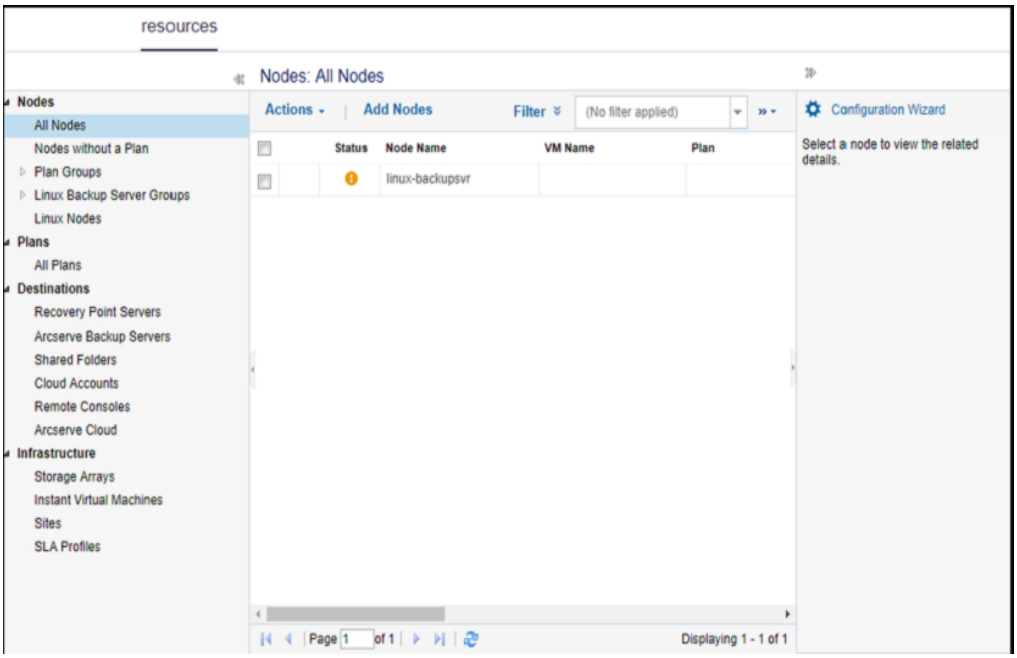
1. Klicken Sie in der Arcserve UDP-Konsole auf die Registerkarte **Ressourcen**.
2. Klicken Sie im rechten Fensterbereich auf **Alle Knoten**.
3. Klicken Sie im mittleren Fensterbereich auf **Knoten hinzufügen**.

   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**.



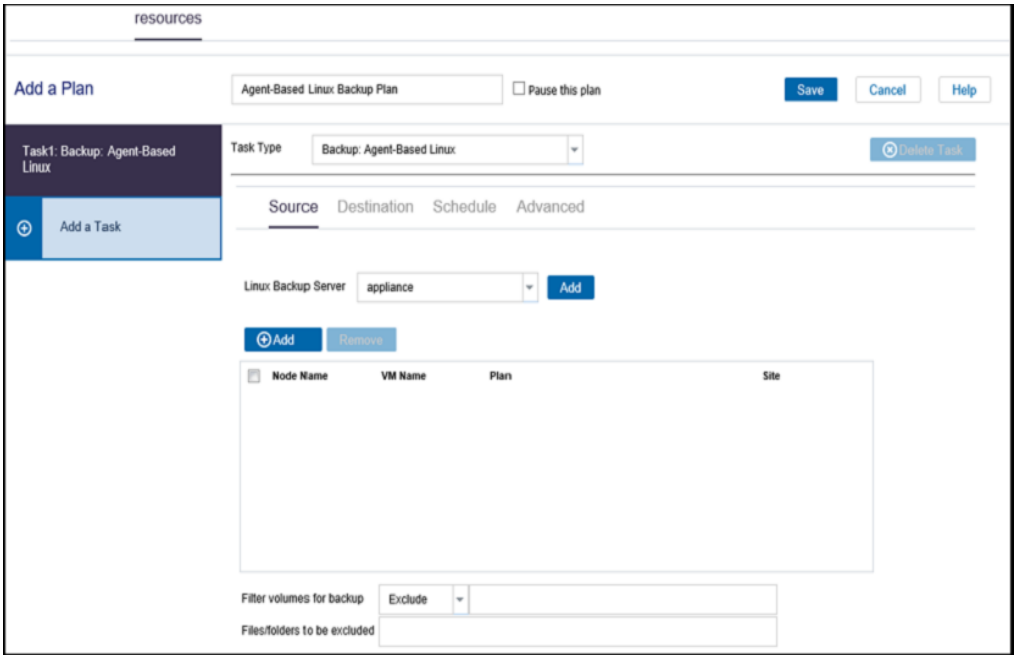
6. Klicken Sie auf **Speichern**.

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

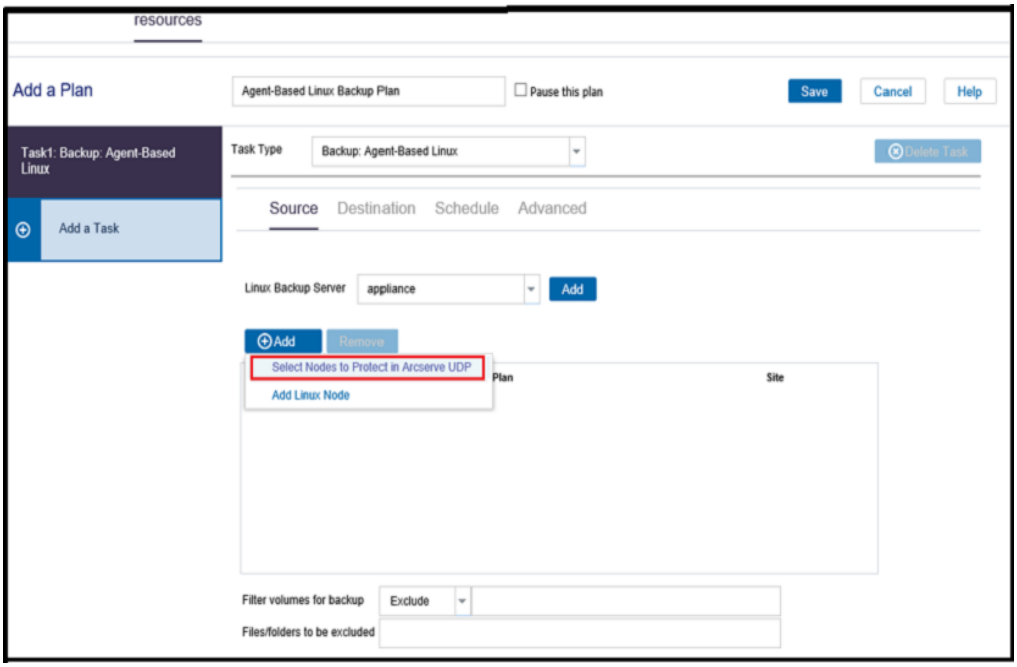


7. Navigieren Sie zu **Alle Pläne**, und erstellen Sie einen agentenbasierten Linux-Plan.

Die Registerkarte **Quelle** wird angezeigt.

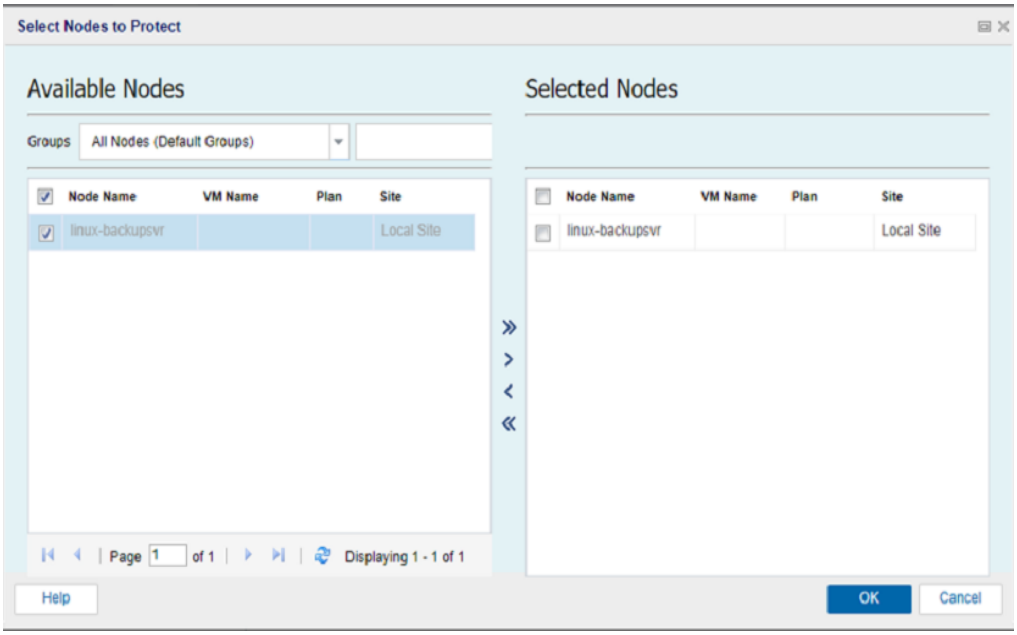


8. Wählen Sie den Drop-down-Liste **Hinzufügen** die Option *In Arcserve UDP zu schützende Knoten* aus.



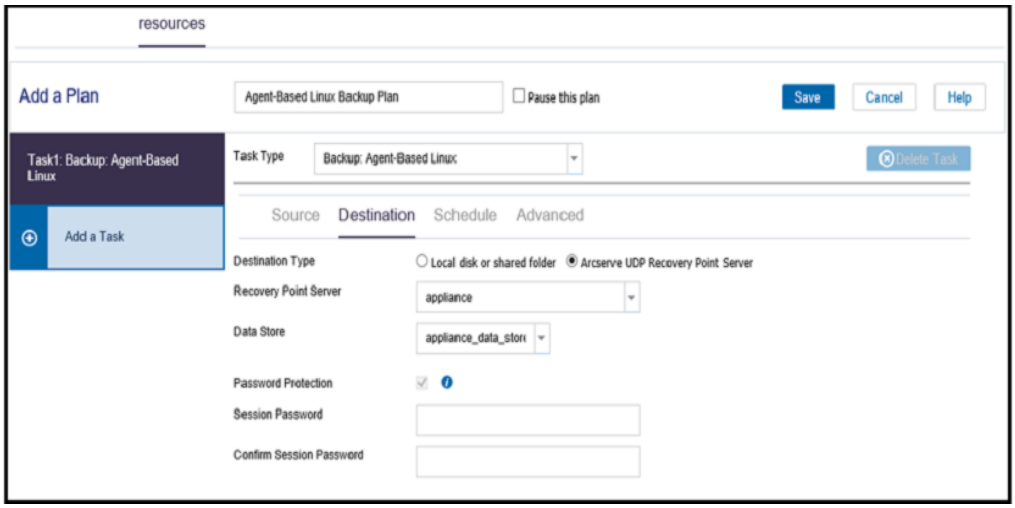
Das Dialogfeld "**Zu schützende Knoten auswählen**" wird geöffnet.

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

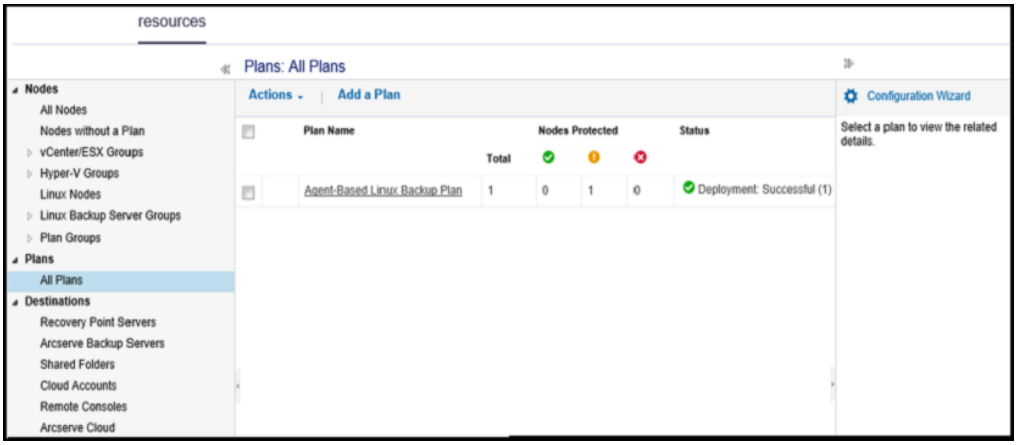


Die Registerkarte **Ziel** wird angezeigt.

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. Schalten Sie den Linux-Sicherungsserver aus, und fügen Sie einen externen Switch zum Linux-Sicherungsserver hinzu.
4. Schalten Sie den Linux-Sicherungsserver ein, und fügen Sie ein Profil zu den Netzwerkeinstellungen unter der neuen Ethernet-Verbindung hinzu, um eine IP-Adresse zu erhalten.

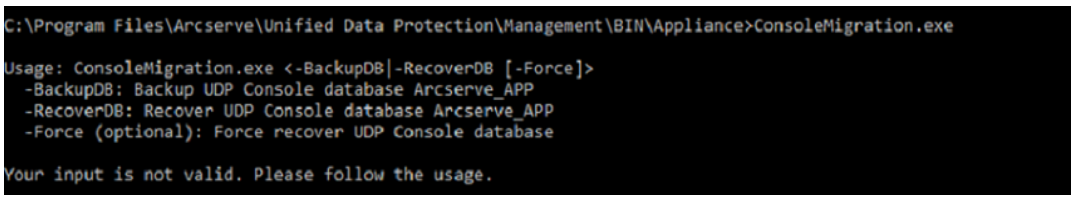
   Hinweis: Der Linux-Sicherungsserver wird während des Vorgangs neu gestartet, wenn keine IP-Adresse zugewiesen wird.
5. Zum Ausführen eines Linux-Instant VM-Job zum lokalen Hyper-V wählen Sie den neu hinzugefügten virtuellen Netzwerk-Switch aus.

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

Migrieren der Arcserve UDP-Konsole mithilfe von ConsoleMigration.exe

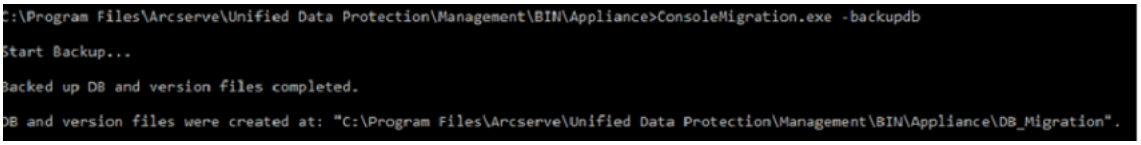
Auf der Arcserve Appliance können Sie die Arcserve UDP-Konsole mit *ConsoleMigration.exe* auf eine andere Appliance migrieren. Ab Arcserve UDP 6.5 Update 2 oder höher können Sie die Arcserve UDP-Konsole zwischen zwei beliebigen Arcserve UDP-Konsolen migrieren, auch wenn sie nicht zur Appliance gehören.

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:

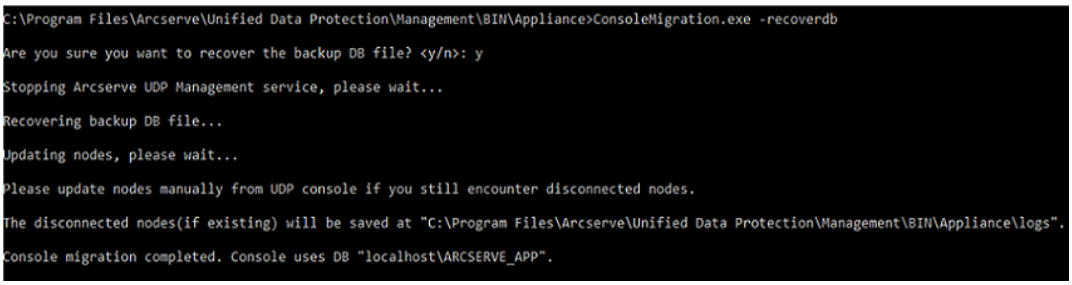
   <UDP_Home> *Management**BIN**Appliance*\

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

Durchführen der Migration zwischen Arcserve Appliances

In diesem Thema wird die Lösung vorgestellt, mit der Benutzer eine Migration von einer vorhandenen Arcserve Appliance auf eine neue Arcserve Appliance durchführen können.

Migrieren wir zum Beispiel Arcserve Appliance 1 zu Arcserve Appliance 2. Es gelten die folgenden Voraussetzungen:

- Stellen Sie sicher, dass Sie eine Verbindung zu Appliance 1 und Appliance 2 herstellen können.
- Auf der Appliance 2 muss genügend Speicher für alle Daten der Appliance 1 frei sein.
- Vergewissern Sie sich, dass auf der Arcserve Appliance 1 kein Job ausgeführt wird.

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

Um von einer beliebigen Appliance zu einer neuen Appliance zu migrieren, folgen Sie der unten angegebenen Lösung.

- Lösung

Lösung

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:

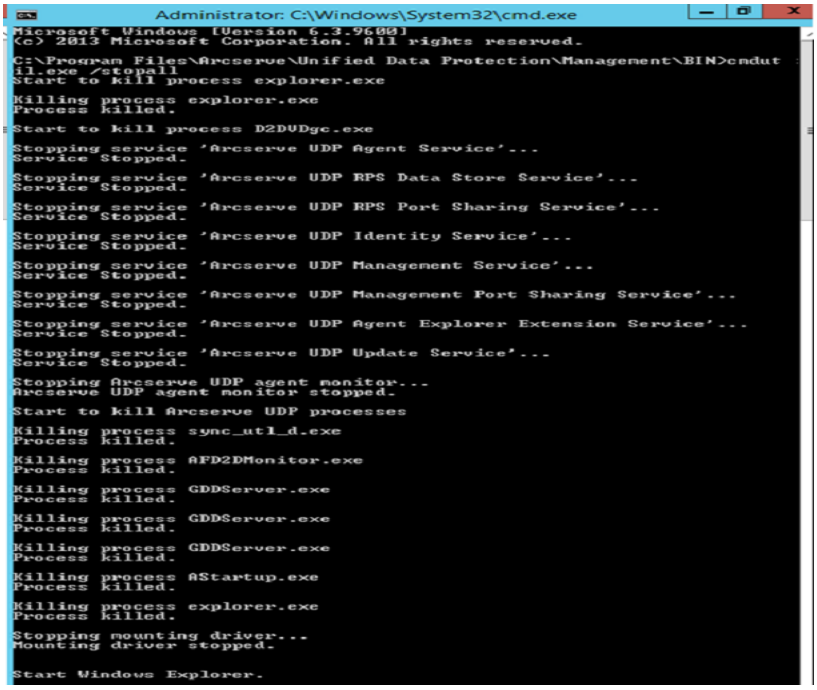
- Stellen Sie auf Arcserve Appliance 1 sicher, dass kein Job ausgeführt wird.
- Sie haben die Arcserve UDP-Konsole von Arcserve Appliance 1 zu 2 migriert.

  Hinweis: Weitere Informationen zur Migration der Arcserve UDP-Konsole von Appliance 1 zu 2 finden Sie unter Migration der Arcserve UDP-Konsole mit ConsoleMigration.exe.

Befolgen Sie diese Schritte:

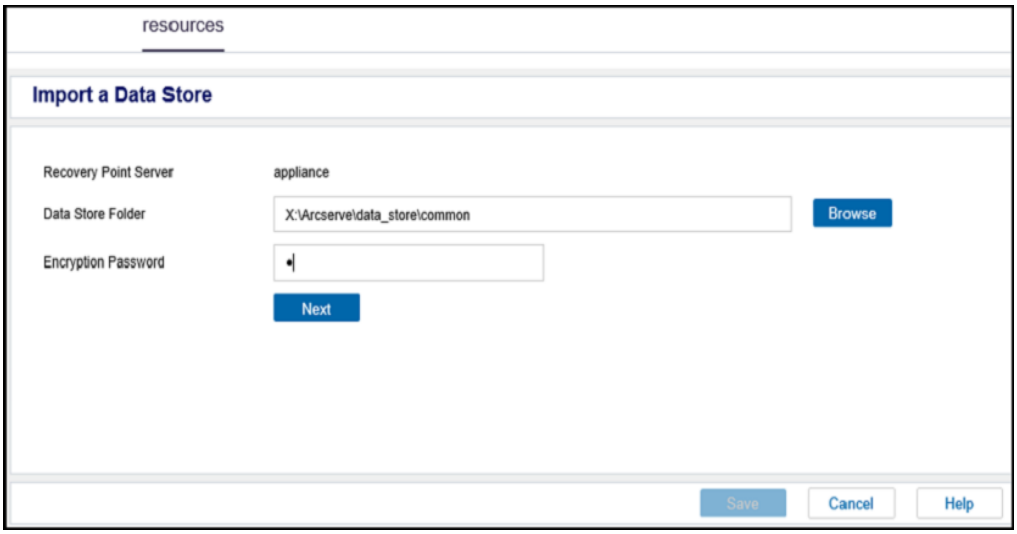
1. Beenden Sie alle Arcserve UDP-Dienste auf Arcserve Appliance 1 mit dem folgenden Befehl in der Befehlszeile:

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



2. Kopieren Sie alle Daten auf Datenträger X und Y manuell von Arcserve Appliance 1 auf 2.
3. Starten Sie auf Appliance 2 alle Arcserve UDP-Dienste, und importieren Sie

dann die Datenspeicher, die Sie von Appliance 1 kopiert haben.



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

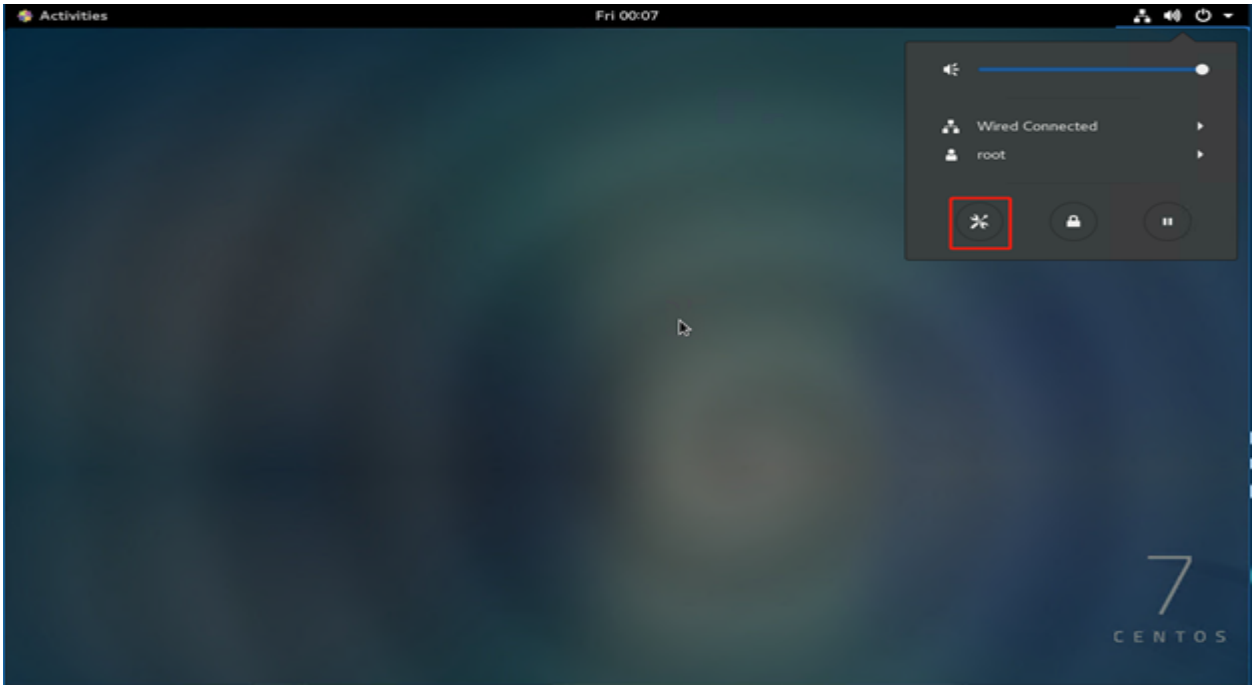
Sie haben die vorhandene Arcserve Appliance- erfolgreich in eine andere neue Arcserve Appliance- migriert.

Ändern der Eingabequelle des vorinstallierten Linux-Sicherungsservers

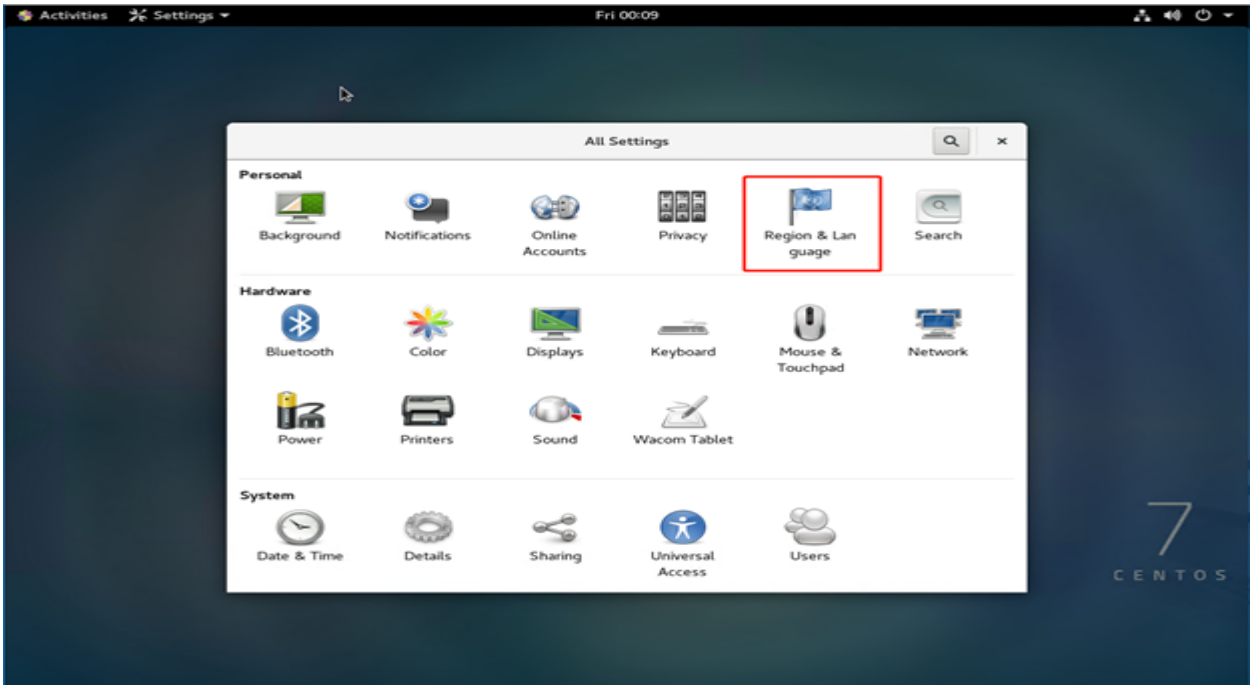
Sie können die Tastatur des vorinstallierten Linux-Sicherungsservers ändern.

Befolgen Sie diese Schritte:

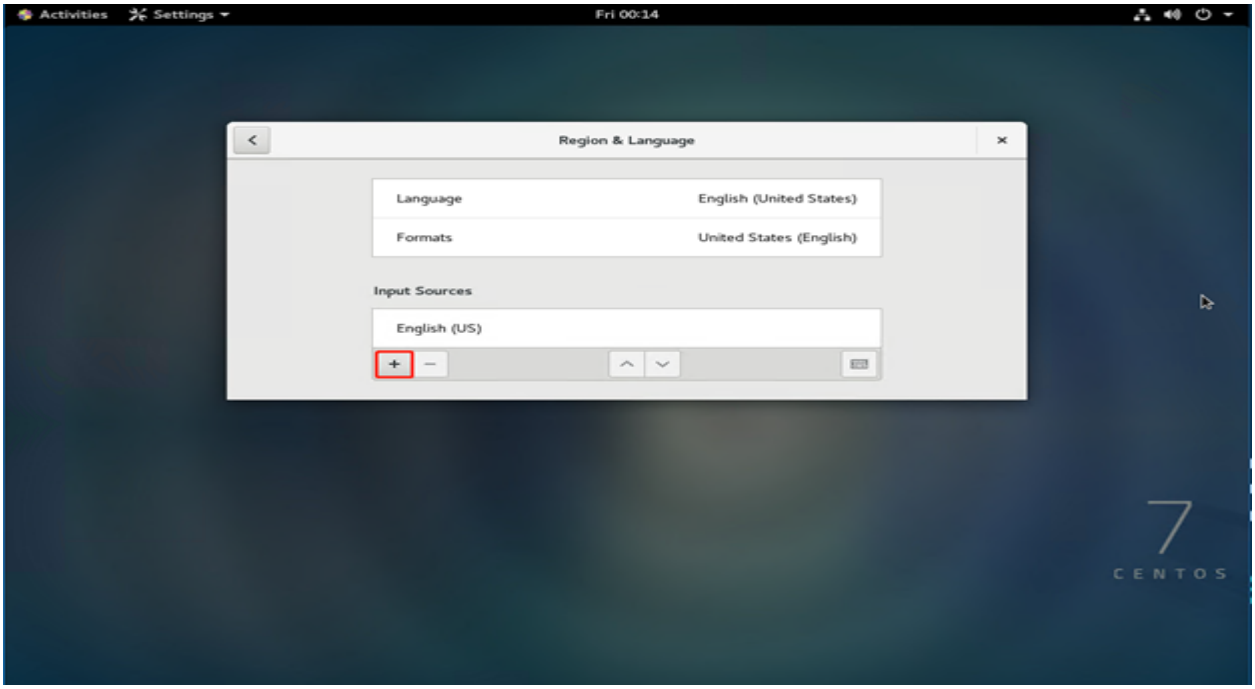
1. Melden Sie sich bei Arcserve Appliance als Administrator an.
2. Klicken Sie auf **Einstellungen**.



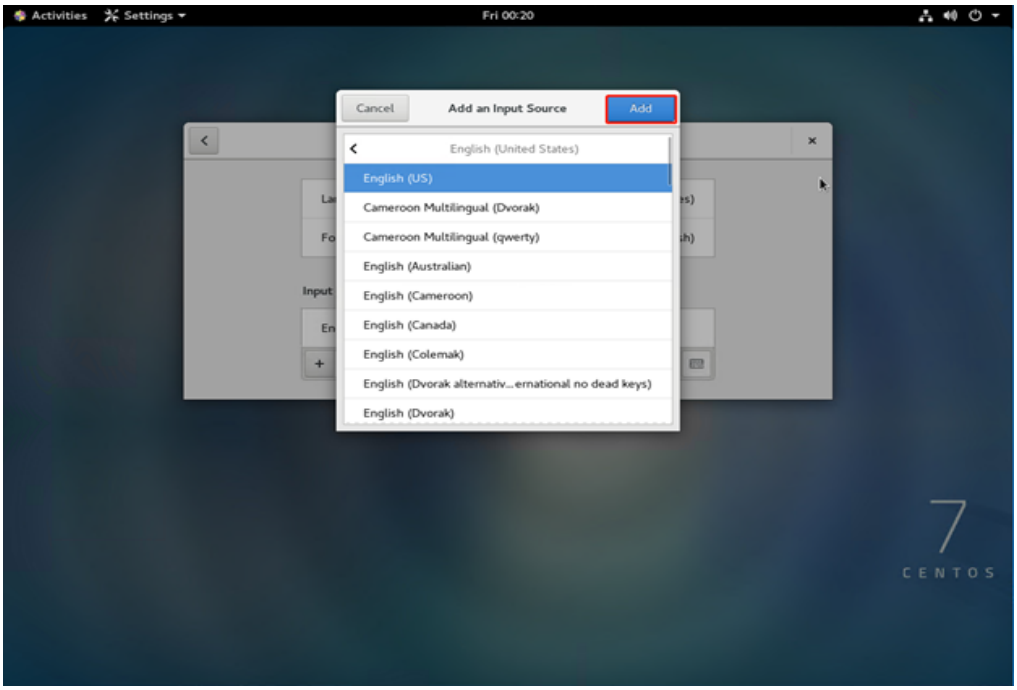
3. Klicken Sie auf **Region & Sprache**.



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 6: Überwachen des Appliance-Servers per Remote-Zugriff

Sie können Arcserve Appliance per Remote-Zugriff überwachen.

Dieser Abschnitt enthält folgende Themen:

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.

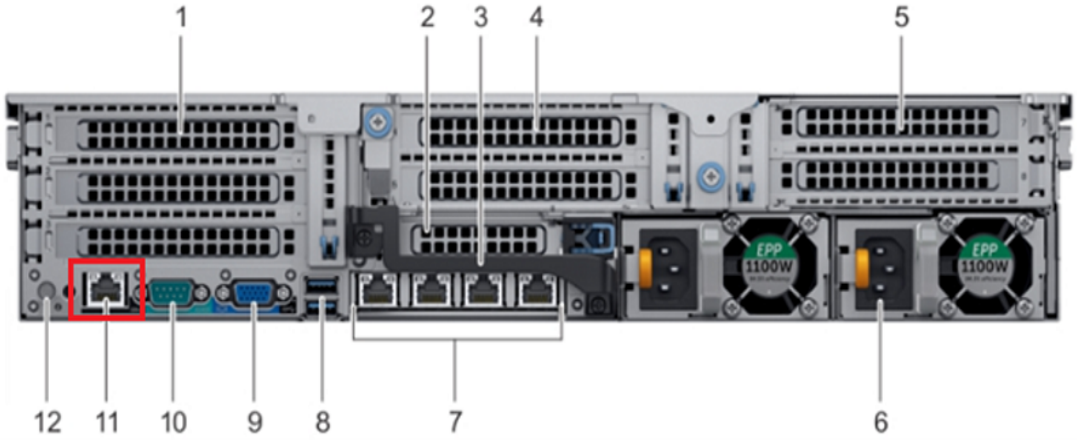
Suchen der IP-Adresse des integrierten Dell Remote Access Controller für die Serie 9000 (iDRAC)

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

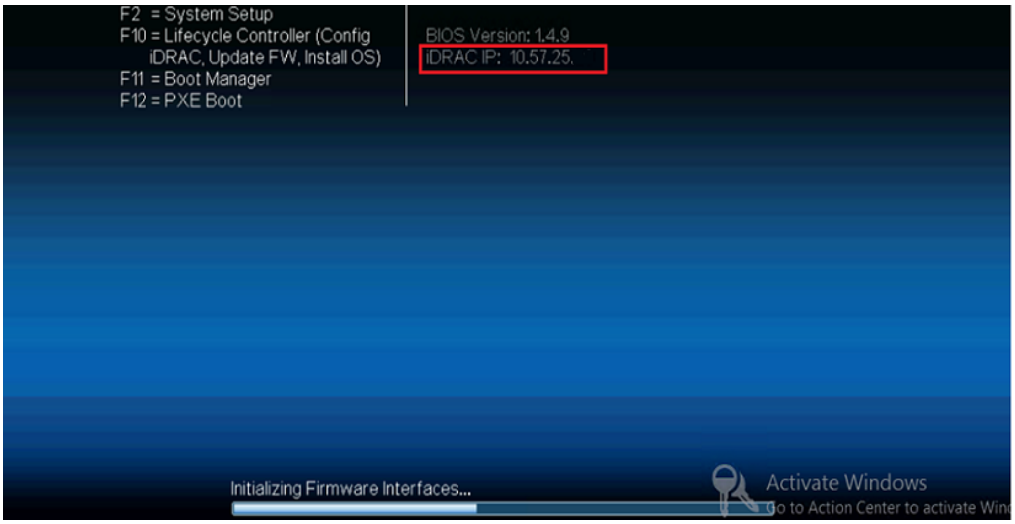


iDRAC9 dedicated network port on
rear panel of Arcserve Appliance 9072DR-9504DR series models

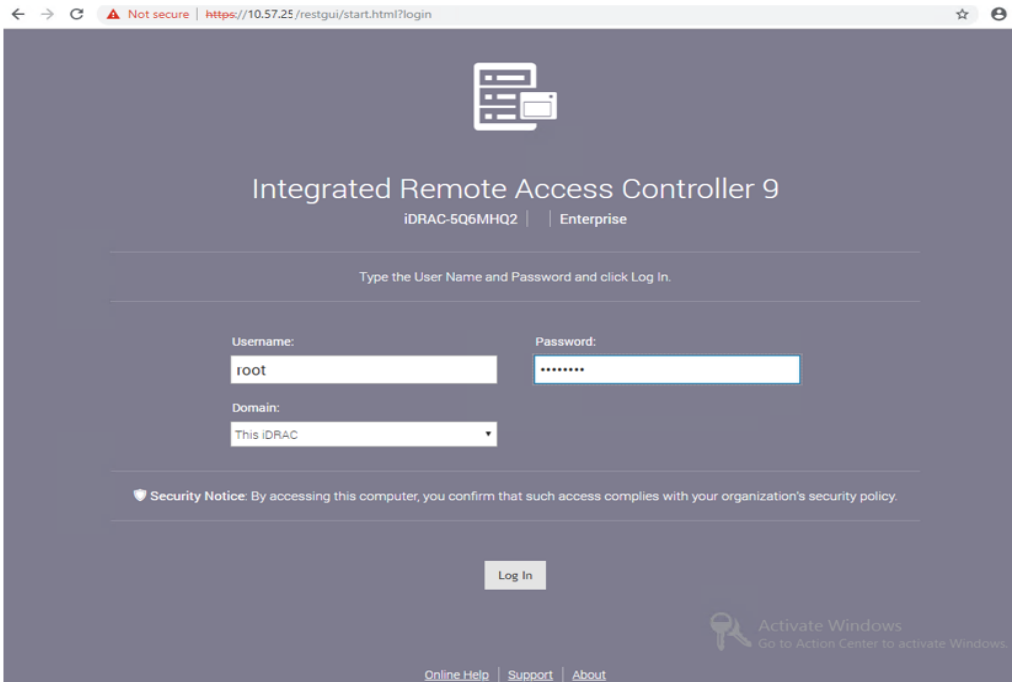
Sie finden die IP-Adresse des iDRAC auf der Appliance.

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.

Suchen der IP-Adresse des integrierten Dell Remote Access Controller für die Serie X (iDRAC)

Das Arcserve Appliance Modell der Serie X ist so konfiguriert, dass DHCP für iDRAC standardmäßig verwendet wird. Um auf iDRAC zugreifen zu können, stellen Sie sicher, dass Sie die Ethernet-Kabel an den dedizierten iDRAC9-Netzwerkport

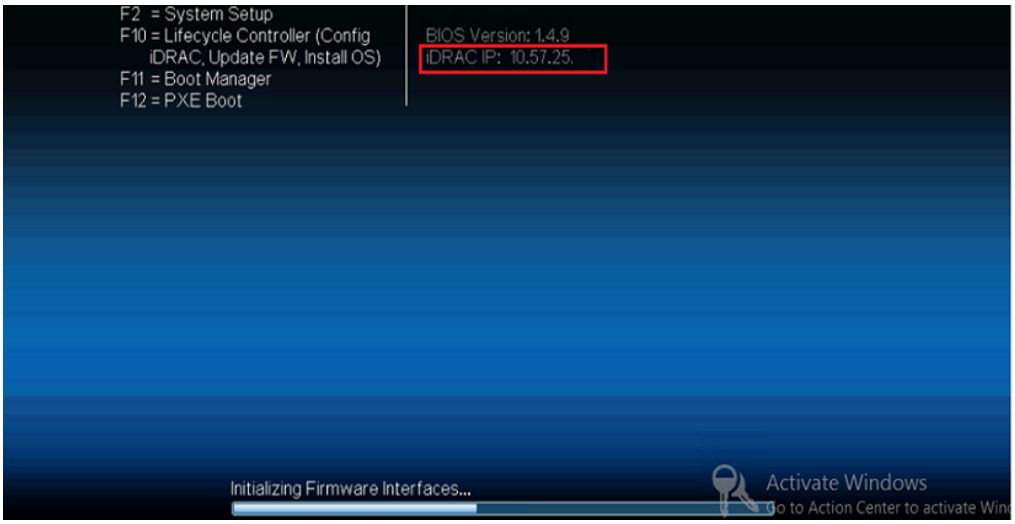
anschließen. Informationen zum Bedienfeld und dedizierten iDRAC9-Netzwerkport der Modelle der Arcserve Appliance Serie X finden Sie unter Bedienfeld der Serie X.

Rückseite der Serie X

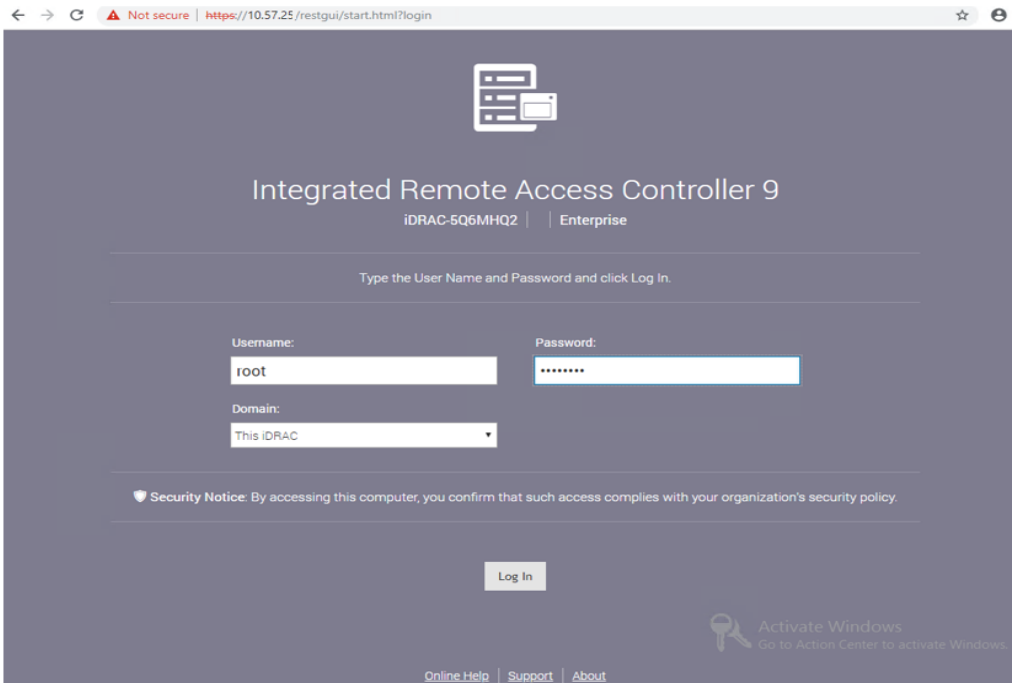
Sie finden die IP-Adresse des iDRAC auf der Appliance.

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*.



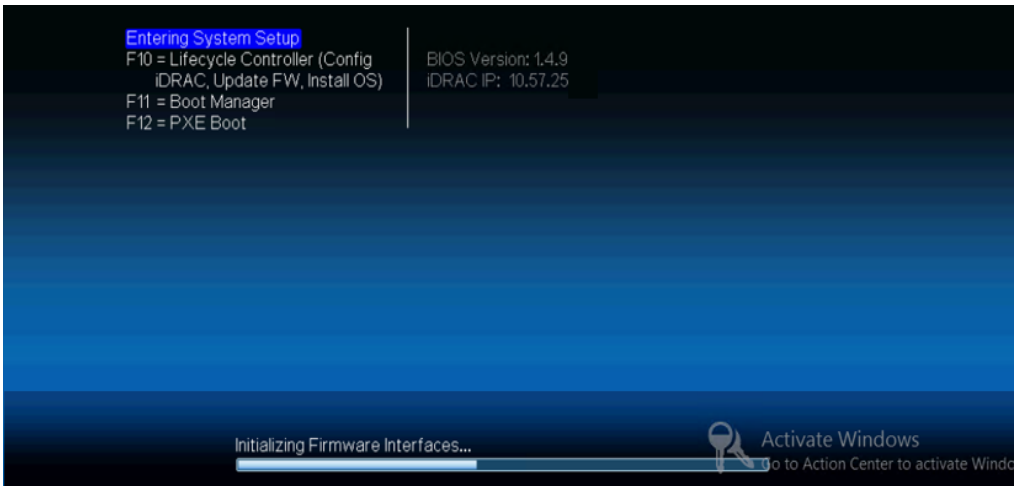
Die Anmeldeseite von iDRAC wird angezeigt.

Konfigurieren der DHCP- oder statischen IP-Adresse des iDRAC

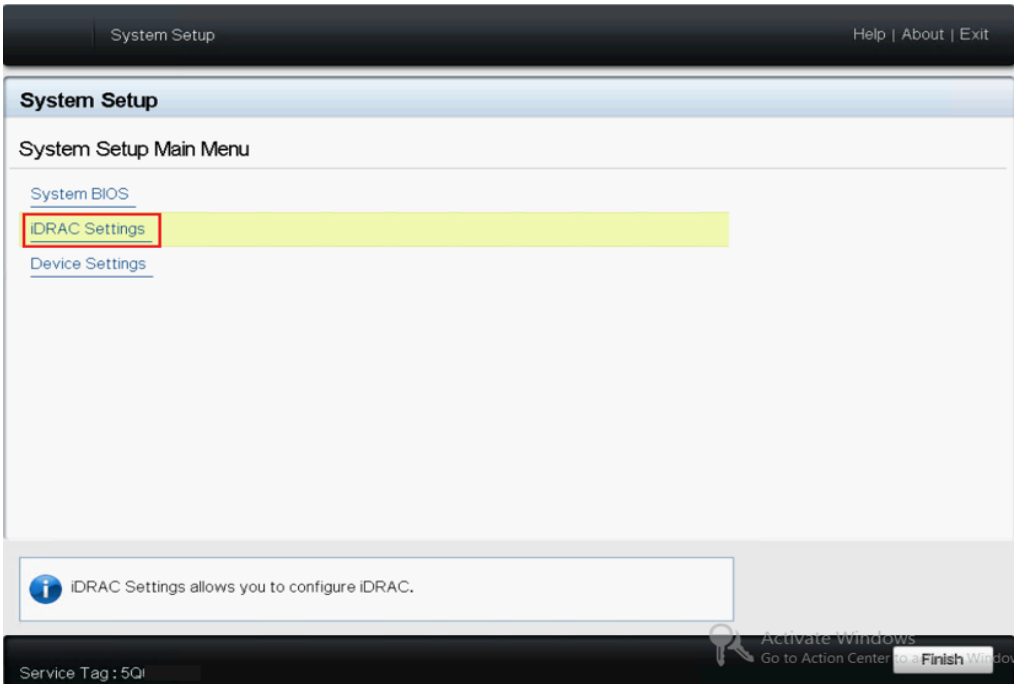
Sie können den DHCP-Netzwerk-Modus für iDRAC festlegen.

Befolgen Sie diese Schritte:

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

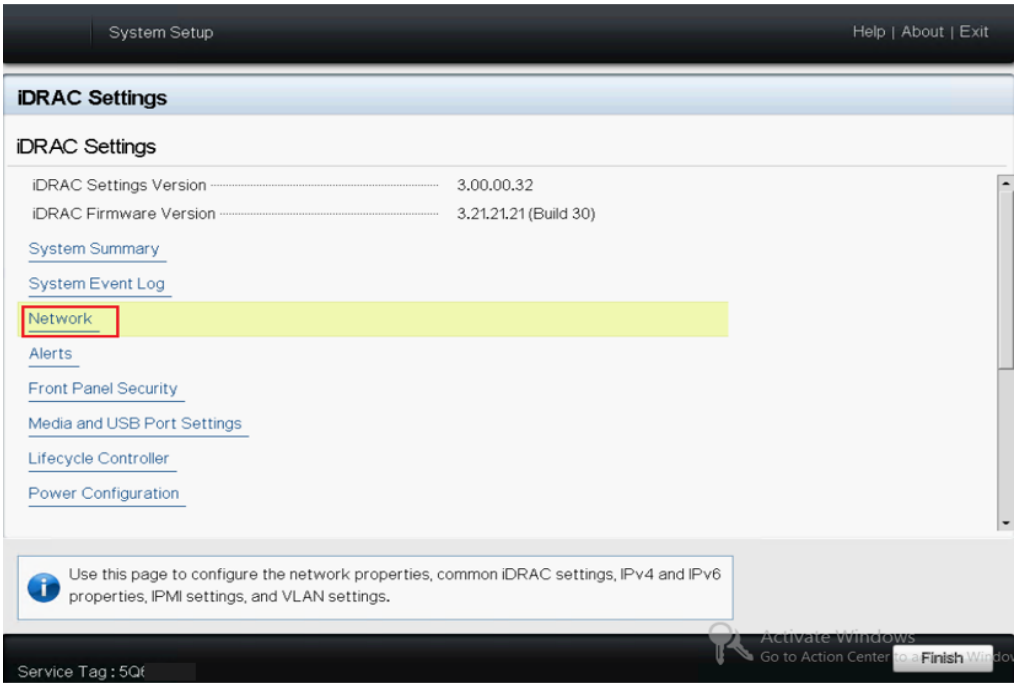


2. Klicken Sie im Bildschirm des Hauptmenüs des System-Setups auf i**DRAC Einstellungen**.

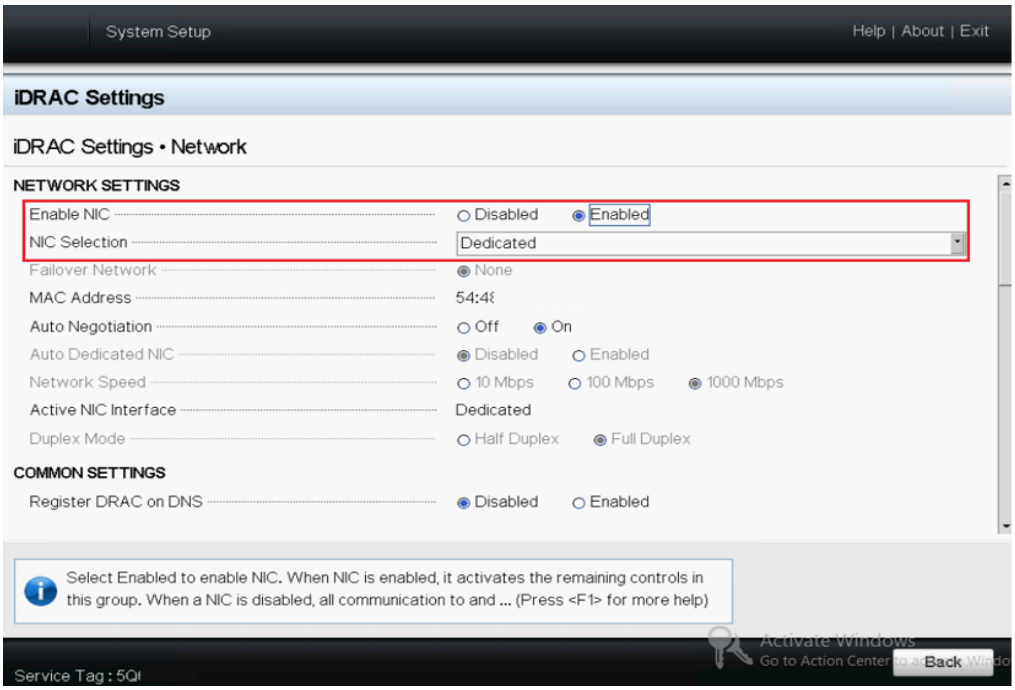


3. Klicken Sie in den Optionen der iDRAC Einstellungen auf**Netzwerk**.

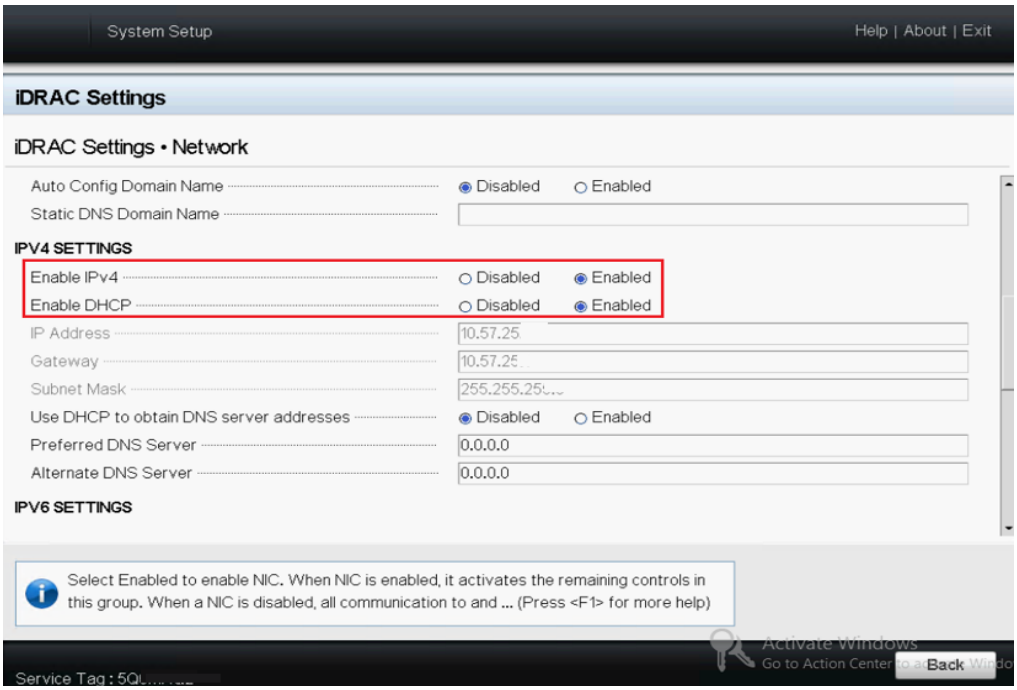
Die Felder für die Netzwerk-Einstellungen werden angezeigt.



