

User Guide

Arcserve® Appliance

Version 9.x

arcserve®

User Guide

Arcserve® Appliance

Version 9.x

The Table of Contents appears on the left pane. To view all topics, click the  TOC icon available on top.

arcserve®

Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by Arcserve at any time. This Documentation is proprietary information of Arcserve and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Arcserve.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

© 2023 Arcserve, including its affiliates and subsidiaries. All rights reserved. Any third party trademarks or copyrights are the property of their respective owners.

Contact Arcserve Support

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

[Contact Support](#)

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.
- You can access other helpful resources appropriate for your Arcserve product.

Arcserve Appliance Return Policy

A valid RMA (Return Material Authorization) number is required to return a product to Arcserve. Contact the Arcserve Technical Support department to obtain an RMA number. Refer to arcserve.com/support to contact customer care. Support team can inform where to send the RMA data.

Returns are subject to a re-stocking fee of 10%. Exceptions are: 1) If an order was fulfilled incorrectly, Arcserve will accept RMA and provide full credit; 2) If a defective item is returned within 30 days, Arcserve will accept RMA and provide full credit; and 3) If there are hardware technical issues that are unresolved by support after a reasonable period of time to resolve, Arcserve will accept RMA and provide a hardware swap for a unit of equivalent value.

Information needed for the RMA request:

- Product serial number (located on the back of the appliance)
- Arcserve Order Number
- Partner contact name
- Partner phone number
- Partner Email address
- Customer contact name (if available)
- Phone number (if available)
- Email address (if available)
- Description of problem and any troubleshooting already performed.
- Shipping service requested and shipping address.

The RMA number must be clearly marked on the outside of the packaging. All RMAs must be shipped using adequate packaging. All RMAs should be shipped using a reputable carrier that offers package tracking and insurance. Any shipping damage or lost RMAs is the responsibility of customer.

Table of Contents

Chapter 1: About Arcserve Appliance Documentation	1
Language Support	2
Product Documentation	3
Chapter 2: Introducing the Arcserve Appliance	5
Introduction	6
Arcserve Unified Data Protection	7
Arcserve Unified Data Protection Agent for Linux	8
Arcserve Backup	9
Arcserve Continuous Availability	10
Safety Precautions	11
What is Included in the Box	12
What is Included in the Box of Appliance 9000 Series	13
What is Included in the Box of Appliance X Series	13
What is Not Included in the Box	16
Available Models	17
Models 9012 - 9504DR	17
Model X Series	18
Controls and Indicators	21
Front Panel of 9012-9048	21
Front Panel of 9072DR - 9504DR	22
Front Panel of X Series	23
Rear Panel of 9012-9048	23
Rear Panel of 9072DR-9504DR	25
Rear Panel of X Series	26
Ports Used by the Appliance	27
Arcserve UDP	28
Components installed on Microsoft Windows	29
Components installed on Linux	34
Node protected by UDP Linux remotely	36
Arcserve Backup	37
Appliance for Linux Support	38
Chapter 3: Installing the Arcserve Appliance	39
How to Install Arcserve Backup 19.0	40

How to Install 9012-9048 Series Appliance	47
How to Install 9072-9504DR Series Appliance	48
How to Install X Series Appliance	48
Chapter 4: Upgrading Arcserve UDP on the Appliance	49
How to Apply a License After Upgrading Arcserve Software	50
Upgrade Sequence on Arcserve Appliance	51
Upgrade the Arcserve Appliance Used as Arcserve UDP Console and RPS	52
Upgrade the Arcserve Appliance Used as Arcserve UDP RPS	53
Upgrade Steps When Two or More Arcserve Appliance Are Used in the Environment	54
Upgrade the Arcserve UDP Linux Agent on the Arcserve Appliance	55
Upgrade the Arcserve Backup on the Arcserve Appliance	56
Upgrade Sequence for UDP Console, RPS, and Agent	57
Chapter 5: Configuring the Arcserve Appliance	58
How to Configure Network Settings for Arcserve Appliance	59
How to Set Up the Arcserve Appliance	63
Configure Arcserve Appliance as Gateway	73
Chapter 6: Working with Arcserve Appliance	74
Activate Arcserve Product on the Appliance	75
Create a Plan Using Arcserve Appliance Wizard	76
Add Nodes to a Plan	77
Add Nodes by Hostname/IP Address	78
Add Nodes by Active Directory	80
Add vCenter/ESX Nodes	82
Add Hyper-V Nodes	85
Create a Backup Plan for Linux Nodes	87
Create a Backup Plan to a Tape Device	88
Create an On-Appliance Virtual Standby Plan	89
Create Plan to Backup the Linux Backup Server	90
Setting-up to Perform Linux Instant VM Job to Local Appliance Hyper-V	94
Migrate Arcserve UDP Console Using ConsoleMigration.exe	95
Perform Migration between Arcserve Appliances	97
Solution 1	98
Solution 2	103
Modify the Input Source of Pre-installed Linux Backup Server	106
Chapter 7: Monitoring the Appliance Server Remotely	110
Working with Integrated Dell Remote Access Controller (iDRAC)	111