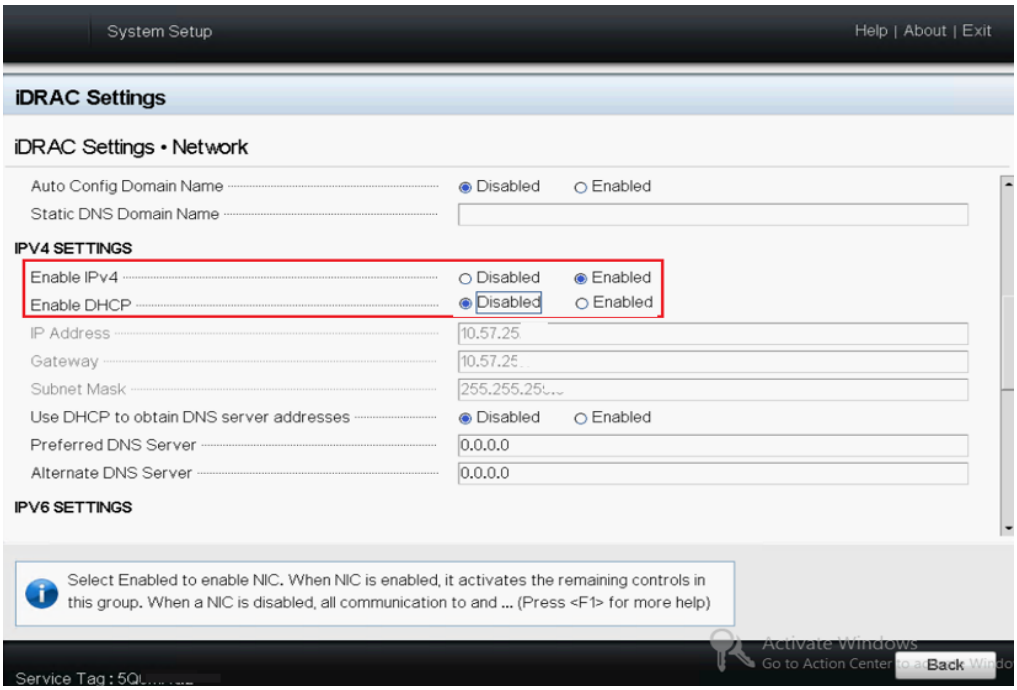
4. Wählen Sie **Aktiviert** für **NIC-Einstellung aktivieren** aus, und wählen Sie **Dedizierte** für **NIC-Auswahl** aus, um verwenden die dedizierte Netzwerkschnittstelle zu verwenden.



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

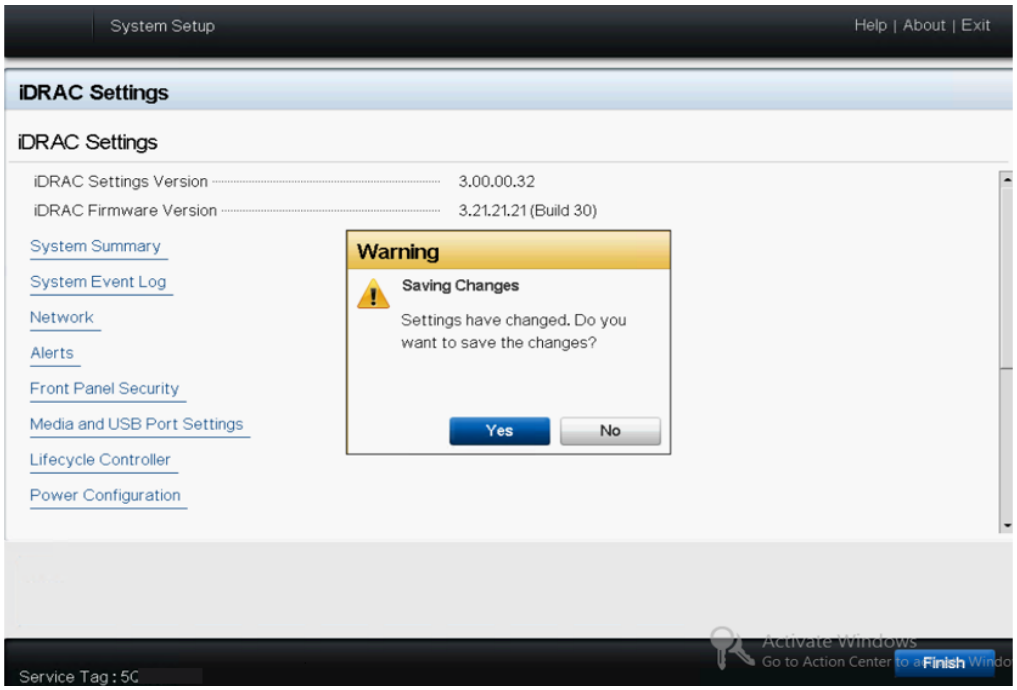


Hinweis: Wenn Sie die statische IP-Adresse für das dedizierte iDRAC-Netzwerk festlegen möchten, legen Sie für **IPv4 aktivieren** die Option **Aktiviert** und für **DHCP aktivieren Deaktiviert** aus. Legen Sie IP-Adresse, Gateway und Subnetzmaske entsprechend der Netzwerkkonfiguration fest.

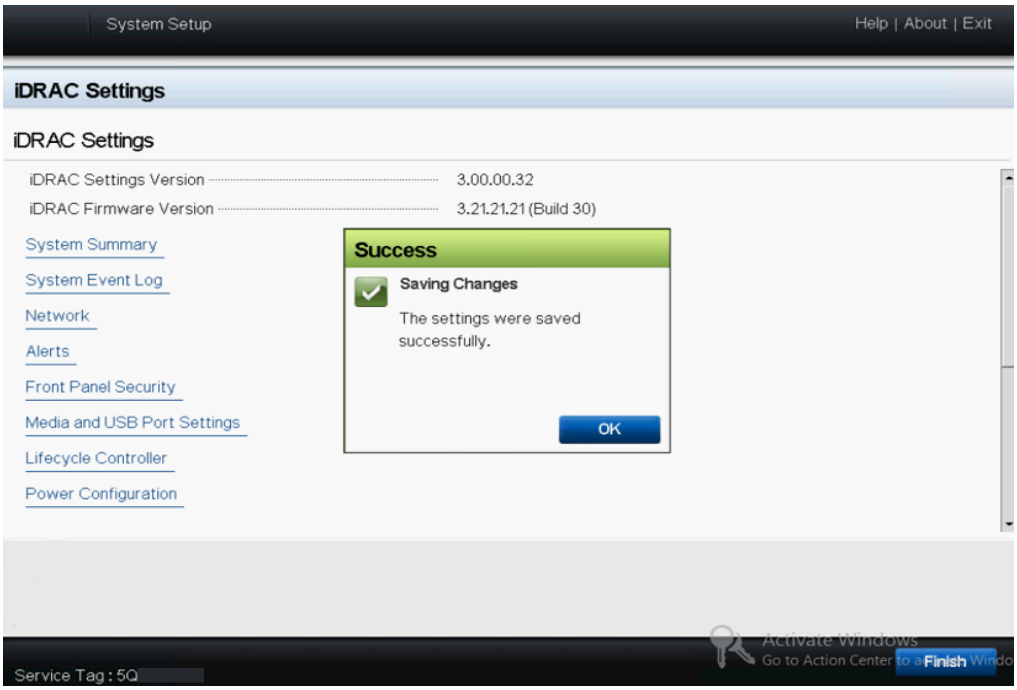


6. Klicken Sie auf **Zurück**, klicken Sie auf **Fertig stellen**, und klicken Sie dann auf **Ja** im Dialogfeld **Warnung**.

Die Netzwerkinformationen werden gespeichert.

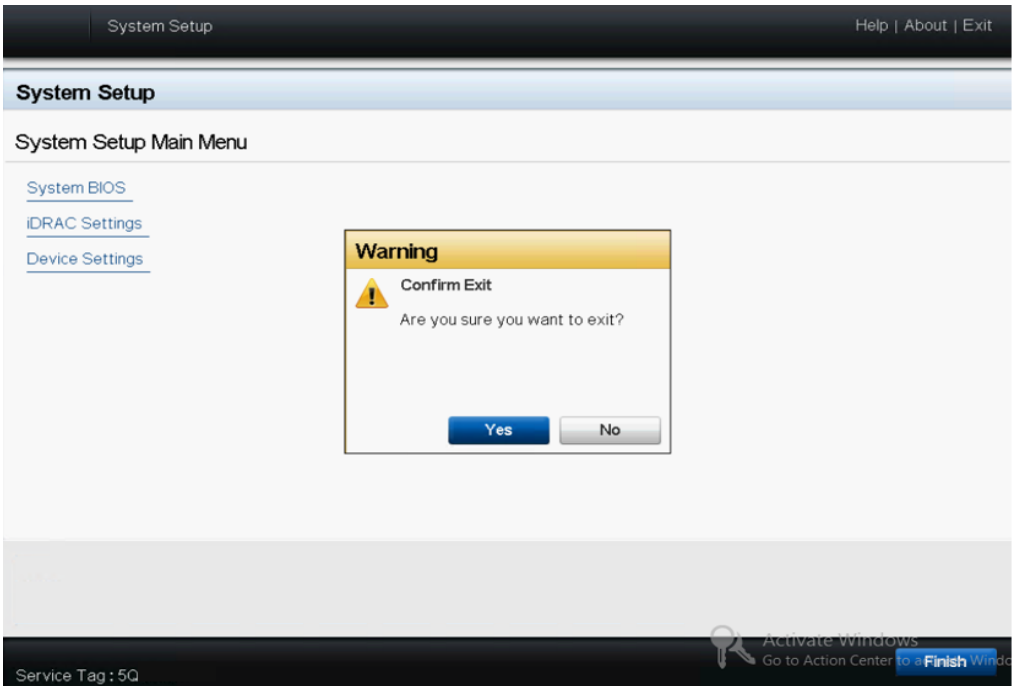


7. Klicken Sie im Dialogfeld **Erfolg** auf **OK**.



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.

Arbeiten mit dem Baseboard Management Controller (BMC)

Dieser Abschnitt enthält folgende Themen:

Überwachen und Verwalten des Baseboard Management Controllers (BMC)

Die Modelle der Arcserve Appliance 10024BU-10576DR-Serie werden mit Baseboard Management Controller (BMC) installiert. Mit dem BMC können Serveradministratoren die allgemeine Verfügbarkeit der Arcserve Appliance verbessern.

Der BMC warnt Administratoren bei Serverproblemen, ermöglicht die Serververwaltung aus der Ferne und reduziert die Notwendigkeit des physischen Zugriffs auf den Server. Er bietet außerdem Fernzugriff für mehrere Benutzer von verschiedenen Standorten für die Wartung und Verwaltung des Systems.

Um den Systemstatus zu überwachen, Systeminformationen zu verwalten und die Remote-Konsole zu starten, müssen Sie sich bei IPMI (Intelligent Platform Management Interface) anmelden.

Befolgen Sie diese Schritte:

1. Öffnen Sie einen Webbrowser, und geben Sie die BMC-IP-Adresse in folgendem Format ein:

   https://BMC-IP-Adresse.

   Der Anmeldebildschirm wird geöffnet.

2. Geben Sie die Anmeldeinformationen wie folgt ein:

   - **Username:** ADMIN.

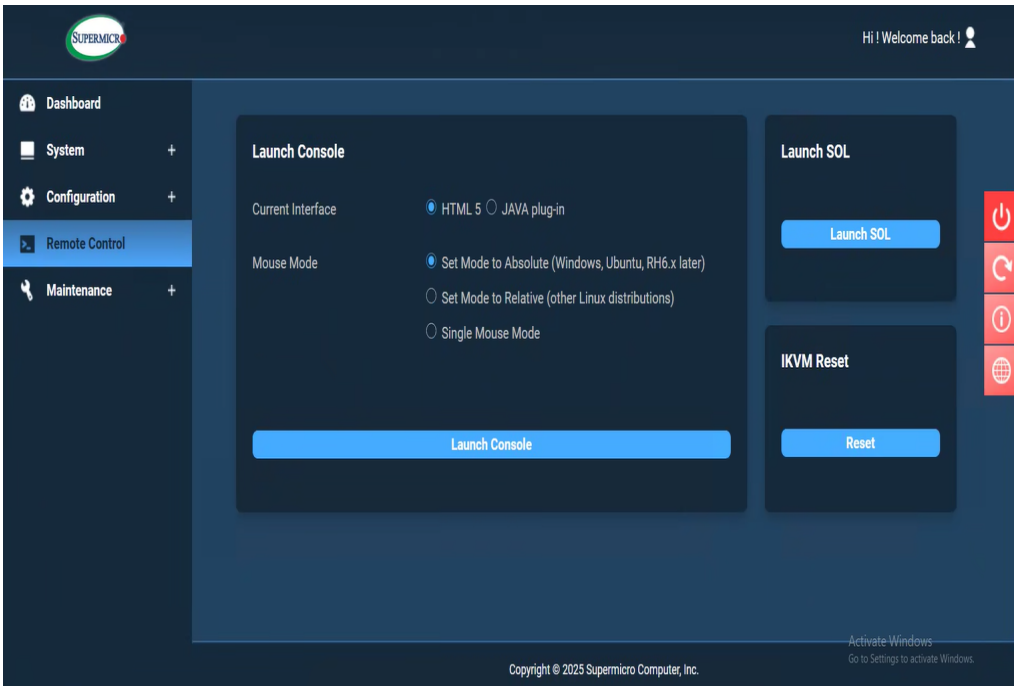
     Hinweis: Der Benutzername muss in Großbuchstaben geschrieben werden.

   - **Password:** Geben Sie das BMC-Kennwort ein.

     Hinweis: Das eindeutige BMC-Kennwort finden Sie im herausziehbaren Tag auf der Vorderseite des Servers. Das BMC-Kennwort wird in der unteren Zeile direkt unter der BMC-/IPMI-MAC-Adresse aufgeführt.

3. Klicken Sie auf **Anmelden**.
4. Navigieren Sie zu **Remote Console**, und klicken Sie auf **Launch Console**.



Der Remote Console Viewer zeigt den Desktop des Remote-Systems an. Sie können die Steuerung des Remote-Systems übernehmen und mithilfe der Tastatur und Maus Vorgänge ausführen.

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

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

So finden Sie die IP-Adresse des BMC

Die Modelle der Arcserve Appliance 10024BU-10576DR-Serie sind standardmäßig für die Verwendung von DHCP für den BMC konfiguriert. Um auf den BMC zugreifen zu können, stellen Sie sicher, dass Sie das Ethernet-Kabel an den dedizierten BMC-Netzwerkport anschließen. Weitere Informationen zur Rückseite und dem für den BMC dedizierten Netzwerkport der Modelle der Arcserve Appliance 10024BU-10576DR-Serie finden Sie unter Rückseite 10024BU-10048BU und Rückseite 10048DR-10576DR.

Sie können die IP-Adresse des BMC folgendermaßen ermitteln:

Suchen der IP-Adresse mithilfe des BIOS

Dieser Abschnitt enthält Anweisungen zum Suchen der IP-Adresse im BIOS.

Befolgen Sie diese Schritte:

1. Schalten Sie den Appliance-Server ein.
2. Drücken Sie während des Systemstarts auf die Taste **Entf**, um das BIOS-Menü aufzurufen.
3. Navigieren Sie zur Registerkarte **Server Managment**, und wählen Sie dann **BMC Network Configuration** aus.

   Der Bildschirm *BMC Network Configuration* wird angezeigt.

   Sie können die IP-Adresse unter dem Parameter *IPV4 Station IP Address* sehen. Sie können auch die von DHCP ausgegebene IP-Adresse in die gewünschte statische IP-Adresse ändern. Weitere Informationen finden Sie unter Konfigurieren der BMC-IP-Adresse mithilfe des BIOS.

Suchen der IP-Adresse im POST-Bildschirm

Dieser Abschnitt enthält Anweisungen zum Suchen der IP-Adresse im POST-Bildschirm.

Befolgen Sie diese Schritte:

1. Schalten Sie den Appliance-Server ein.
2. Leiten Sie den Systemstart ein.

   Der POST-Bildschirm wird angezeigt.

   Sie finden die IP-Adresse in der rechten unteren Ecke des POST-Bildschirms.

Konfigurieren der DHCP- oder statischen IP-Adresse des BMC

Dieser Abschnitt enthält Informationen zum Konfigurieren des UEFI-BIOS und der IP-Adresse des BMC.

Konfigurieren des UEFI-BIOS

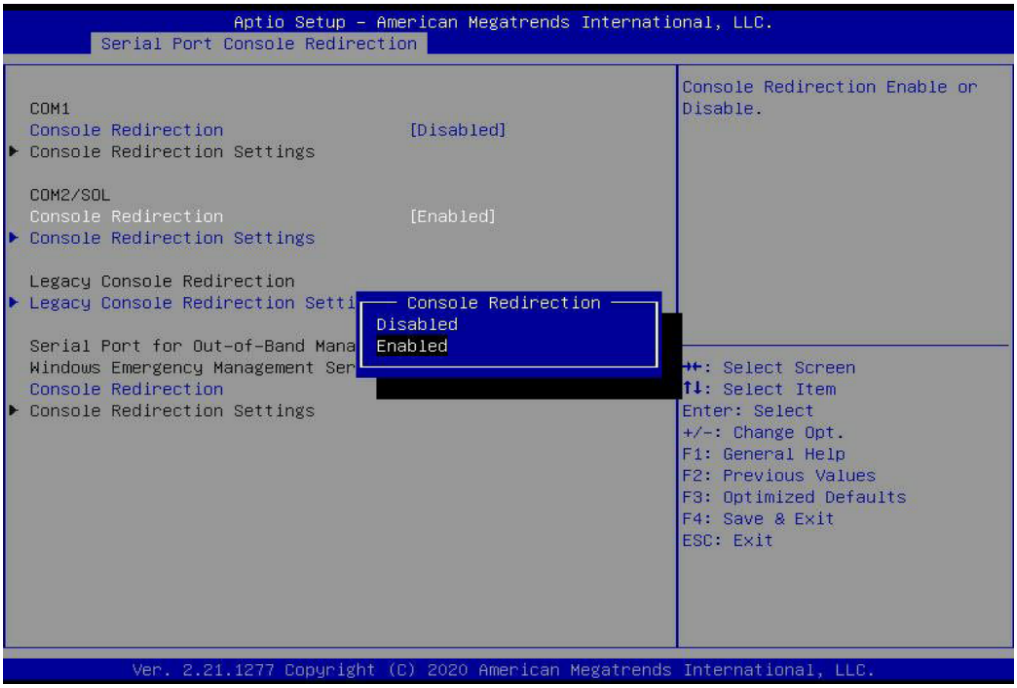
Dieser Abschnitt enthält Informationen zum Konfigurieren des UEFI-BIOS.

Hinweis: Bevor Sie den BMC konfigurieren, müssen Sie das BIOS auf dem Monitor konfigurieren, der direkt an den Arcserve Appliance-Server angeschlossen ist. Sie können diesen Prozess nur im BIOS des BMC ausführen.

Befolgen Sie diese Schritte:

1. Schalten Sie den Arcserve Appliance-Server ein.
2. Klicken Sie während des Systemstarts auf die Taste **Entf**, um das BIOS aufzurufen.

   Hinweis: Verwenden Sie die Pfeiltaste, um durch das BIOS zu navigieren. Drücken Sie zum Auswählen die **Eingabetaste**, und drücken Sie die **Esc**-Taste, um zum vorherigen Bildschirm zurückzukehren.
3. Wählen Sie im Setup-Menü des BIOS die Registerkarte **Advanced** aus.
4. Wählen Sie **Serial Port Console Redirection** aus, und drücken Sie die **Eingabetaste**.
5. Navigieren Sie unter COM2/SOL zu **Console Redirection**, drücken Sie die **Eingabetaste**, und wählen Sie **Enabled** aus.



6. Drücken Sie zum Speichern und Beenden die Taste **F4**.

Das BIOS wurde erfolgreich konfiguriert.

Konfigurieren der IP-Adresse des BMC

Dieser Abschnitt enthält folgende Themen:

Konfigurieren der DHCP-IP-Adresse mithilfe des DHCP-Servers

Dieser Abschnitt enthält Anweisungen zum Konfigurieren der DHCP-IP-Adresse mithilfe des DHCP-Servers.

Befolgen Sie diese Schritte:

1. Suchen Sie auf dem Appliance-Server das ausziehbare ID-Tag mit dem MAC-Adressen-Barcode.
2. Verwenden Sie den MAC-Adresswert, um eine bekannte registrierte DHCP-IP-Adresse auf dem DHCP-Server festzulegen.

Sie können die IP-Adresse im POST-Bildschirm oder im BIOS anzeigen. Weitere Informationen finden Sie unter So finden Sie die IP-Adresse des BMC.

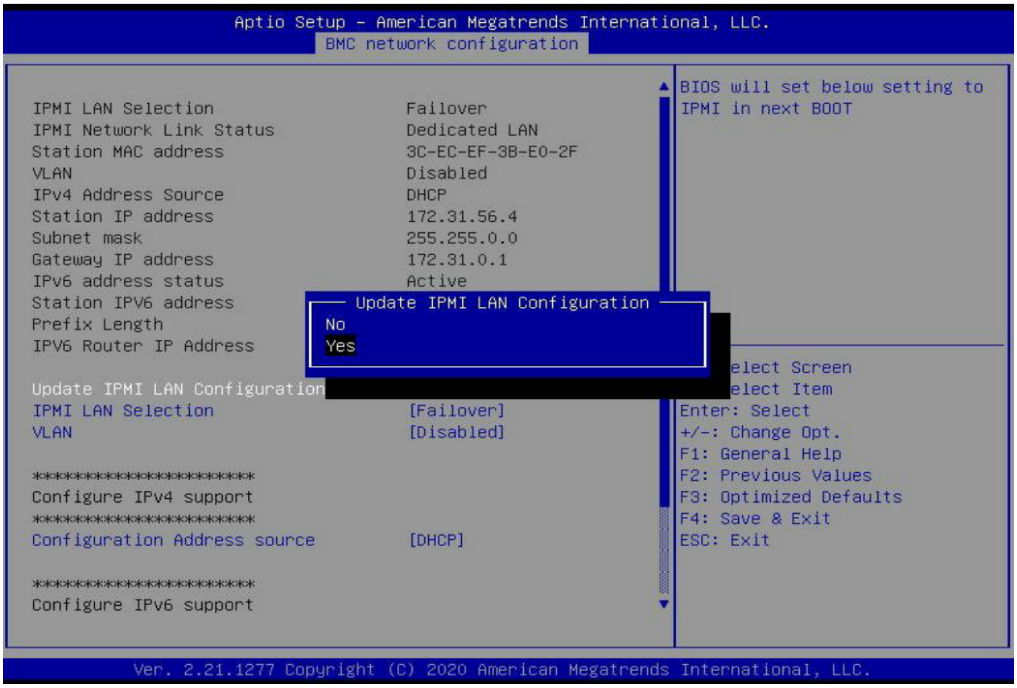
Konfigurieren der statischen IP-Adresse mithilfe des BIOS

Dieser Abschnitt enthält Anweisungen zum Konfigurieren der statischen IP-Adresse mithilfe des BIOS.

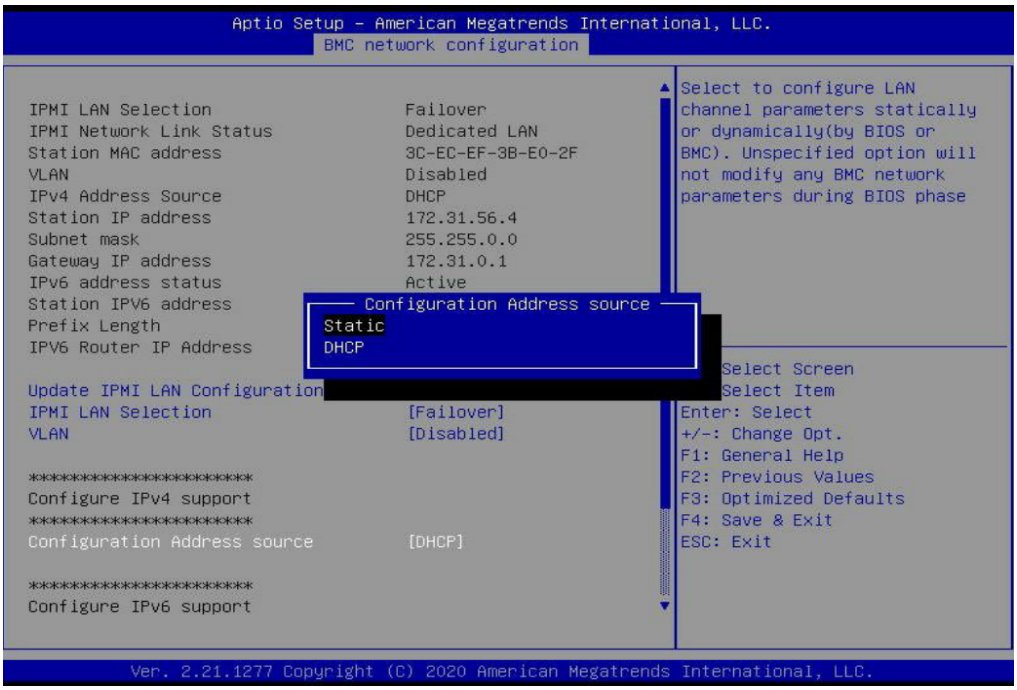
Befolgen Sie diese Schritte:

1. Schalten Sie den Arcserve Appliance-Server ein.
2. Klicken Sie während des Systemstarts auf die Taste **Entf**, um das BIOS aufzurufen.
3. Navigieren Sie zur Registerkarte **Server Management** > **BMC Network Configuration**, und drücken Sie die **Eingabetaste**.

Der Bildschirm *BMC Network Configuration* wird angezeigt.

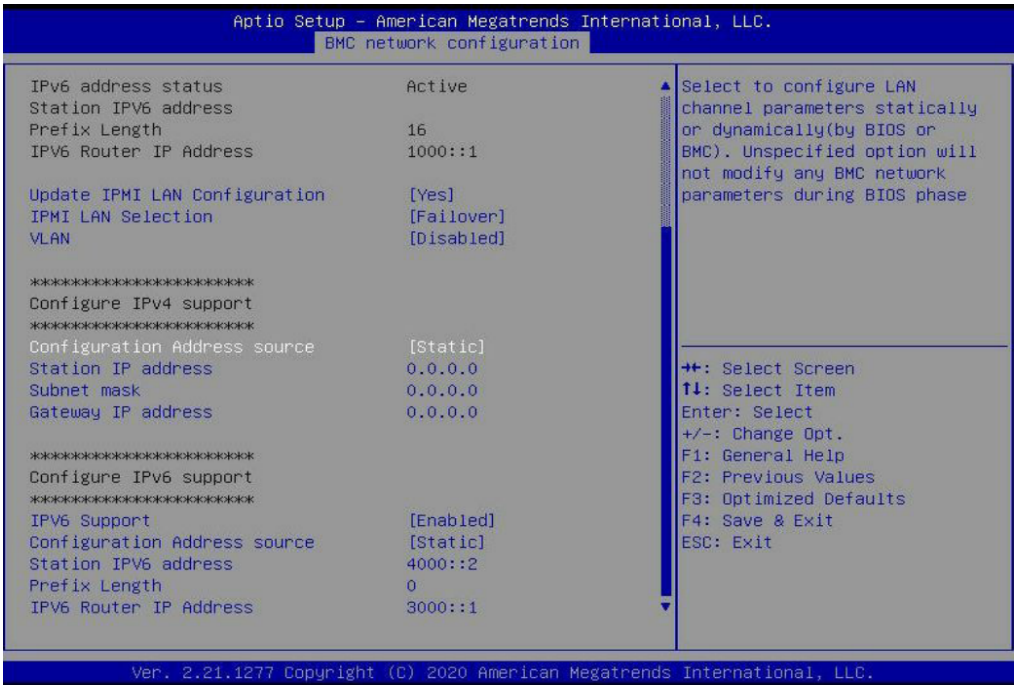


4. Wählen Sie **Update IPMI LAN Configuration** aus, drücken Sie die **Eingabetaste**, und wählen Sie dann **Yes** aus.
5. Wählen Sie **Configuration Address source** aus, drücken Sie die **Eingabetaste** , und wählen Sie dann **Static** aus.



Nachdem die Konfigurationsadressquelle auf "Static" festgelegt wurde, können Sie die Werte "0.0.0.0" in den Feldern "Static IP Address", "Subnet Mask" und "Gateway IP Address" aktualisieren.

6. Geben Sie die gewünschten Werte für "Static IP Address", "Subnet Mask" und "Gateway IP Adresse" ein, und drücken Sie die **Eingabetaste**.



7. Drücken Sie zum Speichern und Beenden die Taste **F4**.

Die statische IP-Adresse des BMC wurde erfolgreich konfiguriert.

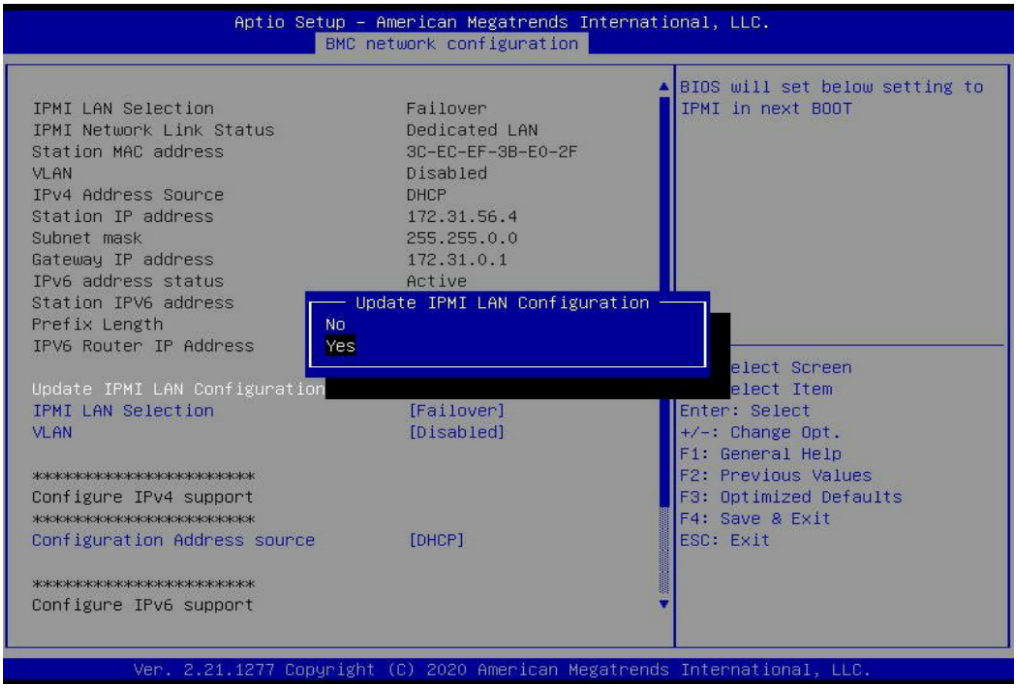
Herstellen einer Verbindung zum BMC über BIOS

Um eine Verbindung zum BMC herzustellen und das BIOS-Menü auf Ihrem Gerät aufzurufen, schließen Sie ein Ende eines Ethernet-Kabels an den Ethernet-Port des Laptops oder Geräts an. Stecken Sie dann das andere Ende des Kabels in den IPMI- oder SHARED-Port des Servers ein. Jetzt sind der BMC und das Gerät an dieselbe Netzwerkverbindung angeschlossen.

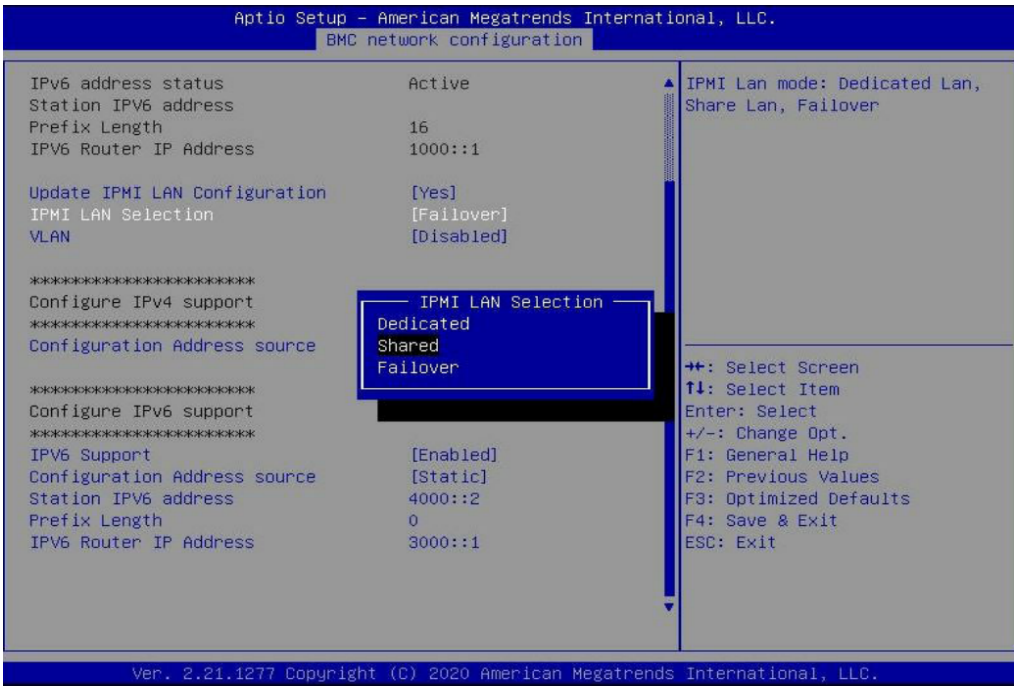
Befolgen Sie diese Schritte:

1. Schalten Sie den Arcserve Appliance-Server ein.
2. Klicken Sie während des Systemstarts auf die Taste **Entf**, um das BIOS aufzurufen.
3. Navigieren Sie zur Registerkarte **Server Management** > **BMC Network Configuration**, und drücken Sie die **Eingabetaste**.

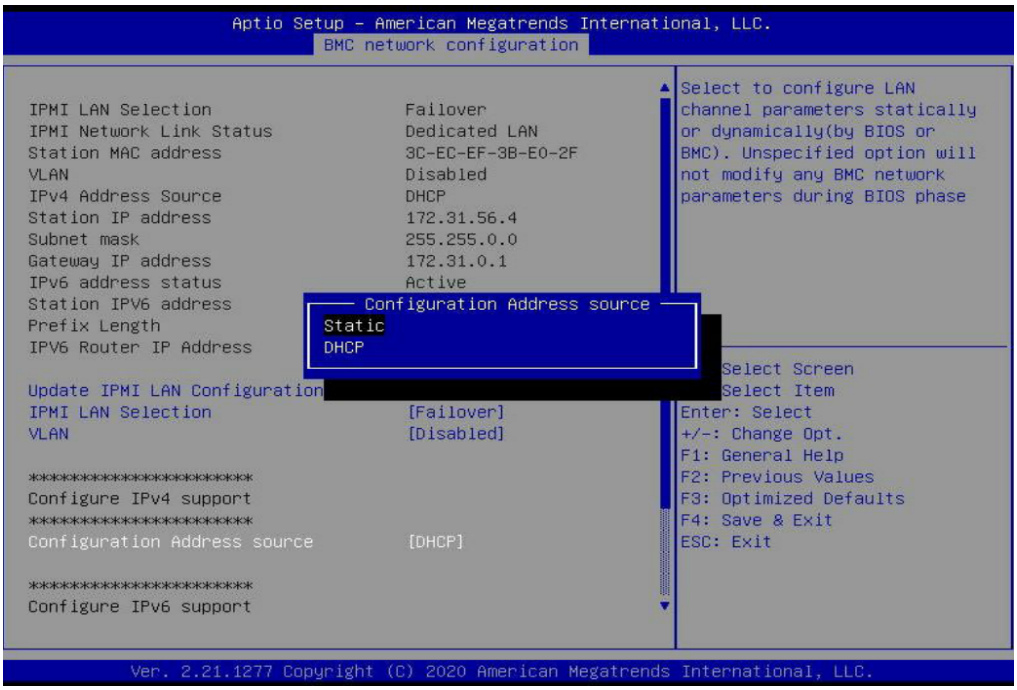
   Der Bildschirm *BMC Network Configuration* wird angezeigt.
4. Wählen Sie **Update IPMI LAN Configuration** aus, drücken Sie die **Eingabetaste**, und wählen Sie dann **Yes** aus.



5. Wählen Sie **IPMI LAN Selection** aus, drücken Sie die **Eingabetaste**, und wählen Sie dann **Shared** aus.

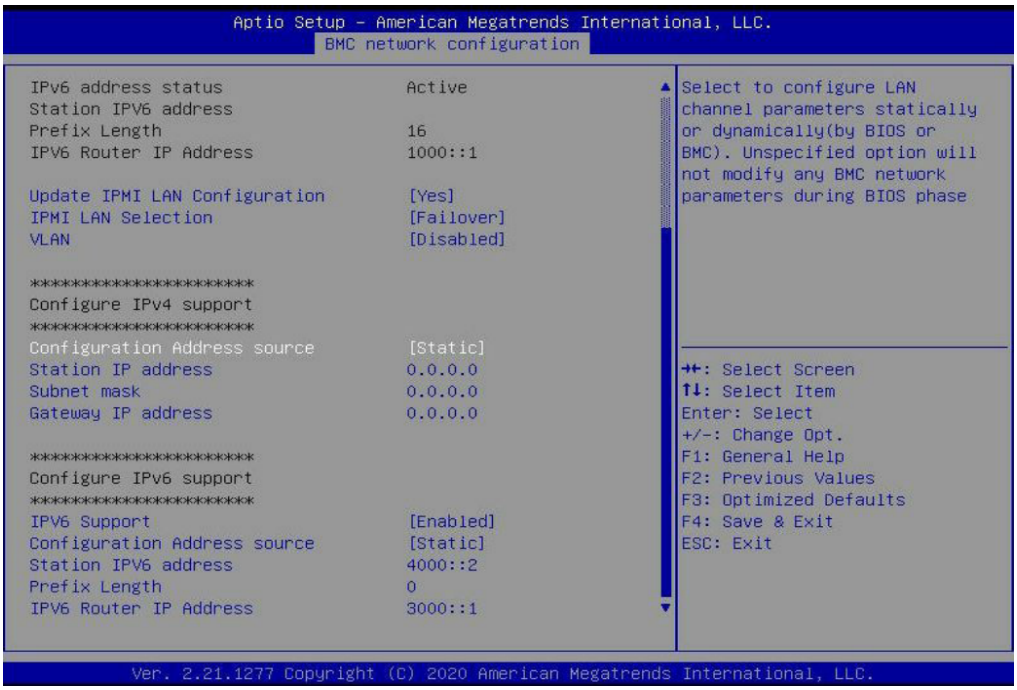


6. Wählen Sie **Configuration Address source** aus, drücken Sie die **Eingabetaste** , und wählen Sie dann **Static** aus.



Nachdem die Konfigurationsadressquelle auf "Static" festgelegt wurde, können Sie die Werte "0.0.0.0" in den Feldern "Static IP Address", "Subnet Mask" und "Gateway IP Address" aktualisieren.

7. Geben Sie die gewünschten Werte für "Static IP Address", "Subnet Mask" und "Gateway IP Adresse" ein, und drücken Sie die **Eingabetaste**.



8. Drücken Sie zum Speichern und Beenden die Taste **F4**.

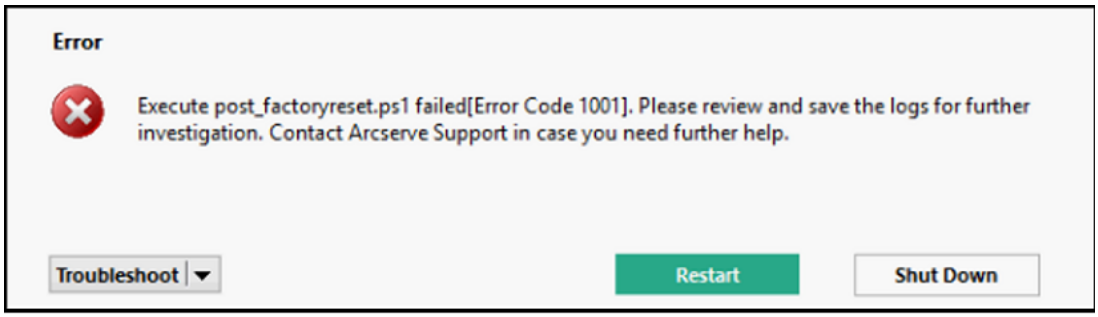
Das Gerät ist jetzt erfolgreich mit dem BMC verbunden.

Kapitel 7: Wiederherstellen oder Reparieren derArc-serve 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.

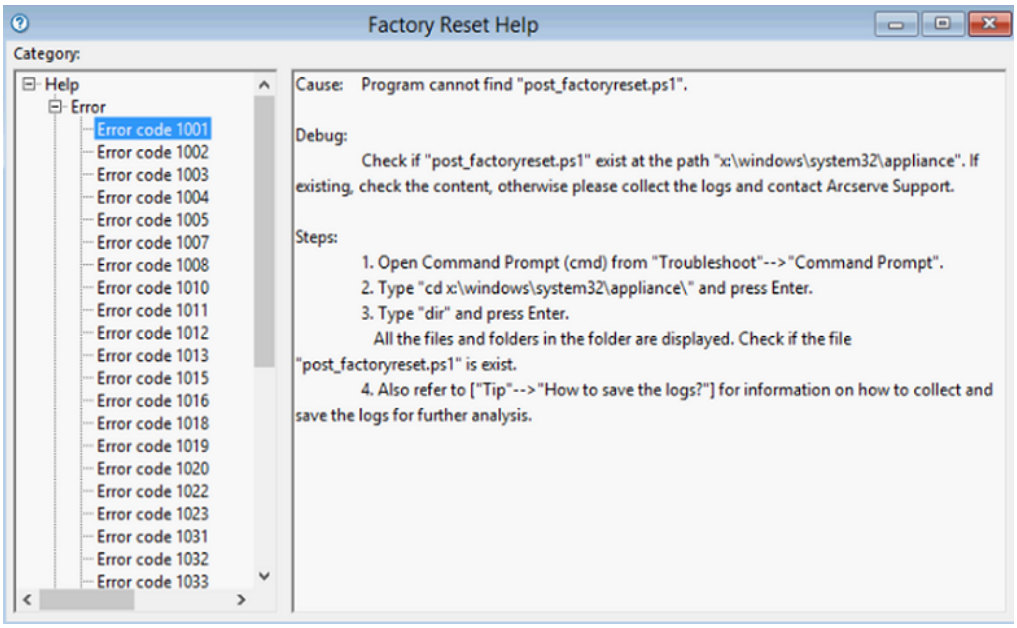
   Hilfe

   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

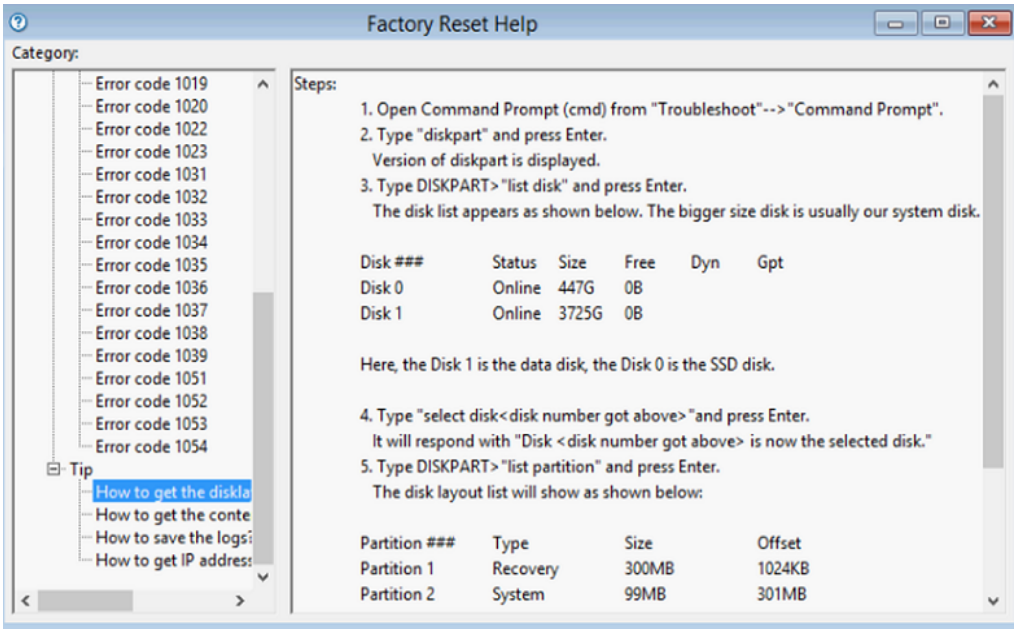
Werkseinstellungen abgerufen wird oder wie Sie die Protokolle speichern.

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.

Installieren der Arcserve Appliance

Dieser Abschnitt enthält folgende Themen:

So installieren Sie Arcserve Backup 19.0

Arcserve Backup 19.0 ist nicht auf der Appliance vorinstalliert. Um Arcserve Backup 19.0 zu installieren, laden Sie die Datei "InstallASBU.iso", die sich auf dem Desktop befindet.

Befolgen Sie diese Schritte:

1. Suchen Sie auf dem Desktop die Datei **InstallASBU.iso**, laden Sie diese, navigieren Sie zum Setup der Anwendung, und führen Sie das Setup als Administrator aus.

   Klicken Sie in der rechten Spalte des Produktinstallationsbrowsers auf "Arcserve Backup für Windows installieren".

   Das Dialogfeld "Erforderliche Komponenten" wird angezeigt.

2. Klicken Sie auf "Installieren", um die erforderlichen Komponenten zu installieren.

   Das Dialogfeld "Erforderliche Komponenten" wird nur angezeigt, wenn Setup keine installierten erforderlichen Komponenten von Arcserve Backup auf dem Zielcomputer findet.

   Hinweis: Wenn Sie Arcserve Backup auf dem aktiven Knoten in einer Cluster-fähigen Umgebung installieren, werden die Cluster-Ressourcen vom aktiven Knoten zum passiven Knoten übertragen, während der aktive Knoten neu startet. Nachdem der aktive Knoten neu gestartet ist, sollten Sie die Cluster-Ressourcen zurück auf den ursprünglichen aktiven Knoten übertragen.

3. Akzeptieren Sie im Dialogfeld "Lizenzvereinbarung" die Bedingungen der Lizenzvereinbarung, und klicken Sie auf "Weiter".

4. Folgen Sie den Aufforderungen, und geben Sie alle erforderlichen Informationen in die nachfolgenden Dialogfelder ein.

   Die folgende Liste beschreibt Dialogfeld-spezifische Informationen zum Installieren von Arcserve Backup.

   Dialogfeld "Installations-/Upgrade-Typ wählen"

   Wenn Sie die Remote-Installationsoption wählen, können Sie Arcserve Backup auf mehreren Systemen installieren.

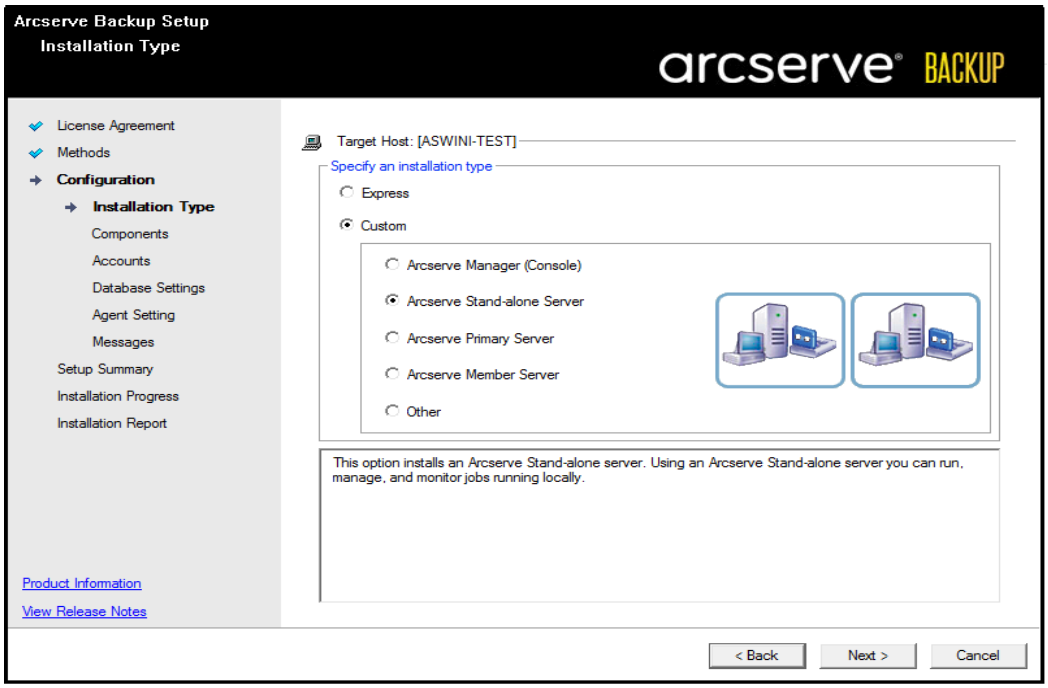
   Bei Remote-Installationen kann das Remote-Zielsystem aus verschiedenen Arcserve-Servertypen, verschiedenen Arcserve Backup-Agents und -Optionen oder beidem bestehen.

Hinweis: Das Setup-Programm für Cluster-Rechner unterstützt keine Remote-Installation für das Arcserve Backup-Basisprodukt oder die Arcserve Backup-Agents. Diese Einschränkung der Remote-Installation von Arcserve Backup-Agents (zum Beispiel dem Agent für Microsoft SQL Server und dem Agent für Microsoft Exchange Server) gilt nur, wenn Sie einen virtuellen Host verwenden. Die Remote-Installation von Arcserve Backup-Agents wird bei Verwendung von physischen Cluster-Hosts unterstützt.

Dialogfeld "Installationstyp"

Hier können Sie die Art der Arcserve Backup-Komponenten eingeben, die Sie installieren möchten. Wählen Sie entweder die Express-Installation oder die benutzerdefinierte Installation aus.

Hinweis: Wenn Sie eine Vorgängerversion upgraden, erkennt der Installationsassistent die aktuelle Arcserve-Konfiguration und wählt den geeignetsten Installations-/Upgradetyp für die neue Installation aus. Weitere Informationen finden Sie unter Installationstypen für Arcserve Backup-Server und Arcserve Backup-Serveroptionen.



Dialogfeld "Komponenten"

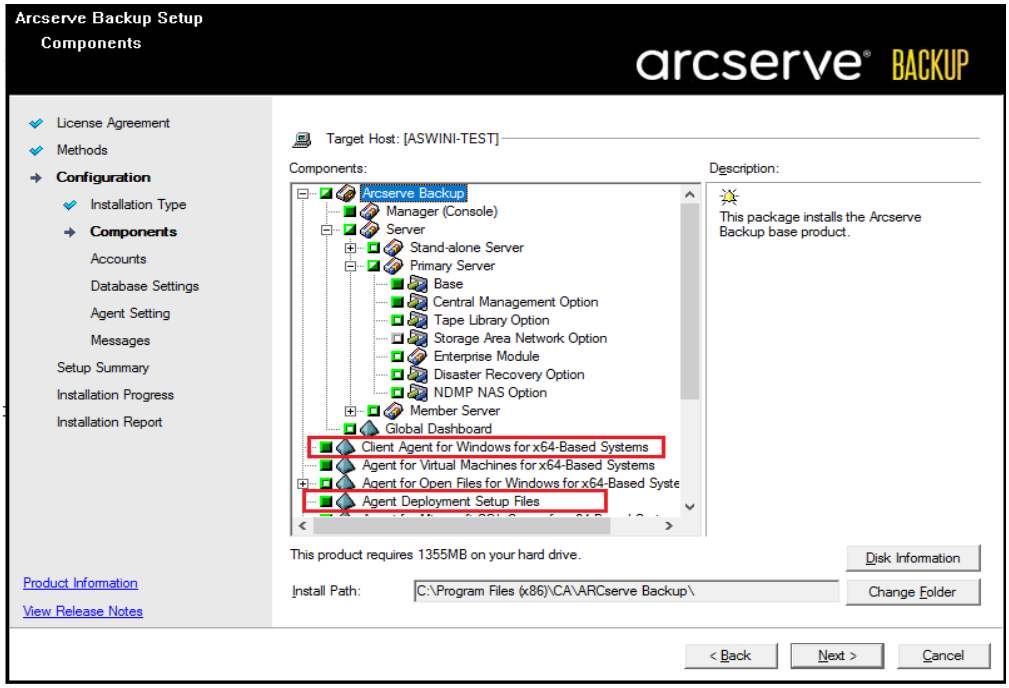
Geben Sie hier die Arcserve Backup-Komponenten an, die Sie auf dem Zielsystem installieren möchten.