Monitor and Manage Integrated Dell Remote Access Controller (iDRAC)	112
Find the IP address of Integrated Dell Remote Access Controller for 9000 Series (iDRAC)	114
Find the IP address of Integrated Dell Remote Access Controller for X Series (iDRAC)	116
Configure DHCP or Static IP address of iDRAC	118
Chapter 8: Restoring or Repairing the Arcserve Appliance	124
Debug Factory Reset	125
Apply Arcserve UDP Factory Reset Using Boot Option in 9012-9504DR Series Appliance	127
Apply Arcserve UDP Factory Reset Using Boot Option in X Series Appliance	129
Clear Configuration and Apply Appliance Factory Reset	132
Replace Factory Reset Image Using Set Appliance Image Utility	134
Remove and Replace a Hard Drive	137
Perform Bare Metal Recovery (BMR) without Preserving Data	139
Perform Bare Metal Recovery (BMR) and Preserving Data	155
Chapter 9: Performing Appliance Capacity Expansion	163
Working with Arcserve Appliance Expansion Kit - X Series Models	163
Working with SSD Flash Expansion Kit in Arcserve X Series Appliance	167
Working with Expansion Kit in Arcserve Appliance 9072-9504 DR Models	177
Working with SSD Flash Expansion Kit in Arcserve Appliance 9072-9504 DR Models	182
Chapter 10: Working with Network Configuration	189
Understanding the Network Configuration Details	190
How to Disable DHCP Server	195
How to Configure IP Address for the Preinstalled Linux Backup Server	196
How to Enable Round Robin on the DNS Server to Balance Load	198
How to Check Network Status on Appliance	199
Chapter 11: Understanding Safety Precautions	200
General Safety Precautions	201
Electrical Safety Precautions	203
FCC Compliance	204
Electrostatic Discharge (ESD) Precautions	205
Chapter 12: Activating Sophos on the Arcserve Appliance for 9000 Series	206
Activate Sophos on the Arcserve Appliance using Email	207
Manually Installing Sophos Intercept X Advanced for Server on Arcserve UDP	208
Chapter 12: Activating Sophos on the Arcserve Appliance for X Series	212
Manually Installing Sophos Intercept X Advanced for Server on Arcserve UDP	212