Beachten Sie Folgendes:

- Um einen Primärserver zu installieren, müssen Sie die Central Management Option von Arcserve Backup auf dem Primärserver installieren.
- Zur Installation von Mitgliedsservern muss der Installationsassistent in der Lage sein, den Arcserve Backup-Domänennamen und den Namen des Primärservers in Ihrem Netzwerk zu erkennen. Aus diesem Grund sollten Sie mindestens eine Primärserverinstallation abgeschlossen haben, bevor Sie Mitgliedsserverinstallationen durchführen.
- Wenn Sie im Dialogfeld "Produkte wählen" auf das Arcserve Backup-Objekt oder das Server-Objekt klicken, gibt der Installationsassistent unabhängig vom Installationstyp, den Sie im Dialogfeld "Installations-/Upgrade-Typ wählen" festgelegt haben, die standardmäßigen Installationskomponenten des eigenständigen Servers an. Um sicherzustellen, dass Sie die korrekten Komponenten installieren, blenden Sie das Server-Objekt ein, blenden Sie dann das Objekt für den Arcserve Backup-Servertypen ein, den Sie installieren möchten, und aktivieren Sie die entsprechenden Kontrollkästchen für die Komponenten, die Sie installieren möchten.
- Agent Deployment ist ein assistentenähnliches Tool, mit dem Sie Arcserve Backup-Agents auf mehreren Remote-Systemen installieren oder Upgrades durchführen können, nachdem Sie Arcserve Backup installiert haben. Damit diese Funktion unterstützt wird, müssen Quelldateien von Setup auf den Arcserve Backup-Server kopiert werden. Um den Inhalt des Installationsdatenträgers auf den Arcserve Backup-Server zu kopieren, müssen Sie im Dialogfeld "Komponenten" die Option "Agent Deployment" auswählen. Die Installation oder Upgrade von Arcserve Backup nimmt deutlich mehr Zeit in Anspruch, wenn Sie "Agent Deployment" auswählen.
- Wenn Sie eine Remote-Installation oder eine automatische Installation ausführen, sollten Sie den Arcserve Backup-Client Agent für Windows nicht im selben Verzeichnis wie das Arcserve Backup-Basisprodukt installieren.
- Global Dashboard kann auf Primärservern, eigenständigen Servern und Mitgliedsservern installiert werden. Allerdings können Sie Mitgliedsserver nicht so konfigurieren, dass Sie als zentrale Primärserver und primäre Zweigstellenserver fungieren. Weitere Informationen zu zentralen Primärservern und primären Zweigstellenservern finden Sie im *Dashboard-Benutzerhandbuch*.
- Auf Computern, auf denen Windows Server Core ausgeführt wird, können Sie nur die folgenden Arcserve Backup-Produkte installieren:

- Mitgliedsserver und unterstützte Optionen
- Agent for Open Files
- Agent für virtuelle Rechner
- Client Agent für Windows
- Disaster Recovery Option

Das folgende Diagramm zeigt den Standardinstallationspfad für den Client Agent für Windows. Darüber hinaus wird die Komponente "Agent Deployment" angegeben:

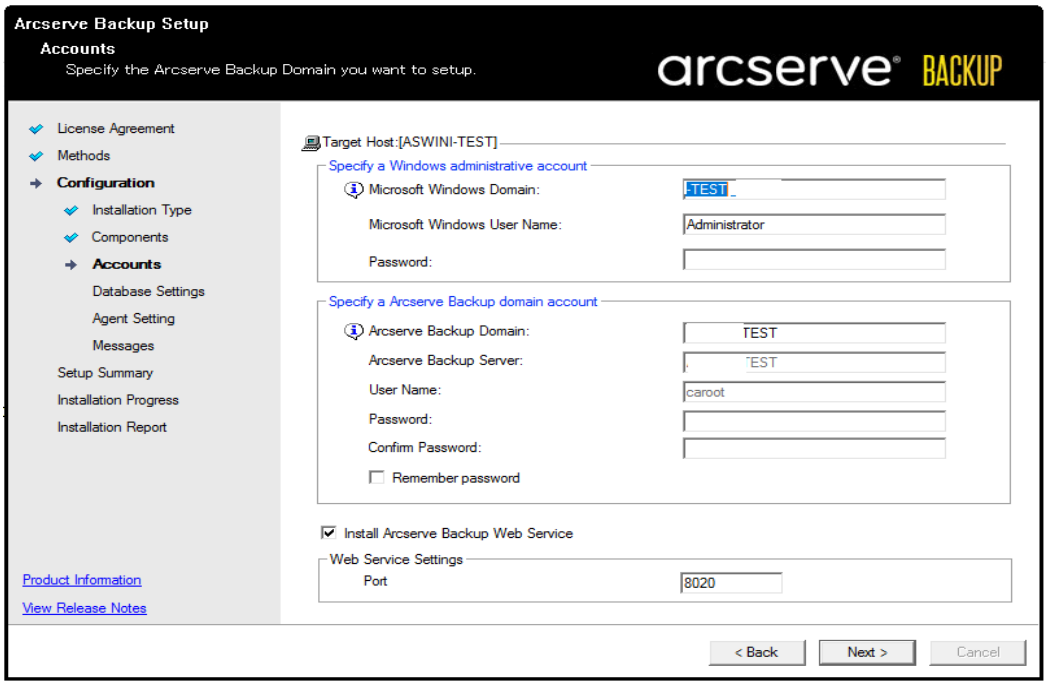


Dialogfeld "Konten"

Hier können Sie Ihre Arcserve Backup-Konten einrichten und eine Option zur Aktivierung der **Installation des Arcserve Backup-Webservices** wählen.

Wenn der Setup-Assistent eine Cluster-fähige Anwendung entdeckt, die in Ihrer Umgebung ausgeführt wird, und Sie Arcserve Backup in der Cluster-fähigen Umgebung installieren möchten, aktivieren Sie die Option "Cluster-Umgebung – Installation", und geben Sie den Pfad zum gemeinsam genutzten Laufwerk an, auf dem Sie Arcserve Backup installieren möchten.

Hinweis: Arcserve Backup-Servernamen und Arcserve Backup-Domänennamen dürfen 15 Byte nicht überschreiten. Ein Name mit 15 Byte entspricht etwa 7 bis 15 Zeichen.



Der Arcserve Backup-Webservice dient als Brücke zwischen dem UDP-Archiv und der Band-Aufgabe sowie Arcserve Backup. Standardmäßig wird die **Installation des Arcserve Backup-Webservices** aktiviert, wenn Sie Arcserve Backup installieren. Die standardmäßige Portnummer für die **Webservice-Einstellungen** ist 8020. Sie können die Portnummer ändern oder wechseln.

Deaktivieren Sie das Kontrollkästchen **Arcserve Backup-Webservice installieren** , um den Arcserve Backup-Webservice zu deaktivieren.

Sie können die Arcserve Backup-Nachinstallation **des Arcserve Backup-Webservices** aktivieren/ändern.

Hinweis: Geben Sie dieselbe Portnummer an, wenn Sie den Arcserve Backup-Webservice auf allen Servern der Arcserve Backup-Domäne installieren. Arcserve UDP verwendet dieselbe Portnummer, um eine Verbindung zu beiden Servern, dem Arcserve Backup-Primärserver und dem Mitgliedsserver in der Arcserve Backup-Domäne herzustellen.

Befolgen Sie diese Schritte:

1. Navigieren Sie von der Befehlszeile aus in den Arcserve Backup-Basisinstallationspfad.

2. Geben Sie in der Befehlszeile folgenden Befehl ein:

   Bconfig –c

   Das <Arcserve Backup>-Dialogfeld "Konten" wird geöffnet.

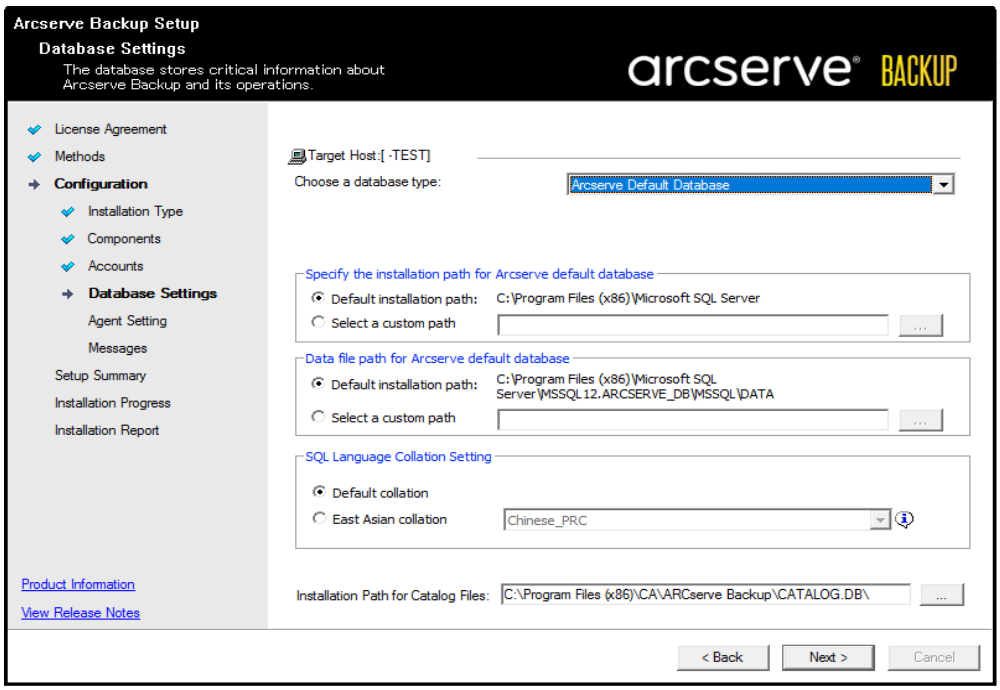
3. Konfigurieren oder aktualisieren Sie den Webservice.

Dialogfeld "Datenbankeinstellungen"

Hier können Sie die Arcserve Backup-Datenbank konfigurieren.

Geben Sie eine Datenbankanwendung (Arcserve Backup-Standarddatenbank oder Microsoft SQL Server) an, und füllen Sie die erforderlichen Felder in diesem Dialogfeld aus. Klicken Sie dann auf "Weiter".

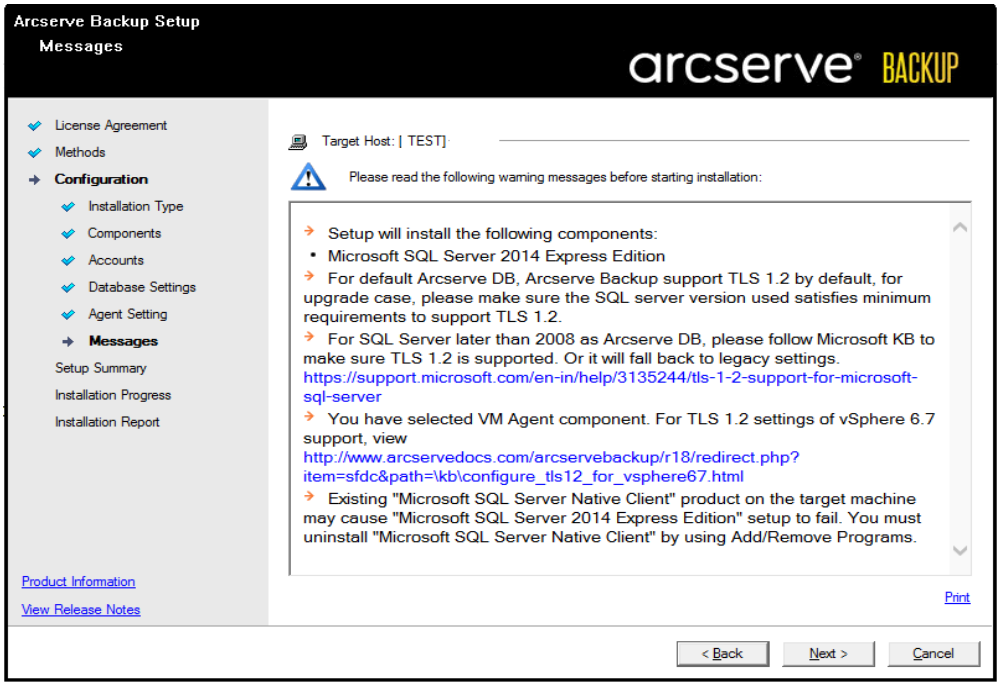
Hinweis: Wenn Sie Daten schützen, die auf Unicode basierende Zeichen aus ostasiatischen Sprachen (z. B. JIS2004) enthalten, müssen Sie die SQL-Sortierreihenfolge aktivieren, damit die Daten von Arcserve Backup durchsucht und sortiert werden können. Klicken Sie zu diesem Zweck auf "Sortierung für ostasiatische Sprachen", und wählen Sie dann aus der Drop-down-Liste eine Sprache aus.



Dialogfeld "Meldungen"

Nachdem Sie die Meldungen im Dialogfeld "Meldungen" gelesen haben, sollten Sie versuchen, die Probleme zu lösen.

Die folgende Abbildung veranschaulicht das Dialogfeld "Wichtige Warnhinweise":



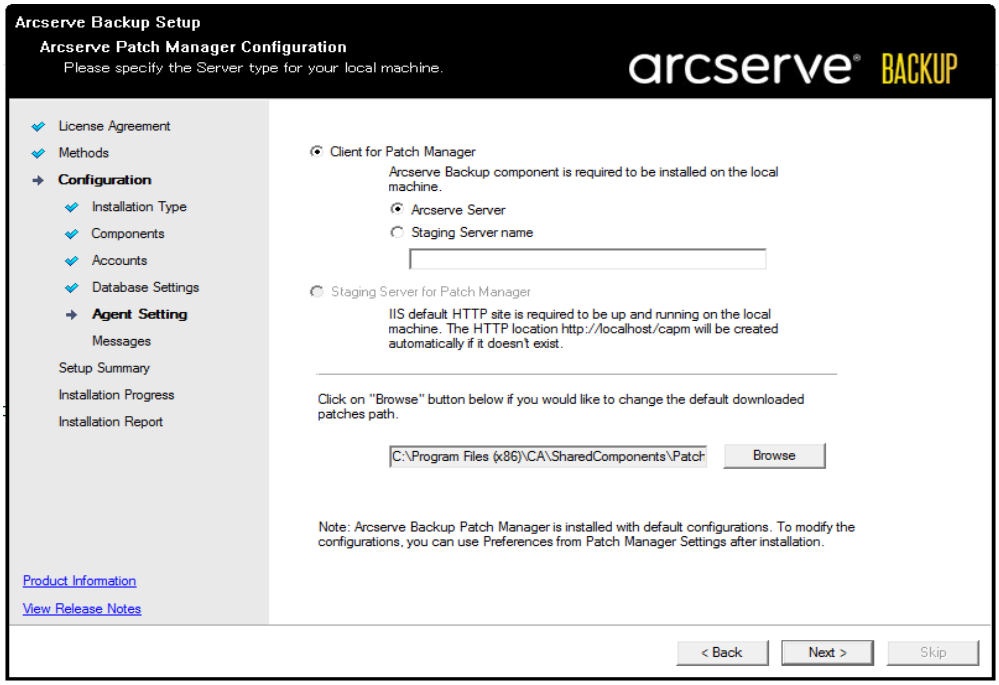
Dialogfeld "Setup-Übersicht"

Um die Komponenten, die Sie installieren möchten, zu ändern, klicken Sie so oft wie notwendig auf "Zurück", um zum Dialogfeld mit den Installationsoptionen zurückzukehren, die Sie ändern möchten.

Dialogfeld "Installationsbericht"

Wenn eine der ausgewählten Komponenten konfiguriert werden muss, werden im Setup-Assistenten die entsprechenden Dialogfelder für die Konfiguration am Ende der Installation angezeigt. Sie können die Komponente entweder sofort oder später mithilfe der Gerätekonfiguration oder der Enterprise-Modul-Konfiguration konfigurieren. Wenn Sie beispielsweise einen Bandwechsler mit einem Laufwerk verwenden, der konfiguriert werden muss, können Sie mithilfe des Setup-Assistenten die Gerätekonfiguration starten, indem Sie auf die entsprechende Meldung im Dialogfeld "Installation – Zusammenfassung" doppelklicken.

Das folgende Diagramm zeigt das Dialogfeld "Installationsbericht". Der Agent für Microsoft SQL Server muss konfiguiert werden.



Hinweis: Sie müssen den Server möglicherweise neu starten, nachdem Sie Arcserve Backup installiert haben. Dies hängt davon ab, ob alle Dateien, Dienste und Registrierungseinstellungen auf der Betriebssystemebene aktualisiert wurden.

Dialogfeld "Installation – Zusammenfassung"

Wenn eine der ausgewählten Komponenten konfiguriert werden muss, werden im Setup-Assistenten die entsprechenden Dialogfelder für die Konfiguration am Ende der Installation angezeigt. Sie können die Komponente entweder sofort oder später mithilfe der Gerätekonfiguration oder der Enterprise-Modul-Konfiguration konfigurieren. Wenn Sie beispielsweise einen Bandwechsler mit einem Laufwerk verwenden, der konfiguriert werden muss, können Sie mithilfe des Setup-Assistenten die Gerätekonfiguration starten, indem Sie auf die entsprechende Meldung im Dialogfeld "Installation – Zusammenfassung" doppelklicken.

5. Klicken Sie im Dialogfeld "Installation – Zusammenfassung" auf "Fertig", um die Installation zu beenden.

So installieren Sie die Appliance der 10024BU-10048BU-Serie

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

Den vollständigen Installationsprozess finden Sie unter Appliance-Installation für die Serie 10024BU-10048BU.

So installieren Sie die Appliance der 10048DR-10576DR-Serie

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

Den vollständigen Installationsprozess finden Sie unter Appliance-Installation für die Serie 10048DR-10576DR.

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 Appliance-Installation für die Serie 9012-9048.

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.

So installieren Sie die Appliance Serie X

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

Weitere Informationen zum vollständigen Installationsprozess finden Sie unter Appliance Installation Serie X – Compute Node und Appliance Installation Serie X – Storage Node.

Zurücksetzen von Appliances der 10024BU-10576DR-Serie auf die Arcserve UDP-Werkseinstellungen

Dieser Abschnitt enthält Informationen zum Zurücksetzen von Appliances der 10000-Serie auf die Werkseinstellungen.

Mit Hilfe der Option zum Zurücksetzen auf die UDP-Werkseinstellungen können Sie die Arcserve Appliance der 10000-Serie in einen bereinigten und unkonfigurierten Status zurücksetzen.

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

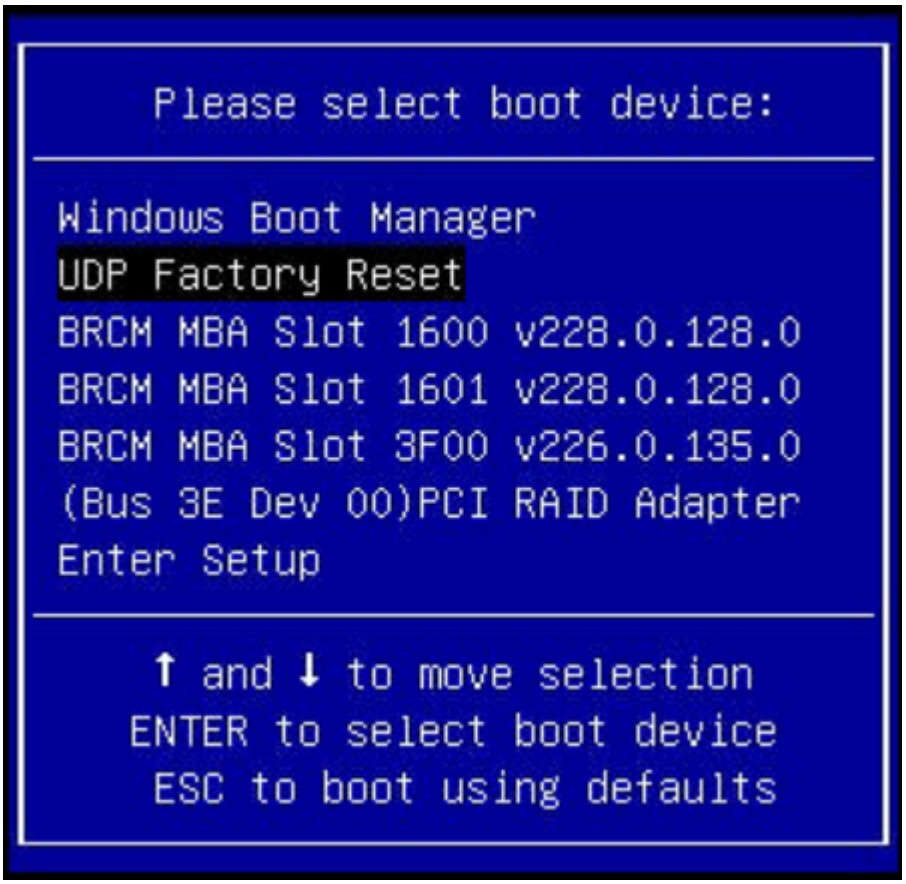
Verwenden Sie eine der beiden folgenden Methoden, um Appliances der 10000-Serie auf die Werkseinstellungen zurückzusetzen:

Wiederherstellen der Werkseinstellungen über BIOS

Dieser Abschnitt enthält Informationen zum Zurücksetzen auf die UDP-Werkseinstellungen über das BIOS.

Befolgen Sie diese Schritte:

1. Schalten Sie die Arcserve Appliance ein.
2. Drücken Sie **F11** auf der Tastatur, um das Startmenü aufzurufen.
3. Wählen Sie die Startoption zum **Zurücksetzen auf die UDP-Werkseinstellungen**.

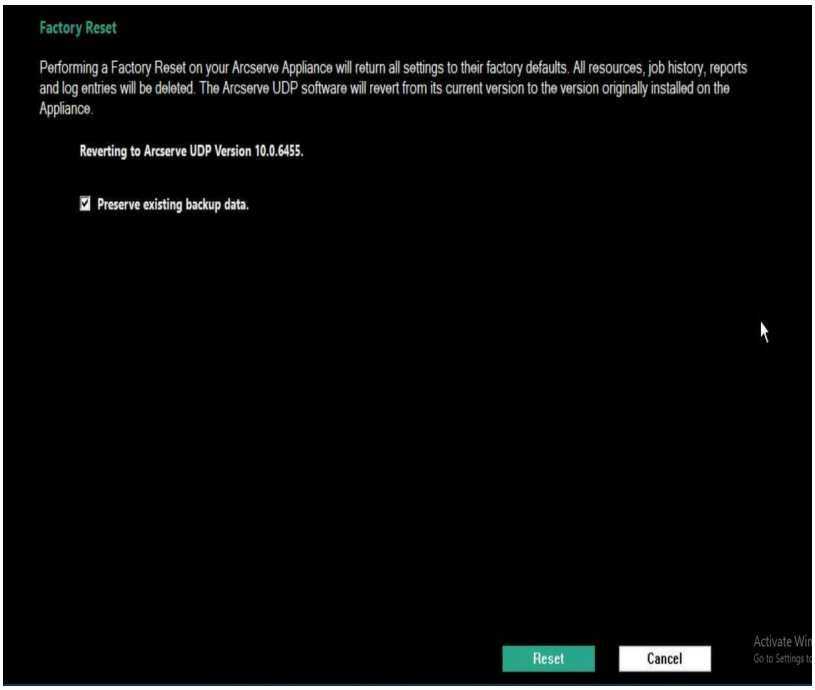


Der Assistent zum Zurücksetzen auf die Werkseinstellungen wird angezeigt.

4. Klicken Sie auf **Zurücksetzen**.

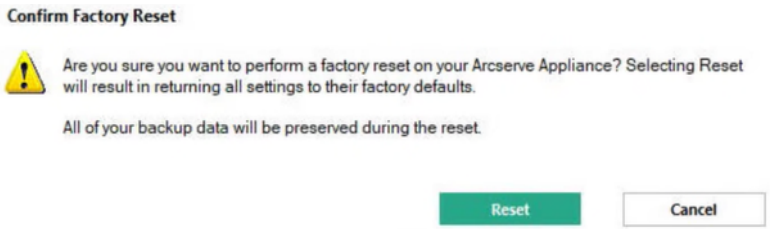
Hinweise:

- Das Kontrollkästchen **Vorhandene Sicherungsdaten erhalten** ist standardmäßig aktiviert. Alle Sicherungsdaten werden während des Zurücksetzens beibehalten. Nur C:\ im ursprünglichen Betriebssystem wird neu erstellt.
- Wenn Sie das Kontrollkästchen **Vorhandene Sicherungsdaten erhalten** deaktivieren, werden alle Sicherungsdaten beim Zurücksetzen gelöscht. Die Daten auf den jeweiligen Volumes von C: \, X: \ und Y: \ im ursprünglichen Betriebssystem werden rekonstruiert.

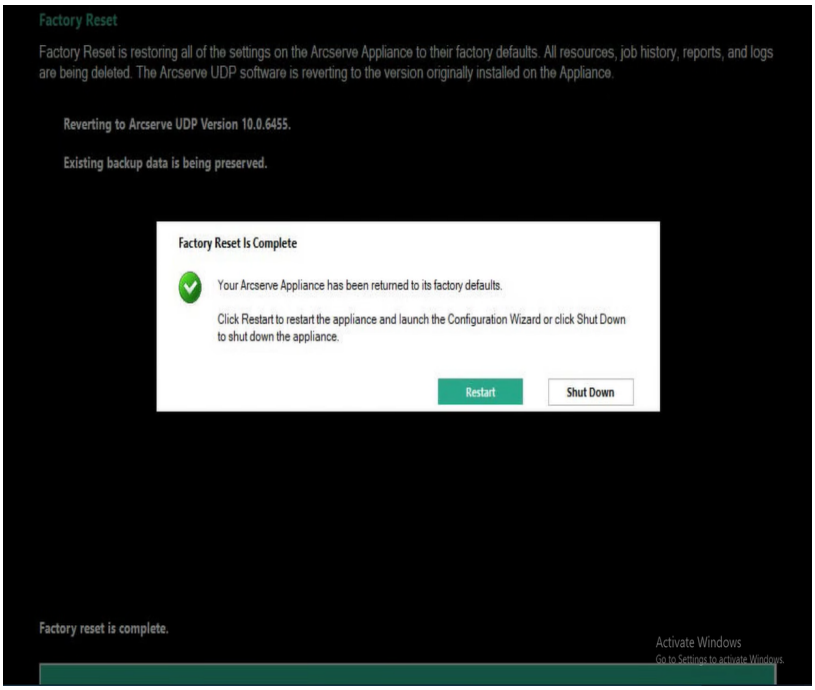


Ein Bestätigungsdialogfeld wird angezeigt.

5. Um die Werkseinstellungen wiederherzustellen, klicken Sie auf **Zurücksetzen**.



6. Nachdem das Zurücksetzen auf die Werkseinstellungen abgeschlossen ist, können Sie eine der folgenden Aktionen ausführen:
   - Um die Appliance neu zu starten, klicken Sie auf **Neu starten**.
   - Um die Appliance zu schließen, klicken Sie auf **Herunterfahren**.



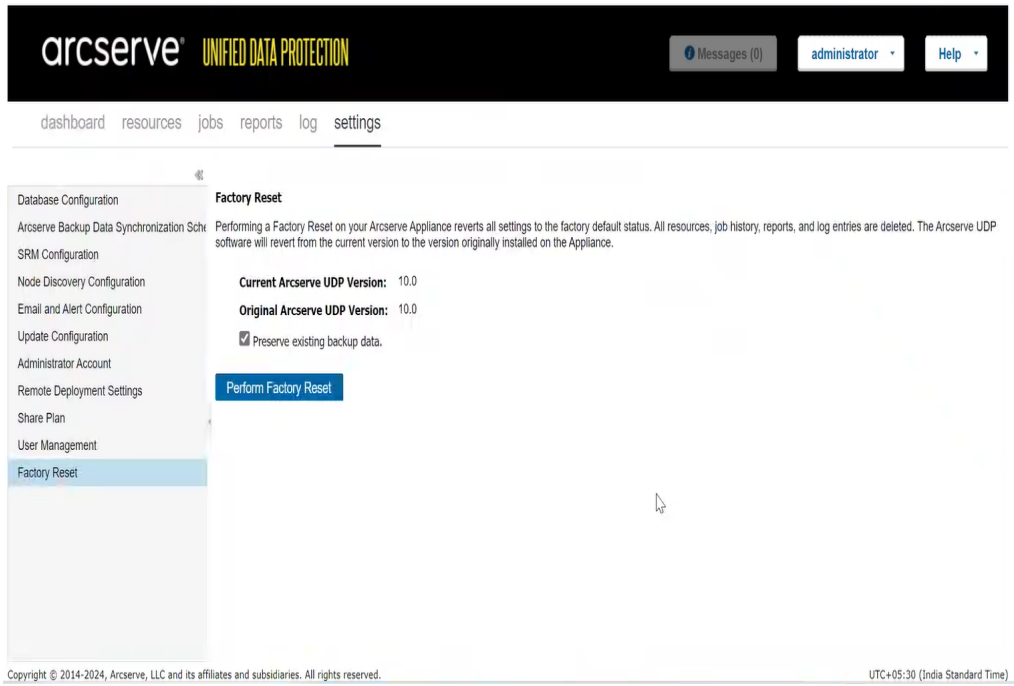
Das Zurücksetzen auf die Werkseinstellungen über das BIOS für die Appliance der 10000-Serie wurde erfolgreich abgeschlossen.

Wiederherstellen der Werkseinstellungen über die Arcserve UDP-Konsole

Dieser Abschnitt enthält Informationen zum Zurücksetzen auf die Werkseinstellungen über die Arcserve UDP-Konsole.

Befolgen Sie diese Schritte:

1. Melden Sie sich bei der Arcserve UDP-Konsole an.
2. Navigieren Sie zu **Einstellungen** > **Auf Werkseinstellungen zurücksetzen**.



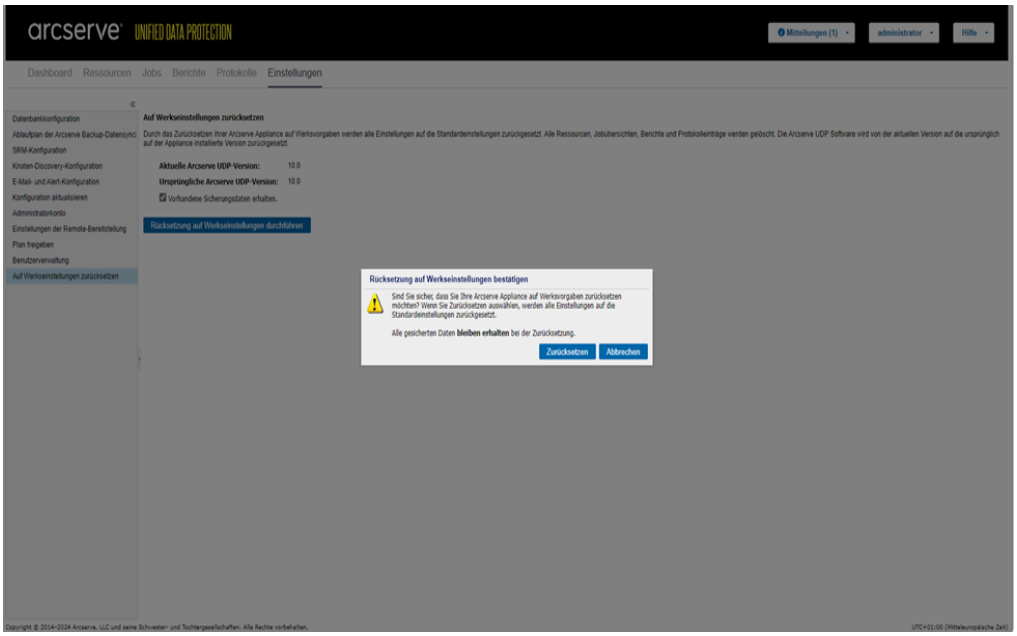
3. Klicken Sie im Bildschirm *Auf Werkseinstellungen zurücksetzen* auf **Rücksetzung auf Werkseinstellungen durchführen**.

Hinweise:

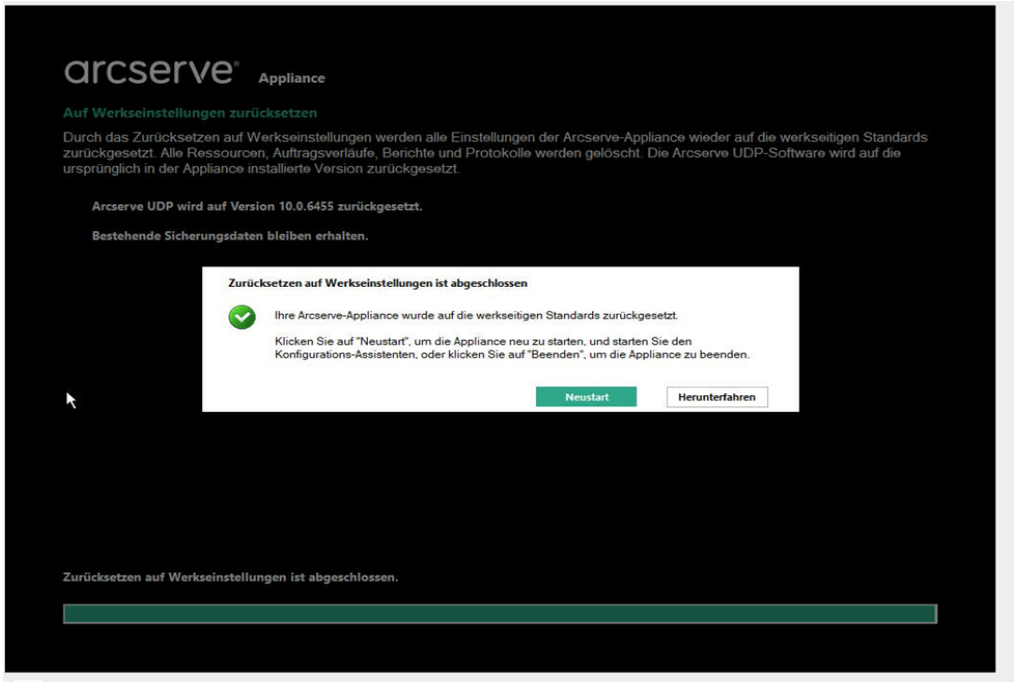
- Das Kontrollkästchen **Vorhandene Sicherungsdaten erhalten** ist standardmäßig aktiviert. Alle Sicherungsdaten werden während des Zurücksetzens beibehalten. Nur C:\ im ursprünglichen Betriebssystem wird neu erstellt.
- Wenn Sie das Kontrollkästchen **Vorhandene Sicherungsdaten erhalten** deaktivieren, werden alle Sicherungsdaten beim Zurücksetzen gelöscht. Alle Daten auf den jeweiligen Volumes von C: \, X: \ und Y: \ im ursprünglichen Betriebssystem werden rekonstruiert.

Ein Bestätigungsdialogfeld wird angezeigt.

4. Um die Werkseinstellungen wiederherzustellen, klicken Sie auf **Zurücksetzen**.



5. Nachdem das Zurücksetzen auf die Werkseinstellungen abgeschlossen ist, können Sie eine der folgenden Aktionen ausführen:
   - Um die Appliance neu zu starten, klicken Sie auf **Neu starten**.
   - Um die Appliance zu schließen, klicken Sie auf **Herunterfahren**.



Das Zurücksetzen auf die Werkseinstellungen über die Arcserve UDP-Konsole für die Appliance der 10000-Serie wurde erfolgreich abgeschlossen.

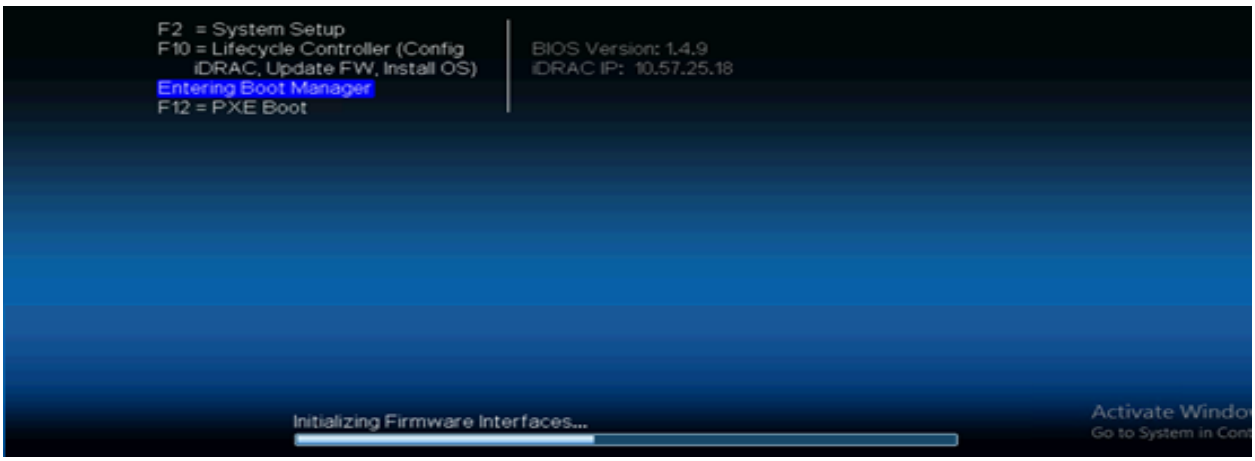
Anwenden von Arcserve UDP-Werkseinstellungen unter Verwendung der Startoption für Geräte der 9012-9504DR Serie

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.

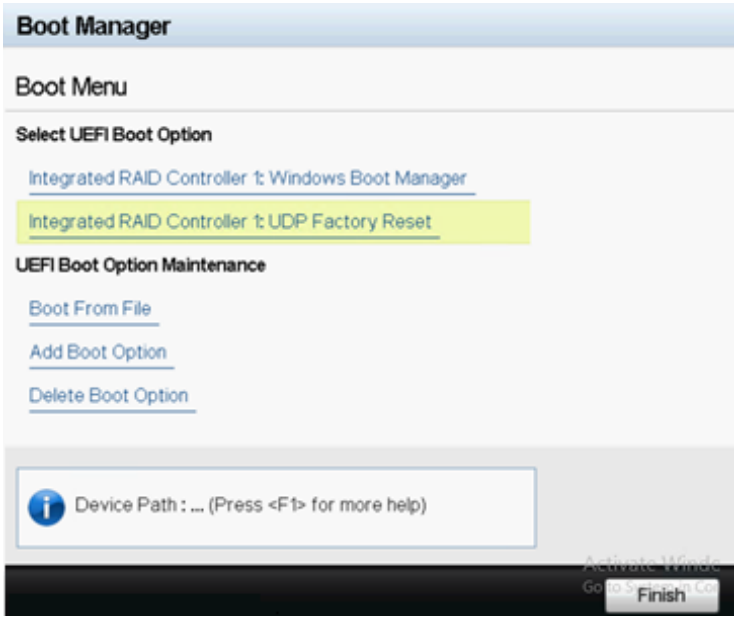
Hinweis: Sie können auch die Option „Sicherungsdaten beibehalten“ auswählen, während Sie das Gerät auf die UDP-Werkeinstellungen zurücksetzen.

Befolgen Sie diese Schritte:

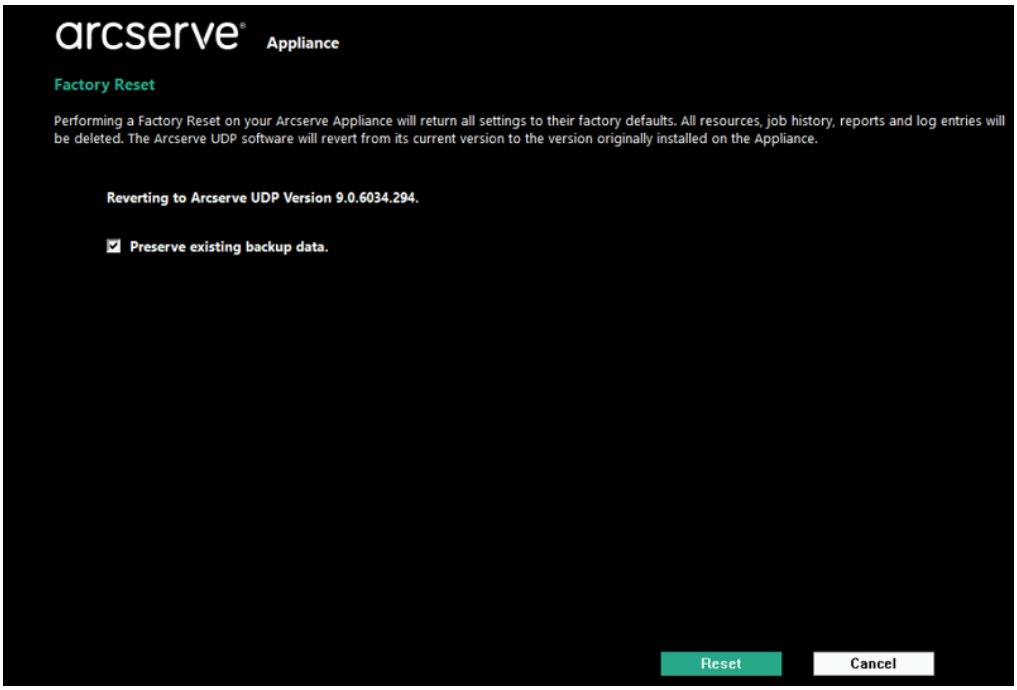
1. Drücken Sie F11 auf der Tastatur, um das Startmenü aufzurufen.



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



Es wird eine Seite zum Zurücksetzen auf Werkseinstellungen angezeigt.

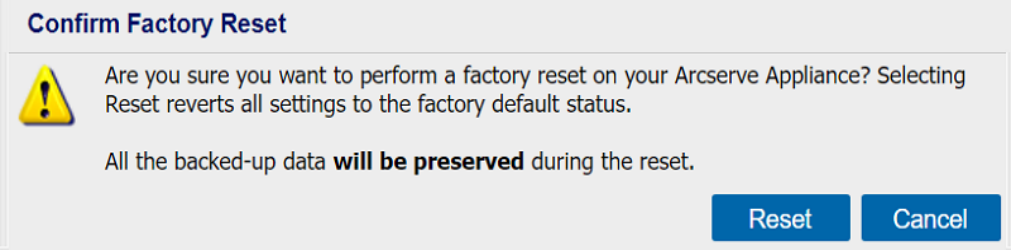


Hinweise:

- 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**.

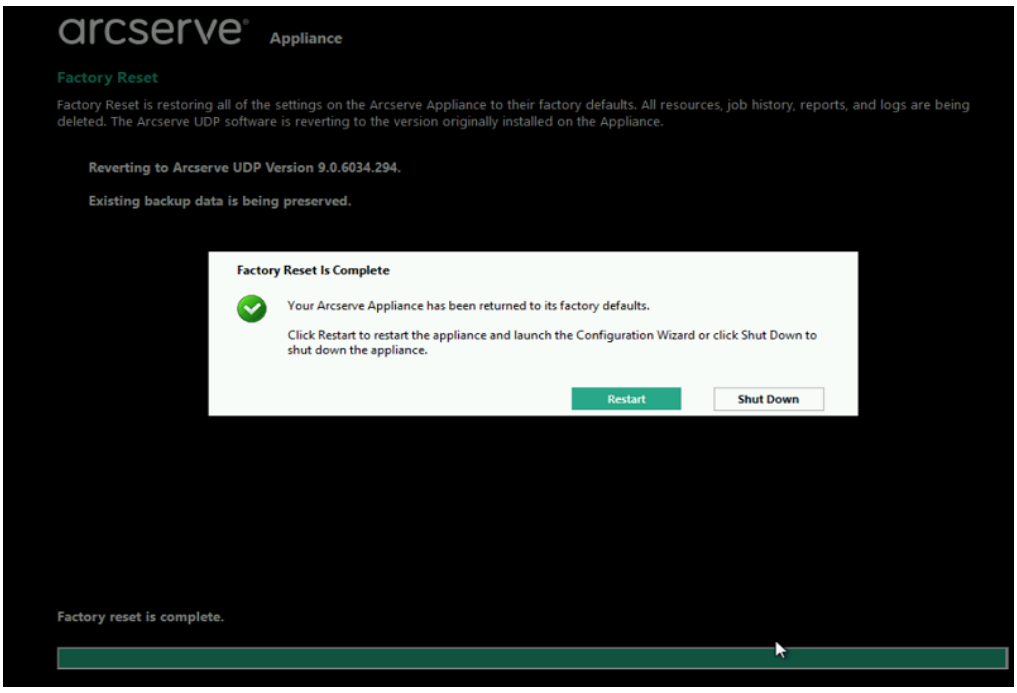
   Ein Bestätigungsdialogfeld wird angezeigt.



   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.



Anwenden von Arcserve UDP-Werkseinstellungen unter Verwendung der Startoption in Appliance Serie X

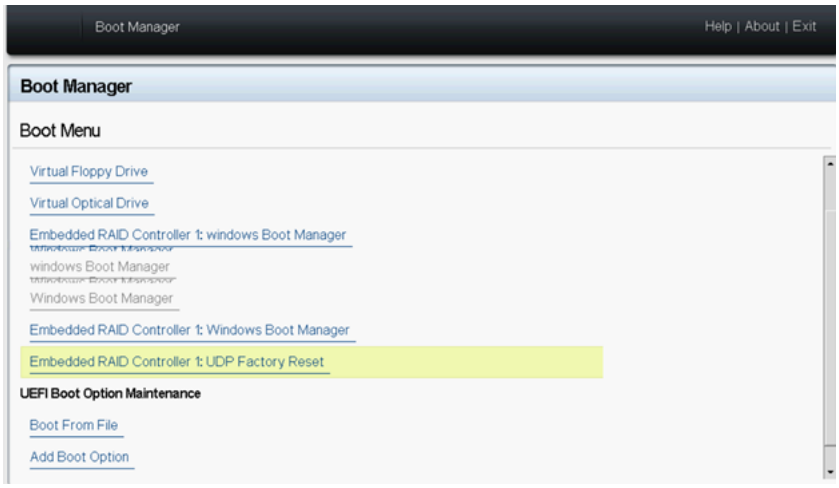
Sie können die UDP-Werkeinstellung auf dem Startmenü der Serie Arcserve Appliance X anwenden. Mit den UDP-Werkeinstellungen können Sie die Arcserve Appliance X-Serie in den ursprünglichen Zustand ohne Konfiguration zurücksetzen.

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

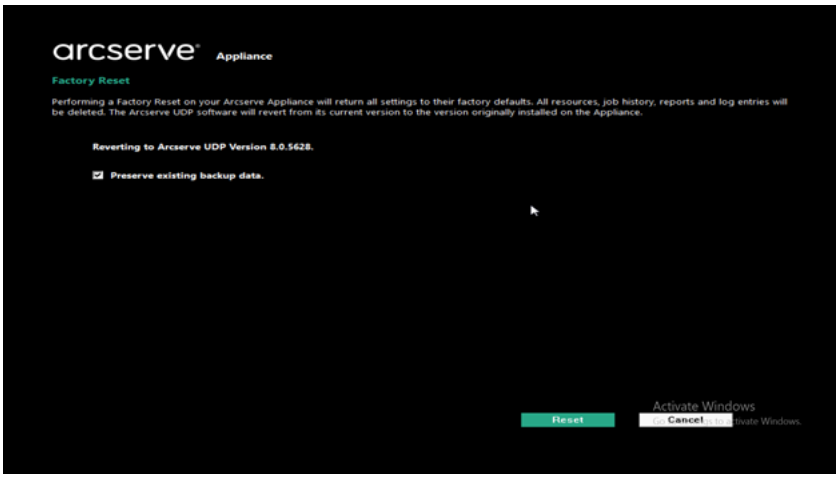
Befolgen Sie diese Schritte:

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

2. Wählen Sie die Startoption **Eingebetteter 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.

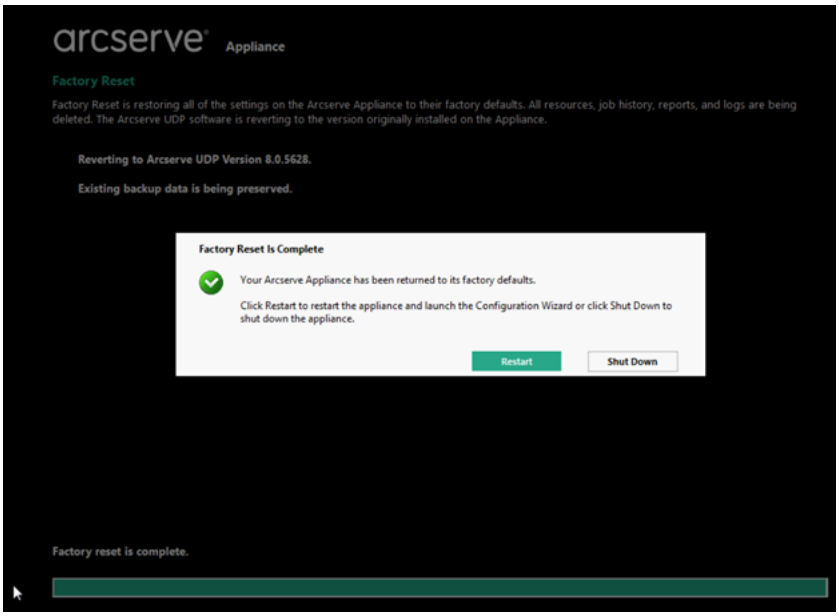
3. Klicken Sie auf **Zurücksetzen**.

   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.

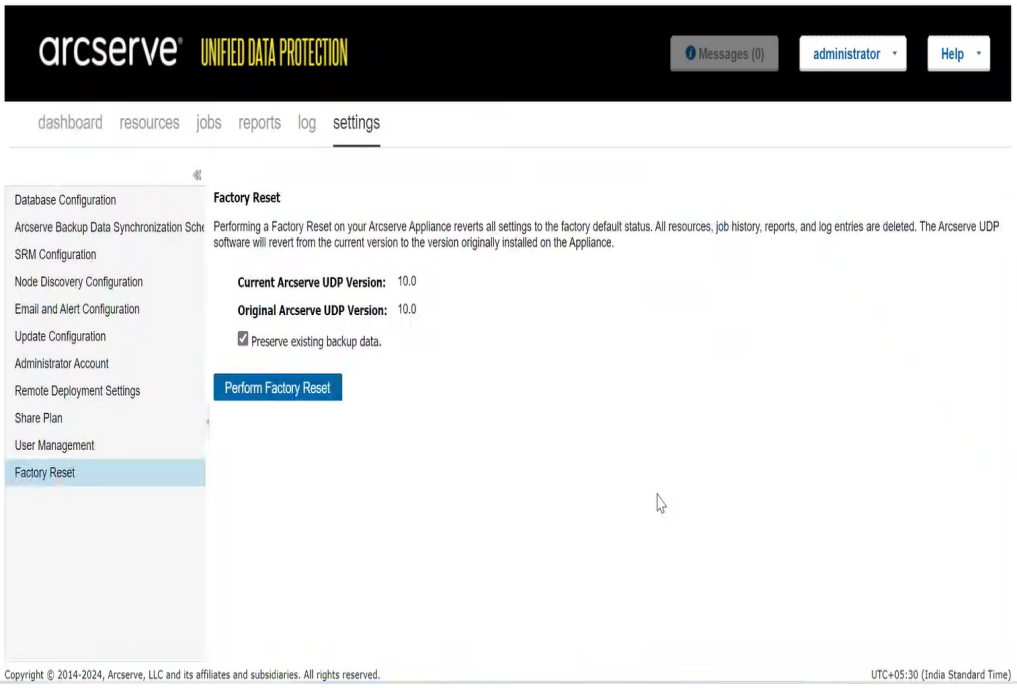

arcserve Appliance
Factory Reset
Factory Reset is restoring all of the settings on the Arcserve Appliance to their factory defaults. All resources, job history, reports, and logs are being deleted. The Arcserve UDP software is reverting to the version originally installed on the Appliance.
Reverting to Arcserve UDP Version 8.0.5628.
Existing backup data is being preserved.
Factory Reset Is Complete
Your Arcserve Appliance has been returned to its factory defaults.
Click Restart to restart the appliance and launch the Configuration Wizard or click Shut Down to shut down the appliance.
Restart
Shut Down
Factory reset is complete.

Löschen der Konfiguration und Zurücksetzung der Appliance auf Werkseinstellungen

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

Befolgen Sie diese Schritte:

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



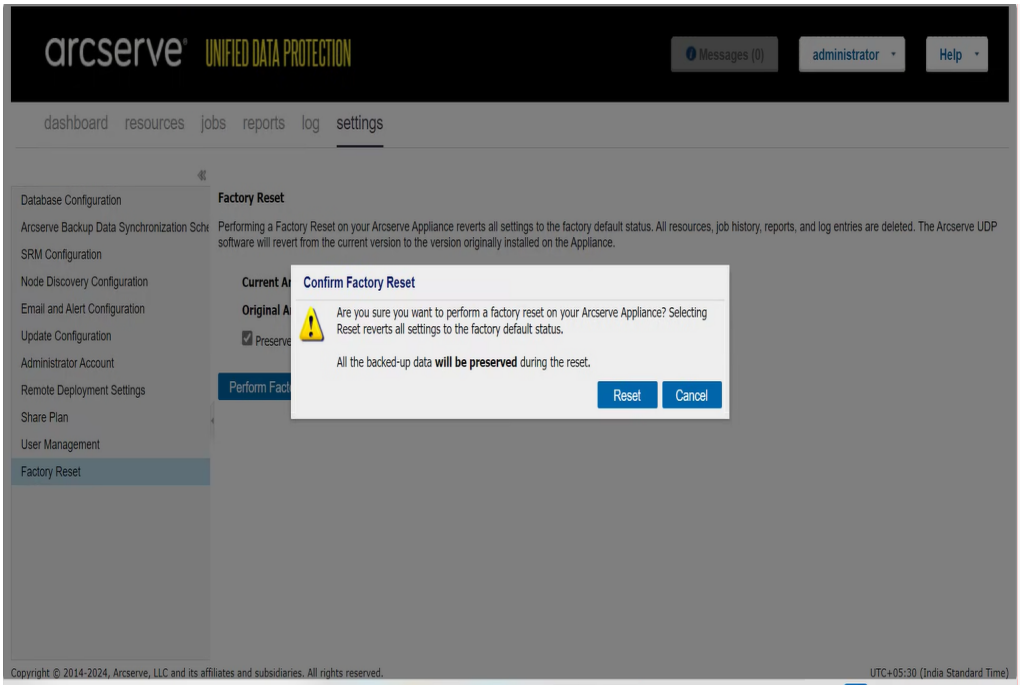
   Alle gesicherten Daten werden standardmäßig beibehalten.

   Hinweis: 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 Bestätigungsdialogfeld wird angezeigt.

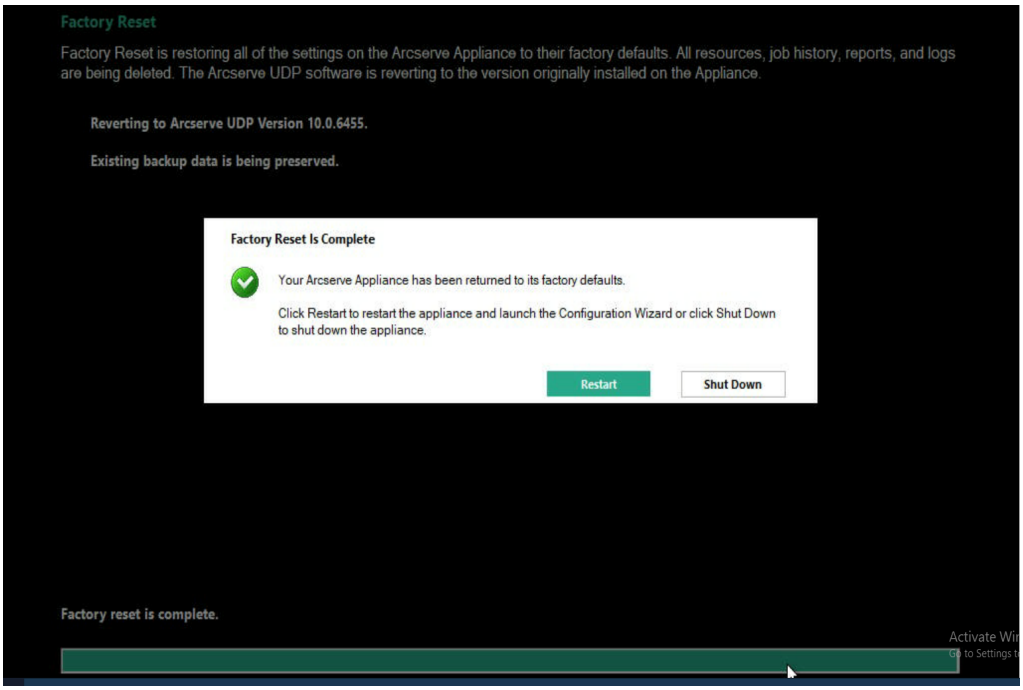


3. Klicken Sie im Bestätigungsdialog auf **Zurücksetzen**, um die Zurücksetzung auf Werkseinstellungen zu starten.

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

Nach Abschluss der Zurücksetzung wird ein Bestätigungsdialog angezeigt.

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



Festplatte entfernen und ersetzen

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

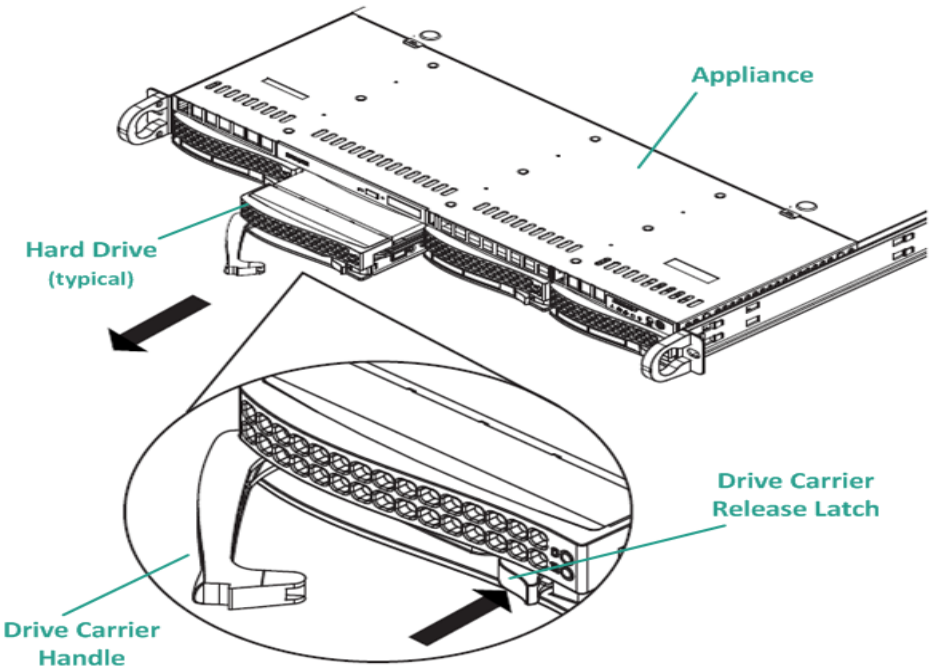
Die Arcserve Appliance enthält vier Festplattenträger, die von links nach rechts mit 0, 1, 2 und 3 gekennzeichnet sind. Wenn Sie mehr als eine Festplatte ersetzen, sollten Sie die Ersatzfestplatten kennzeichnen, sodass Sie wissen, welche Festplatte in den einzelnen Festplattenträgern platziert werden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

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

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

Befolgen Sie diese Schritte:

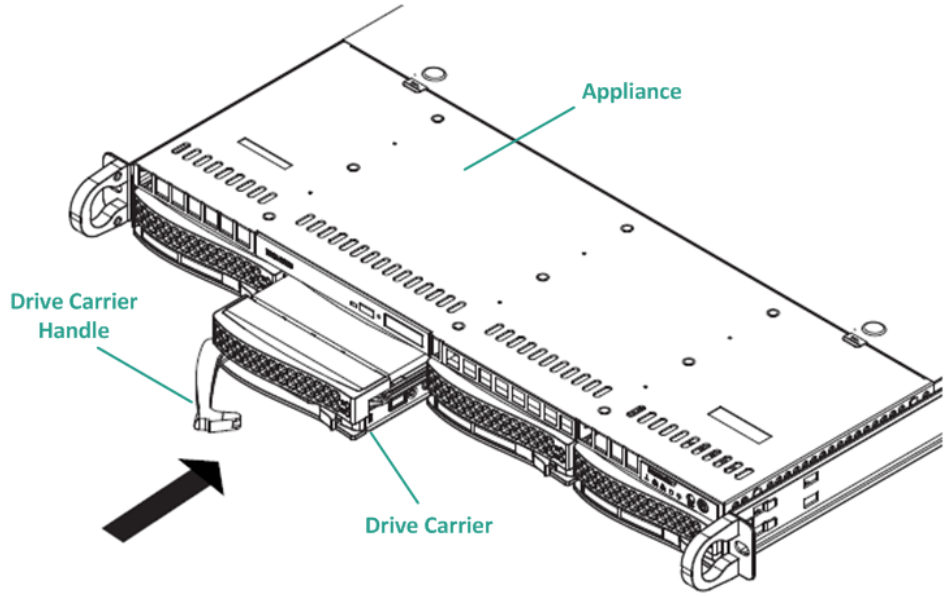
1. Um auf die Laufwerkshalter zugreifen zu können, müssen Sie zunächst die Abdeckplatte entfernen:
    a. Lösen Sie die Verriegelung der Abdeckplatte.
    b. Drücken Sie auf den Entriegelungsknopf, um die Stifte der Abdeckplatte einzuziehen.
    c. Nehmen Sie vorsichtig die Abdeckplatte ab (mit beiden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



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

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

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



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

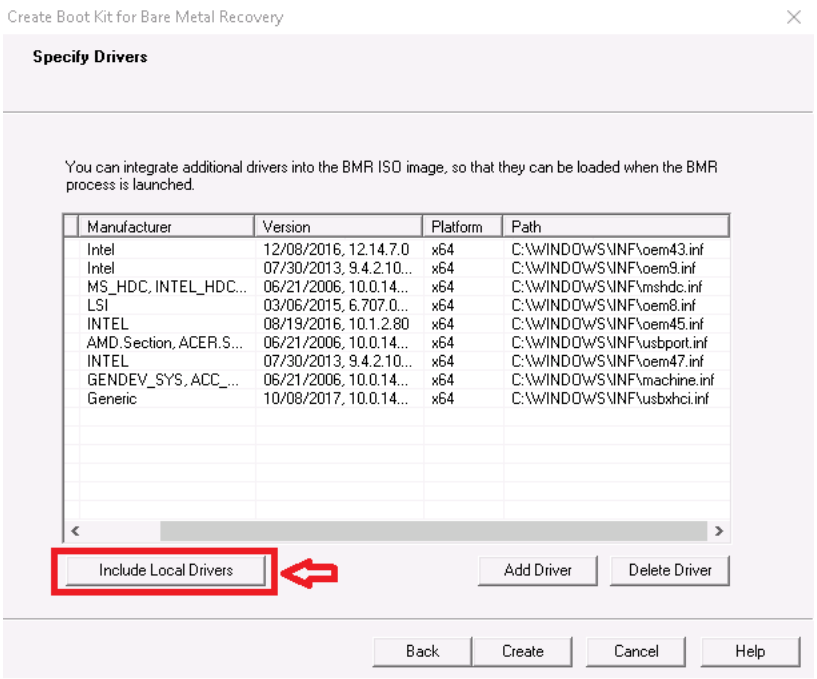
Durchführen einer Bare Metal Recovery (BMR) ohne Beibehalten der Daten in der Appliance der 9012-9504DR-Serie

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.

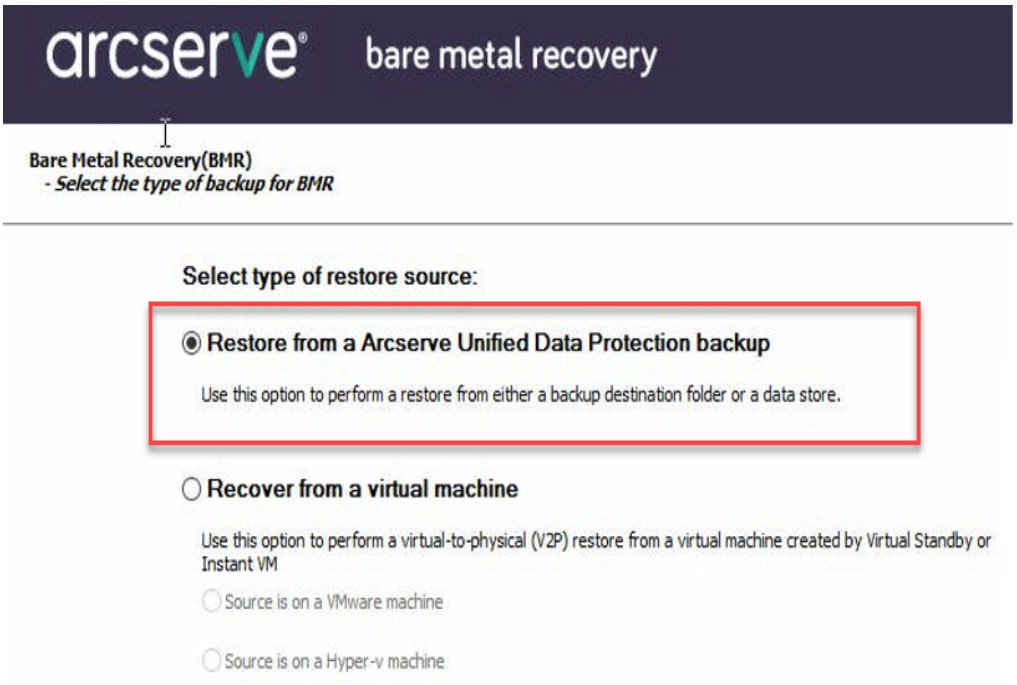


2. Starten Sie die Arcserve Appliance mit dem BMR-ISO-Image oder dem USB-Stick.

   Das **ArcserveBare-Metal-Recovery** Setup wird angezeigt.

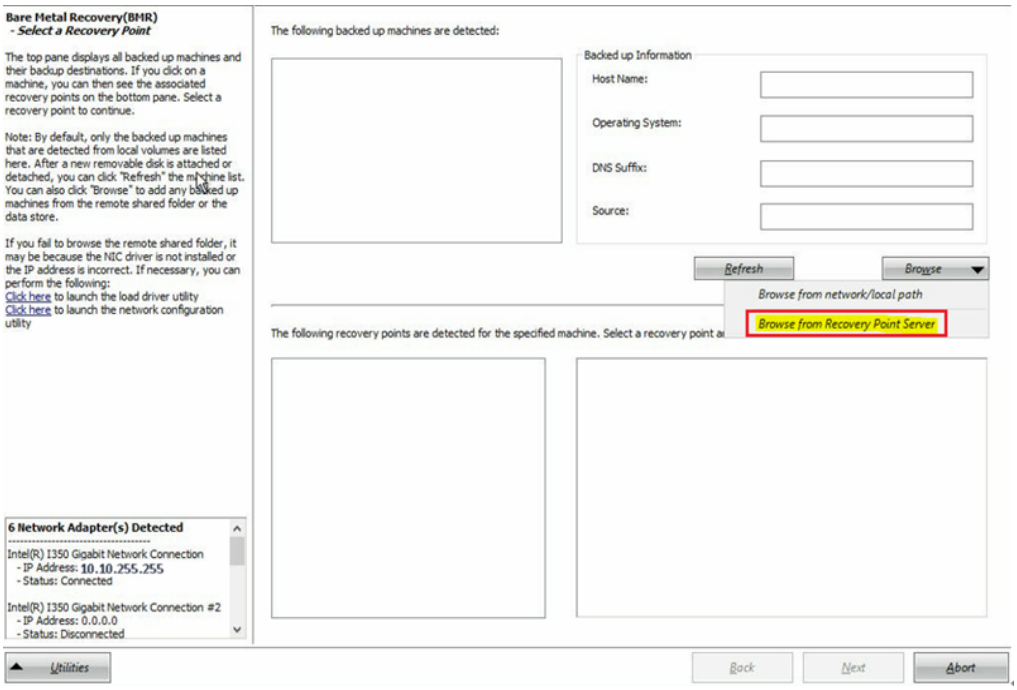
3. Wählen Sie die erforderliche Sprache aus, und klicken Sie auf **Weiter**.

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



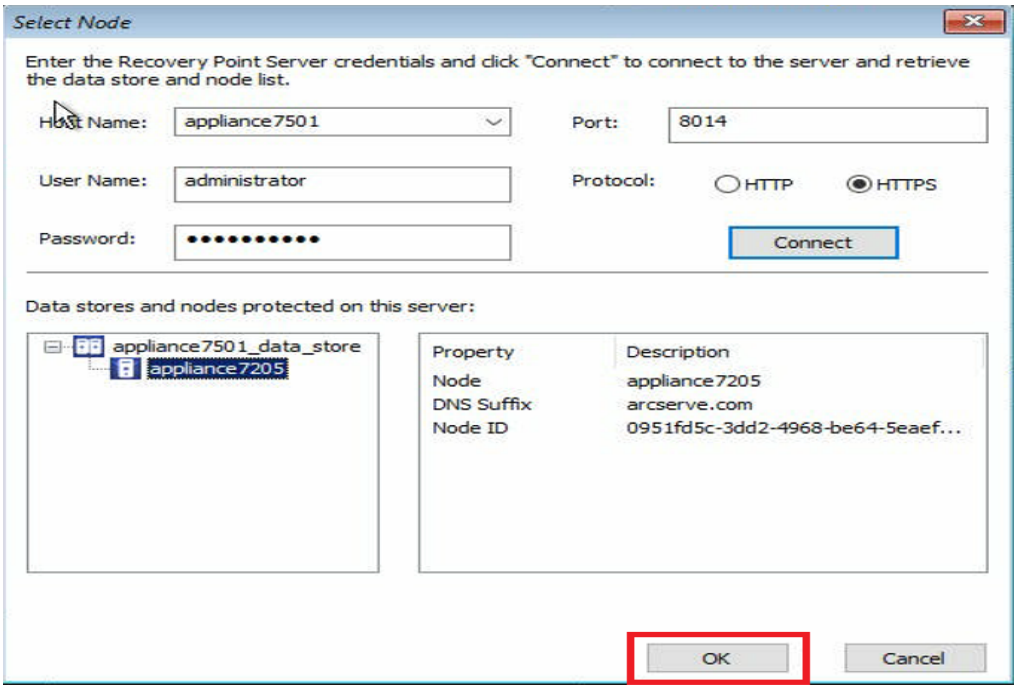
Das Fenster **Assistent zum Auswählen eines Wiederherstellungspunkts** wird angezeigt.

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



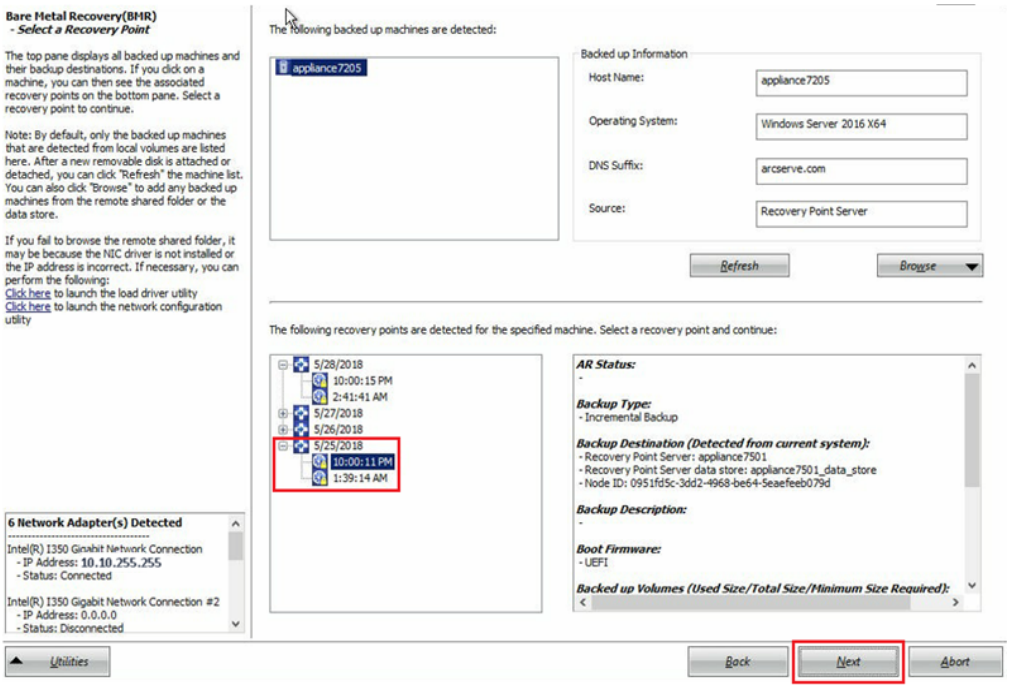
Das Fenster **Knoten auswählen** wird angezeigt.

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.

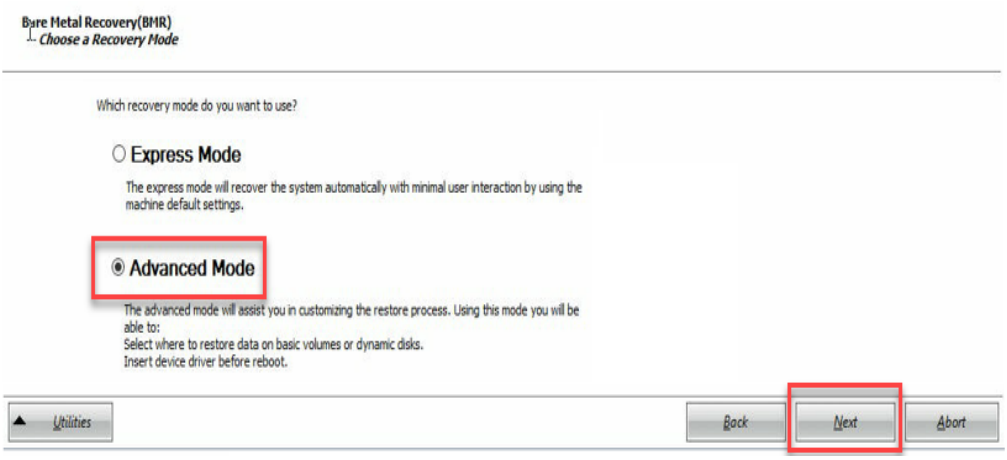
9. Wählen Sie den gewünschten Wiederherstellungspunkt aus, und klicken Sie auf **Weiter**.



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

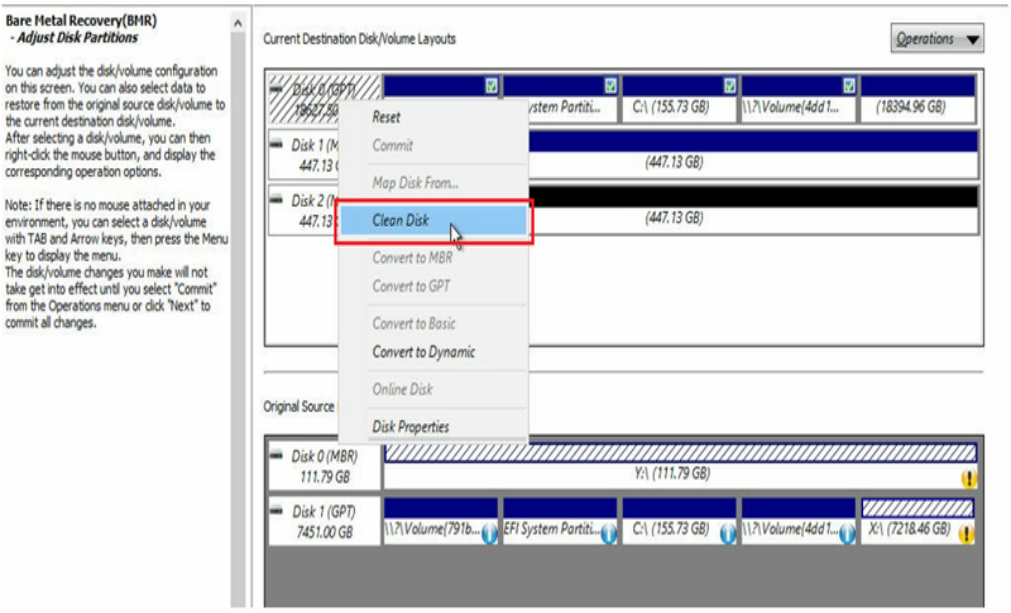
Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungsmodus auswählen** wird angezeigt.

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

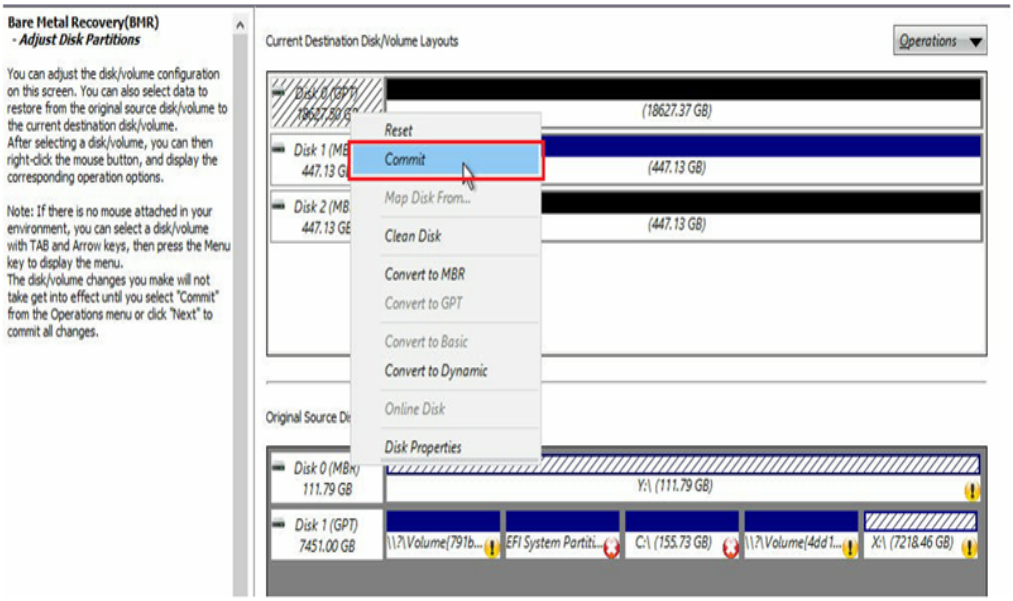


Das Dialogfeld **Bare-Metal-Recovery (BMR) – Datenträgerpartitionen anpassen** wird angezeigt.

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

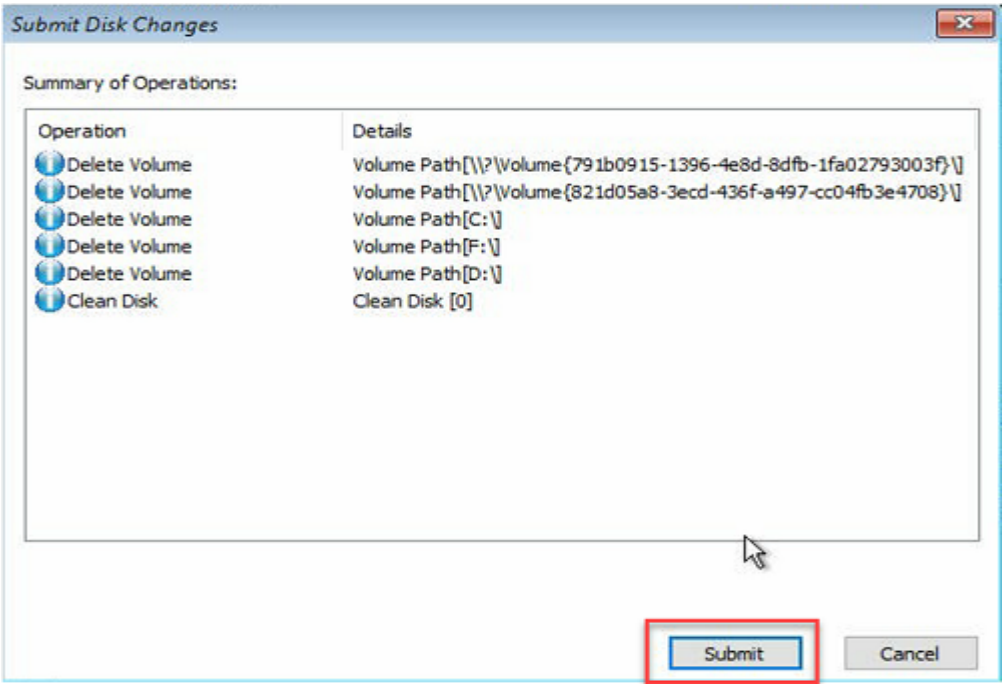


13. Klicken Sie nach der Reinigung der Festplatte mit der rechten Maustaste auf denselben Datenträger, und klicken Sie auf **Commit**.

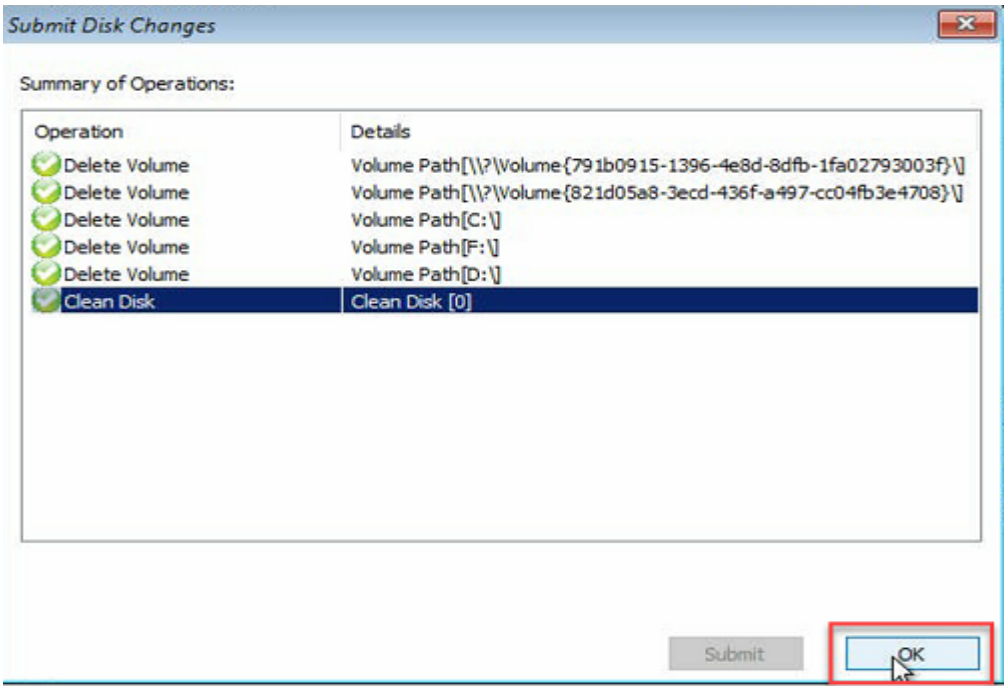


Das Fenster **Datenträgeränderungen übergeben** wird angezeigt.

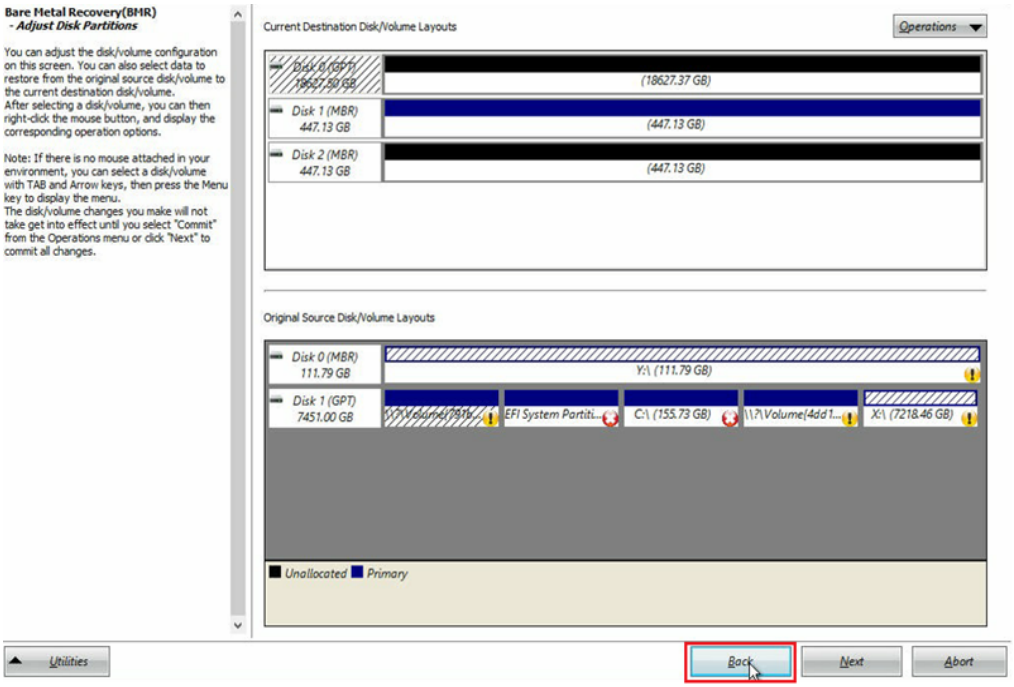
14. Klicken Sie auf **Übergeben**.



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

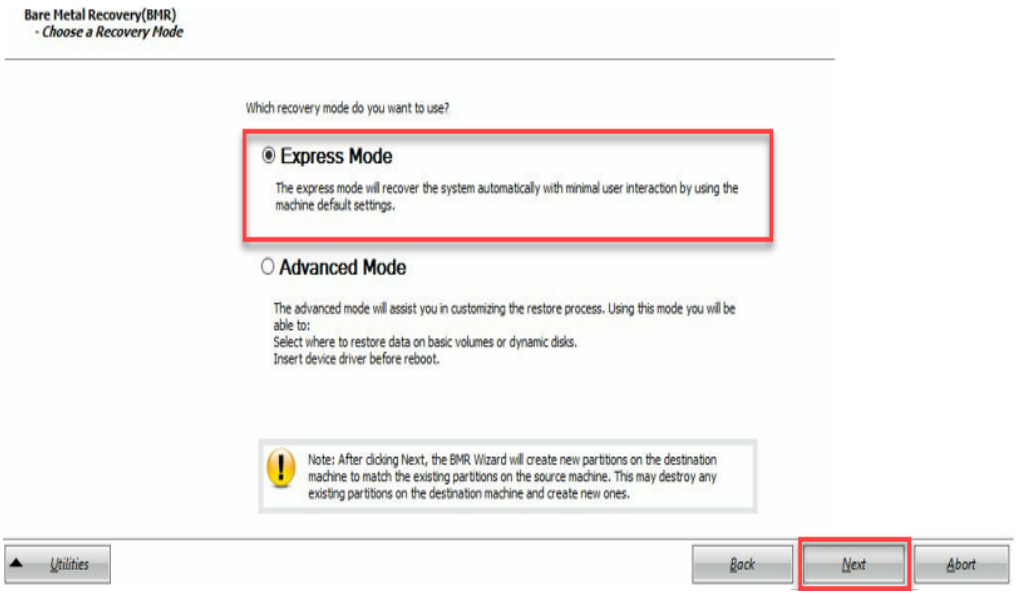


16. Klicken Sie im Dialogfeld **Bare-Metal-Recovery (BMR) – Datenträgerpartitionen anpassen** auf **Zurück**.



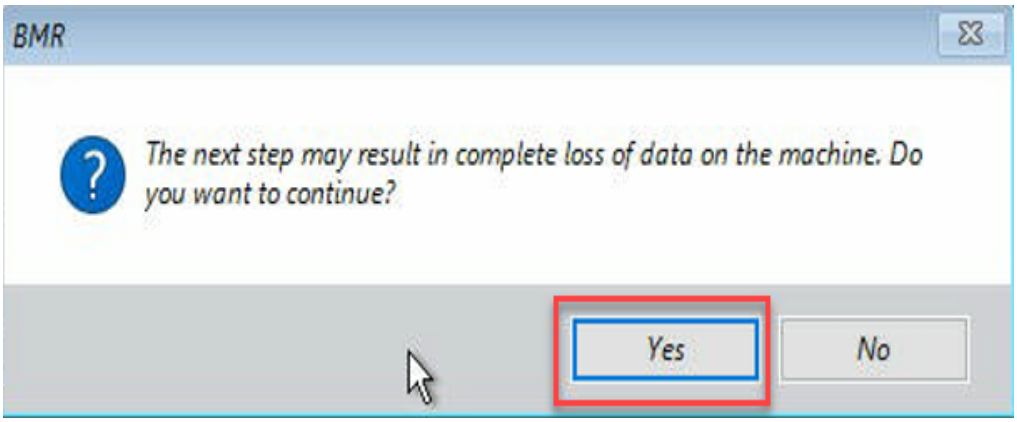
Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungsmodus auswählen** wird angezeigt.

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



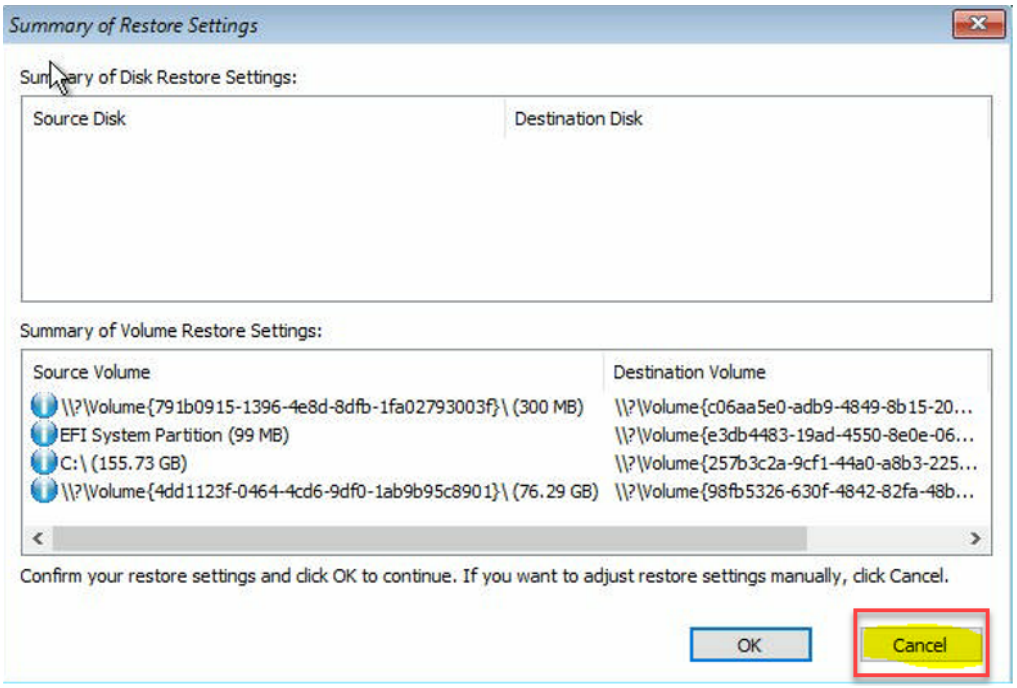
Das Dialogfeld **BMR** wird angezeigt.

18. Klicken Sie auf **Ja**.



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

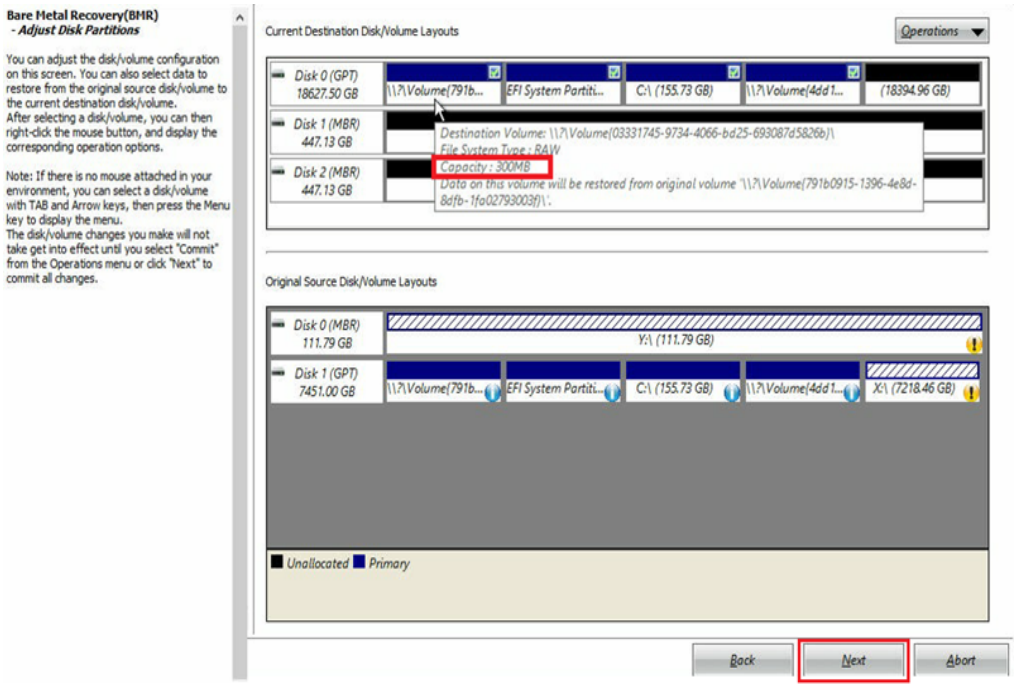
19. Klicken Sie auf **Abbrechen**.



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

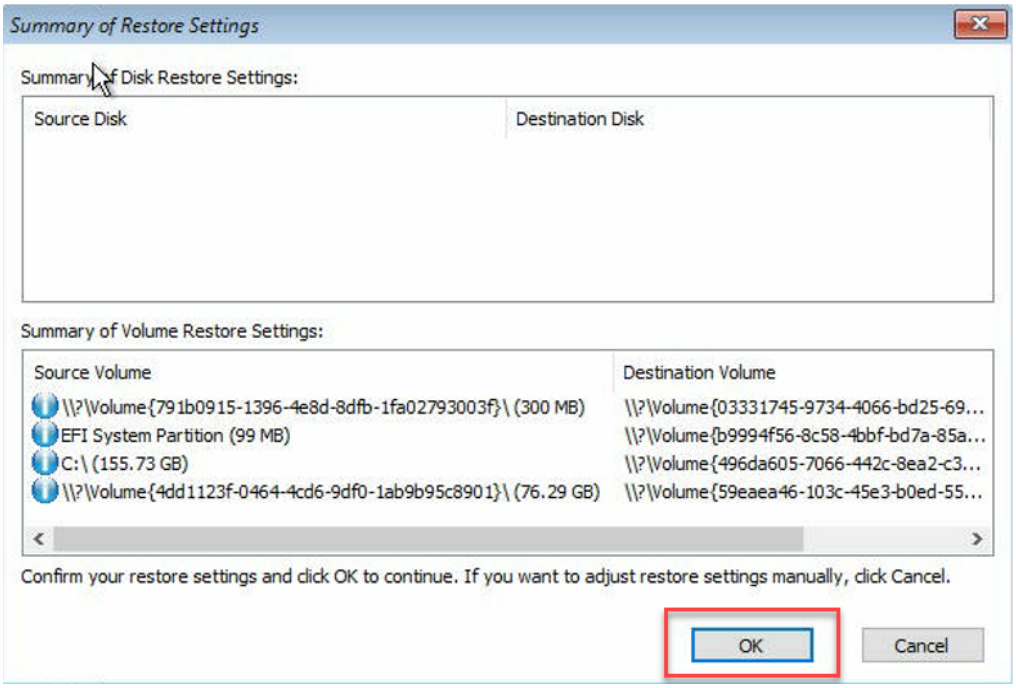
20. Vergleichen und überprüfen Sie, ob die Kapazität der ersten vier Partitionen auf der Registerkarte **Aktuelle Zieldatenträger/Volume-Layouts** dem größten verfügbaren GPT-Datenträger auf der Registerkarte **Ursprüngliche Quelldatenträger/Volume-Layouts** entspricht, und klicken Sie auf **Weiter**.

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



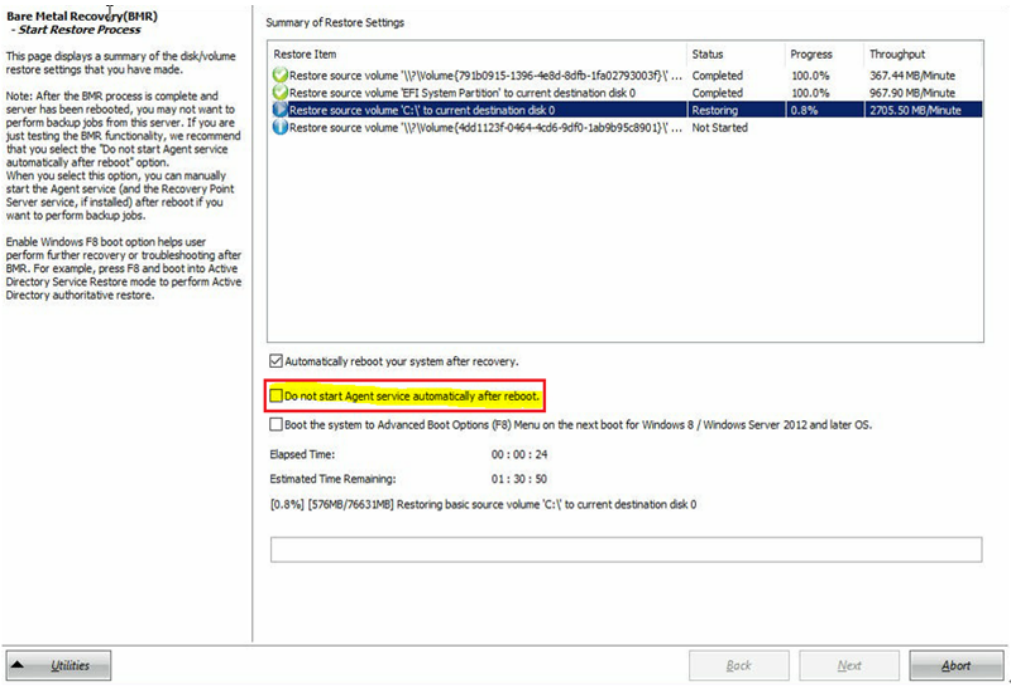
Das Dialogfeld **Übersicht über die Wiederherstellungseinstellungen** wird angezeigt.

21. Klicken Sie auf **OK**.



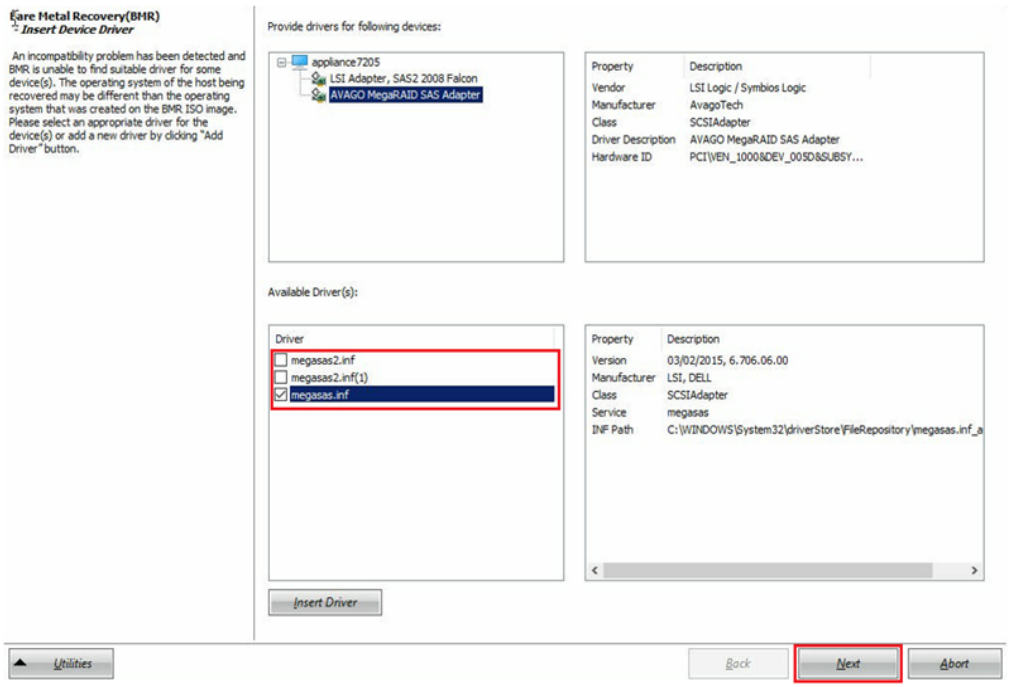
Das Dialogfeld **Bare-Metal-Recovery (BMR) – Wiederherstellungsprozess starten** wird angezeigt.

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

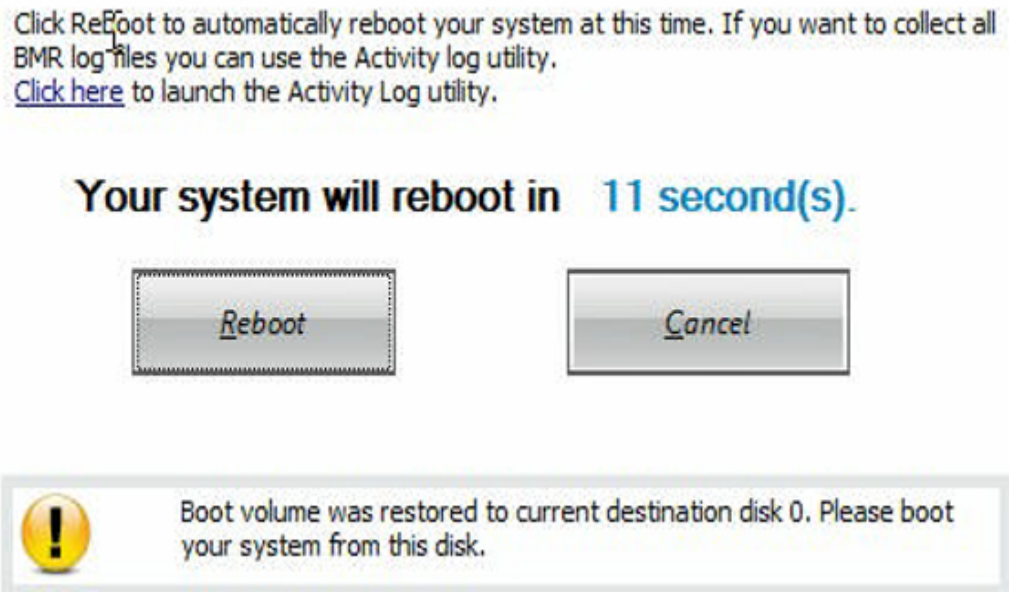


Das Dialogfeld **Bare-Metal-Recovery (BMR) – Gerätetreiber einfügen** wird angezeigt.

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.

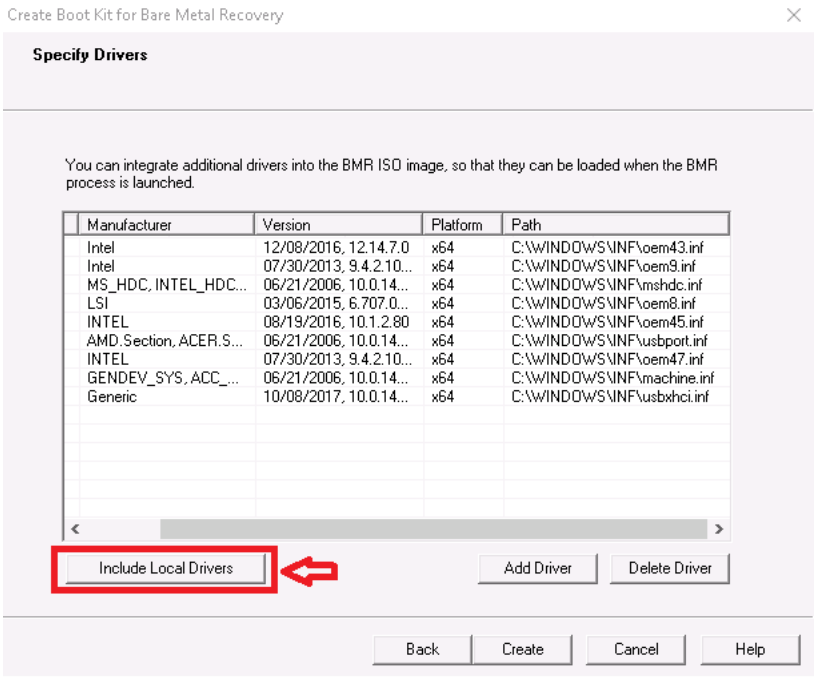
Durchführen einer Bare Metal Recovery (BMR) und Beibehalten der Daten in der Appliance der 9012-9504DR-Serie

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.

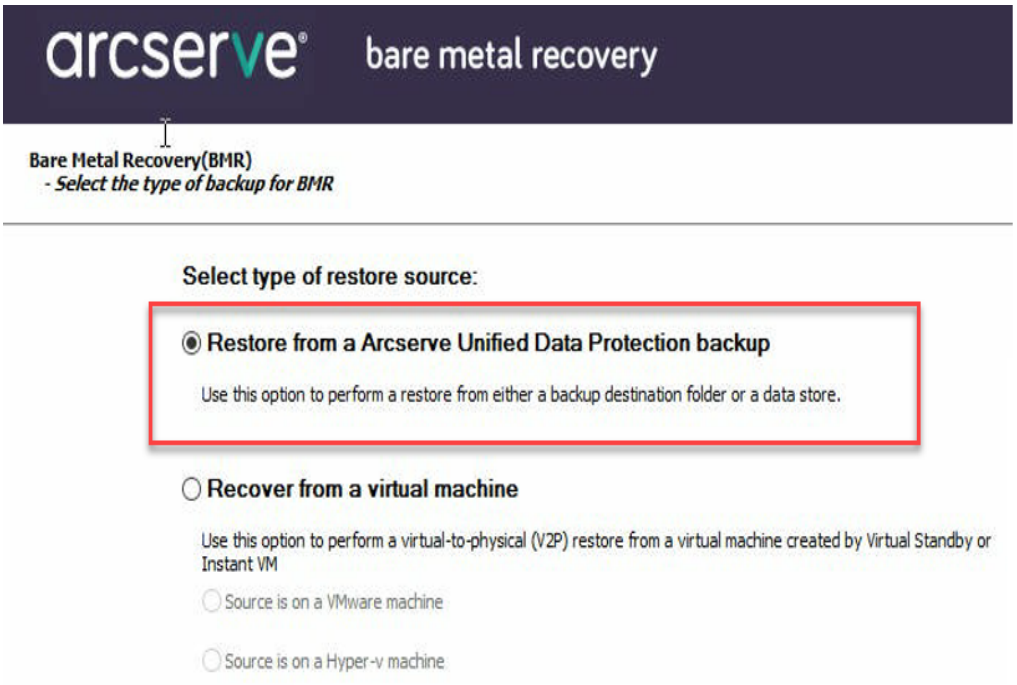


2. Starten Sie die Arcserve Appliance mit dem BMR-ISO-Image oder dem USB-Stick.

   Das **ArcserveBare-Metal-Recovery** Setup wird angezeigt.