Chapter 12: Upgrading Firmware for Arcserve Appliance 9000 Series	216
Upgrade BIOS Firmware for Arcserve Appliance 9000 Series	216
Viewing BIOS Firmware Version	216
Method 1: View BIOS firmware version from iDRAC Web Interface	216
Method 2: View BIOS firmware version from BIOS Arcserve Appliance 9000 series	217
Download the Updated Package for BIOS	218
Upgrade BIOS	218
Verify Updated BIOS	219
Verify Updated BIOS using System Logs	219
Verify Updated BIOS from iDRAC Web Interface or BIOS	220
Upgrade iDRAC Firmware for Arcserve Appliance 9000 Series	220
Viewing iDRAC Firmware Version	220
View iDRAC Firmware Version from iDRAC Web Interface	221
Method 2: View iDRAC Firmware Version from BIOS Arcserve Appliance 9000 series	221
How to Change the iDRAC Password	222
Download the Updated Package for iDRAC	224
Upgrade iDRAC	224
Verify Updated iDRAC	225
Verify Updated iDRAC using System Logs	225
Verify Updated iDRAC from iDRAC Web Interface or BIOS	226
Upgrade Firmware for Arcserve Appliance X Series	227
Upgrade BIOS Firmware for Arcserve Appliance X Series	227
Viewing BIOS Firmware Version	227
Method 1: View BIOS firmware version from iDRAC Web Interface	227
Method 2: View BIOS firmware version from BIOS Arcserve Appliance X series	228
Download the Updated Package for BIOS	229
Upgrade BIOS	229
Verify Updated BIOS	230
Upgrade iDRAC Firmware for Arcserve Appliance X Series	230
Viewing iDRAC Firmware Version	231
Method 1: View iDRAC firmware version from iDRAC Web Interface	231
Method 2: View iDRAC firmware version from BIOS Arcserve Appliance X series	232
Download the Updated Package for iDRAC	233
Upgrade iDRAC	233
Verify Updated iDRAC	234
Chapter 13: Troubleshooting	236

Linux Backup Server Fails to Connect from the Console	237
Backing Up Arcserve Appliance from Another Appliance Reports Duplicated Nodes.....	238
Linux Backup Server Cannot Communicate with Any Node in the Network	239
Linux Backup Server Cannot Get the Network DNS Suffix	241
Default Time Zone on the Appliance	242
Licenses Error even when the licenses are available	243
Chapter 14: Applying Best Practices	244
Best Practices for Network Configuration	245
Best Practices for Windows Defender with PowerShell cmdlets	248
Configure Preinstalled Linux Backup Server to External Network	248
Best Practices for replacing Factory Reset Image When Secured by Sophos	249
Best Practice for Creating Deduplication Datastore across Volumes	257
Chapter 15: Acknowledgements	260
PuTTY	261

Chapter 1: About Arcserve Appliance Documentation

Arcserve Appliance User Guide helps you understand how to use Arcserve Appliance. To understand about Arcserve Appliance, view Introduction. Rest of the sections help you install and use Arcserve Appliance.

This section contains the following topics:

Language Support	2
Product Documentation	3

Language Support

A translated product (sometimes referred to as a localized product) includes local language support for the user interface of the product, online help and other documentation, as well as local language default settings for date, time, currency, and number formats.

This release is available only in English.

Product Documentation

For all Arcserve UDP related documentation, click this link for the [Arcserve Documentation](#).

The Arcserve UDP Knowledge Center consists of the following documentation:

- **Arcserve UDP Solutions Guide**

Provides detailed information on how to use the Arcserve UDP solution in a centrally-managed Console environment. This guide includes such information as how to install and configure the solution, how to protect and restore your data, how to get reports, and how to manage Arcserve High Availability. Procedures are centered around use of the Console and includes how to use the various protection Plans.

- **Arcserve UDP Release Notes**

Provides high-level description of the major features, system requirements, known issues, documentation issues, and limitations of Arcserve Unified Data Protection.

- **Arcserve UDP Agent for Windows User Guide**

Provides detailed information on how to use Arcserve UDP Agent in a Windows operating system. This guide includes such information as how to install and configure the agent and how to protect and restore your Windows nodes.

- **Arcserve UDP Agent for Linux User Guide**

Provides detailed information on how to use Arcserve UDP Agent in a Linux operating system. This guide includes such information as how to install and configure the agent and how to protect and restore your Linux nodes.

Chapter 2: Introducing the Arcserve Appliance

This section contains the following topics:

Introduction	6
Safety Precautions	11
What is Included in the Box	12
What is Not Included in the Box	16
Available Models	17
Controls and Indicators	21
Ports Used by the Appliance	27

Introduction

Arcserve Appliance is the first complete and most cost-effective data protection appliance, featuring Assured Recovery™. Each Arcserve Appliance is a self-contained, "set and forget" backup and recovery solution. Architected with cloud-native capabilities, its unmatched ease of deployment and usability combine with a broad set of features such as global source-based deduplication, multi-site replication, tape support, and automated data recovery capabilities. The Arcserve Appliance delivers unmatched operational agility and efficiency, and truly simplifies disaster recovery activities.