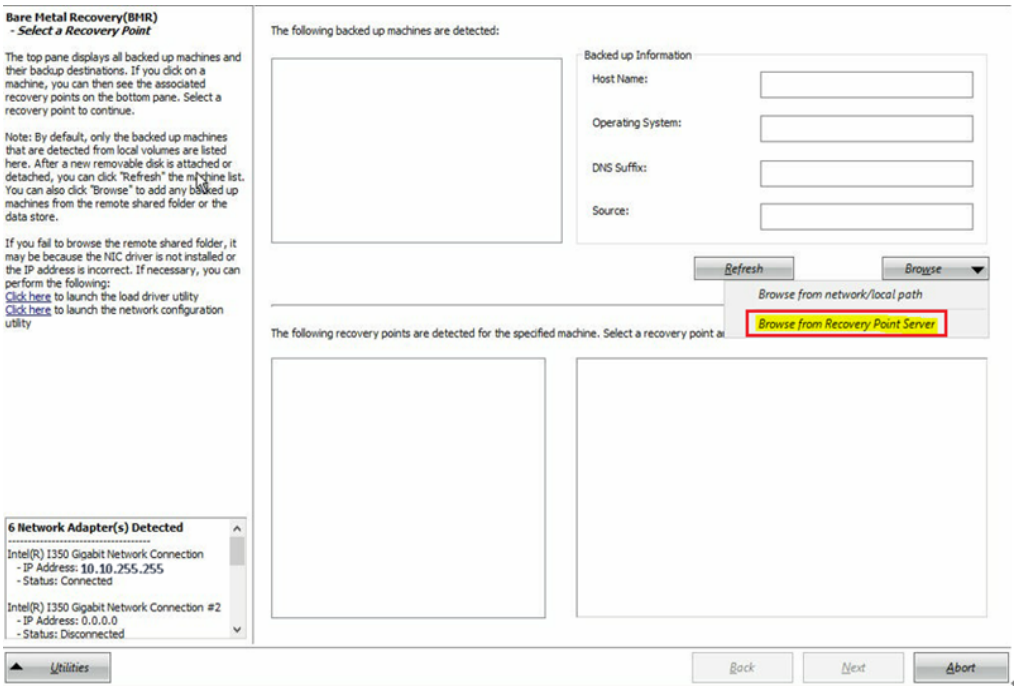
3. Wählen Sie die erforderliche Sprache aus, und klicken Sie auf **Weiter**.

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



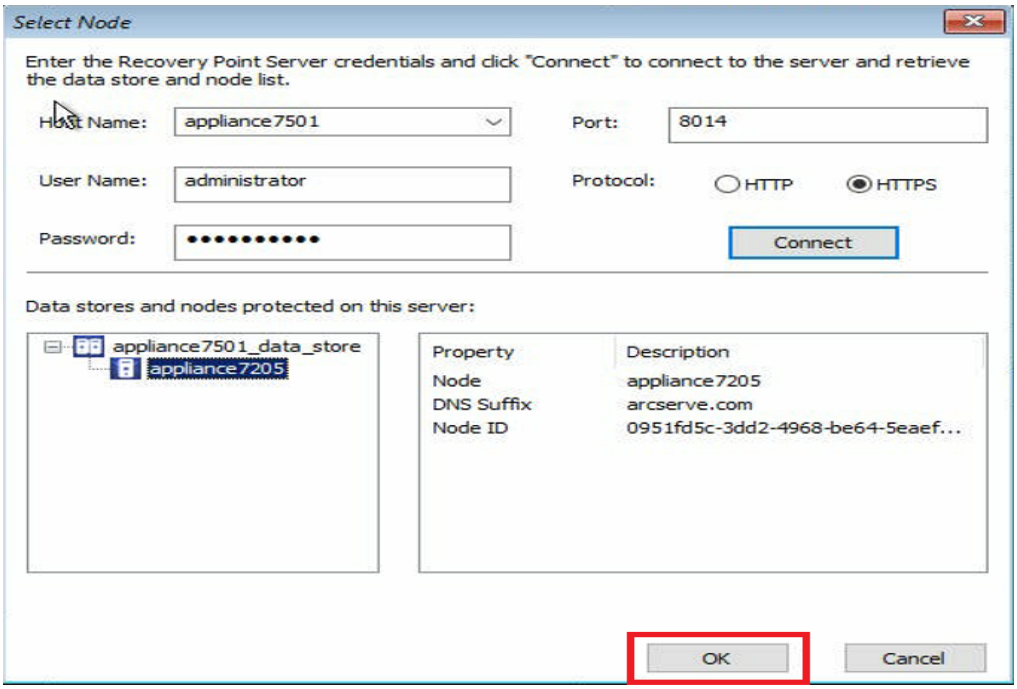
Das Fenster **Assistent zum Auswählen eines Wiederherstellungspunkts** wird angezeigt.

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



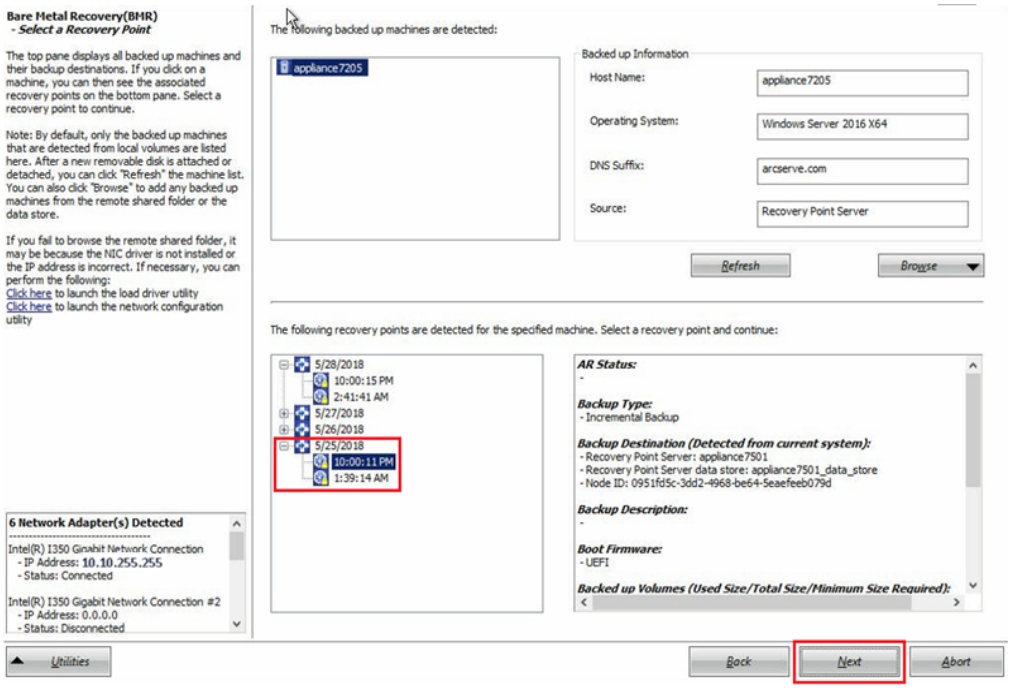
Das Fenster **Knoten auswählen** wird angezeigt.

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



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

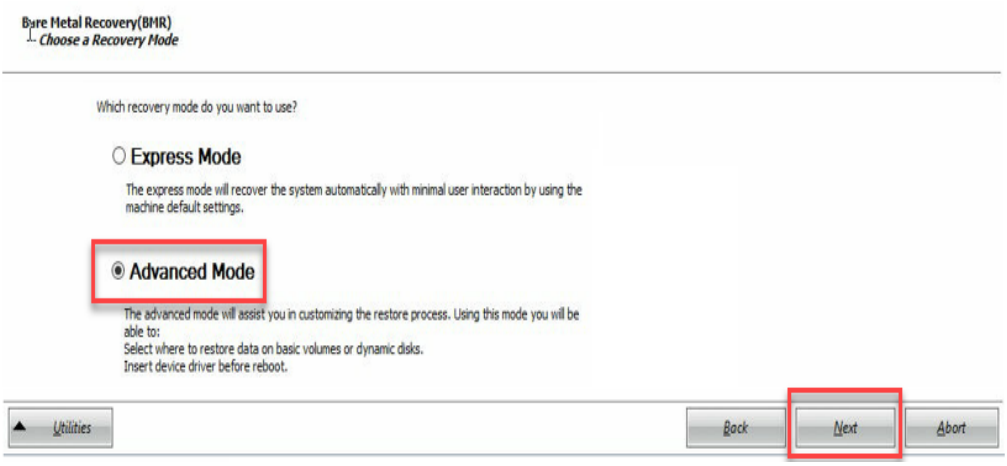
9. Wählen Sie den gewünschten Wiederherstellungspunkt aus, und klicken Sie auf **Weiter**.



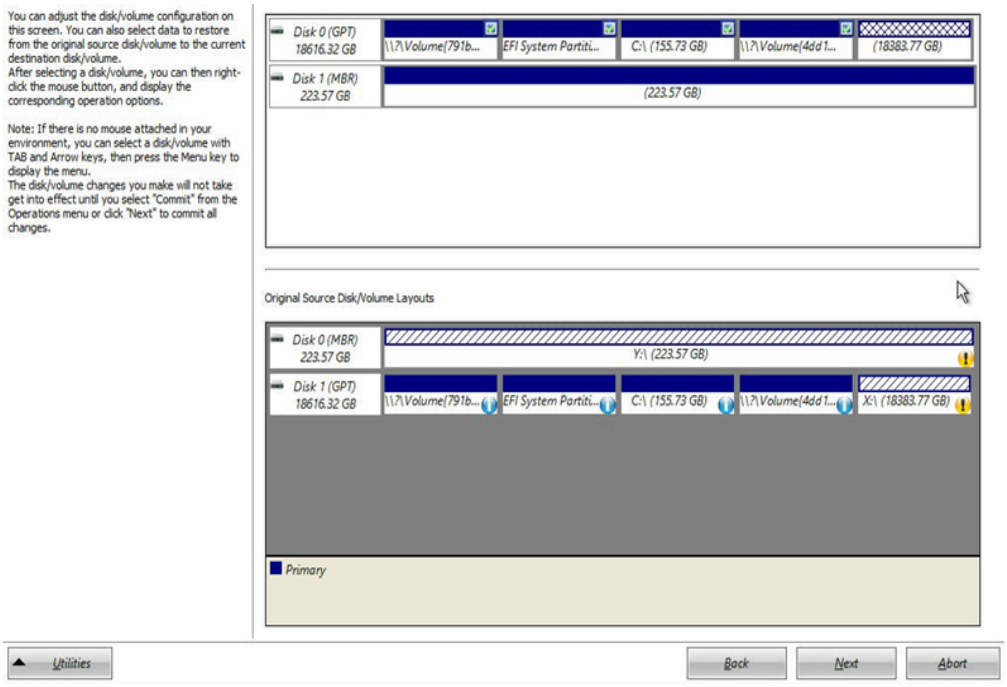
10. (Optional) Geben Sie das Sitzungskennwort ein, wenn Sie dazu aufgefordert werden, und klicken Sie dann auf **OK**.

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

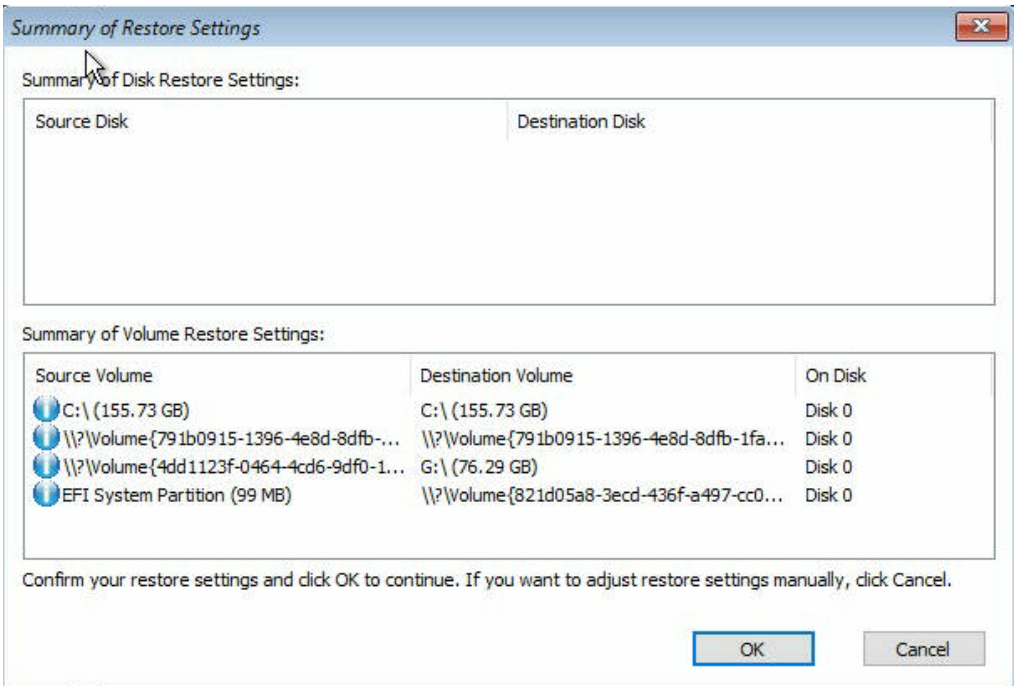
11. Wählen Sie **Erweiterter Modus** aus, und klicken Sie auf **Weiter**.



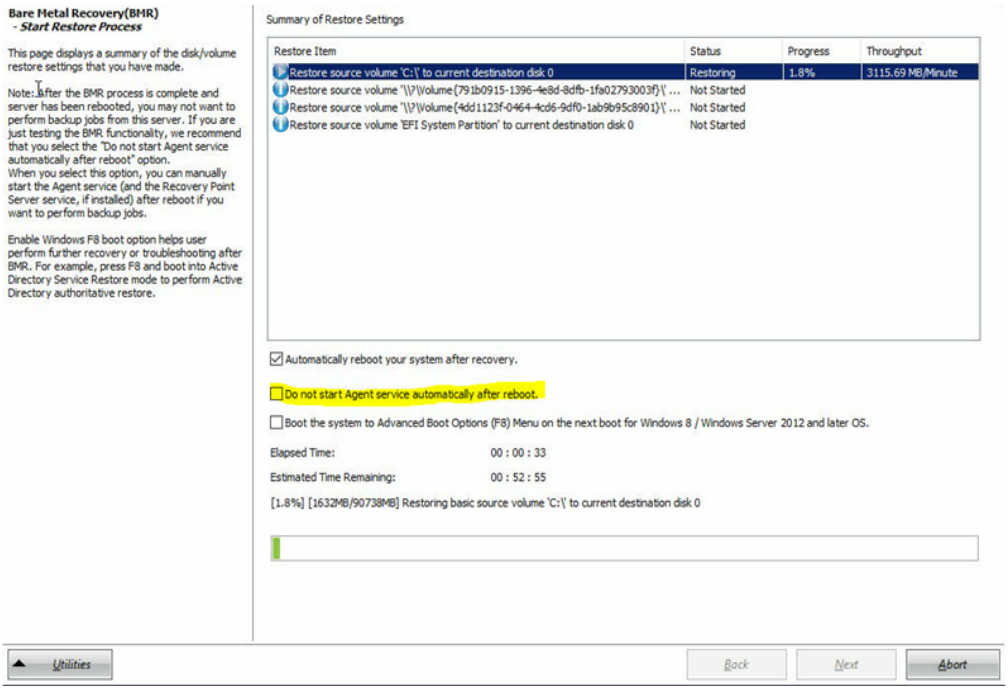
12. Klicken Sie im Dialogfeld **Bare Metal Recovery (BMR)-Datenträgerpartitionen anpassen** auf **Weiter**.



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



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



Der BMR-Prozess wurde erfolgreich abgeschlossen.

Kapitel 9: Durchführung einer Kapazitätserweiterung der Appliance

Dieser Abschnitt enthält folgende Themen:

Arbeiten mit dem Erweiterungs-Kit für Arcserve Appliance 10024BU-10576DR-Modelle

Mit dem Arcserve Erweiterungs-Kit können Sie die Datenkapazität von Arcserve Appliance 10024BU-10576DR-Modellen erweitern.

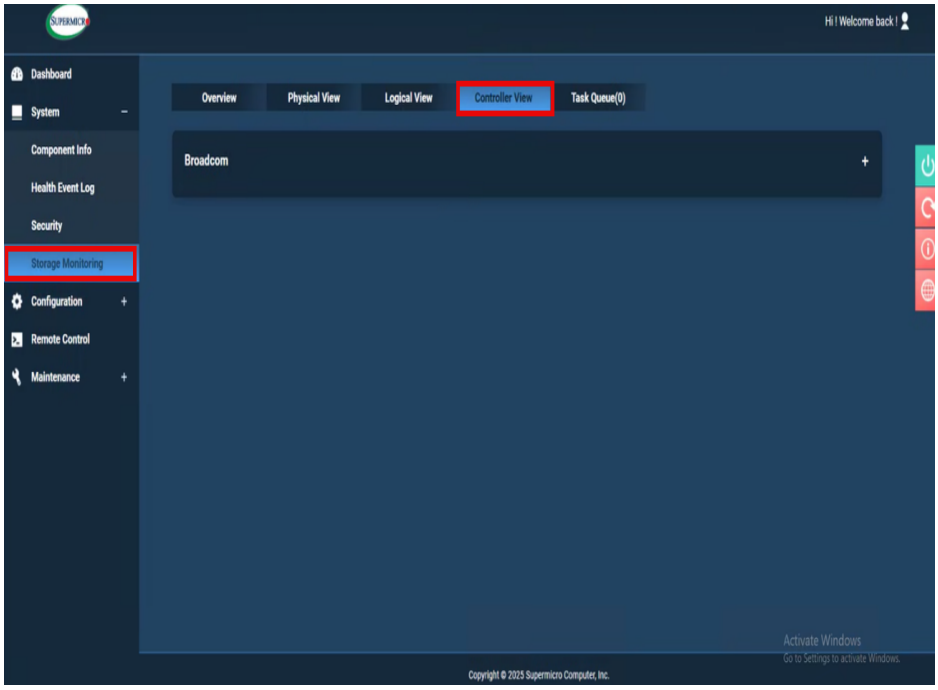
Befolgen Sie diese Schritte:

1. Gehen Sie wie folgt vor, um die Festplatten in die leeren Datenträger-Slots einzulegen:
   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.

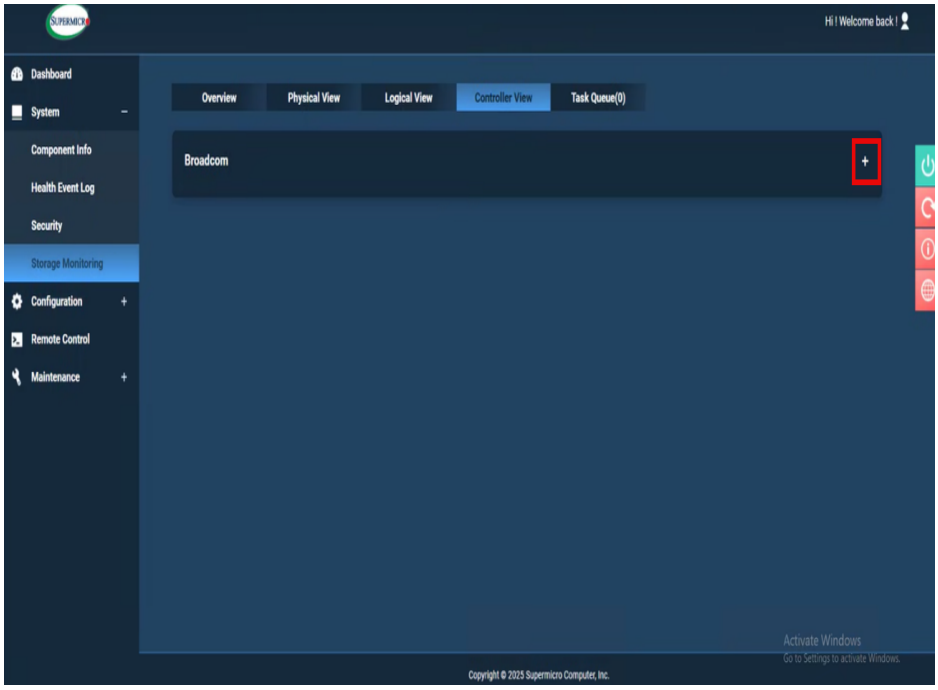
2. Um Raid-6 über die IPMI-Webschnittstelle zu erstellen und zu konfigurieren, gehen Sie wie folgt vor:

a. Melden Sie sich bei der IPMI-Konsole an.

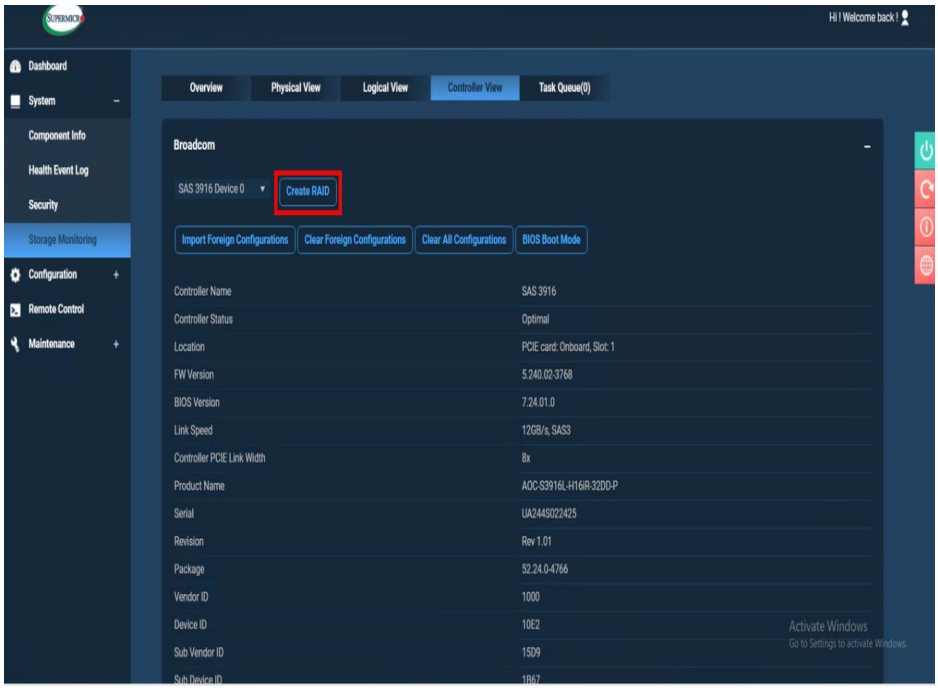
b. Navigieren Sie zu **System** > **Storage Monitoring** > **Controller view**.



c. Klicken Sie auf der Registerkarte "Controller View" auf das **Pluszeichen (+)**, um **Broadcom** zu erweitern.



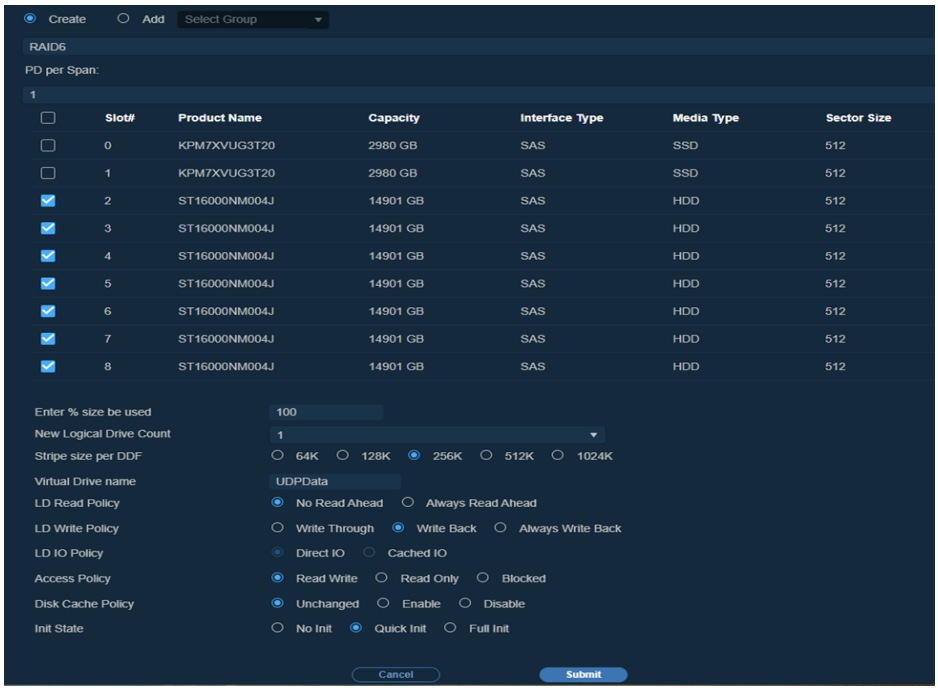
d. Klicken Sie im Fenster "Broadcom" auf **Create RAID**.



e. Wählen Sie auf der Seite "Create" alle HDD-Slots aus, und geben Sie dann Folgendes an:

- **RAID**: Wählen Sie in der Dropdown-Liste für die RAID-Ebene "RAID6" aus.
- **PD per Span**: 1
- **Enter % size be used**: Geben Sie den Wert **100** ein.
- **New Logical Drive Count**: Geben Sie den Wert **1** ein.
- **Stripe size per DDF**: Wählen Sie die Option **256K** aus.
- **Virtual Drive name**: Geben Sie den gewünschten Namen für das virtuelle Laufwerk ein.
- **LD Read Policy**: Wählen Sie die Option **No Read Ahead** aus.
- **LD Read Policy**: Wählen Sie die Option **Write Back** aus.
- **LD IO Policy**: Standardmäßig ist die Option **Direct IO** ausgewählt.
- **Access Policy**: Wählen Sie die Option **Read Write** aus.
- **Disk Cache Policy**: Wählen Sie die Option **Unchanged** aus.
- **Init-Status**: Wählen Sie die Option **Quick Init** aus.

f. Klicken Sie auf **Übergeben**.



g. Geben Sie im Suchfeld der Taskleiste **Computer Management** ein, und drücken Sie die Eingabetaste.

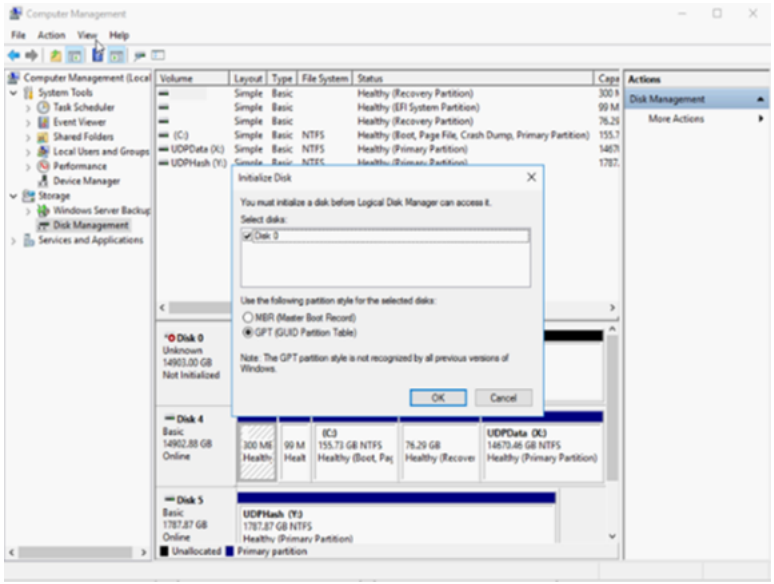
   Das Fenster für die Computerverwaltung wird geöffnet.

h. Navigiere Sie zu **Storage** > **Disk Management**.

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

   Das Fenster "Datenträger initialisieren" wird angezeigt.

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



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

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

3. 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 vom Arcserve Appliance-Desktop aus den Assistenten **Arcserve Appliance** .

Die Seite "Arcserve Appliance-Konfiguration" wird geöffnet.

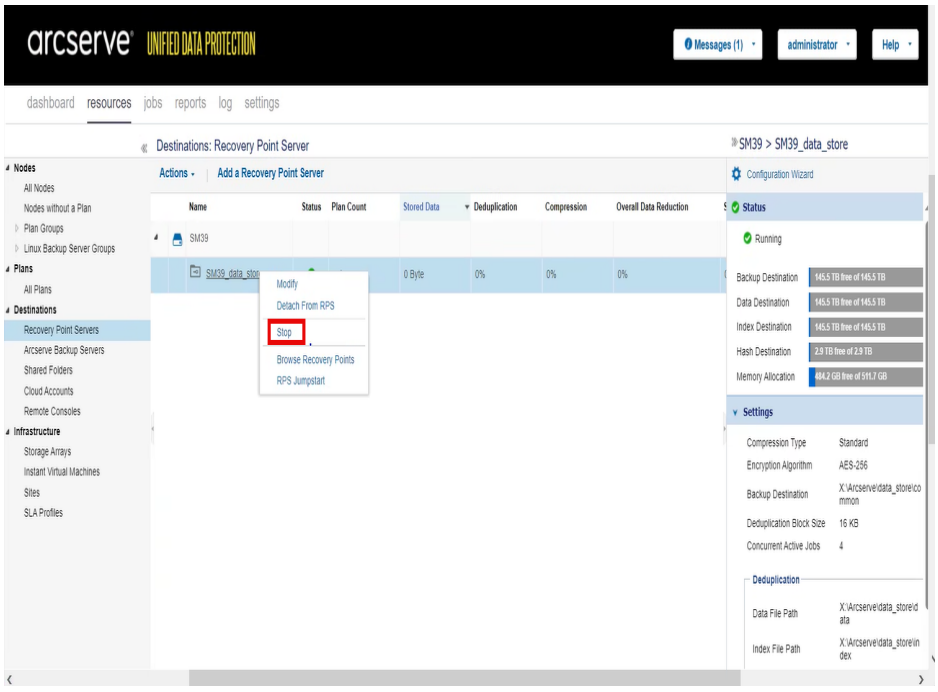
c. Klicken Sie auf **UDP-Konsole starten**.

Die Anmeldeseite der Arcserve UDP-Konsole wird angezeigt.

d. Melden Sie sich bei der UDP-Konsole als Administrator an.

e. Navigieren Sie zu **Ressourcen** > **Ziele** > **Recovery Point Server**.

f. Klicken Sie mit der rechten Maustaste auf den Datenspeicher, und wählen Sie dann **Beenden** aus.



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 <neuer 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>

Der neue erweiterte Datenpfad wird erfolgreich zum Datenspeicher hinzugefügt.

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

i. Klicken Sie mit der rechten Maustaste auf den Datenspeicher, und wählen Sie dann **Starten** aus.

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

Die Datenkapazität der Arcserve Appliance wurde erfolgreich erweitert.

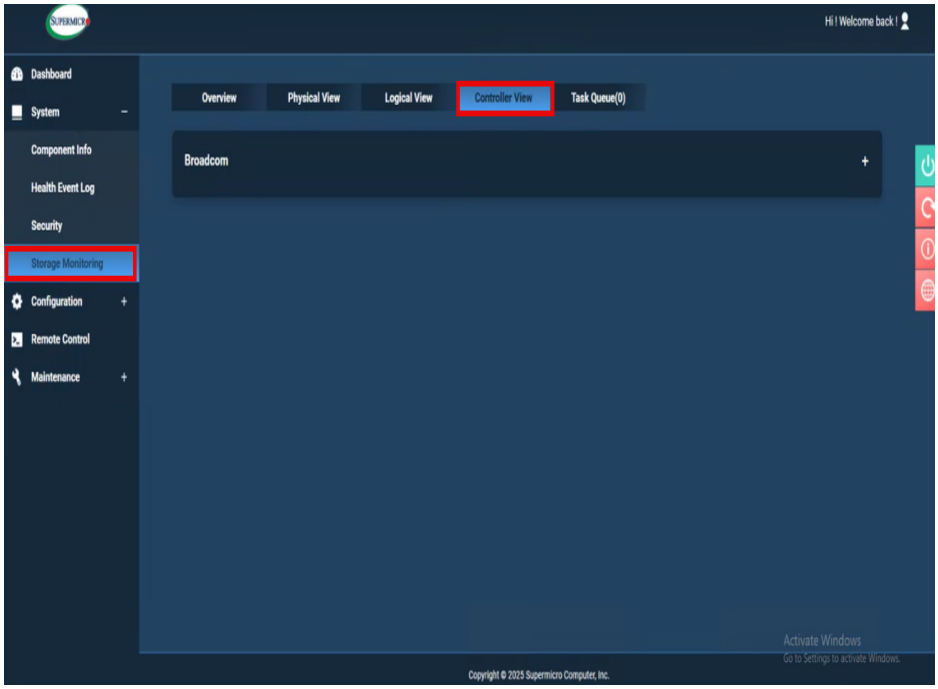
Arbeiten mit dem SSD-Flash-Erweiterungs-Kit für Arcserve Appliance 10024BU-10576DR-Modelle

Mit dem Arcserve SSD-Flash-Erweiterungs-Kit können Sie einen sekundären Datenspeicher erstellen und DR-bezogene Vorgänge (IVM/VSB/Continuous Availability) in den Arcserve Appliance 10024BU-10576DR-Modellen ausführen.

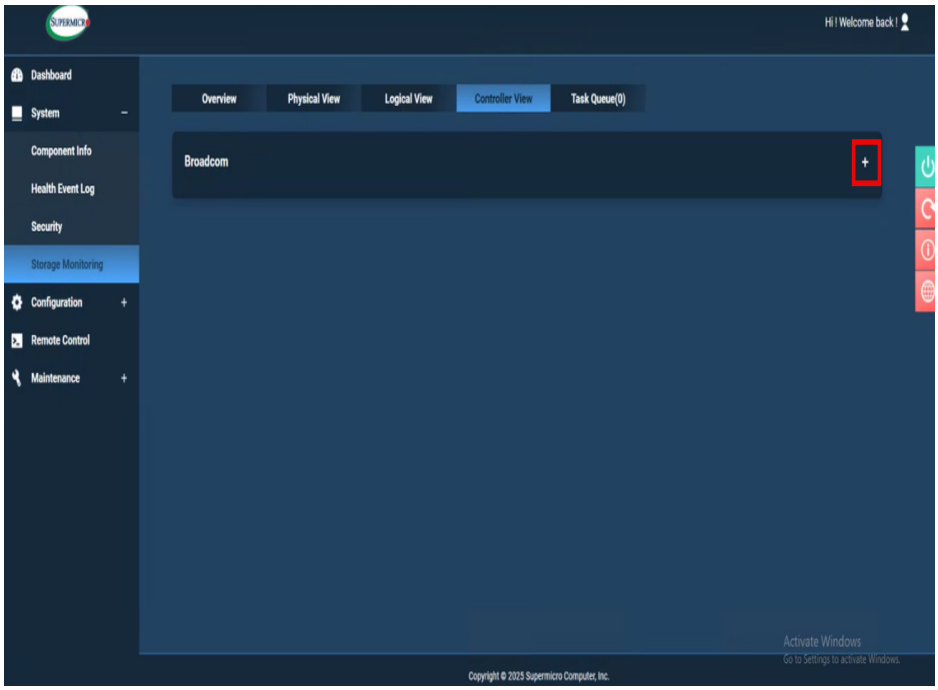
Befolgen Sie diese Schritte:

1. Gehen Sie wie folgt vor, um die SSDs in die leeren Datenträger-Slots einzulegen:
   a. Überprüfen Sie in der Arcserve UDP-Konsole, dass keine Jobs auf dem Appliance-Server ausgeführt werden. Falls Jobs ausgeführt werden, unterbrechen Sie die entsprechenden Pläne.
   b. Setzen sie die SSDs in die leeren Datenträgersteckplätze ein.

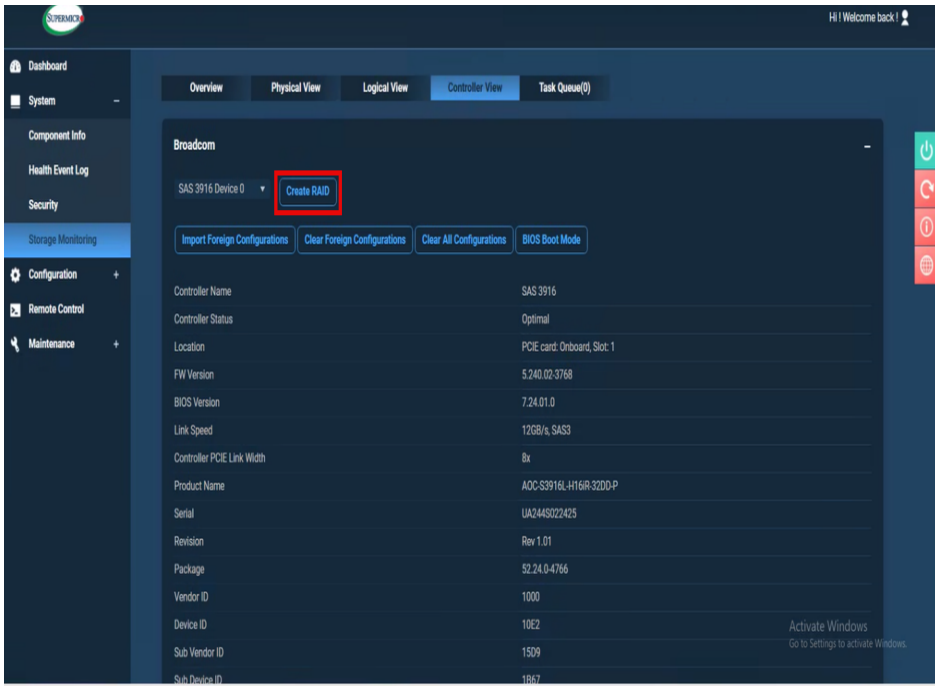
2. Um Raid-5 über die IPMI-Webschnittstelle zu erstellen und zu konfigurieren, gehen Sie wie folgt vor:
   a. Melden Sie sich bei der IPMI-Konsole an.
   b. Navigieren Sie zu **System** > **Storage Monitoring** > **Controller view**.



   c. Klicken Sie auf der Registerkarte *Controller View* auf das **Pluszeichen (+)**, um **Broadcom** zu erweitern.



d. Klicken Sie im Fenster "Broadcom" auf **Create RAID**.

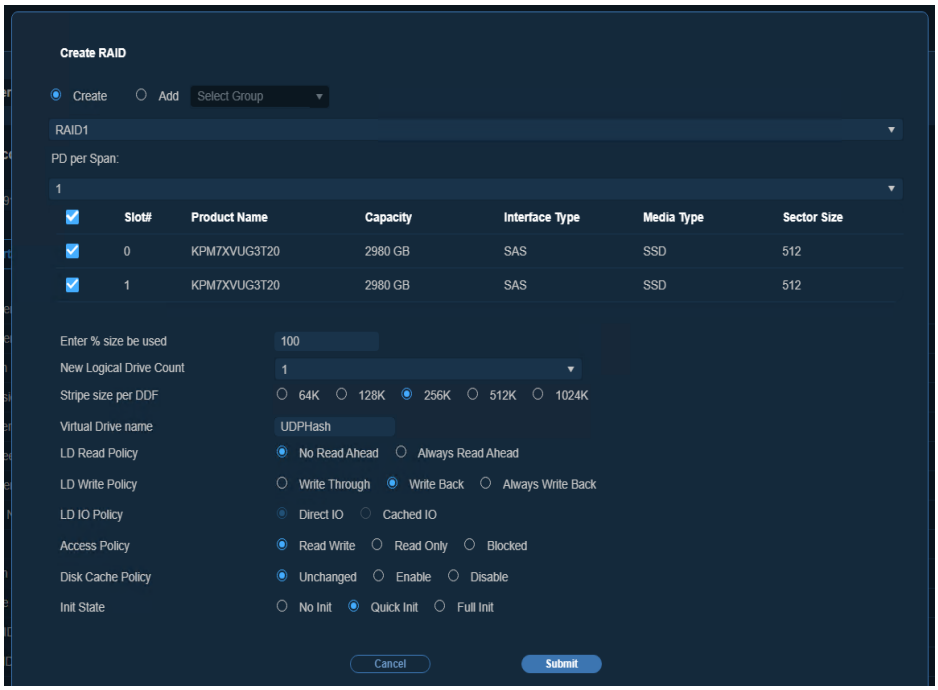


e. Wählen Sie auf der Seite "Create" alle SSD-Slots aus, und geben Sie dann Folgendes an:

- **RAID**: Wählen Sie in der Dropdown-Liste für die RAID-Ebene "RAID1" aus.
- **PD per Span**: 1
- **Enter % size be used**: Geben Sie den Wert **100** ein.

- **New Logical Drive Count**: Geben Sie den Wert **1** ein.
- **Stripe size per DDF**: Wählen Sie die Option **256K** aus.
- **Virtual Drive name**: Geben Sie den gewünschten Namen für das virtuelle Laufwerk ein.
- **LD Read Policy**: Wählen Sie die Option **No Read Ahead** aus.
- **LD Read Policy**: Wählen Sie die Option **Write Back** aus.
- **LD IO Policy**: Standardmäßig ist die Option **Direct IO** ausgewählt.
- **Access Policy**: Wählen Sie die Option **Read Write** aus.
- **Disk Cache Policy**: Wählen Sie die Option **Unchanged** aus.
- **Init-Status**: Wählen Sie die Option **Quick Init** aus.

f. Klicken Sie auf **Übergeben**.



g. Geben Sie im Suchfeld der Taskleiste **Computer Management** ein, und drücken Sie die Eingabetaste.

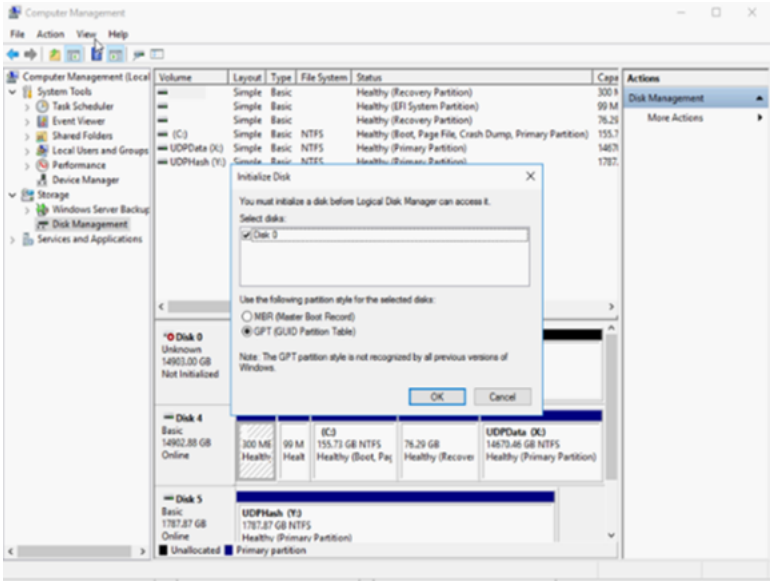
   Das Fenster für die Computerverwaltung wird geöffnet.

h. Navigiere Sie zu **Storage** > **Disk Management**.

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

   Das Fenster "Datenträger initialisieren" wird angezeigt.

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



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

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

Der virtuelle Datenträger wurde erfolgreich erstellt.

Arbeiten mit dem Arcserve Appliance Erweiterungs-Kit – Modelle der Serie X

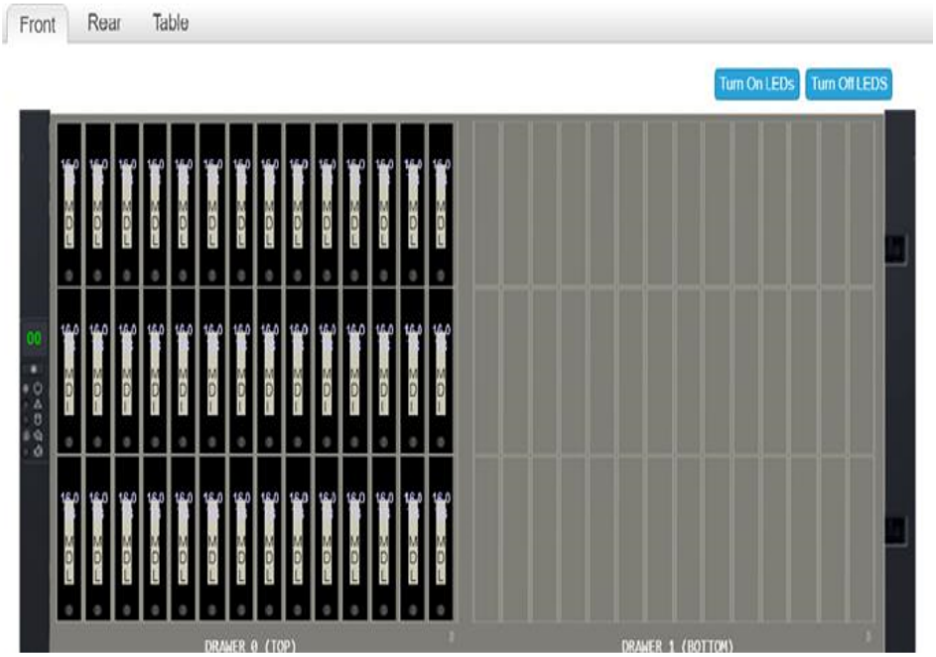
Mit dem ARCserve Erweiterungs-Kit können Sie die Kapazität der Modelle der Arcserve Appliance X-Serie erweitern.

Befolgen Sie diese Schritte:

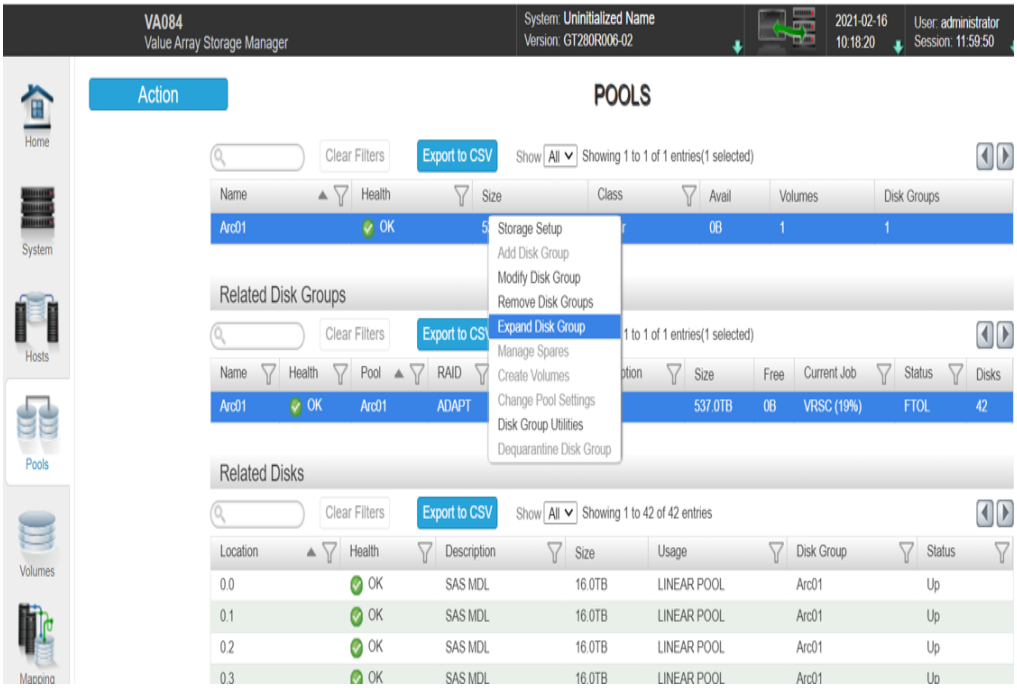
1. Für Erweiterungs-Kits der Serie X – [Kapazität eines beliebigen Modells (außer X3000DR)] können Sie eine lineare Erweiterung mit optionalen Erweiterungs-Kits so oft wie erforderlich durchführen, bis Sie das größte Modell X3000DR erreichen.
2. Gehen Sie folgendermaßen vor, um die Festplatten in die 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. Setzen Sie die Festplatten in die leeren Festplattensteckplätze der Speichereinheit ME4084 Value Array ein. Jedes Kit im Erweiterungs-Kit der Serie X besteht aus 14 x 16 TB-Festplatten.

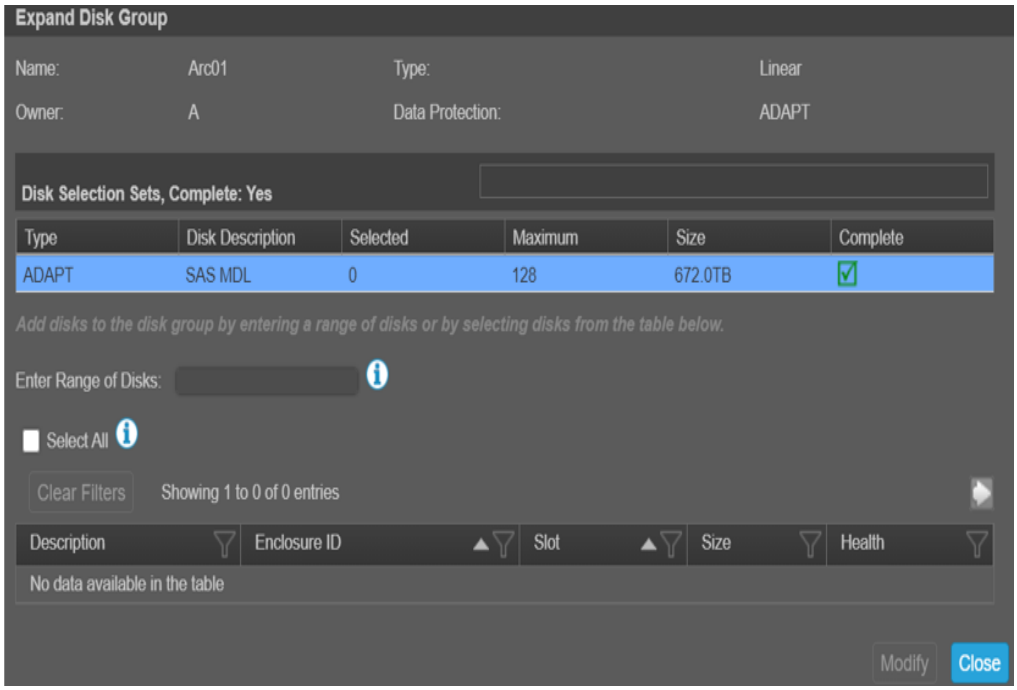


3. Melden Sie sich bei der ME-Einheit – Value Array Storage Manager an, gehen Sie zu "Pools", und wählen Sie dann die Datenträgergruppe aus, die Sie erweitern möchten.



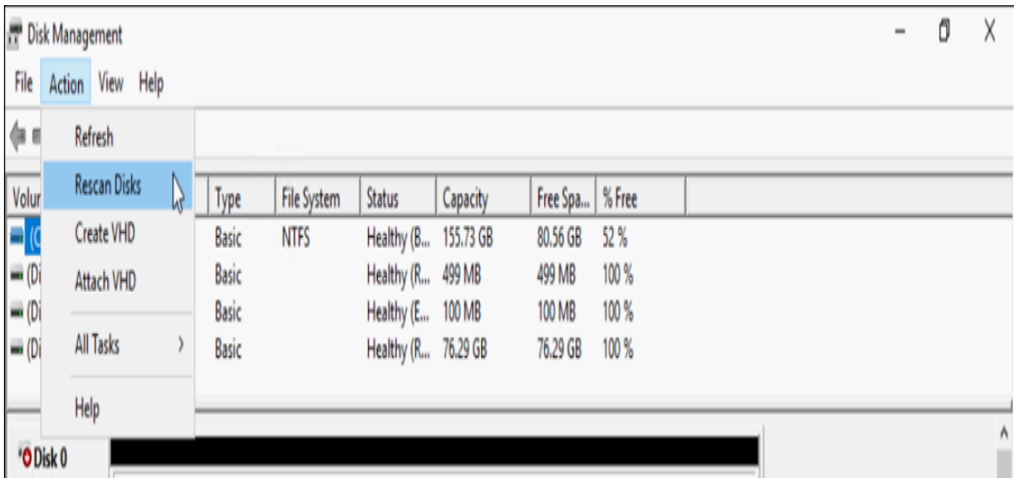
4. Klicken Sie mit der rechten Maustaste auf die ausgewählte Datenträgergruppe, und wählen Sie **Datenträgergruppe erweitern** aus.

   Der Bereich "Datenträgergruppe erweitern" wird geöffnet und zeigt die Datenträgergruppeninformationen und Datenträgertabellen an.

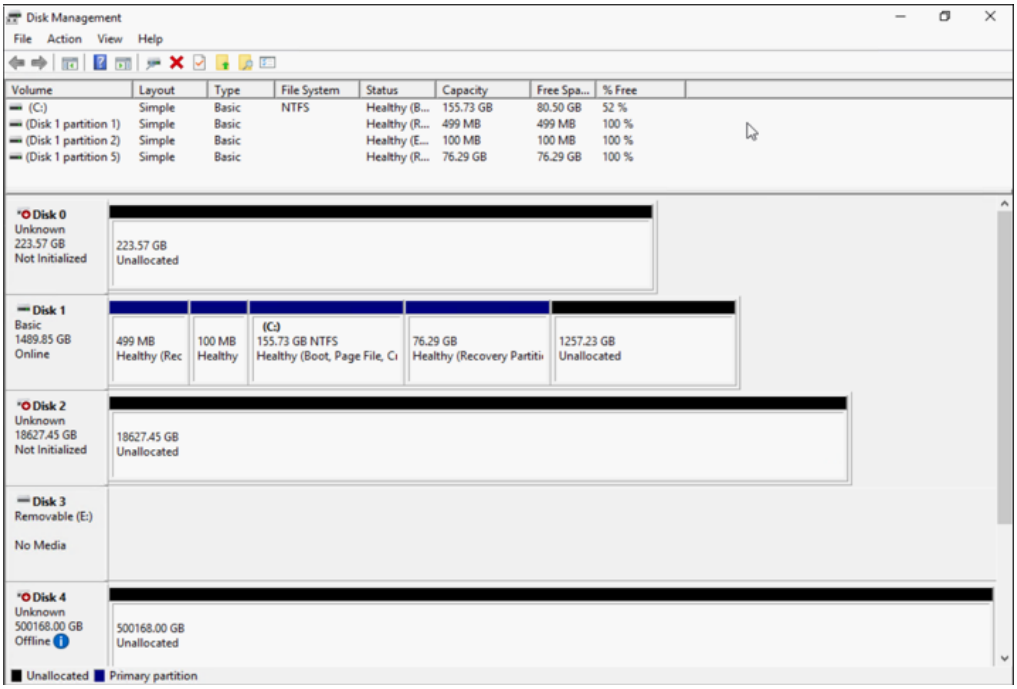


5. Um der Datenträgergruppe weitere Datenträger hinzuzufügen, geben Sie einen Datenträgerbereich in das Feld **Datenträgerbereich eingeben** ein, oder wählen Sie die Datenträger aus der Tabelle aus.
6. Klicken Sie auf **Ändern**.
7. Klicken Sie im Bestätigungsfenster auf **Ja**, um die Gruppenerweiterung zu starten, und klicken Sie dann auf **OK**, um das Fenster zu schließen.

   Hinweis: Nach Abschluss des Erweiterungsjobs wird ein Job zum Neuausgleich für die Datenträgergruppe ausgelöst.
8. Öffnen Sie nach Abschluss der Jobs für Erweiterung und Neuausgleich die **Datenträgerverwaltung** in der Recheneinheit, und wählen Sie dann **Aktion> Datenträger neu scannen** aus.



Nach dem erneuten Scan wird der Datenträger aus der Speichereinheit mit dem erweiterten Speicher angezeigt.



Arbeiten mit dem SSD Flash-Erweiterungs-Kit in der Arcserve Appliance X-Serie

Mit dem Arcserve SSD Flash Erweiterungs-Kit können Sie die Datenkapazität durch erweitern, indem Sie einen sekundären Datenspeicher erstellen und DR-bezogene Vorgänge (IVM/VSB/Continuous Availability) in den Arcserve Appliance-Modellen der X-Serie ausführen.

Befolgen Sie diese Schritte:

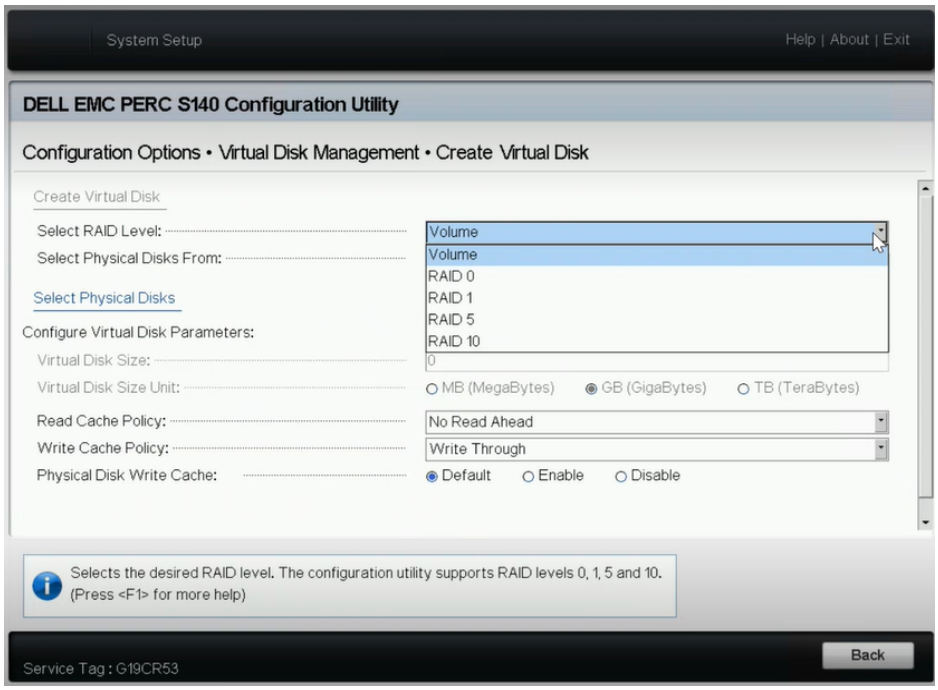
1. Gehen Sie folgendermaßen vor, um SSDs in die leeren Datenträgersteckplätze einzufügen:
   a. Überprüfen Sie in der Arcserve UDP-Konsole, dass keine Jobs auf dem Appliance-Server ausgeführt werden. Falls Jobs ausgeführt werden, unterbrechen Sie die entsprechenden Pläne.
   b. Setzen sie die SSDs in die leeren Datenträgersteckplätze ein.

2. Führen Sie die folgenden Schritte aus, um Raid-5 über die BIOS Boot Manager-Option zu konfigurieren:
   a. Um das Dashboard der virtuellen Konsole zu starten, melden Sie sich bei iDRAC an, und klicken Sie dann auf **Start the Virtual Console**.
   b. Klicken Sie in der virtuellen Konsole auf **Boot**, und wählen Sie dann die Option **BIOS Boot Manager** aus.

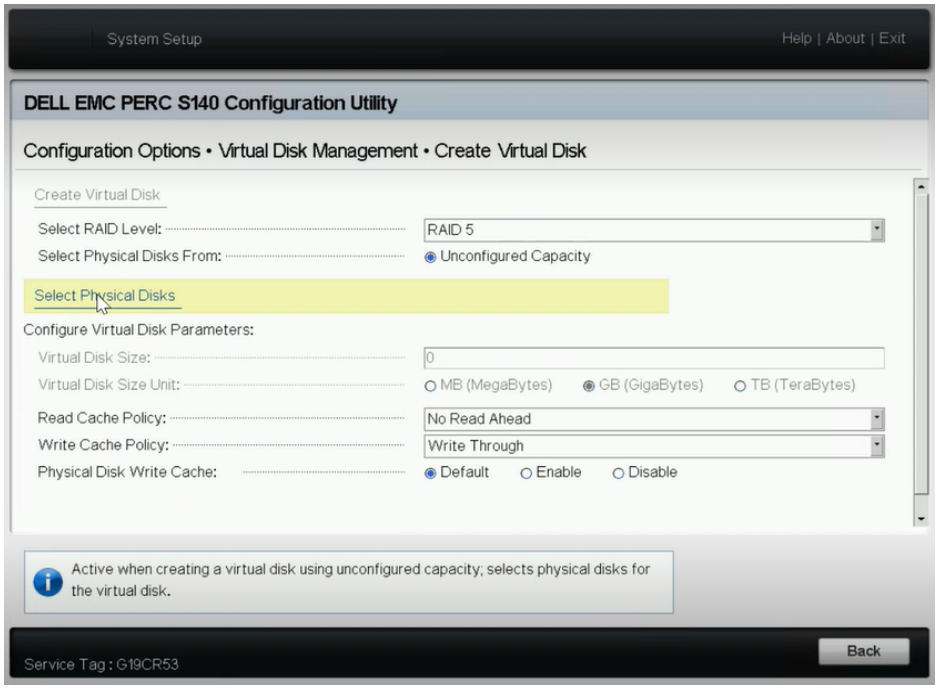
      Klicken Sie im Bestätigungsfenster auf **Yes**, um BIOS Boot Manager neu zu starten.
   c. Klicken Sie auf **Power**, und wählen Sie dann **Reset system (warm boot)**.

      Die Appliance startet, und die Setup-Seite von Boot Manager wird neu gestartet.
   d. Klicken Sie im Hauptmenü von Boot Manager auf **Launch System Setup**, und navigieren Sie dann zu **Device Settings** > **Dell EMC PERC S140 Controller** > **Virtual Disk Management** > **Create Virtual Disk**.
   e. Wählen Sie aus der Drop-down-Liste "Select RAID Leven" die Option **RAID 5**aus.

      Hinweis: Der virtuelle RAID 5-Datenträger wird für das Erweiterungskit verwendet und enthält neu angeschlossene Datenträger mit 3,63 TB für jeden physischen Datenträger.



f. Wählen Sie die Option **Select Physical Disks** aus.

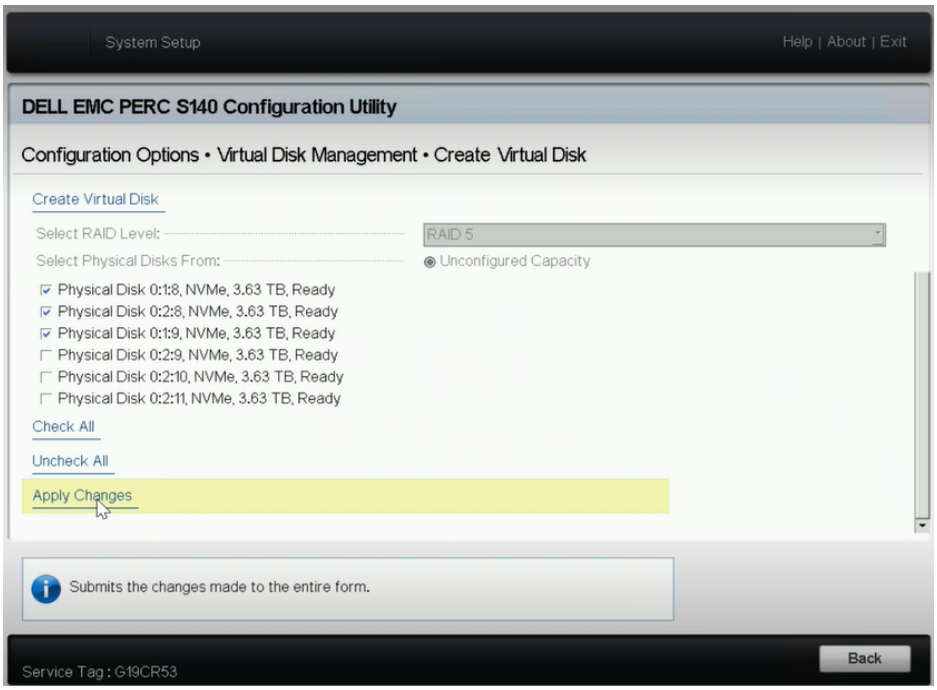


Das Fenster "Select Physical Disk Operation" wird geöffnet.

g. Klicken Sie für die Option "Select Interface Type" auf **NVMe**.

Eine Liste der physischen Datenträger wird angezeigt.

h. Wählen Sie aus der Liste der physischen Datenträger den gewünschten Datenträger aus, und klicken Sie dann auf **Apply Changes**.



Hinweise: Wählen Sie mindestens drei und maximal 16 Datenträger aus.

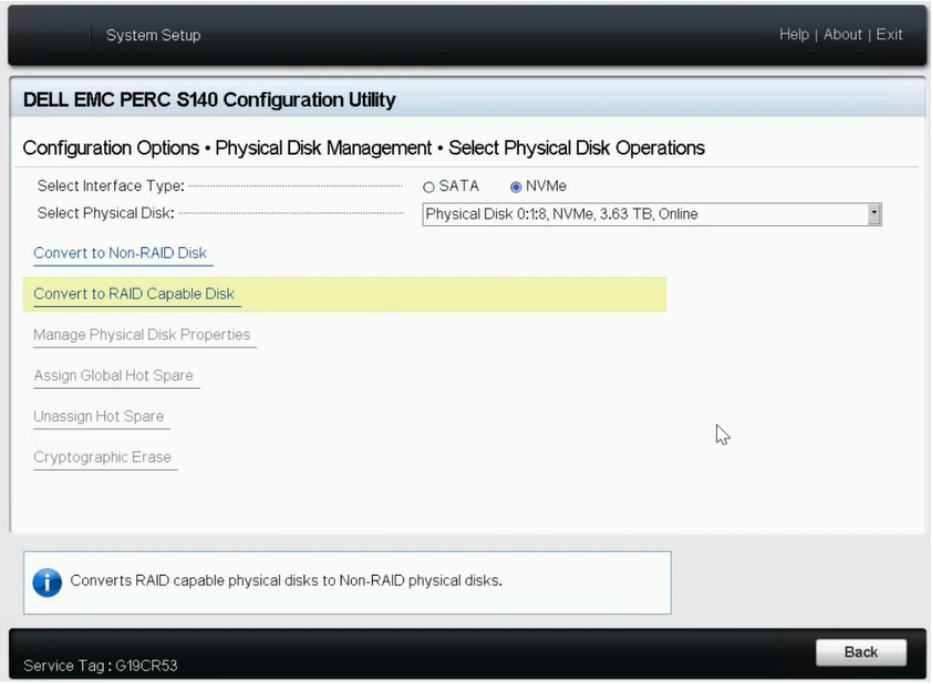
i. Nachdem die Änderungen angewendet wurden, klicken Sie erneut auf die Option **Create Virtual Disk**, um die Erstellung des virtuellen Datenträgers abzuschließen.

3. Navigieren Sie zu **Configuration Options** > **Physical Disk Management** > **Select Physical Disk Operations**.

   a. Wählen Sie unter "Select Interface Type" den Typ **NVMe** aus.

   b. Wählen Sie in der Drop-down-Liste "Select Physical Disk" die gewünschte Option aus, und klicken Sie dann auf **Convert to RAID Capable Disk**.

   Hinweis: Sie können die Option "Convert to RAID Capable Disk" nacheinander auf alle physischen Datenträger anwenden.

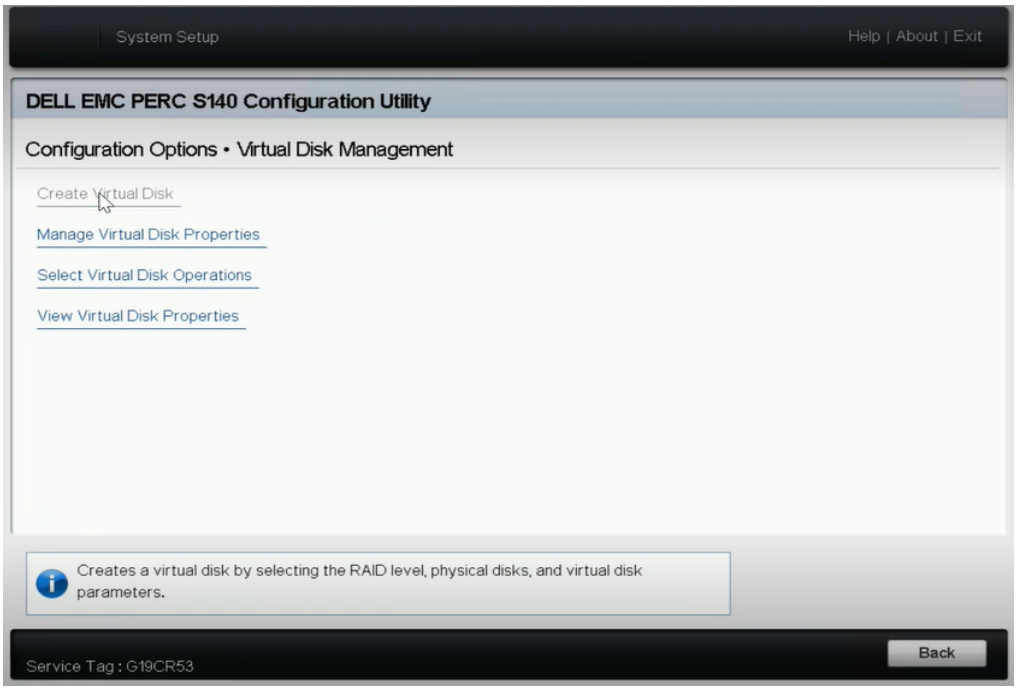


c. Wenn die folgende Warnmeldung angezeigt wird, gehen Sie folgendermaßen vor:

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

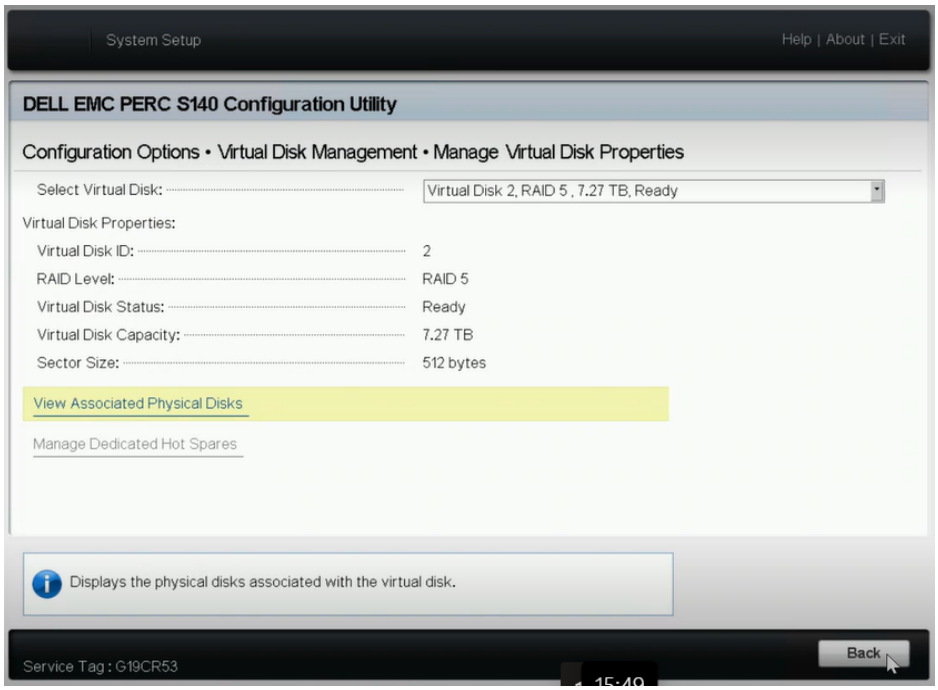
   1. Stellen Sie sicher, dass keine durch das Betriebssystem konfigurierten RAID-Arrays vorhanden sind, und klicken Sie dann auf "OK".
   2. Klicken Sie auf "OK".

4. Navigieren Sie zu **Configuration Options** > **Virtual Disk Management**, und gehen Sie dann wie folgt vor:

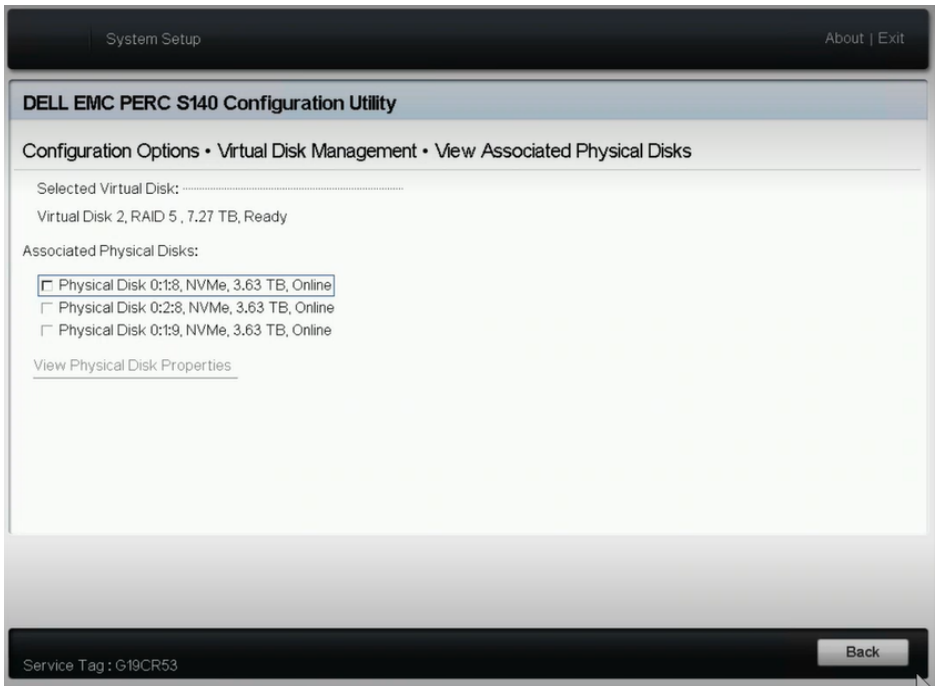


a. Um Ihre virtuellen Datenträger zu verwalten, klicken Sie auf **Manage Virtual Disk Properties**.

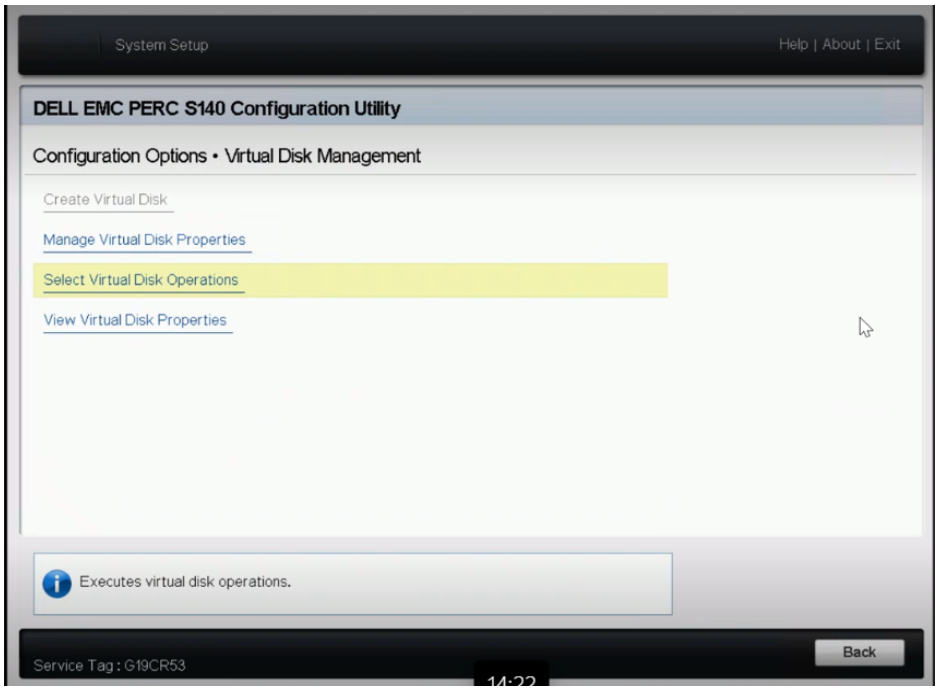
   Wählen Sie in der Drop-down-Liste "Select Virtual Disks" einen beliebigen RAID-5-Datenträger aus, und klicken Sie auf **View Associated Physical Disks**.



   Die zugeordneten Datenträger werden angezeigt.

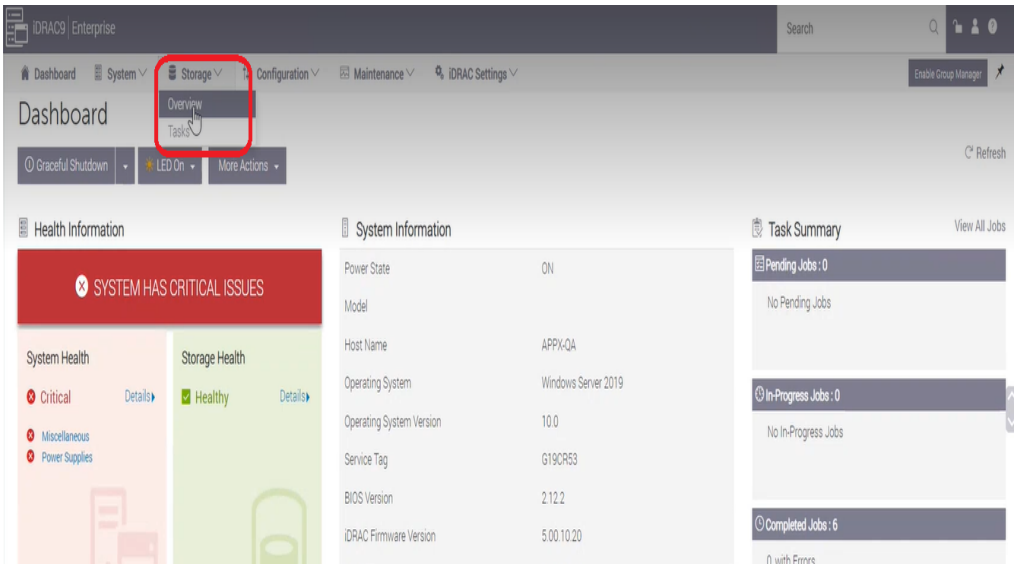


b. Um die Vorgänge für virtuelle Datenträger auszuwählen, klicken Sie auf **Select Virtual Disk Operations**.

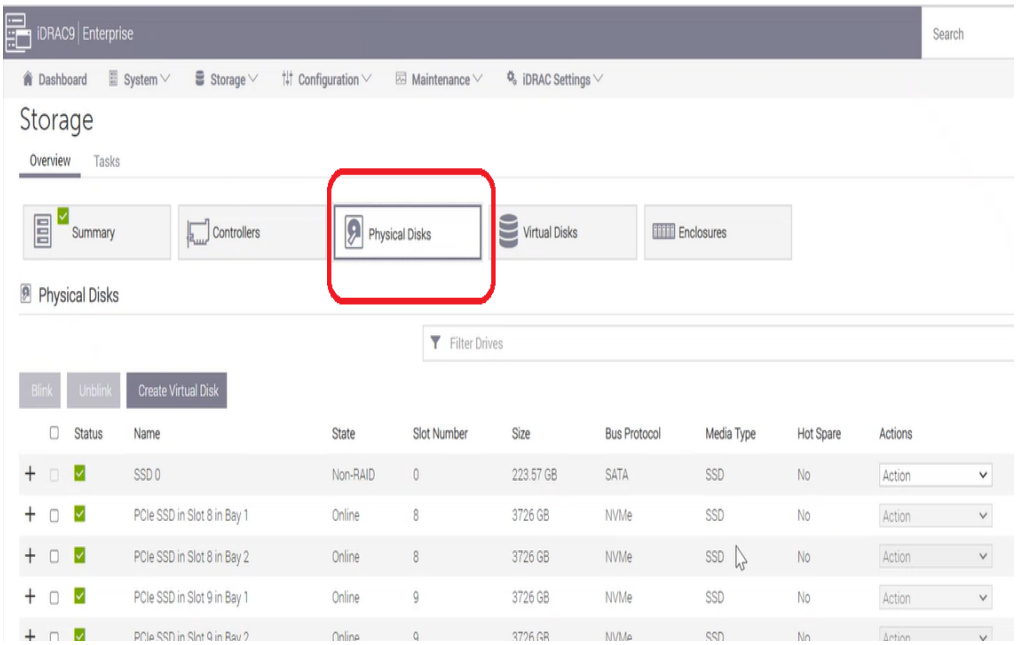


c. Um die Eigenschaften des virtuellen Datenträgers im Start-Manager anzuzeigen, klicken Sie auf **View Virtual Disk Properties**.

5. Um die Datenträgerinformationen in iDRAC anzuzeigen, melden Sie sich bei iDRAC an, und klicken Sie auf **Speicher** > **Übersicht**.



Klicken Sie im Abschnitt "Übersicht" auf **Physische Datenträger**, um die Liste der von Ihnen erstellten physischen Datenträger anzuzeigen.

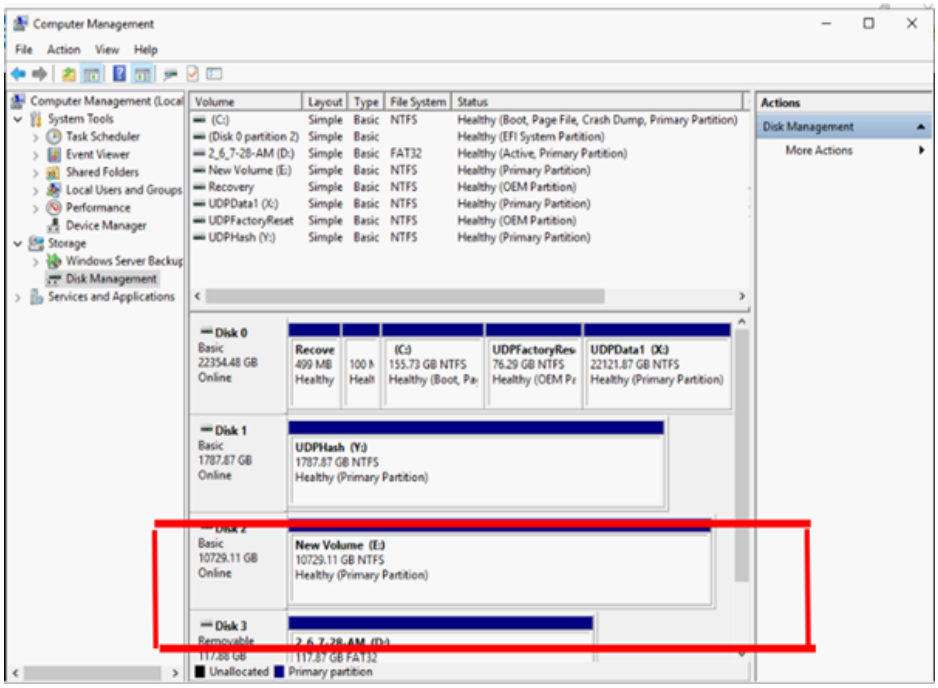


6. Gehen Sie wie folgt vor, um den neu hinzugefügten virtuellen Datenträger zu initialisieren und zu formatieren:
   a. Navigieren Sie zu **Computerverwaltung und Datenträgerverwaltung**.
   b. Doppelklicken Sie auf den neuen virtuellen Datenträger, den Sie hinzugefügt haben.

      Das Fenster "Datenträger initialisieren" wird angezeigt.
   c. Wählen Sie die **GPT-Datenträger (GUID-Partitionstabelle)** aus, und klicken Sie auf **OK**.

d. 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



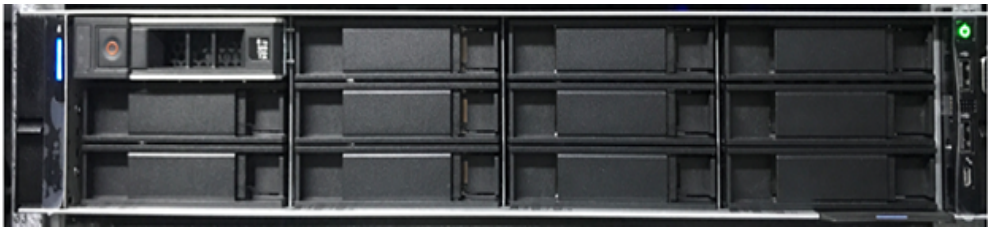
Der virtuelle Datenträger wird erstellt.

Arbeiten mit dem Erweiterungs-Kit für Arcserve Appliance 9072-9504DR-Modelle

Mit dem Arcserve Erweiterungs-Kit können Sie die Kapazität der Arcserve Appliance 9072-9504DR-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.

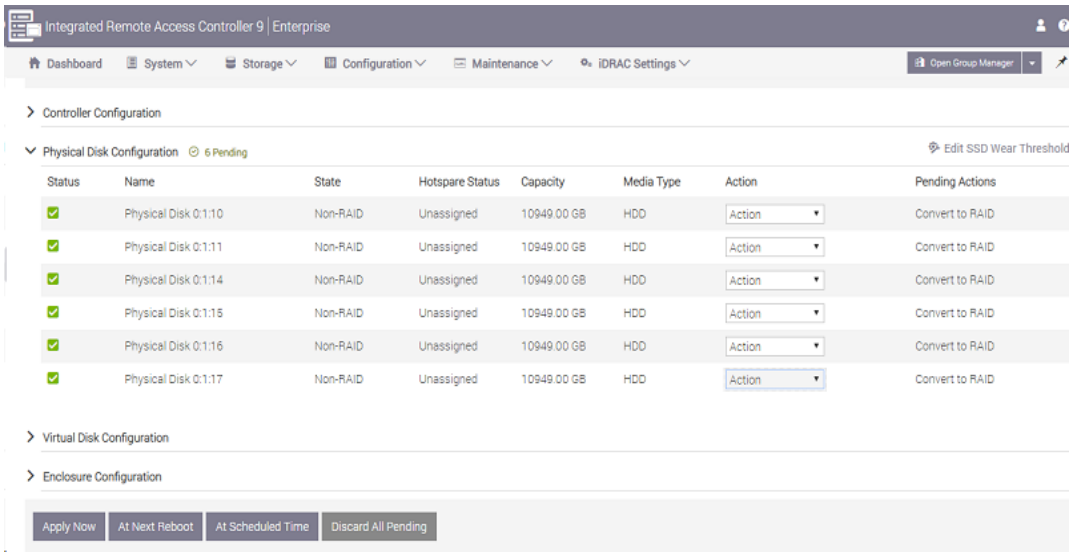
   Ein Dialogfeld wird mit der folgenden Fehlermeldung angezeigt:

   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 zum Konvertieren in RAID abgeschlossen ist, ändert sich der Status in **Abgeschlossen (100 %)**.

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

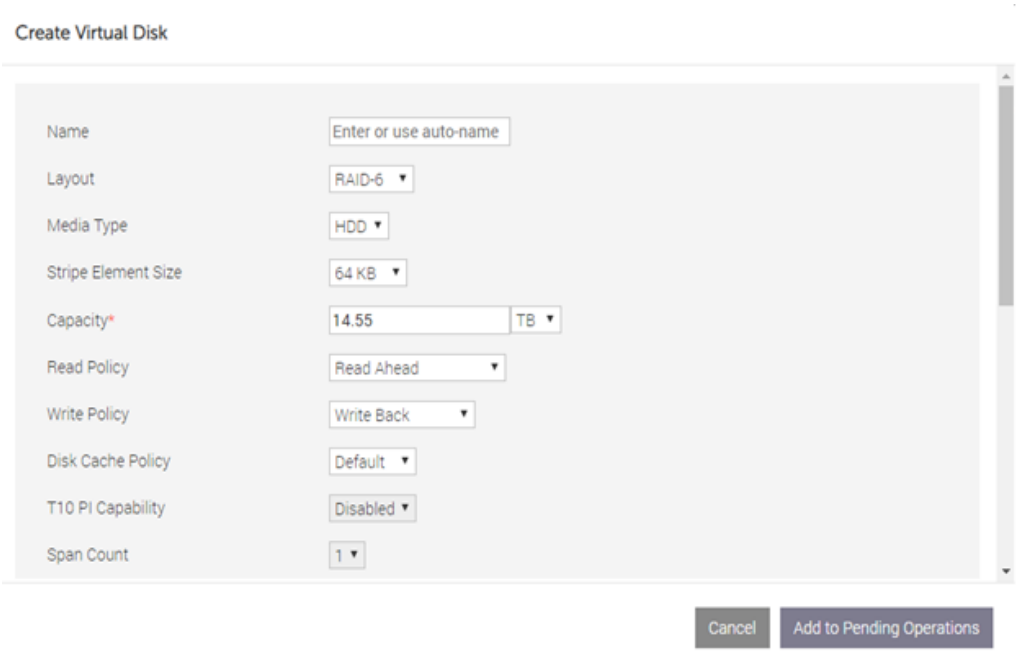
a. Navigieren Sie zu "Konfiguration, "Speicherkonfiguration“ und "Virtuelle Datenträgerkonfiguration".

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 ausstehenden 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 zum Erstellen des virtuellen Datenträgers abgeschlossen ist, ändert sich der Status in **Abgeschlossen (100 %)**.

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

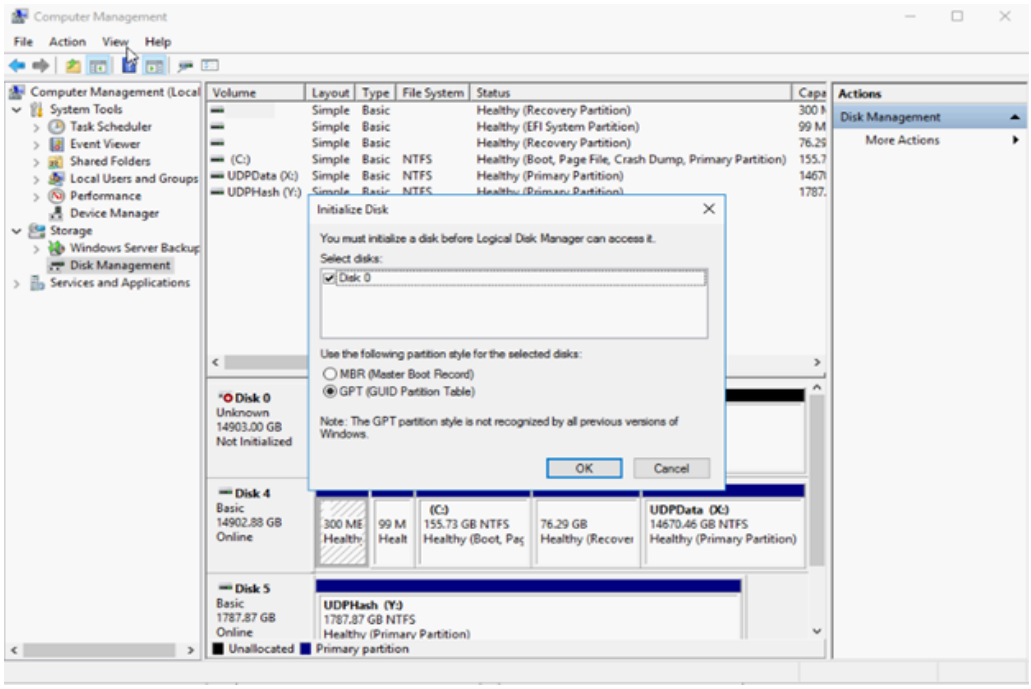
j. Doppelklicken Sie auf den neuen virtuellen Datenträger, den Sie hinzugefügt haben.

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.

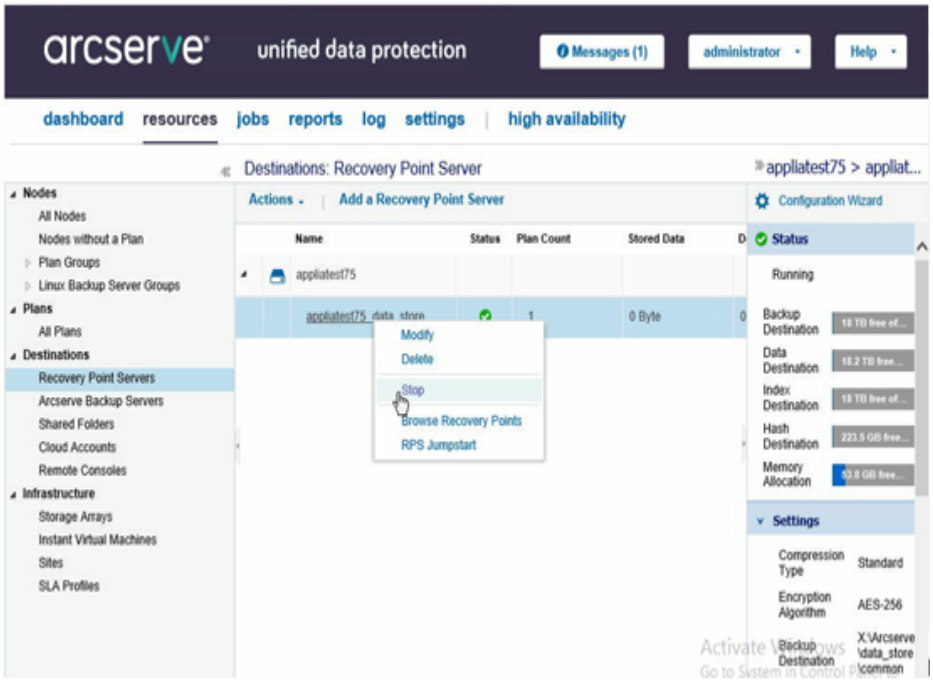
c. Klicken Sie auf **UDP-Konsole starten**.

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 <neuer 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.

Arbeiten mit dem SSD Flash Erweiterungs-Kit in Arcserve Appliance 9072-9504 DR-Modellen

Mit dem Arcserve SSD Flash Erweiterungs-Kit können Sie einen sekundären Datenspeicher erstellen und DR-bezogene Vorgänge (IVM/VSB/Continuous Availability) in den Arcserve Appliance 9072-9504DR-Modellen ausführen.

Befolgen Sie diese Schritte:

1. Gehen Sie folgendermaßen vor, um SSDs in die leeren Datenträgersteckplätze einzufügen:

   a. Überprüfen Sie in der Arcserve UDP-Konsole, dass keine Jobs auf dem Appliance-Server ausgeführt werden. Falls Jobs ausgeführt werden, unterbrechen Sie die entsprechenden Pläne.

b. Setzen sie die SSDs in die leeren Datenträgersteckplätze ein.

2. Gehen Sie folgendermaßen vor, um Raid-5 in iDRAC zu konfigurieren:

   a. Melden Sie sich in iDRAC an und navigieren Sie zu **Konfiguration, Speicherkonfiguration > Physische Datenträgerkonfiguration**.

   b. Wählen Sie im Abschnitt "Physische Datenträgerkonfiguration" in der Drop-down-Liste **Aktionen** für jede neue SSD DISK die Option **In RAID konvertieren** aus.

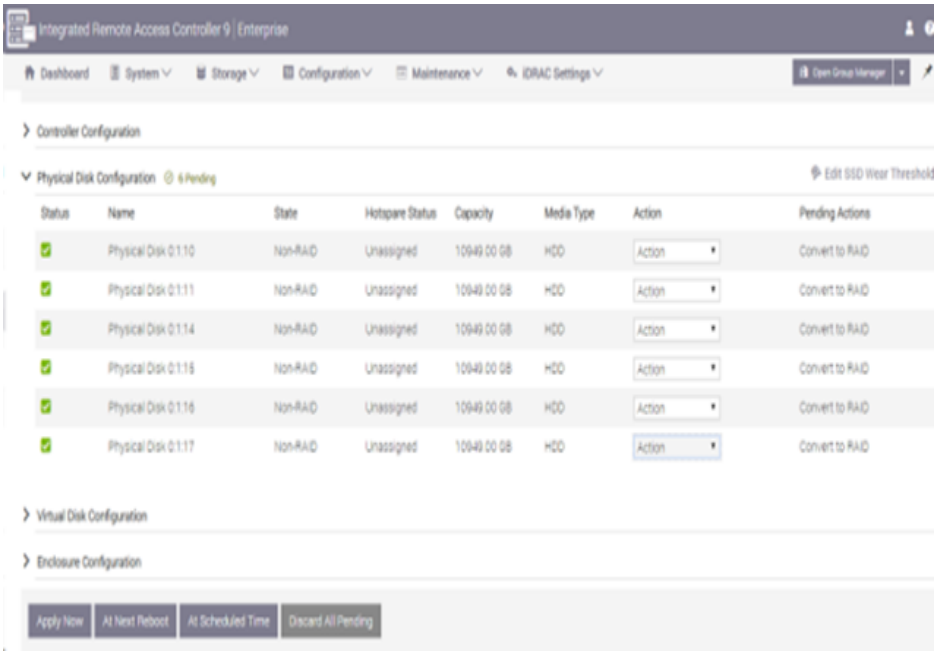
      Ein Dialogfeld wird mit der folgenden Fehlermeldung angezeigt:

      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**.

      Da der Datenträgertyp SSD ist, wird der Status "In Raid konvertieren" in der Spalte "Ausstehende Aktionen" 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

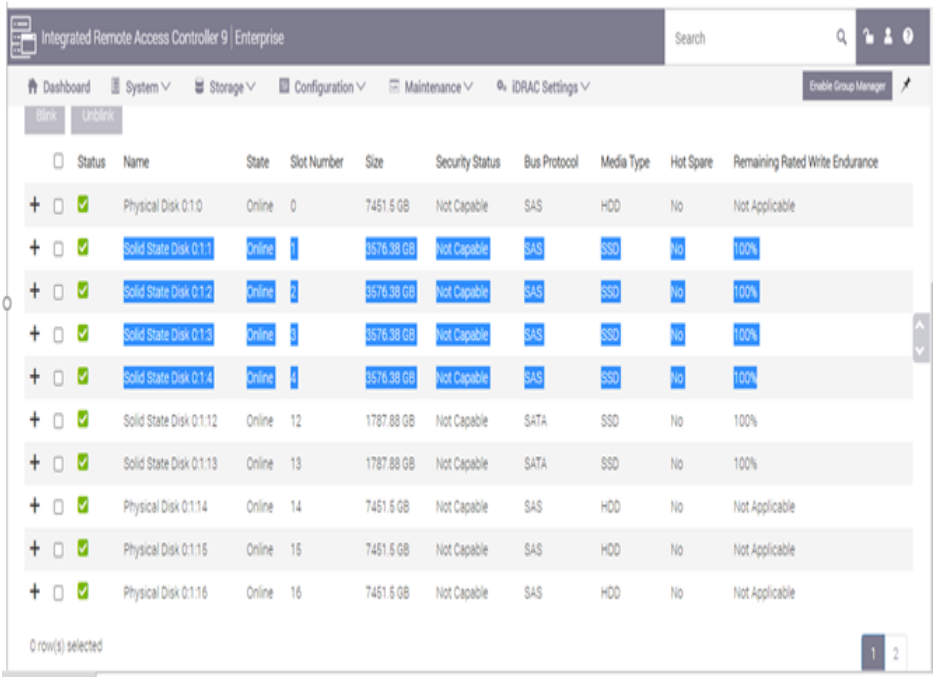
Die Aktion zur Konvertierung in Raid wird zum geplanten Zeitpunkt gestartet.

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 die Job zur Konvertierung in RAID abgeschlossen ist, wird der Status als 100 % angezeigt.



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

a. Navigieren Sie zu **Konfiguration > Speicherkonfiguration > Virtuelle Datenträgerkonfiguration**.

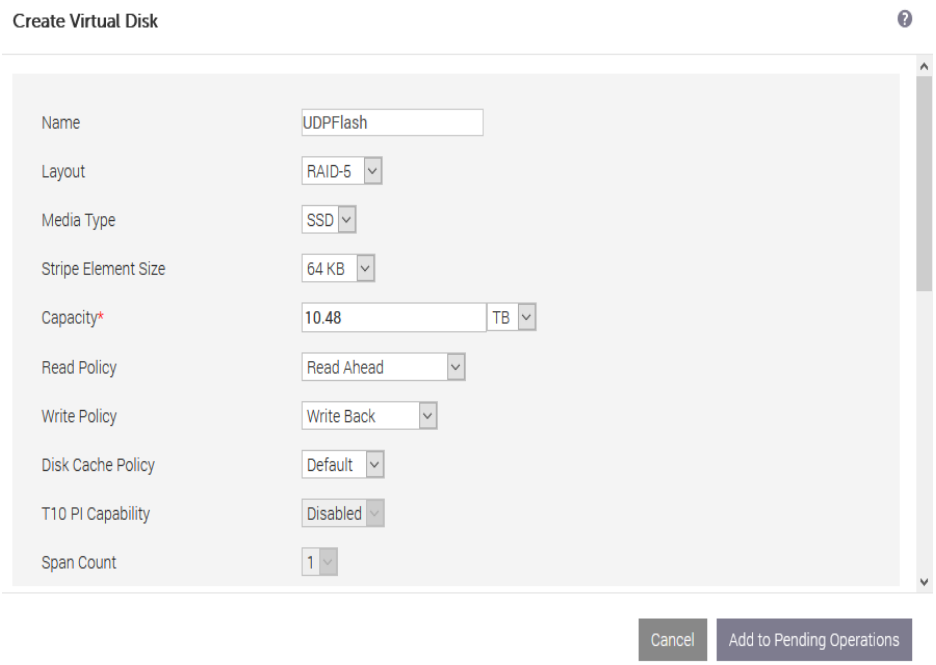
b. Klicken Sie unter Virtuelle Datenträgerkonfiguration auf **Virtuellen Datenträger erstellen**.

c. Gehen Sie im Fenster "Virtuellen Datenträger erstellen" wie folgt vor, und behalten Sie die restlichen Standardeinstellungen bei:

   - **Layout:** Wählen Sie in der Drop-down-Liste "RAID-5" aus.
   - **Datenträgertyp:** Wählen Sie in der Drop-down-Liste SSD aus.

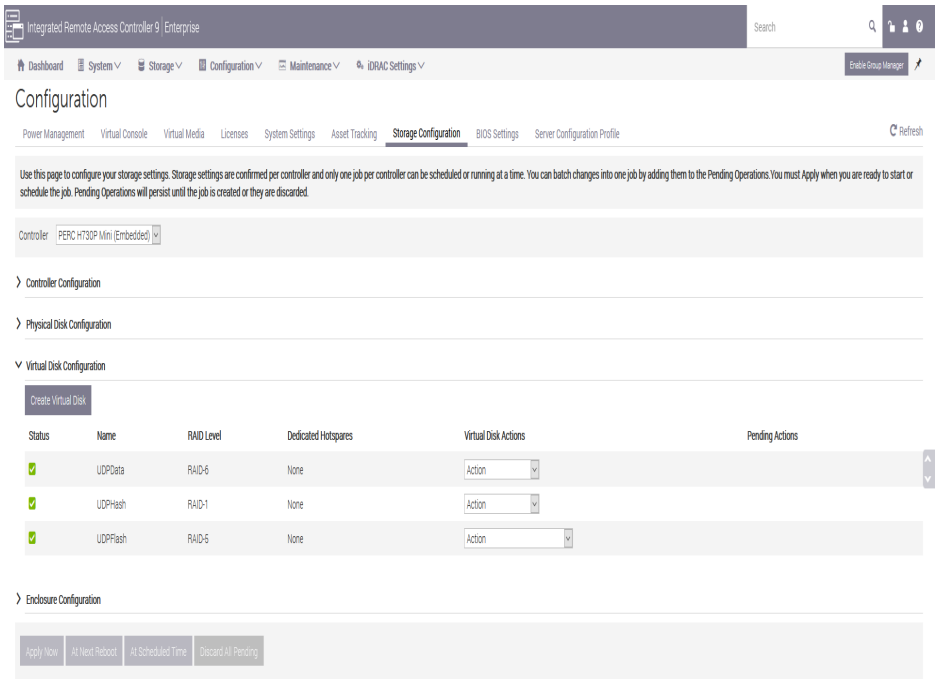
d. Blättern Sie im Abschnitt "Physischen Datenträger auswählen" nach unten, und wählen Sie alle SSD-Datenträger aus, die in RAID konvertiert werden.

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



f. Navigieren Sie zu **Konfiguration > Speicherkonfiguration**.

g. Um den Vorgang zum Erstellen eines virtuellen Datenträgers sofort durchzuführen, klicken Sie auf **Jetzt anwenden**.



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

   Die Liste der laufenden Jobs zum Erstellen eines virtuellen Datenträgers wird angezeigt. Wenn der Job zum Erstellen des virtuellen Datenträgers abgeschlossen ist, ändern sich der Status in **100 %**.

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

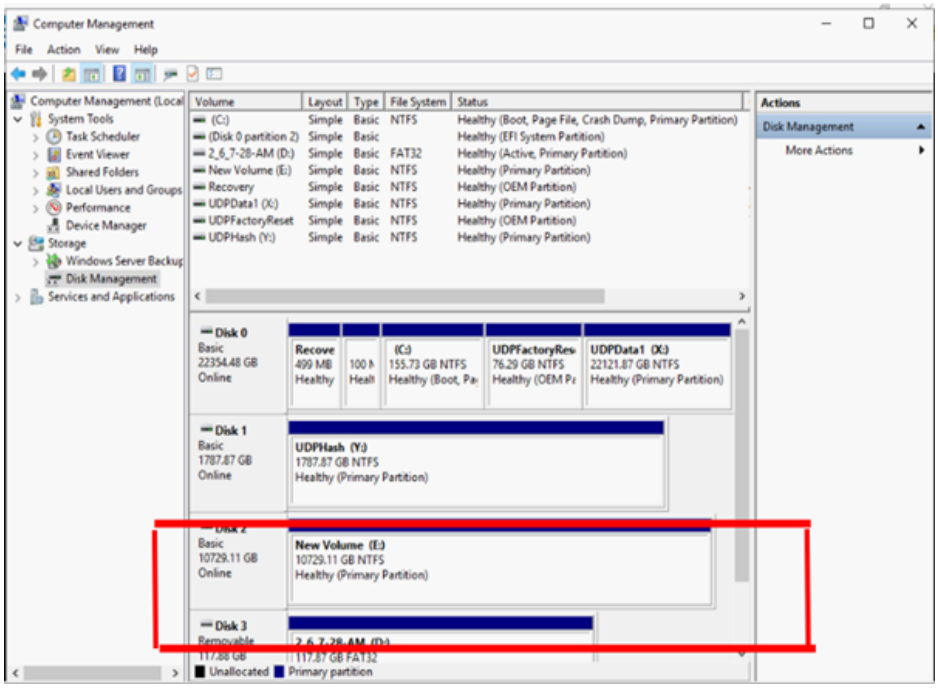
j. Doppelklicken Sie auf den neuen virtuellen Datenträger, den Sie hinzugefügt haben.

   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



Der virtuelle Datenträger wird erstellt.