Arcserve Appliance is fully integrated with the industry-leading Arcserve Unified Data Protection software pre-installed in state-of-the-art hardware. The appliance provides a complete and integrated data protection solution for all users to not only meet your current demands, but also the ever-changing backup, archive, and disaster recovery (DR) requirements of the future.

The following software are pre-installed in the Arcserve Appliance:

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

Arcserve Appliance is defined with Hardware Warranty. For more information about Appliance warranty, see [Appliance Warranty](#).

Arcserve Unified Data Protection

The Arcserve UDP software is a comprehensive solution to protect complex IT environments. The solution protects your data residing in various types of nodes such as Windows, Linux, and virtual machines on VMware ESX Servers or Microsoft Hyper-V Servers. You can back up data to either a local machine or a recovery point Server. A recovery point Server is a central Server where backups from multiple sources are stored.

For more information about supported operating systems, see [Compatibility Matrix](#).

Arcserve UDP provides the following capabilities:

- Back up the data to deduplication/non-deduplication datastores on recovery point Servers
- Back up recovery points to tape, using integration with Arcserve Backup (which is also included within the appliance)
- Create virtual standby machines from backup data
- Replicate backup data to recovery point Servers and remote recovery point Servers
- Restore backup data and performs Bare Metal Recovery (BMR)
- Copy selected data backup files to a secondary backup location
- Configure and manage Arcserve Full System High Availability (HA) for critical Servers in your environment

Arcserve UDP replicates backup data that is saved as recovery points from one Server to another recovery point Server. You can also create virtual machines from the backup data that can act as standby machines when the source node fails. The standby virtual machine is created by converting recovery points to VMware ESX or Microsoft Hyper-V virtual machine format.

The Arcserve UDP solution provides integration with Arcserve High Availability. After you create scenarios in Arcserve High Availability, you can then manage and monitor your scenarios and perform operations like adding or deleting destination machines.

For more information, see [Arcserve UDP Solution Guide](#).

Arcserve Unified Data Protection Agent for Linux

Arcserve Unified Data Protection Agent for Linux is a disk-based backup product that is designed for Linux operating systems. It provides a fast, simple, and reliable way to protect and recover critical business information. Arcserve Unified Data Protection Agent for Linux tracks changes on a node at the block level and then backs up only those changed blocks in an incremental process. As a result, it lets you perform frequent backups, reducing the size of each incremental backup (and the backup window) and providing a more up-to-date backup. Arcserve Unified Data Protection Agent for Linux also provides the capability to restore files or folders and perform a bare metal recovery (BMR) from a single backup. You can store the backup information either on a Network File System (NFS) share or in the Common Internet File System (CIFS) share, in the backup source node.

The latest version of Arcserve Unified Data Protection Agent for Linux is pre-installed in a virtual machine within the appliance. This virtual machine becomes the Linux Backup Server. Arcserve Unified Data Protection Agent for Linux is installed at the default installation path in the Arcserve Appliance.

When you open the Console, the Linux Backup Server is already added to the Console. The native host name of the Linux Backup Server is *Linux-BackupSvr*. However, on the Console, the Linux Backup Server adopts the host name of the Appliance with port 8018 configuration. The Linux Backup Server works behind NAT through port direction. The Linux Backup Server uses port 8018 to communicate and transfer data in the Arcserve Appliance.

Note: For more information about creating backup plans and restoring Linux machines, see [Arcserve UDP Agent for Linux User Guide](#).

The Linux Backup Server uses the following default login information:

- Username – root
- Password – Arcserve

Note: We recommend to change the default password.

Arcserve Backup

Arcserve Backup is a high-performance data protection solution that addresses the needs of businesses with heterogeneous environments. It provides flexible backup and restore performance, easy administration, broad device compatibility, and reliability. It helps you to maximize your data storage abilities that lets you customize your data protection strategies based on your storage requirements. In addition, the flexible user interface allows advanced configurations and provides a cost-effective way for users at all levels of technical expertise to deploy and maintain an extensive range of agents and options.

Arcserve Backup delivers comprehensive data protection for distributed environments and provides virus-free backup and restore operations. An extensive set of options and agents extends data protection throughout the enterprise and delivers enhanced functionality, including online hot backup and restore of application and data files, advanced device and media management, and disaster recovery.