Kapitel 10: Arbeiten mit Netzwerkkonfiguration

Dieser Abschnitt enthält folgende Themen:

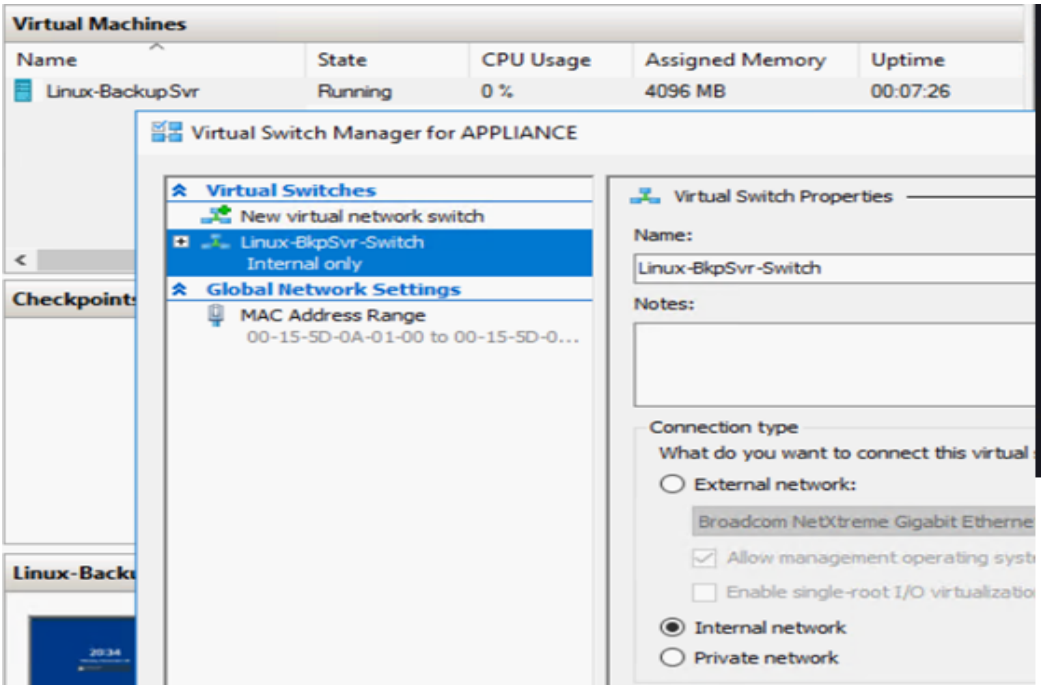
Funktionsweise der Netzwerkkonfigurationsdetails

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:

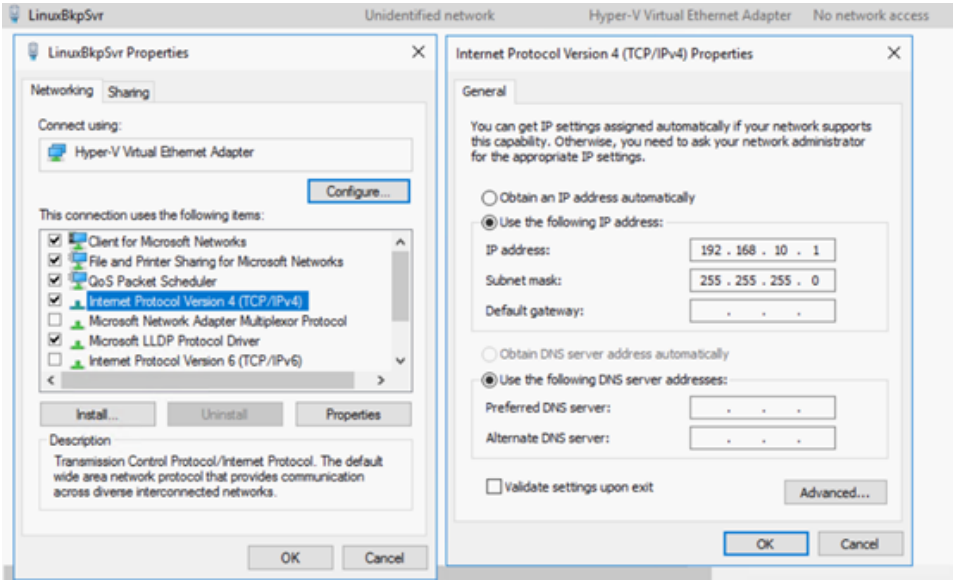
- Der Benutzer muss den Hostnamen des integrierten Linux nicht ändern.
- Der Benutzer speichert eine IP-Adresse für den Linux-Sicherungsserver im Netzwerk.
- Der Linux-Sicherungsserver kann eine Verbindung zu jedem beliebigen Rechner im öffentlichen Netzwerk herstellen.
- Jeder Rechner im öffentlichen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

Netzwerkkonfigurationsdetails:

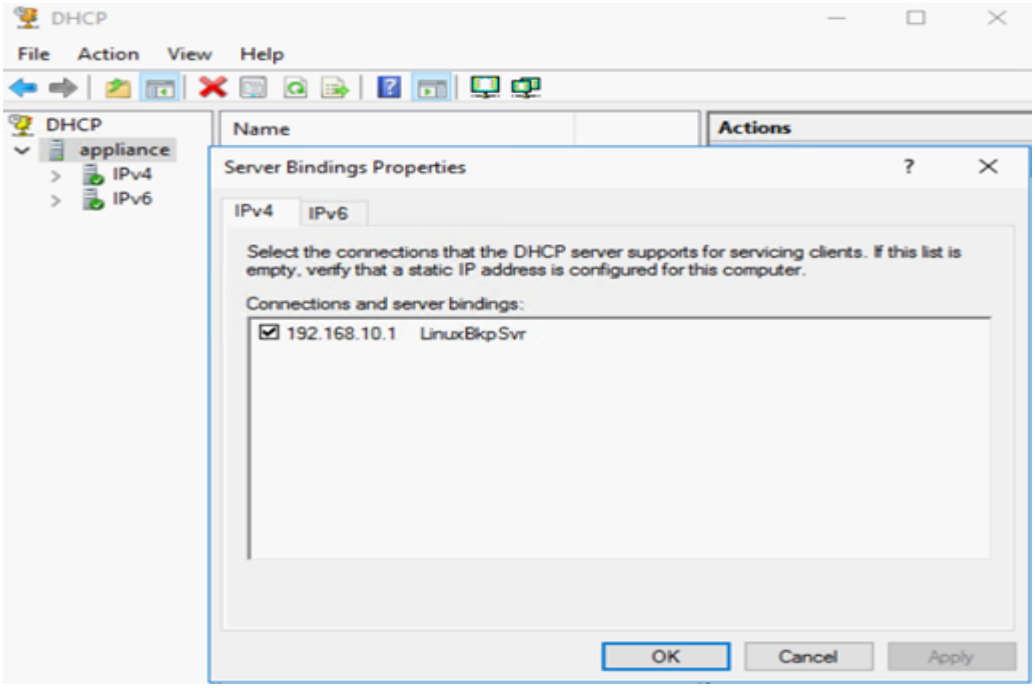
- Auf dem Hyper-V-Manager gibt es einen rein internen virtuellen Switch (*Linux-BkpSvr-Switch*), der nur von Linux-BackupSvr verwendet wird.



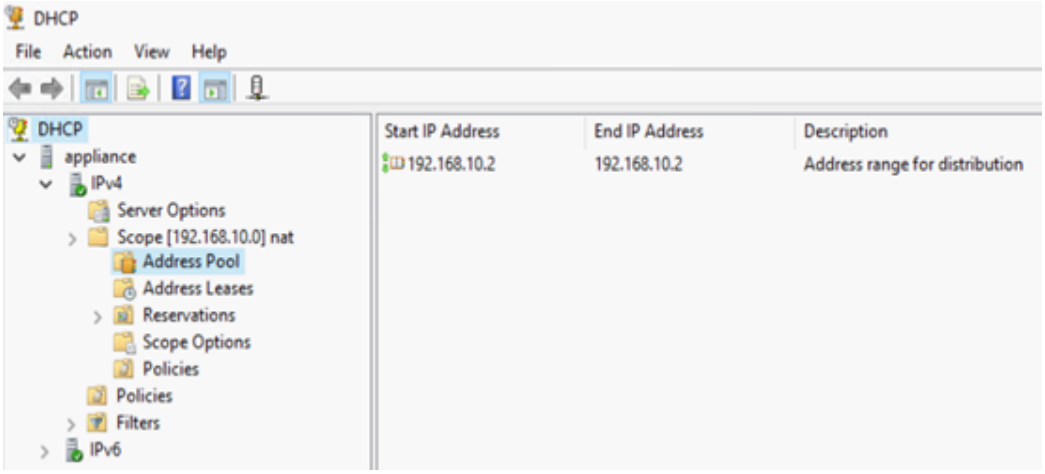
- Unter *Systemsteuerung\Netzwerk und Internet\Netzwerkverbindungen* wird ein "Hyper-V-Adapter für virtuelles Ethernet" namens "LinuxBkpSvr" angezeigt. Die IPv4-Adresse für diesen Switch wurde standardmäßig auf "192.168.10.1" festgelegt, wie unten gezeigt.



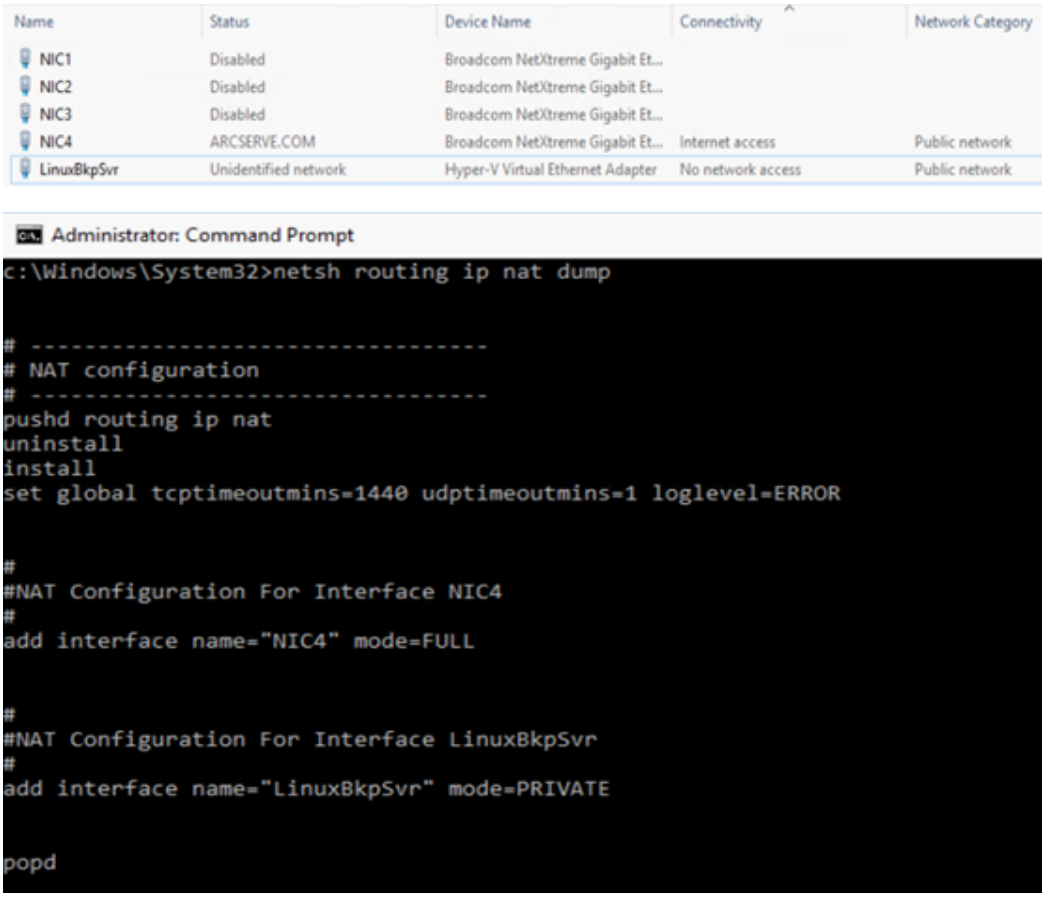
- Sie haben in der Standardeinstellung DHCP-Server auf dem Appliance-Rechner konfiguriert. Der DHCP-Server funktioniert nur auf dem virtuellen Hyper-V-Adapter.



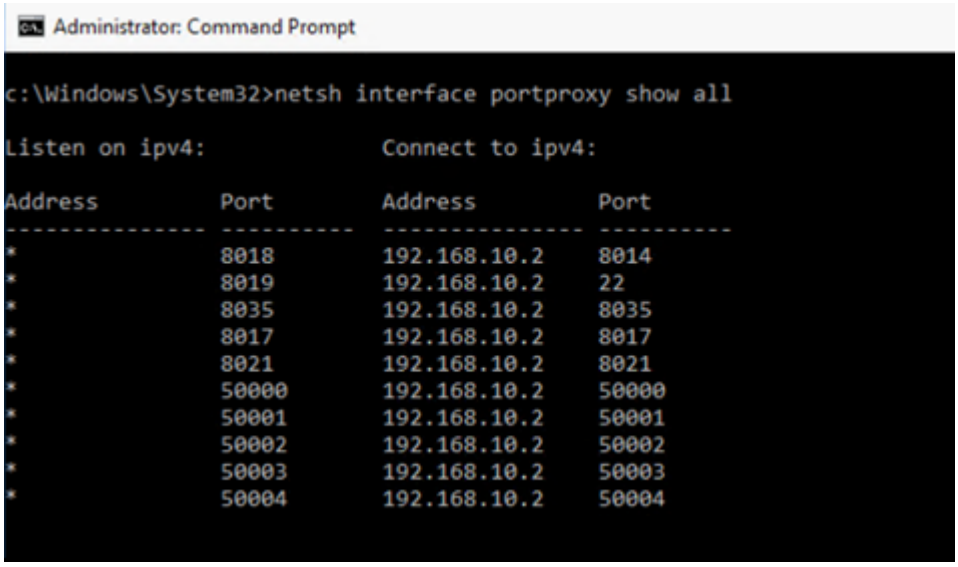
- Standardmäßig stellt nur eine 192.168.10.2 im Adresspool sicher, dass der integrierte Linux-Sicherungsserver die IP 192.168.10.2 erhält.



- 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
```

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

Hinweis: Diese Methode ist anwendbar auf eine Arcserve Appliance der 9000-Serie und höher.

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 des vorinstallierten Linux-Sicherungsservers finden Sie weitere Informationen darüber, 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.

   Hinweise:

   - 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\User_Utilities\UpdateIcsHostAdapter.ps1* aus, um die IP-Adresse für die Netzwerkschnittstelle "LinuxBkpSvr" und den vorinstallierten Linux-Sicherungsserver zurückzusetzen.

   Hinweise:

   - Der vorinstallierte Linux-Sicherungsserver wird während des Vorgangs heruntergefahren und neu gestartet, wenn Sie die Einstellung für *Linux_IPAddress* ändern.
   - Um das Internet des Produktions-NIC-Adapters für den LinuxBkpSvr-Adapter freizugeben, führen Sie die Datei *UpdateIcsHostAdapter.ps1* aus. Wenn Sie möchten, dass das Internet eines bestimmten NIC-Adapters für den LinuxBkpSvr-Adapter freigegeben wird, verwenden Sie die folgende Registrierungsoptimierung.

     Erstellen Sie den folgenden Registrierungsschlüssel, um den Namen des Netzwerkadapters anzugeben, über den ein Internet freigegeben werden muss.

     Pfad: *"HKLM:\SOFTWARE\Arcserve\Unified Data Protection\Appliance"*

     Werttyp: *"String"*

     Wertname: *"IcsHostAdapter"*

     Wertdaten: *"<Adapter Name>"*

6. Nachdem die obige Registrierung geändert wurde, führen Sie den folgenden Befehl aus:

C:\Programme\Arcserve\Unified Data Protection\Engine\BIN\Appliance\User_Utilities >powershell .\ UpdateIcsHostAdapter.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.

Überprüfen des Netzwerkstatus auf der Appliance

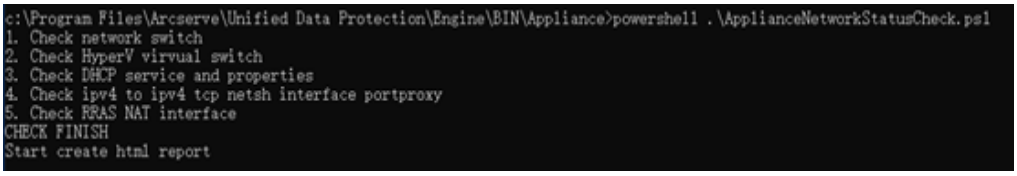
Das Tool ApplianceNetworkStatusCheck.ps1 wird verwendet, um Informationen über den aktuellen allgemeinen Netzwerkstatus des Arcserve Appliance-Servers zu sammeln und einen Bericht im XML-Format zu generieren. Der Bericht enthält Informationen über den Netzwerkadapter, den Netzwerk-Switch, den virtuellen 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 folgendermaßen vor, um den Netzwerkstatusbericht für den Appliance-Server mit diesem Tool zu generieren:

1. Melden Sie sich als Administrator beim Arcserve Appliance-Server 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 Bericht mit dem Netzwerkstatus 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.

  A급기기(업무용방송통신기자재)

  이기기는업무용(A급)으로전자파적합기기로서판매자또는사용자는이점을주의하시기바라며,가정외의지역에서사용하는것을목적으로합니다

  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.

Aktualisieren der Firmware für Arcserve Appliance 10000 Series

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

Anzeigen der Firmwareversion

Dieser Abschnitt enthält Informationen zum Anzeigen der aktuellen Firmware-Version.

Befolgen Sie diese Schritte:

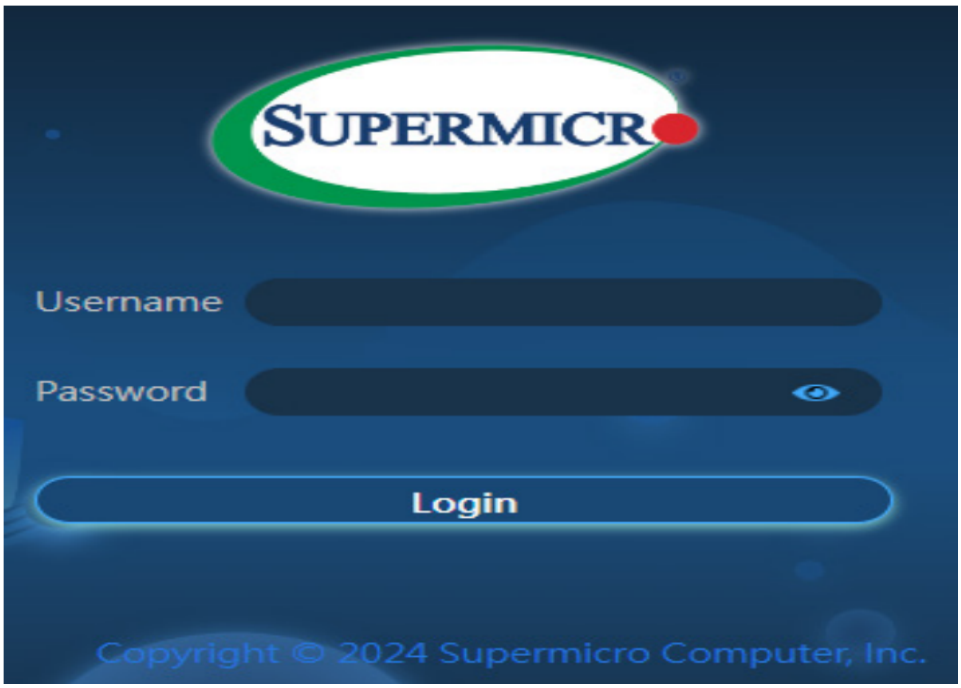
1. Öffnen Sie einen Webbrowser, und geben Sie die statische IP für IPMI (Intelligent Platform Management Interface) ein.

   Der Anmeldebildschirm wird geöffnet.

2. Geben Sie die Anmeldeinformationen wie folgt ein:
   - **Benutzername:** ADMIN.

     Hinweis: Der Benutzername muss in Großbuchstaben geschrieben werden.
   - **Kennwort:** Geben Sie das BMC-Kennwort ein**.**

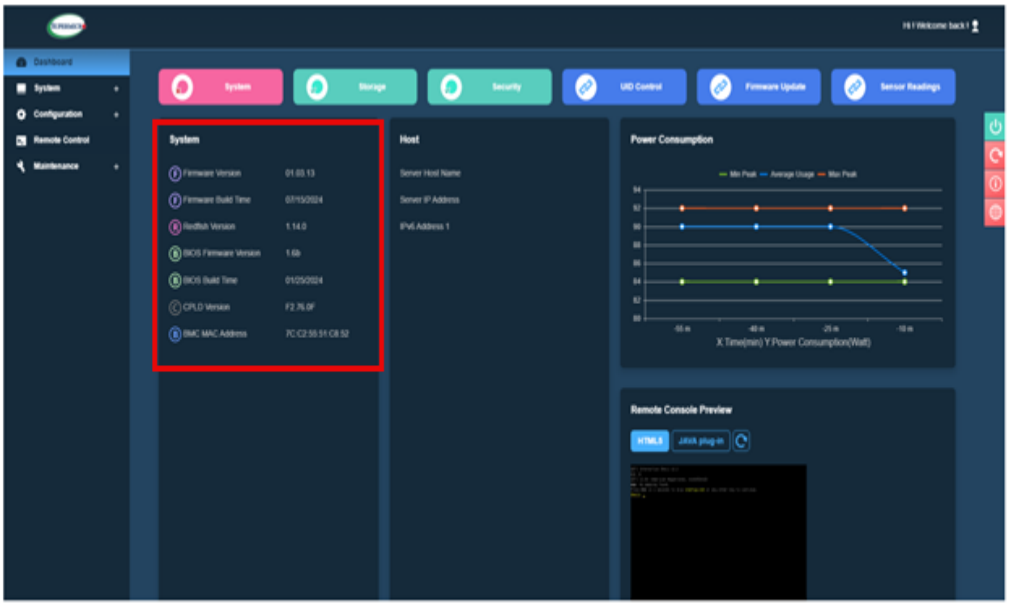
3. Klicken Sie auf **"Login".**



Die Benutzeroberfläche des IPMI-Webservers wird angezeigt.

Hinweis: Das eindeutige BMC-/IPMI-Kennwort finden Sie im herausziehbaren Tag auf der Vorderseite des Servers. Das BMC-Kennwort wird in der unteren Zeile direkt unter der BMC-/IPMI-MAC-Adresse aufgeführt.

Der Dashboard-Bildschirm zeigt die Firmware-Version unter "System" an.



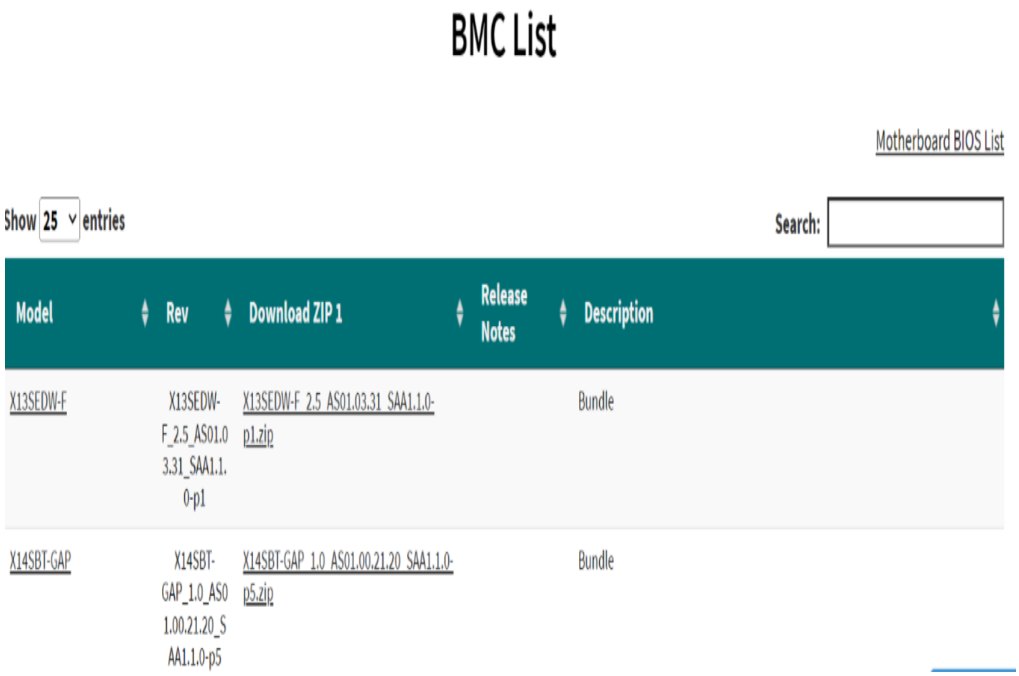
Herunterladen des Firmware-Upgradepakets

Dieser Abschnitt enthält Informationen zum Herunterladen der aktuellen Firmware-Version.

Befolgen Sie diese Schritte:

Hinweis: Sie können das neueste Firmware-Updatepaket von der Supermicro-Website herunterladen oder sich an den Support von Supermicro wenden.

1. Rufen Sie die Supermicro-Website auf.
2. Suchen Sie in der BMC-Liste nach dem Hauptplatinenmodell von Server 1U (X13SEW-F) oder 2U (X13DEI-T), um das Firmware-Update herunterzuladen.


BMC List

Motherboard BIOS List

Show 25 entries Search:

Model	Rev	Download ZIP 1	Release Notes	Description
X13SEDW-F	X13SEDW-F_2.5_AS01.03.31_SAA1.1.0-p1	X13SEDW-F_2.5_AS01.03.31_SAA1.1.0-p1.zip		Bundle
X14SBT-GAP	X14SBT-GAP_1.0_AS01.00.21.20_SAA1.1.0-p5	X14SBT-GAP_1.0_AS01.00.21.20_SAA1.1.0-p5.zip		Bundle

3. Klicken Sie auf **Download Zip 1** für das ausgewählte Hauptplatinenmodell.

   Die Seite *End User License Agreement* wird angezeigt.

4. Klicken Sie auf **Accept**, um den Download zu starten.

   Die Firmware-Updatedatei wird heruntergeladen und lokal auf dem System gespeichert.

   Hinweis: Der Dateityp des Firmware-Updates variiert je nach Gerät (BMS, BIOS usw.).

Die Firmware-Updatedatei wurde erfolgreich heruntergeladen.

Aktualisieren der Firmware

Dieser Abschnitt enthält folgende Themen:

So aktualisieren Sie die BMC-Firmware

Dieser Abschnitt enthält Informationen zum Aktualisieren der BMC-Firmware.

Befolgen Sie diese Schritte:

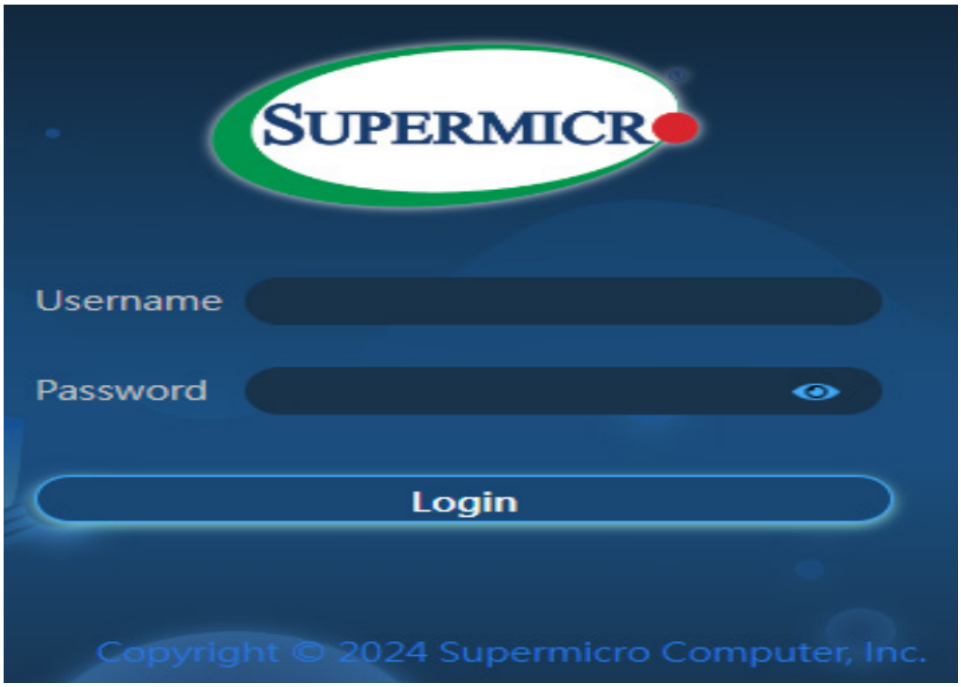
1. Öffnen Sie einen Webbrowser, und geben Sie die statische IP für IPMI (Intelligent Platform Management Interface) ein.

   Der Anmeldebildschirm wird geöffnet.

2. Geben Sie die Anmeldeinformationen wie folgt ein:
   - **Benutzername:** ADMIN.

     Hinweis: Der Benutzername muss in Großbuchstaben geschrieben werden.
   - **Kennwort:** Geben Sie das BMC-Kennwort ein**.**

3. Klicken Sie auf **"Login".**

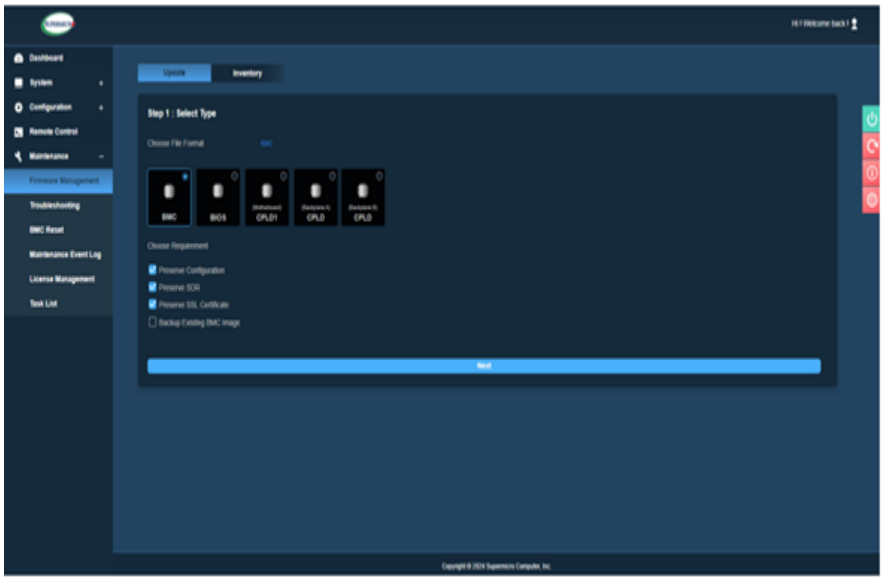


Die Benutzeroberfläche des IPMI-Webservers wird angezeigt.

Hinweis: Das eindeutige BMC-Kennwort finden Sie auf dem Service-Tag am Servergehäuse. Das BMC-Kennwort ist in der unteren Zeile direkt unter der IPMI-MAC-Adresse aufgeführt.

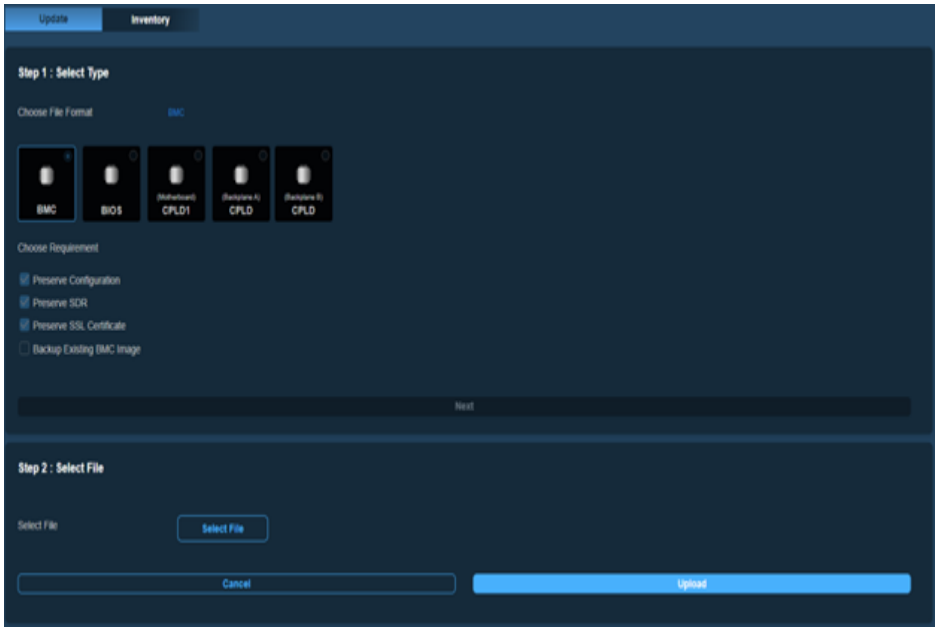
4. Navigieren Sie zu **Maintenance** -> **Firmware Management**.
5. Gehen Sie im Aktualisierungsbildschirm wie folgt vor:
   a. Wählen Sie unter *Step 1: Select Type* als Dateiformat **BMC** aus.
   b. (Optional) Wählen Sie nach Bedarf die folgenden Konfigurationsoptionen aus, und klicken Sie dann auf **Next**.
      - Preserve Configuration:
      - Preserve SDR:
      - Preserve SSL certificate:
      - Backup existing BMC image:

        Um das vorhandene BMC-Image zu sichern, aktivieren Sie das Kontrollkästchen **Backup Existing BMC Image** . Falls die Integration fehlschlägt, können Sie jederzeit das Sicherungs-Image für die automatische Wiederherstellung verwenden. Sie können den BMC auch manuell über die Bestandsseite wiederherstellen.

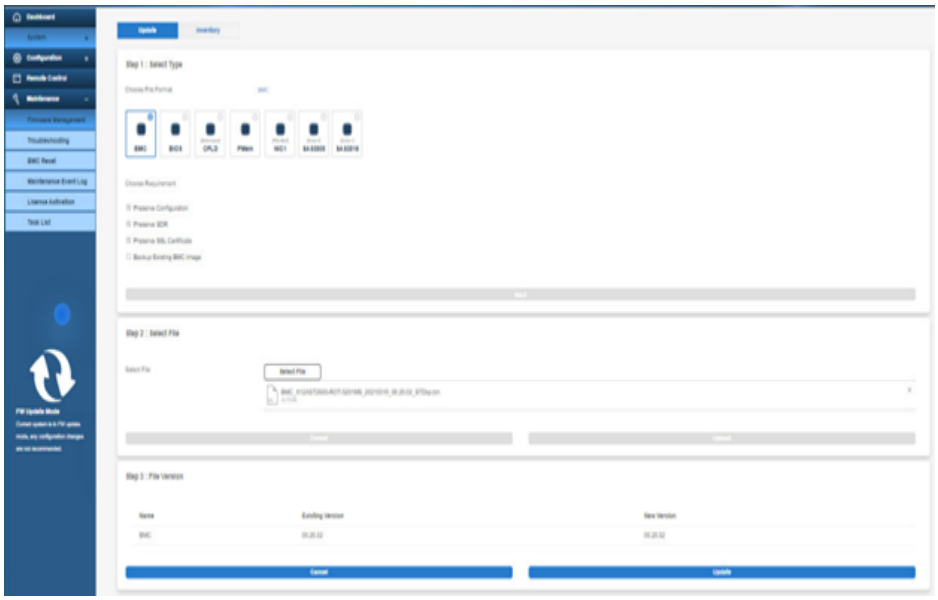


c. Klicken Sie unter *Step 2: Select File* auf **Select File**, navigieren Sie zur lokal gespeicherten Firmware-Updatedatei, und klicken Sie auf **Upload**.

Hinweis: Wenn Sie auf **Upload** klicken, ohne ein BMC-Image einzuschließen, wird die folgende Meldung angezeigt: *Please select an image file. Click here to return.*

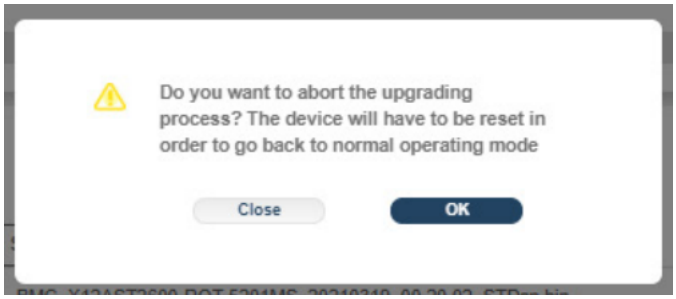


d. Prüfen Sie unter *Step 3: File Version* die vorhandene Firmware-Version und die neue Firmware-Version, und klicken Sie auf **Update**.



Hinweise:

- Für die meisten Firmware-Updates müssen Sie die Hauptplatine gemäß der Systemaufforderung herunterfahren. Nachdem Sie die Hauptplatine heruntergefahren haben, können Sie mit dem Update fortfahren.
- Wenn Sie die Aktualisierung der BMC-Firmware abbrechen, wird eine Warnmeldung angezeigt, in der Sie gefragt werden, ob Sie die Aktualisierung abbrechen möchten. Wenn Sie auf **OK** klicken, wird der BMC zurückgesetzt und die folgende Meldung angezeigt: *BMC is restarting*. Unterbrechen Sie nach der Bestätigung die Stromversorgung nicht, bis der BMC wieder online ist, um Datenverlust zu vermeiden.



- Nach Abschluss des Firmware-Updates kann es zu einer längeren Aktualisierung des Webbrowsers kommen. Die Neustartmeldung wird möglicherweise ein oder zwei Minuten lang angezeigt, wenn Sie sich anmelden.

Das Firmware-Upgrade für BMC wurde erfolgreich aktualisiert.

So aktualisieren Sie die BIOS-Firmware

Gehen Sie folgendermaßen vor, um die BIOS-Firmware zu aktualisieren:

1. Öffnen Sie einen Webbrowser, und geben Sie die statische IP für IPMI (Intelligent Platform Management Interface) ein.

   Der Anmeldebildschirm wird geöffnet.

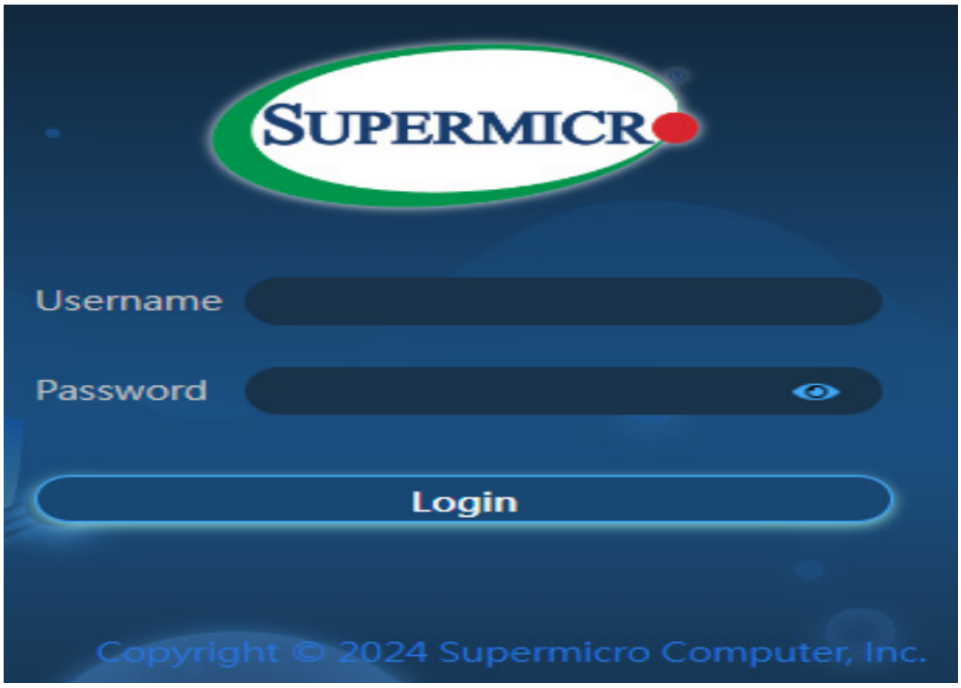
2. Geben Sie die Anmeldeinformationen wie folgt ein:

- **Benutzername:** ADMIN.

  Hinweis: Der Benutzername muss in Großbuchstaben geschrieben werden.

- **Kennwort:** Geben Sie das BMC-Kennwort ein**.**

5. Klicken Sie auf **"Login".**



Die Benutzeroberfläche des IPMI-Webservers wird angezeigt.

Hinweis: Das eindeutige BMC-Kennwort finden Sie auf dem Service-Tag am Servergehäuse. Das BMC-Kennwort ist in der unteren Zeile direkt unter der IPMI-MAC-Adresse aufgeführt.

6. Navigieren Sie zu **Maintenance** -> **Firmware Management**.
7. Gehen Sie im Aktualisierungsbildschirm wie folgt vor:
   a. Wählen Sie unter *Step 1: Select Type* als Dateiformat **BIOS** aus.
   b. (Optional) Wählen Sie nach Bedarf die folgenden Konfigurationsoptionen aus, und klicken Sie dann auf **Next**.
      - Preserve SMBIOS
      - Preserve OA
      - Preserve SMBIOS
      - Preserve BIOS Setup Configuration
      - Preserve BIOS Setup Password
      - Preserve BIOS Setup Secure Boot Keys
      - Preserve BIOS Setup Options Configuration
      - Backup Existing BIOS Image: Um das vorhandene BIOS-Image zu sichern, aktivieren Sie das Kontrollkästchen **Backup Existing BIOS Image** . Falls die Integration fehlschlägt, können Sie jederzeit das Sicherungs-Image für die automatische Wiederherstellung verwenden. Sie können das BIOS auch manuell über die Bestandsseite wiederherstellen.
   c. Wählen Sie eine der folgenden Optionen:

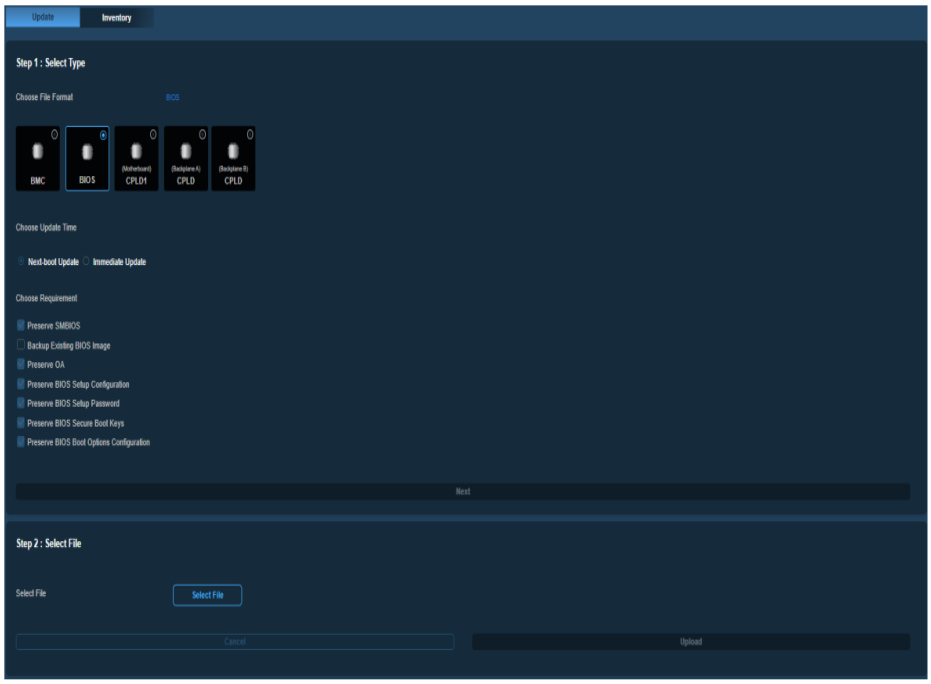
- **Next-boot Update:** Das BIOS-Firmware-Update wird nach dem Neustart des Systems geplant.

  Hinweis: Wenn Sie die für den nächsten Start geplante Aktualisierung abbrechen möchten, verwenden Sie die Option zum Löschen auf der Aufgabenlistenseite.

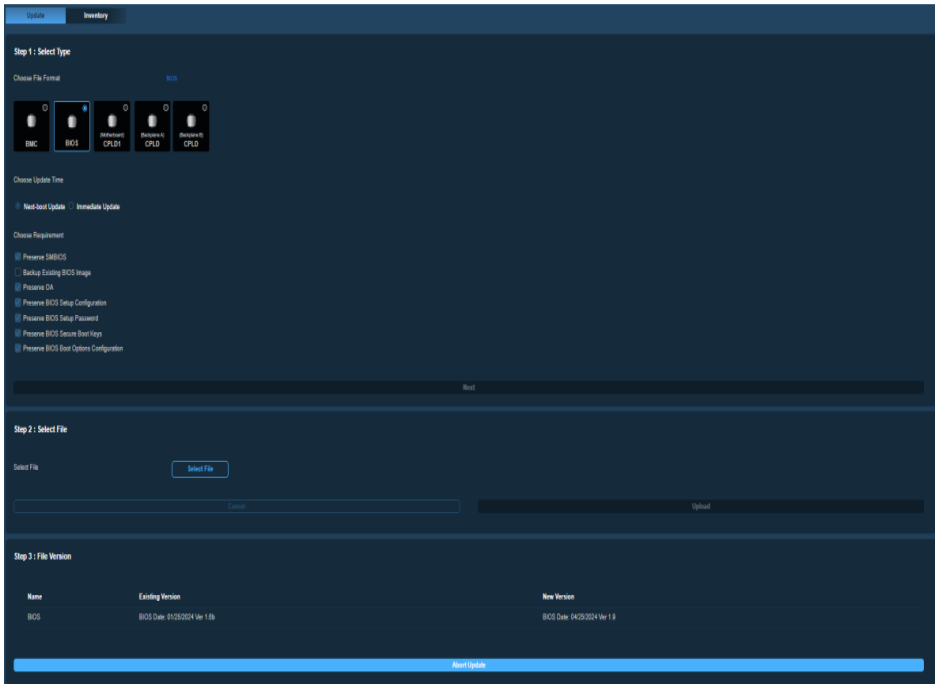
- **Immediate Update:** Das BIOS-Firmware-Update wird sofort gestartet.

d. Klicken Sie unter *Step 2: Select File* auf **Select File**, navigieren Sie zur lokal gespeicherten Firmware-Updatedatei, und klicken Sie auf **Upload**.

Hinweis: Wenn Sie auf **Upload** klicken, ohne ein BIOS-Image einzuschließen, wird die folgende Meldung angezeigt: *Please select an image file. Click here to return*.

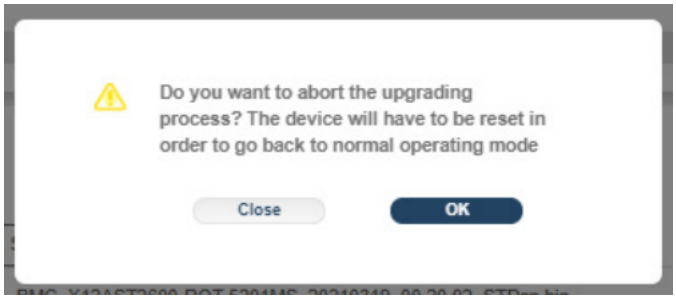


e. Prüfen Sie unter *Step 3: File Version* die vorhandene Firmware-Version und die neue Firmware-Version, und klicken Sie auf **Update**.



Hinweise:

- Für die meisten Firmware-Updates müssen Sie die Hauptplatine gemäß der Systemaufforderung herunterfahren. Nachdem Sie die Hauptplatine heruntergefahren haben, können Sie mit dem Update fortfahren.
- Wenn Sie die Aktualisierung der BIOS-Firmware abbrechen, wird eine Warnmeldung angezeigt, in der Sie gefragt werden, ob Sie die Aktualisierung abbrechen möchten. Wenn Sie auf **OK** klicken, wird das BIOS zurückgesetzt und die folgende Meldung angezeigt: *BIOS is restarting*. Unterbrechen Sie die Stromversorgung nicht, bis das BIOS wieder online ist, um Datenverlust zu vermeiden.



- Nach Abschluss des Firmware-Updates kann es zu einer längeren Aktualisierung des Webbrowsers kommen. Die Neustartmeldung wird möglicherweise ein oder zwei Minuten lang angezeigt, wenn Sie sich anmelden.

Das Firmware-Upgrade für das BIOS wurde erfolgreich aktualisiert.

Überprüfen der aktualisierten Firmware

Dieser Abschnitt enthält Informationen zum Überprüfen des Fortschritts des Firmware-Updates.

Befolgen Sie diese Schritte:

1. Melden Sie sich bei der IPMI-Website an.
2. Navigieren Sie zu **Maintenance** -> **Task List**.

   Das Fenster mit der Aufgabenliste wird angezeigt, und der Wartungsvorgang wird auf dem System ausgeführt.

3. Prüfen Sie das Protokoll, und überprüfen Sie den Status und Fortschritt des Firmware-Updates.

   Der Bildschirm mit der Aufgabenliste enthält folgende Details zum Firmware-Update-Job:

   - **Health Status:** Gibt den Integritätszustand der aktuellen Aufgaben an.
   - **Task Name:** Zeigt den Namen der Aufgabe an.
   - **State:** Zeigt die aktuellen Statuswerte an (Running, Completed oder Failed).
   - **Progress:** Gibt den Fortschritt der derzeit ausgeführten Aufgabe(n) an.

   Hinweis: Administratoren können ausstehende BMC- und BIOS-Firmware-Updates abbrechen. Um den Vorgang abzubrechen, klicken Sie in der Aufgabenliste auf die Option **Abort pending Task**.

Kapitel 11: 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 Firmwareversion

Dieser Abschnitt enthält Informationen zum Anzeigen der aktuellen Firmware-Version.

Befolgen Sie diese Schritte:

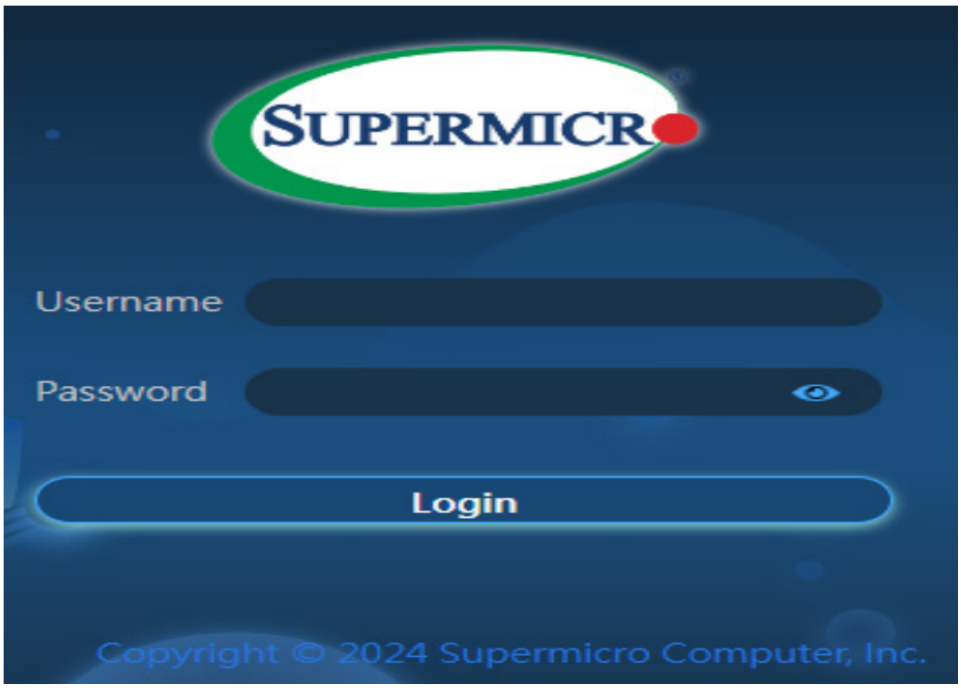
1. Öffnen Sie einen Webbrowser, und geben Sie die statische IP für IPMI (Intelligent Platform Management Interface) ein.

   Der Anmeldebildschirm wird geöffnet.

2. Geben Sie die Anmeldeinformationen wie folgt ein:
   - **Benutzername:** ADMIN.

     Hinweis: Der Benutzername muss in Großbuchstaben geschrieben werden.
   - **Kennwort:** Geben Sie das BMC-Kennwort ein**.**

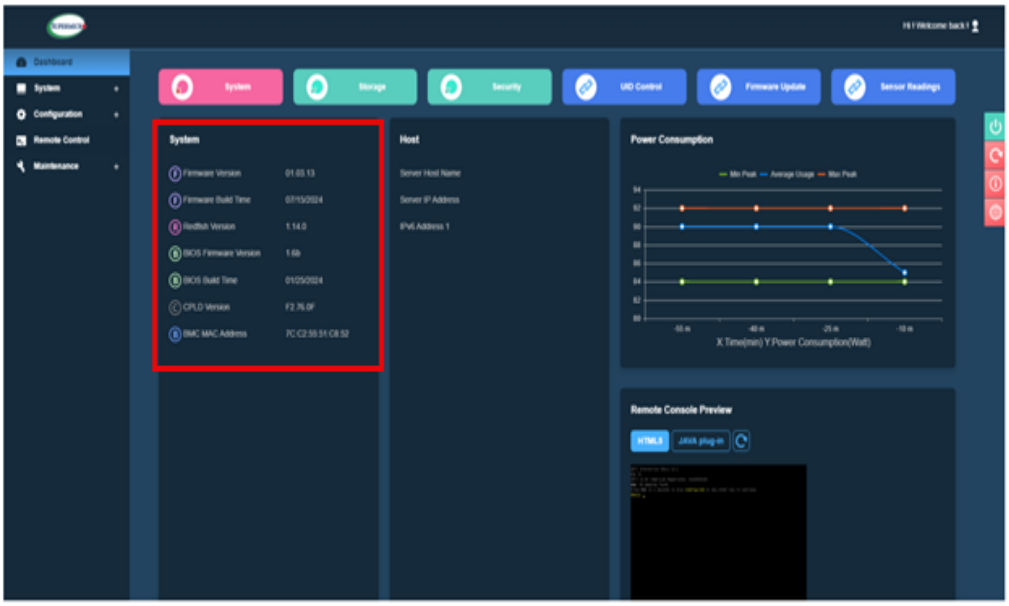
3. Klicken Sie auf **"Login".**



Die Benutzeroberfläche des IPMI-Webservers wird angezeigt.

Hinweis: Das eindeutige BMC-/IPMI-Kennwort finden Sie im herausziehbaren Tag auf der Vorderseite des Servers. Das BMC-Kennwort wird in der unteren Zeile direkt unter der BMC-/IPMI-MAC-Adresse aufgeführt.

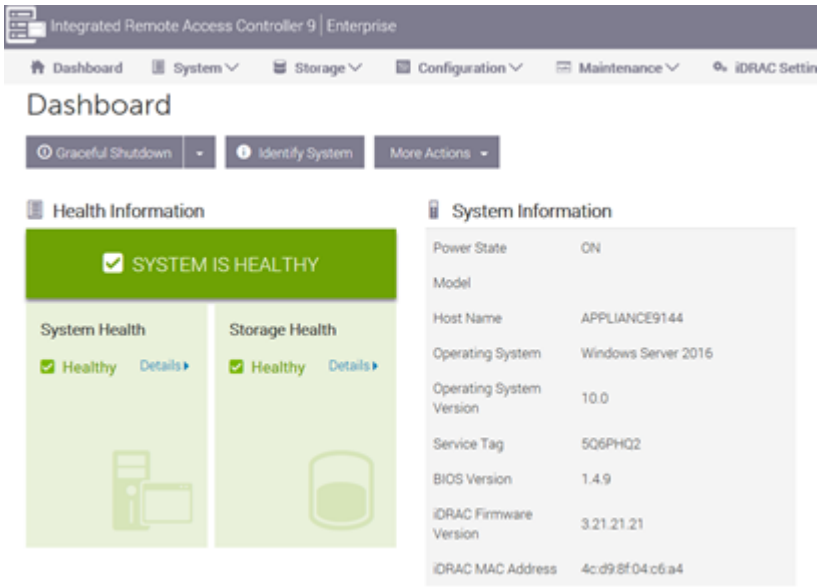
Der Dashboard-Bildschirm zeigt die Firmware-Version unter "System" an.



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

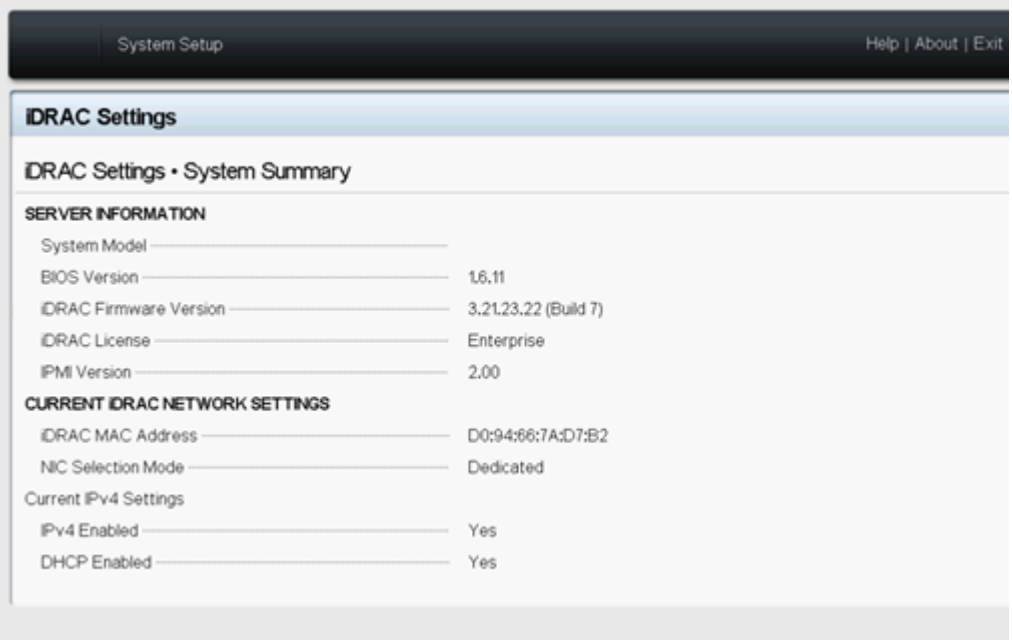


Auf der Seite iDRAC-Dashboard werden die Systeminformationen angezeigt, die die BIOS-Firmwareversion enthalten.

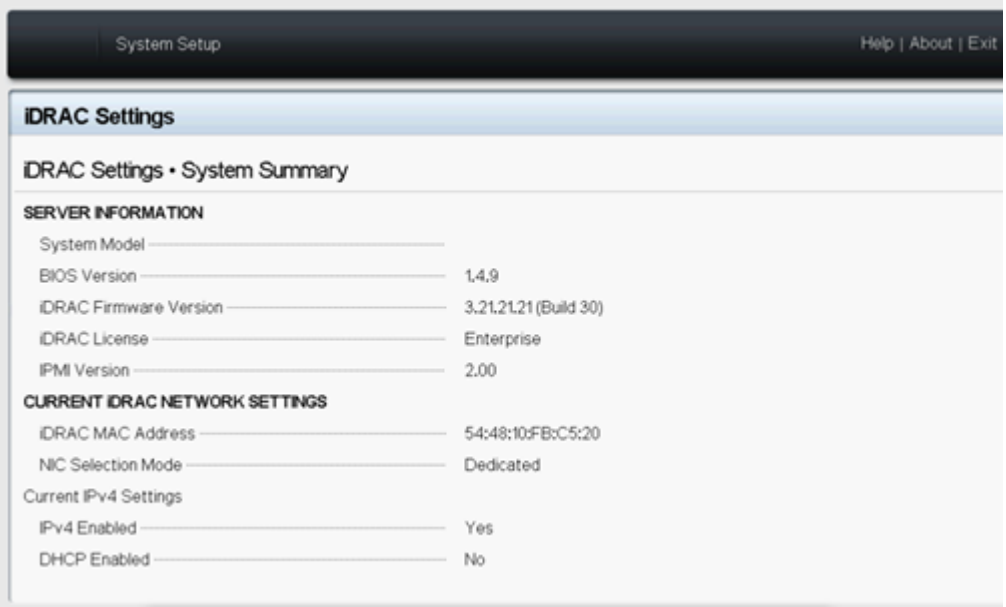
Methode 2: BIOS-Firmware-Version von BIOS Arcserve Appliance 9000 Series anzeigen

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.



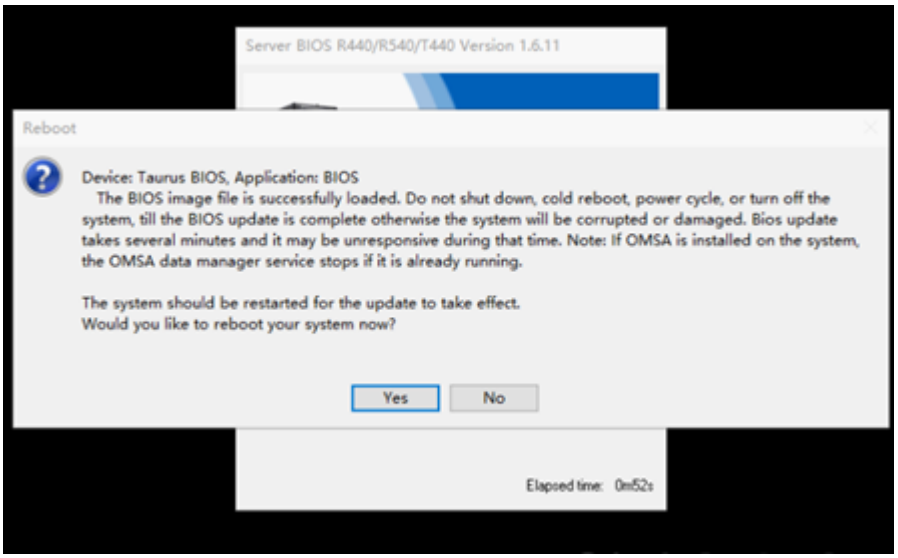
Herunterladen des aktualisierten Pakets für BIOS

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 der aktualisierten Firmware

Dieser Abschnitt enthält Informationen zum Überprüfen des Fortschritts des Firmware-Updates.

Befolgen Sie diese Schritte:

1. Melden Sie sich bei der IPMI-Website an.
2. Navigieren Sie zu **Maintenance** -> **Task List**.

   Das Fenster mit der Aufgabenliste wird angezeigt, und der Wartungsvorgang wird auf dem System ausgeführt.

3. Prüfen Sie das Protokoll, und überprüfen Sie den Status und Fortschritt des Firmware-Updates.

   Der Bildschirm mit der Aufgabenliste enthält folgende Details zum Firmware-Update-Job:

   - **Health Status:** Gibt den Integritätszustand der aktuellen Aufgaben an.
   - **Task Name:** Zeigt den Namen der Aufgabe an.
   - **State:** Zeigt die aktuellen Statuswerte an (Running, Completed oder Failed).
   - **Progress:** Gibt den Fortschritt der derzeit ausgeführten Aufgabe(n) an.

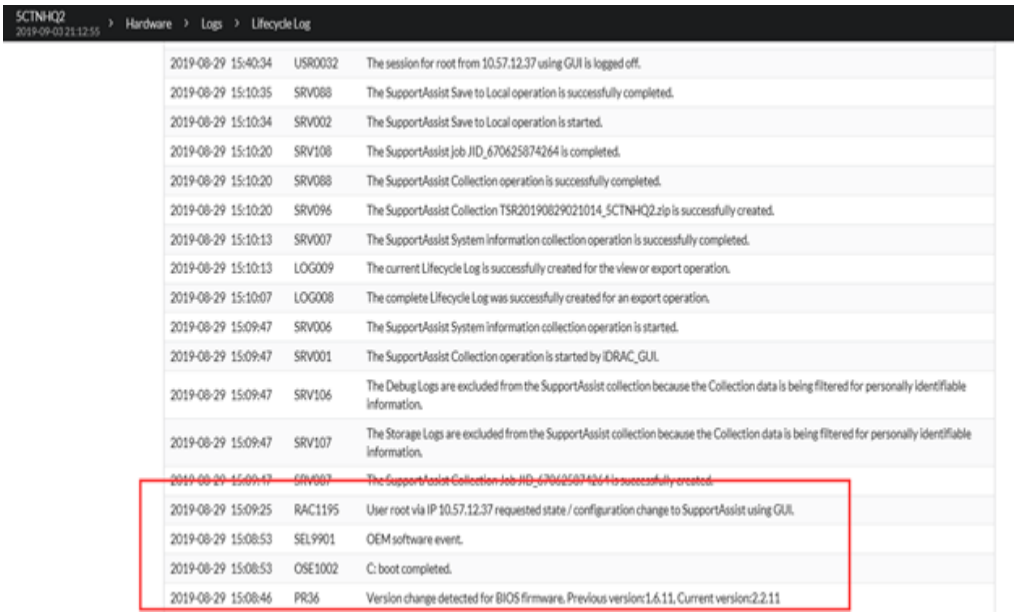
   Hinweis: Administratoren können ausstehende BMC- und BIOS-Firmware-Updates abbrechen. Um den Vorgang abzubrechen, klicken Sie in der Aufgabenliste auf die Option **Abort pending Task**.

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

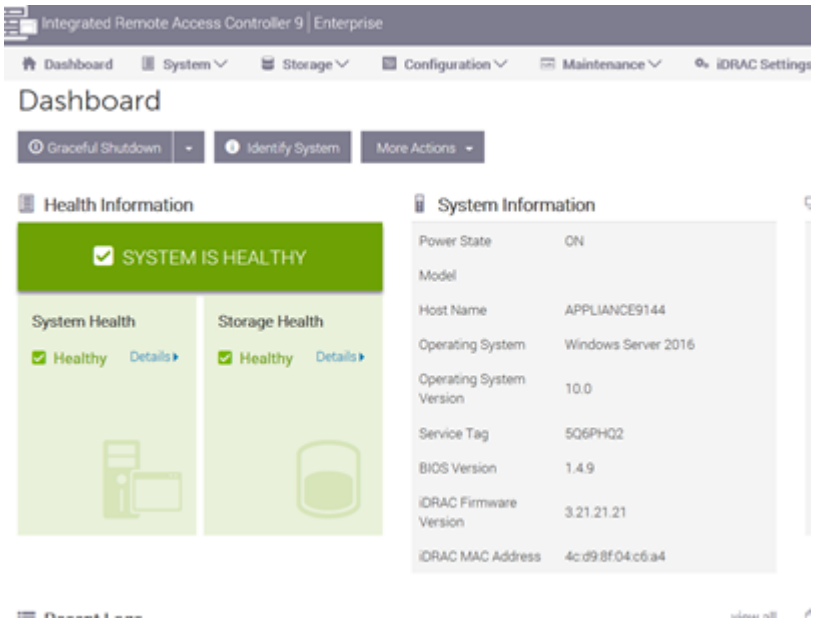
Verwenden Sie eine der folgenden Methoden, um die iDRAC-Firmwareversion anzuzeigen:

- Methode 1: iDRAC-Firmwareversion über die iDRAC-Weboberfläche anzeigen
- Methode 2: iDRAC-Firmwareversion über das BIOS der Arcserve Appliance 9000-Serie anzeigen

Anzeigen der iDRAC-Firmwareversion über die iDRAC-Weboberfläche

Um die iDRAC-Firmwareversion über die iDRAC-Weboberfläche anzuzeigen, melden Sie sich bei der iDRAC-Weboberfläche an.

Hinweis: Es wird dringend empfohlen, das Standardkennwort sofort zu ändern. Informationen zum Ändern des Standardkennworts finden Sie unter So ändern Sie das iDRAC-Kennwort.

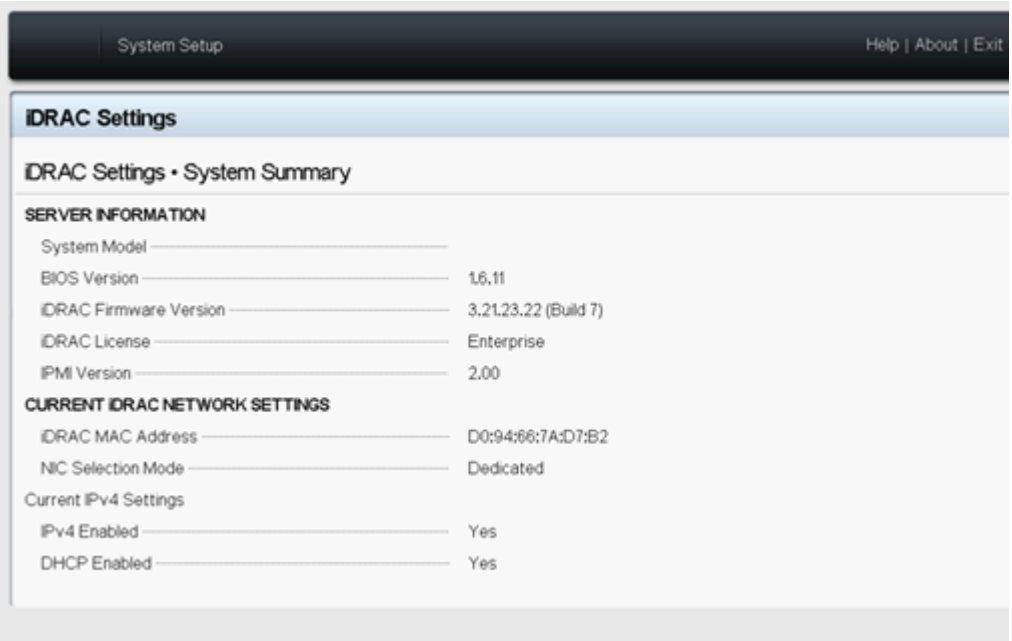


Das iDRAC-Dashboard zeigt die Systeminformationen an, die die iDRAC-Firmwareversion enthalten.

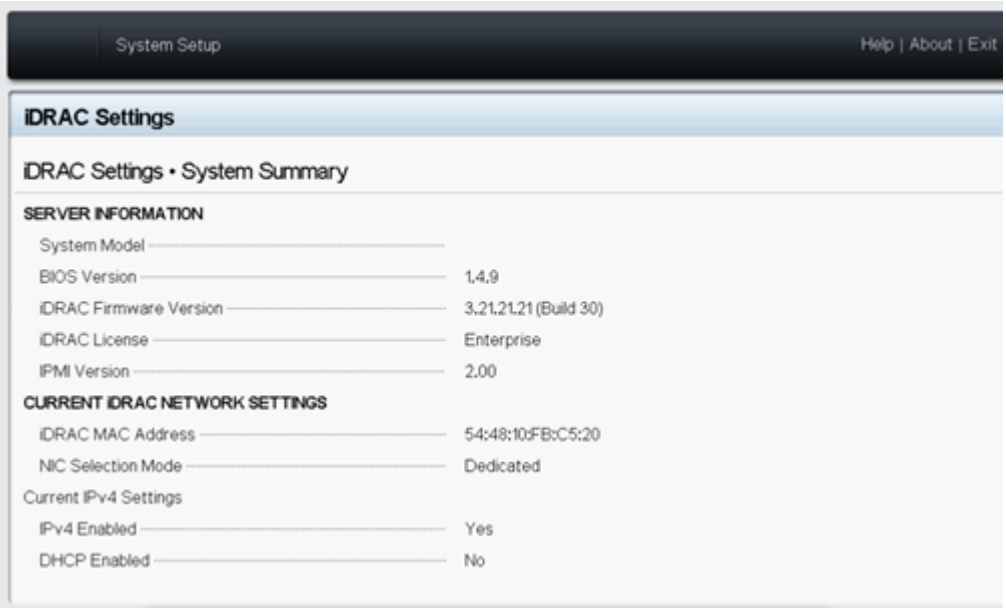
Methode 2: iDRAC-Firmwareversion über das BIOS der Arcserve Appliance 9000-Serie anzeigen

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.

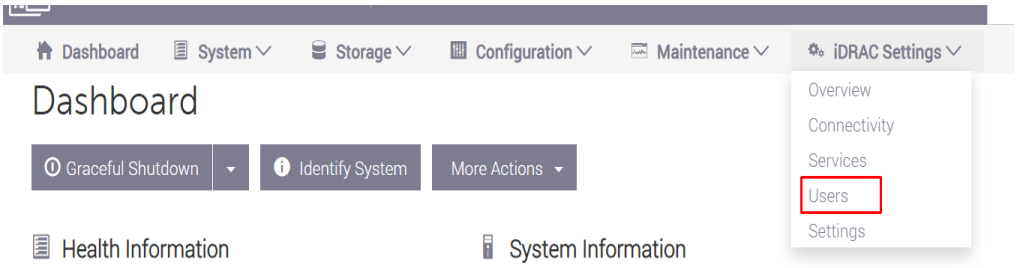


So ändern Sie das iDRAC-Kennwort

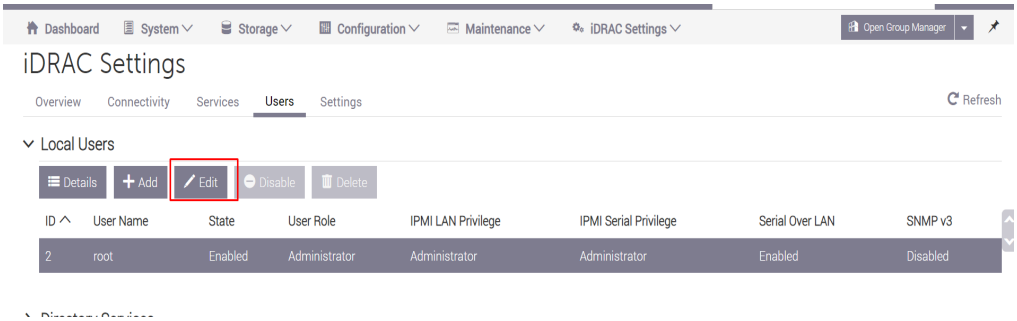
Dieser Abschnitt enthält Informationen zum Ändern des iDRAC-Kennworts.

Befolgen Sie diese Schritte:

1. Melden Sie sich mit dem aktuellen Kennwort bei iDRAC an.
2. Gehen Sie zu **iDRAC Settings**, und wählen Sie dann **Users** aus.



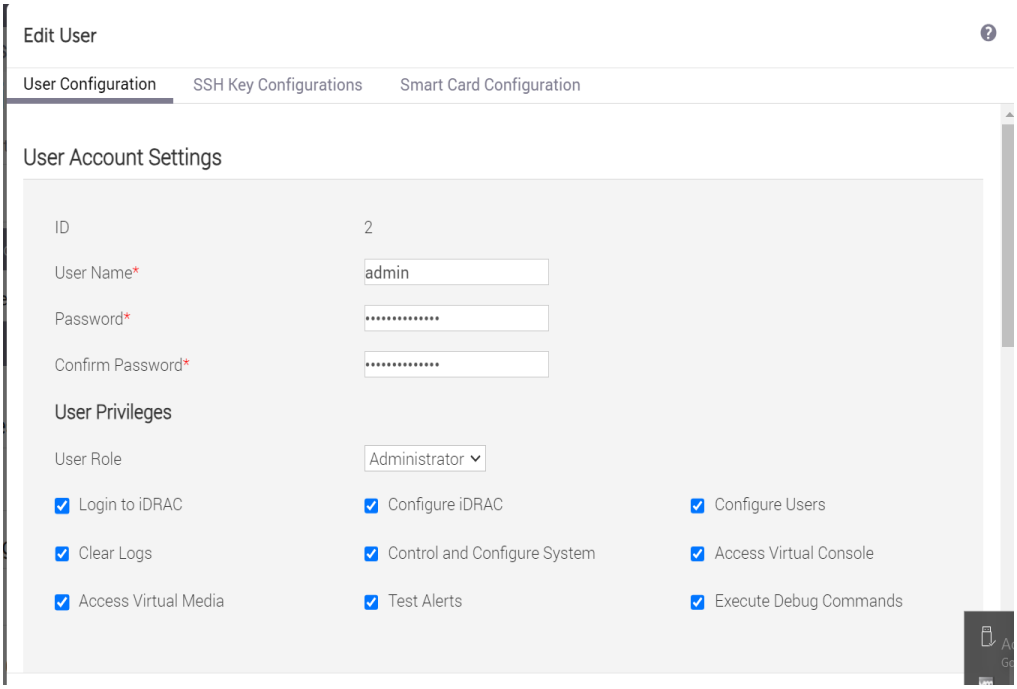
3. Klicken Sie auf der Seite "iDRAC Settings" auf die Dropdown-Liste **Local Users**, und klicken Sie dann auf die Schaltfläche **Edit** .



Das Dialogfeld "Edit User" wird angezeigt.

4. Geben Sie auf der Registerkarte "User Configuration" das neue Kennwort ein, geben Sie es zur Bestätigung erneut ein, und klicken Sie dann auf **Save**.

Hinweis: Es wird empfohlen, dass Sie als Benutzerrolle "Administrator" beibehalten.



Das iDRAC-Kennwort wurde erfolgreich geändert.

Herunterladen des aktualisierten Pakets für iDRAC

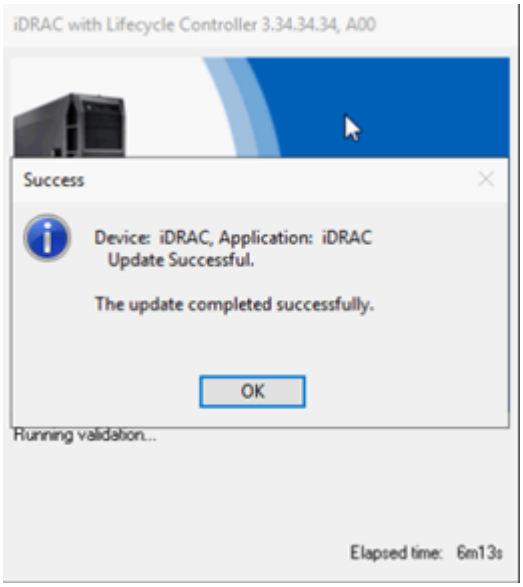
Sie können das neueste iDRAC-Firmwarepaket eines bestimmten Modells der Arcserve Appliance 9000 Series von der Dell-Website herunterladen oder den Arcserve-Support kontaktieren.

iDRAC aktualisieren

Befolgen Sie diese Schritte:

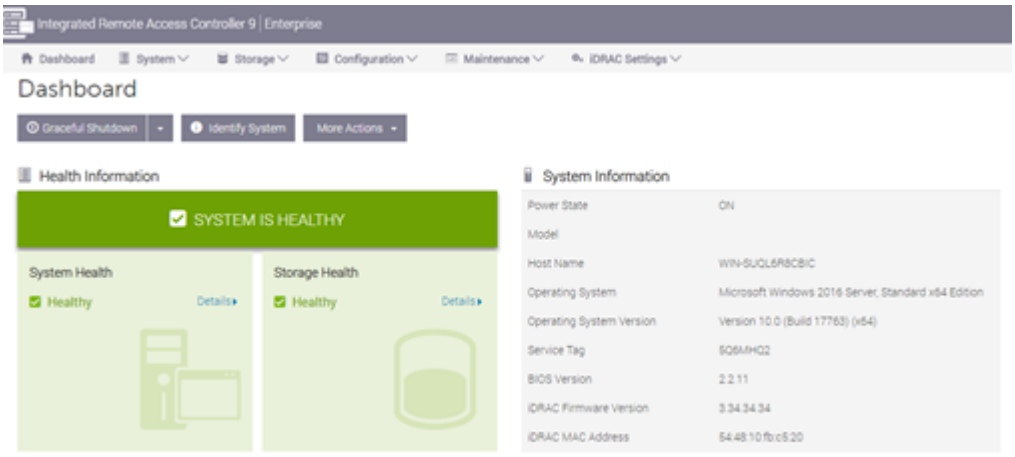
1. Kopieren Sie das Upgradepaket auf den lokalen Datenträger der Arcserve Appliance 9000 Series.
2. Starten Sie das Upgradepaket, und folgen Sie dann den Anweisungen, um das Upgrade abzuschließen.

   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 iDRAC

Verwenden Sie eine der folgenden Methoden:

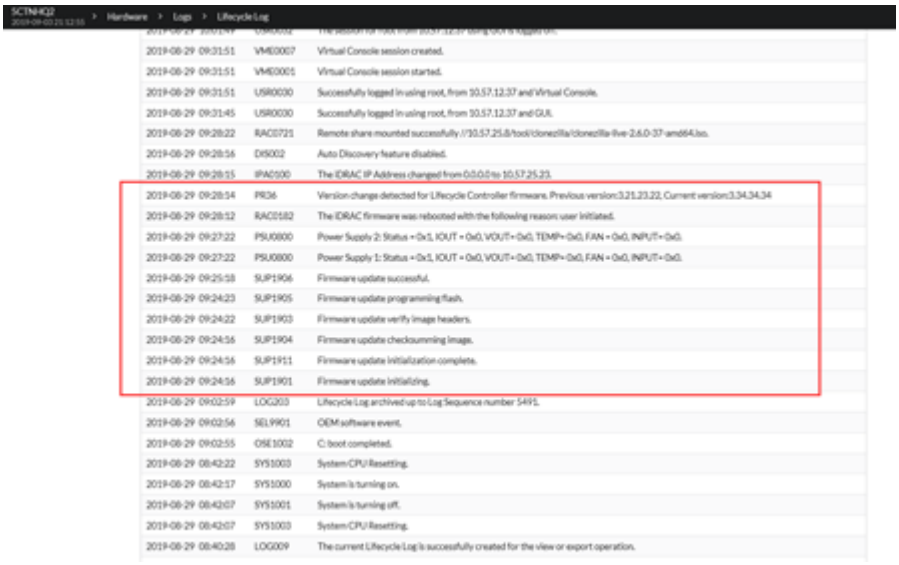
- Überprüfen des aktualisierten iDRAC mithilfe von Systemprotokollen
- Überprüfen des aktualisierten iDRAC von iDRAC Web Interface oder BIOS

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.

Aktualisieren der Firmware für Arcserve Appliance Serie X

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

Aktualisieren der BIOS-Firmware für Arcserve Appliance Serie X

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

Anzeigen der BIOS-Firmwareversion

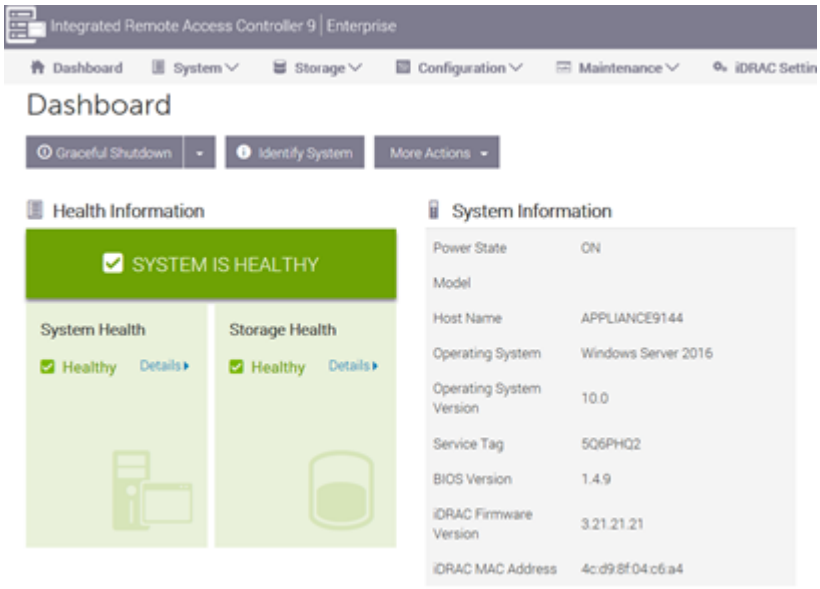
Verwenden Sie eine der folgenden Methoden, um die BIOS-Firmwareversion anzuzeigen:

- Methode 1: BIOS-Firmware-Version von iDRAC Web Interface anzeigen
- Methode 2: BIOS-Firmware-Version von BIOS Arcserve Appliance Serie X 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

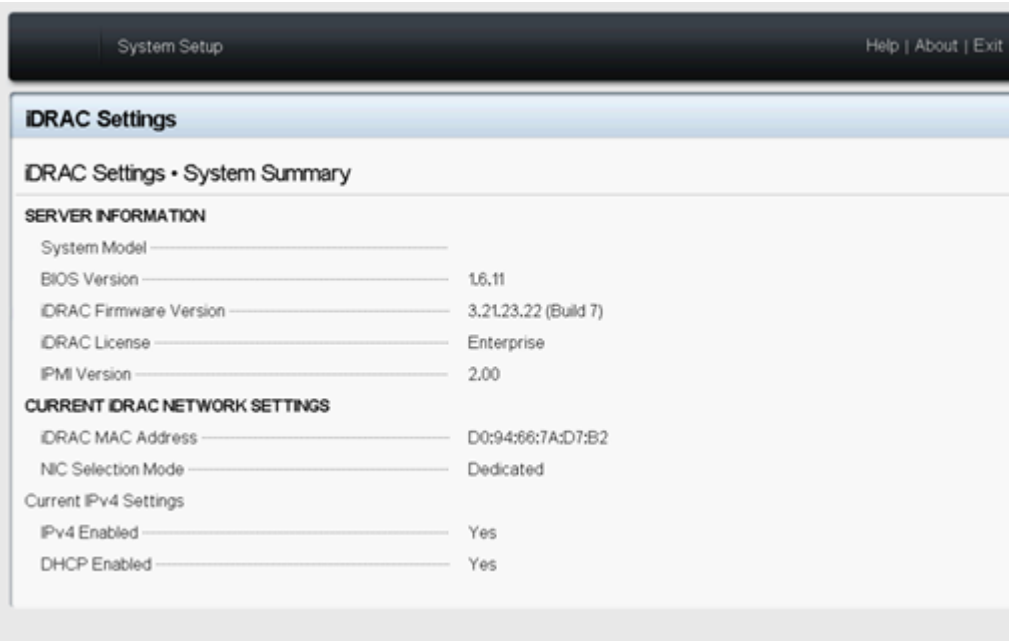


Auf der Seite iDRAC-Dashboard werden die Systeminformationen angezeigt, die die BIOS-Firmwareversion enthalten.

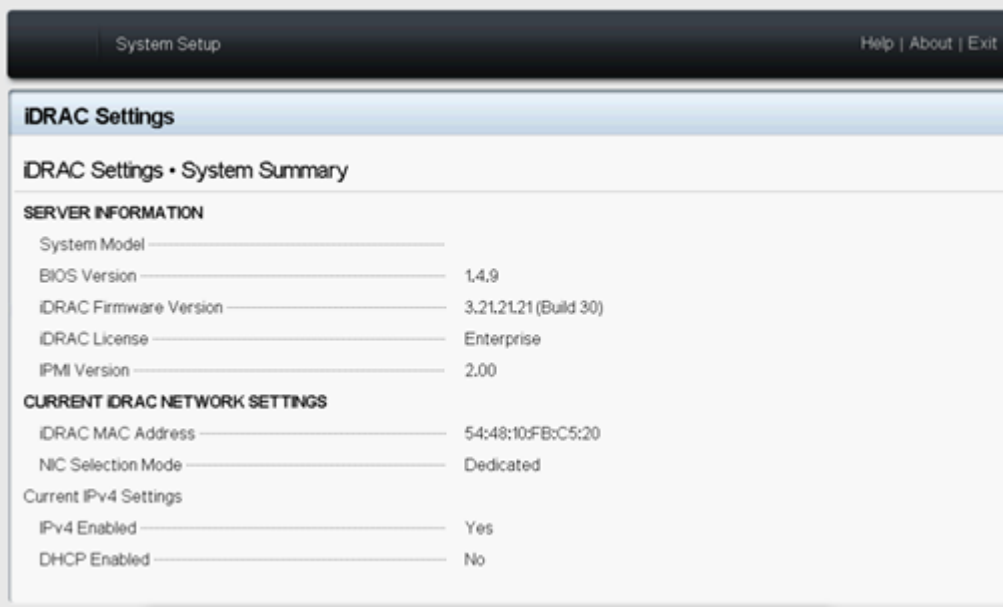
Methode 2: BIOS-Firmware-Version von BIOS Arcserve Appliance Serie X anzeigen

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.



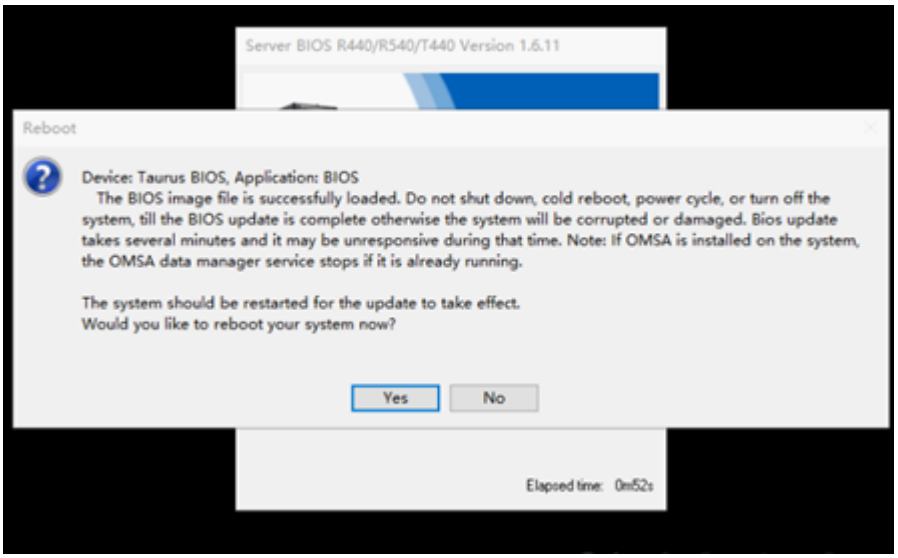
Herunterladen des aktualisierten Pakets für BIOS

Sie können das neueste BIOS-Firmwarepaket eines bestimmten Modells der Arcserve Appliance Serie X 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 Serie X.
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

Aktualisieren der iDRAC-Firmware für Arcserve Appliance Serie X

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

Anzeigen der iDRAC-Firmwareversion

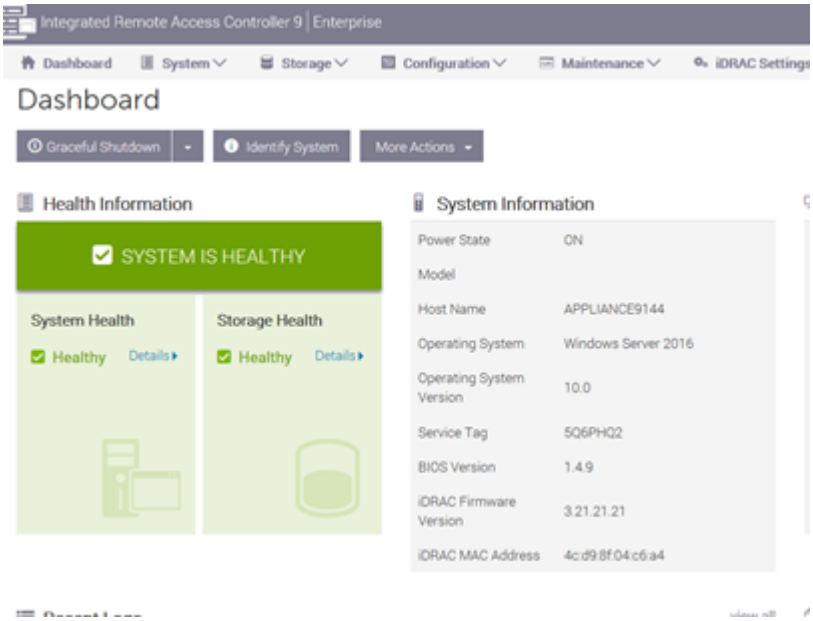
Verwenden Sie eine der folgenden Methoden, um die iDRAC-Firmwareversion anzuzeigen:

- Methode 1: iDRAC-Firmwareversion von iDRAC Web Interface anzeigen
- Methode 2: iDRAC-Firmwareversion von BIOS Arcserve Appliance Serie X anzeigen

Methode 1: iDRAC-Firmwareversion von iDRAC Web Interface anzeigen

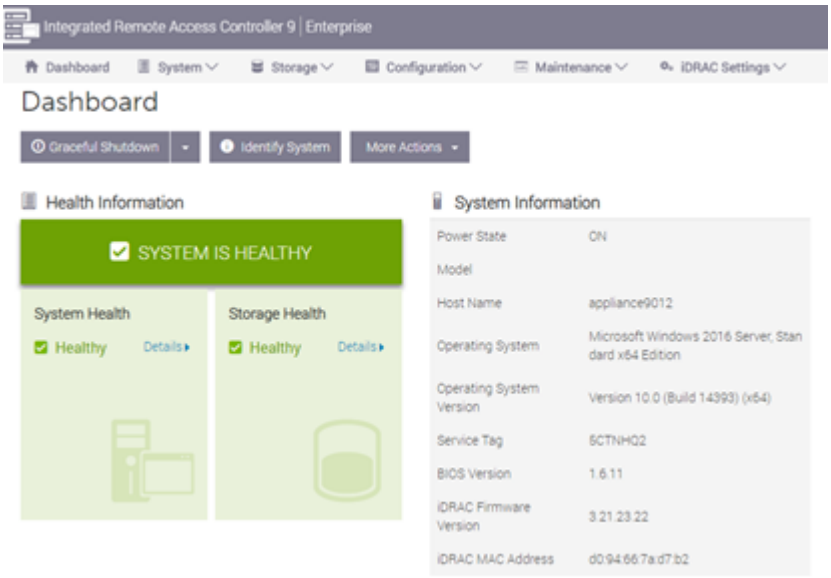
Befolgen Sie diese Schritte:

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-Firm-

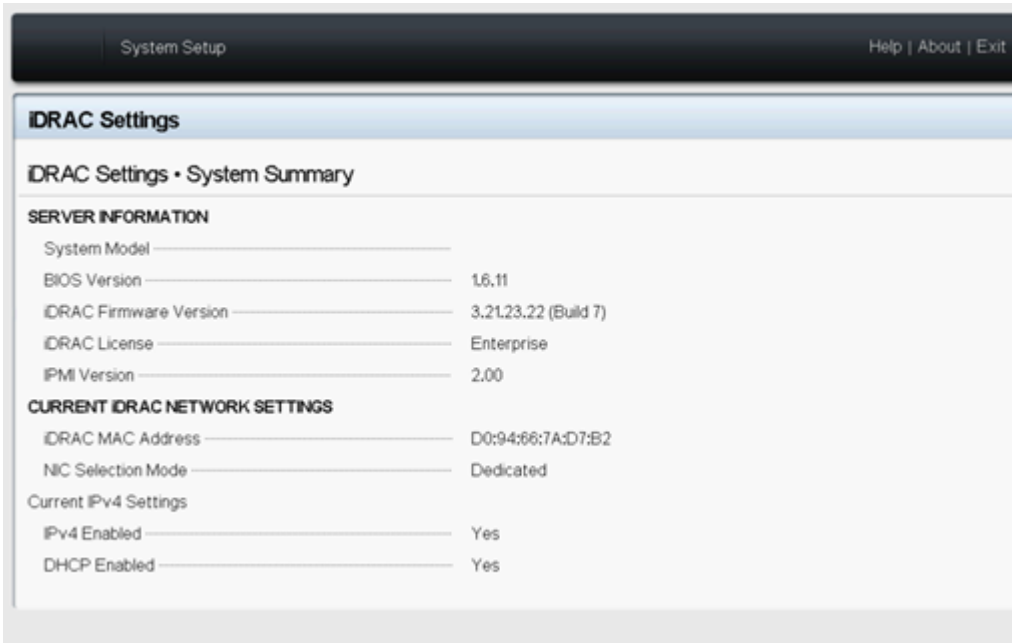
wareversion enthalten.



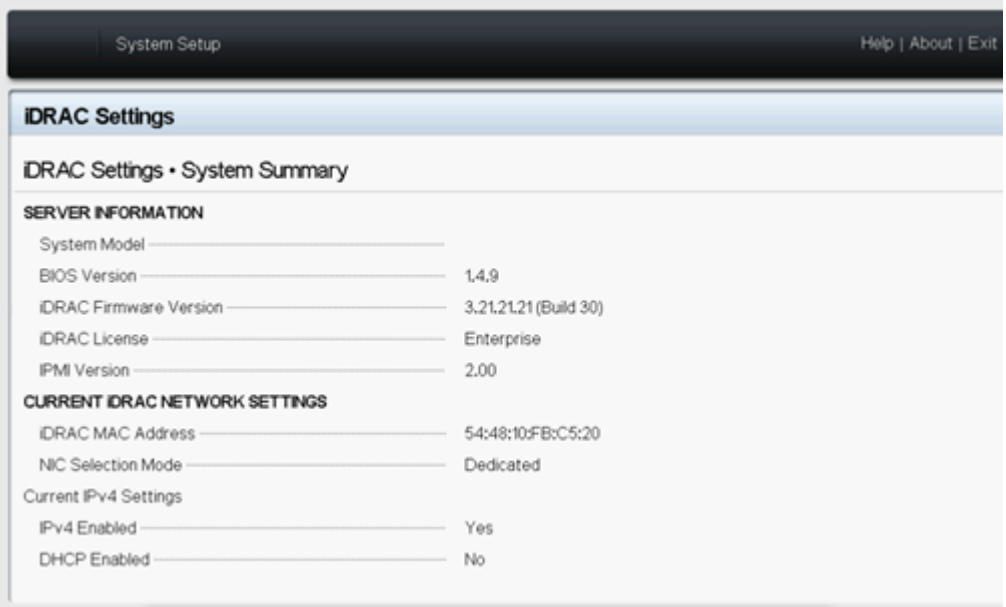
Methode 2: iDRAC-Firmwareversion von BIOS Arcserve Appliance Serie X anzeigen

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

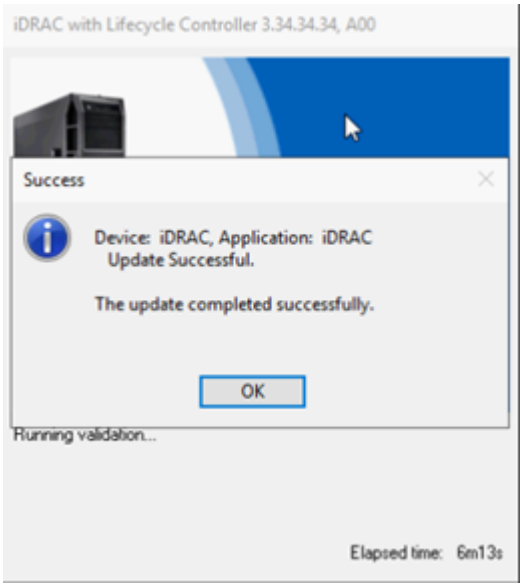
Sie können das neueste iDRAC-Firmwarepaket eines bestimmten Modells der Arcserve Appliance Serie X von der Dell-Website herunterladen oder den Arcserve-Support kontaktieren.

iDRAC aktualisieren

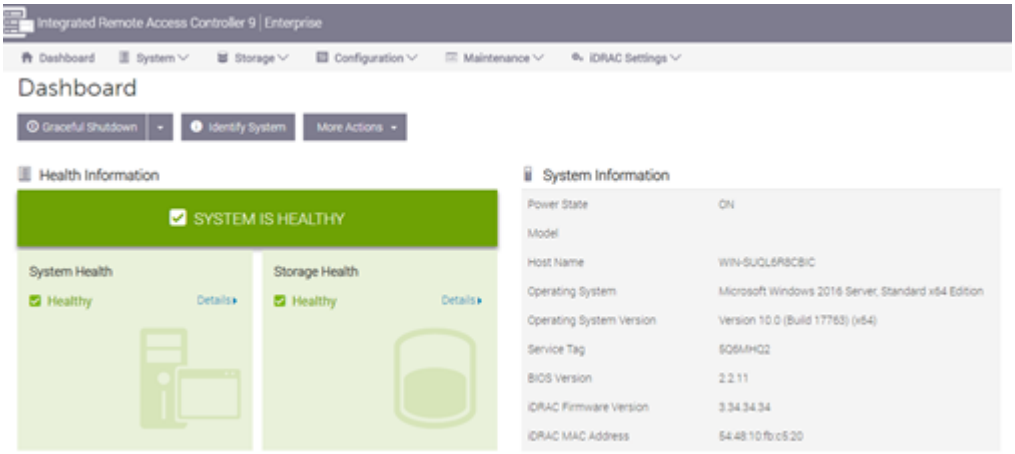
Befolgen Sie diese Schritte:

1. Kopieren Sie das Upgradepaket auf den lokalen Datenträger der Arcserve Appliance Serie X.
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 iDRAC

Verwenden Sie eine der folgenden Methoden:

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

Kapitel 12: 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 den gleichen Agent-Bezeichner, 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. 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 ande-

ren 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.

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

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

6. 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 standardmäßige Zeitzone ist *(UTC + 05:30), Chennai, Kalkutta, Mumbai, Neu-Delhi*, unabhängig davon, welche Region Sie beim ersten Einschalten der Appliance auswählen.

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.

Kapitel 13: Best Practices

In diesem Abschnitt werden die folgenden Themen behandelt:

Best Practices für die Netzwerkkonfiguration

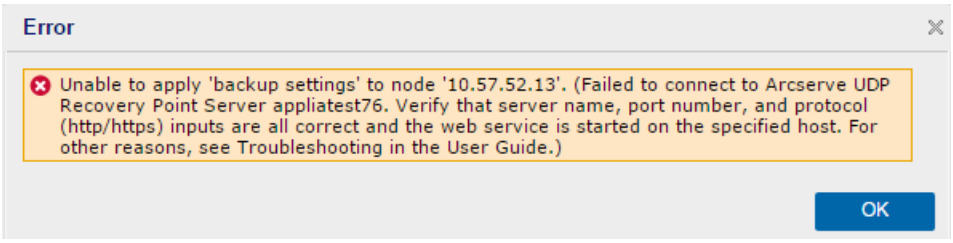
- Wenn mehrere Netzwerkschnittstellen in der Produktionsumgebung verbunden sind, stellen Sie sicher, dass die einzelnen Netzwerkadapter mit unterschiedlichen Subnetzwerken verbunden ist.
- Wenn in der zu schützenden Produktionsumgebung kein Linux-Knoten vorhanden ist, empfehlen wir, VM Linux-BackupSvr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

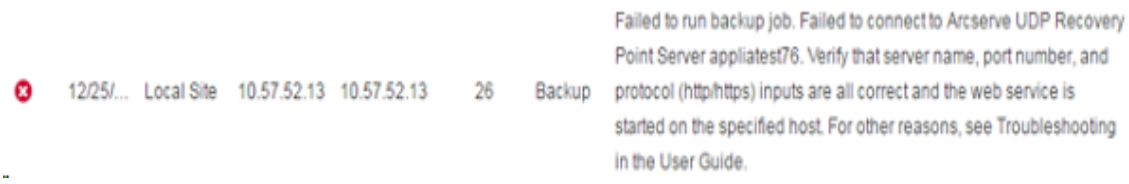
  Problem

  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 auf der Appliance an, und überprüfen Sie, ob das Problem behoben wurde.

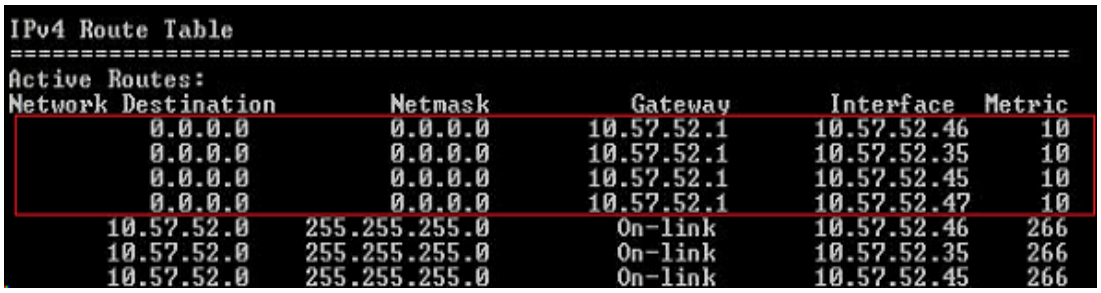
  Weitere Informationen finden Sie unter Deaktivieren des DHCP-Servers.

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

  Schritte auf der Appliance:

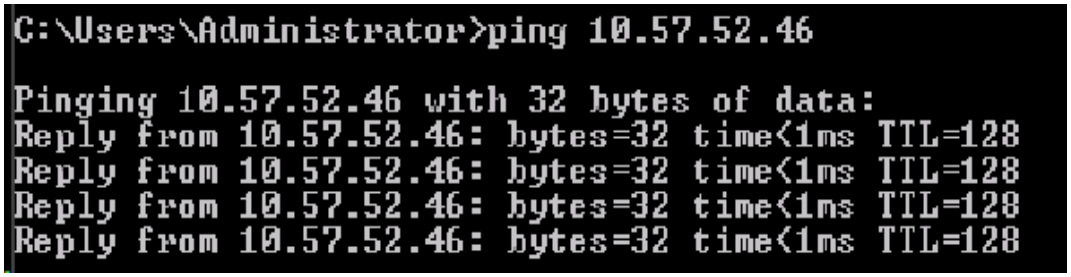
  1. Führen Sie *ipconfig /all* in der DOS-Befehlseingabeaufforderung aus, um die verfügbaren IPv4-Adressen auf der Appliance zu erhalten:
  2. Führen Sie *Route Print* in der DOS-Befehlseingabeaufforderung aus, um die IPv4-Routentabelle abzurufen, und zeichnen Sie die Reihenfolge für alle verfügbaren 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. 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 Verfahren zum Erstellen von Deduplizierungsdatenspeichern über Volumes hinweg

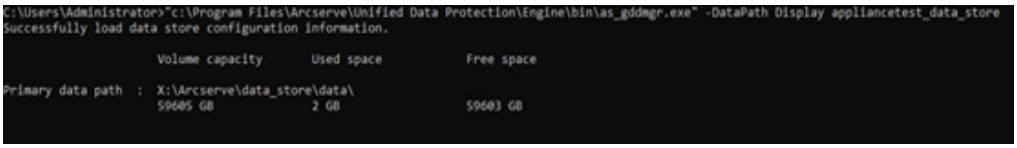
Mit as_gddmgr.exe, einem Befehlszeilentool, können Sie weitere Datenpfade über Volumes hinweg hinzufügen, um die Speicherkapazität des vorhandenen Deduplizierungsdatenspeichers zu erweitern.

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. Halten Sie den Datenspeicher an. 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:

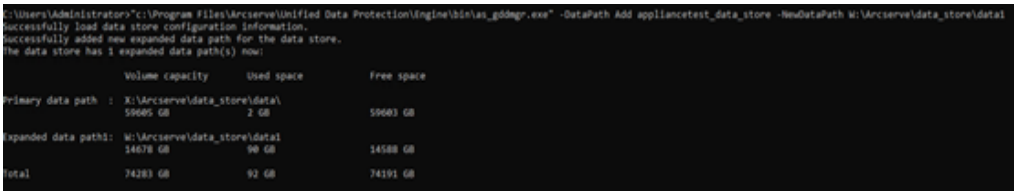


4. Um die Speicherkapazität des Deduplizierungsdatenspeichers zu erweitern, geben Sie den folgenden Befehl ein:

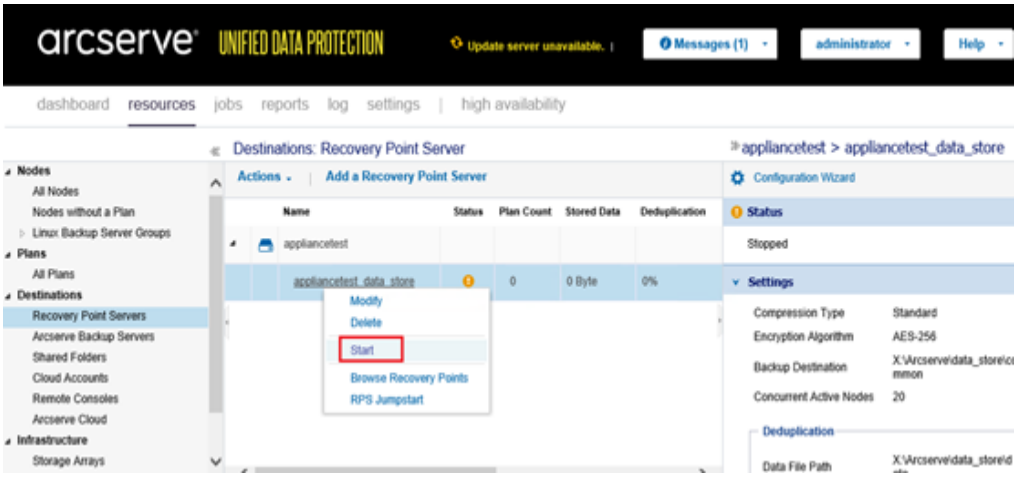
   as_gddmgr.exe -DataPath Add <Name des Datenspeichers> -NewDataPath <neuer Datenordner>

   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.



Hinweis: Es wird empfohlen, den gesicherten Datenspeicher mit ähnlichen Datenträgerpartitionen auf die UDP Appliance zu importieren.

Kapitel 14: 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
Komponentenhersteller	Ursprünglich entwickelt von Simon Tatham
Komponentenversion	0.64
Rechtlicher Hinweis	http://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 Komponentenversion	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	http://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	http://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