Arcserve Appliance includes integration with Arcserve Backup for performing a backup to tape. Arcserve Backup gets installed in the following location "C:\Program Files (x86)\Arcserve" on your computer after you mount and install using the InstallASBU.iso file. The components installed in the Arcserve Appliance lets you back up the destination of Arcserve UDP to a tape. For more information about supported operating systems, see [Compatibility Matrix](#).

You can download the full installation package of Arcserve Backup from Arcserve website to install other components. For details, refer to Arcserve Backup [documentation](#).

Arcserve Backup Server uses the following default login information:

- Username -- caroot
- Password -- Arcserve

Arcserve Continuous Availability

Arcserve Continuous Availability is a solution based on asynchronous real-time replication and automated application switchover and switchback to provide cost-effective business continuity for virtual environments on Windows Servers. For more information about supported operating systems, see [Compatibility Matrix](#).

Arcserve Continuous Availability lets you replicate data to a local or remote Server, helping you to recover that data if you face a Server crash or site disaster. You may switch your users to the replica Server manually or automatically if you have licensed High Availability.

Note: Arcserve Continuous Availability is not pre-installed in the Appliance. For more information about how to install and configure Arcserve Continuous Availability, see [Installation Guide](#)

Safety Precautions

For your safety, please read and follow all instructions before attempting to unpack, connect, install, power on, or operate an Arcserve Appliance. Failure to adhere to the safety precautions can result in personal injury, equipment damage, or malfunction.

For more information about the safety precautions, see the [Safety Precautions Appendix](#).

What is Included in the Box

This section describes what is included in the box of following Appliance series:

- [9000 Series](#)
- [X Series](#)

What is Included in the Box of Appliance 9000 Series

Arcserve Appliance 9000 series contains two boxes: One for 9012, 9024, 9048 and other for 9072DR-9504DR. Below list provides included items in both the boxes.

The following items are included in the 9012, 9024, 9048 Accessory box:

- BEZEL,1U Box, CUS 14G BEZEL ASSEMBLY, LCD, AR, (380-7406)
- QUICK START GUIDE, ARCSERVE, READ ME FIRST SHEET ARCSERVE APPLIANCE
- HARDWARE INSTALLATION GUIDE ARCSERVE DELL R440
- CABLE, FLEXBOOT,CAT6,NETWORK,3FT,RED
- CABLE, FLEXBOOT,CAT6,NETWORK,3FT,BLUE
- CABLE, FLEXBOOT,CAT6,NETWORK,7FT,BLACK
- Dell Safety, Environment, Regulatory book
- US Power cords (2x)a

Note: Inspect the box that the appliance was shipped in and ensure that no items are missing from the box and that there are no visible signs of damage. If any items are missing or damaged, retain all packaging materials and contact [Arcserve Support](#).

The following items are included in the 9072DR-9504DR Accessory box with a Rack Rail kit:

- BEZEL, 2U Box, CUS 14G BEZEL ASSEMBLY, LCD, AR, (380-7405)
- QUICK START GUIDE, ARCSERVE, READ ME FIRST SHEET ARCSERVE APPLIANCE
- HARDWARE INSTALLATION GUIDE ARCSERVE DELL R740
- CABLE, FLEXBOOT,CAT6,NETWORK,3FT,RED
- CABLE, FLEXBOOT,CAT6,NETWORK,3FT,BLUE
- CABLE, FLEXBOOT,CAT6,NETWORK,7FT,BLACK
- CABLE ASSMBLY, MINI-SAS, EXTERNAL, SFF-8088 TO SFF-8644, 1M
- Dell Safety, Environment, Regulatory book
- US Power cords (2x)

What is Included in the Box of Appliance X Series

Arcserve Appliance X series contains the following items:

- **Appliance X Series Compute Node:**

- ♦ MICROSOFT
- ♦ WIN SVR EMB STD 2019 16-CORE

Compute Node Accessory box:

- ♦ Windows 4-Core Expansion Licenses (qty 10)
- ♦ HARDWARE SETUP GUIDE, ARCSERVE R740
- ♦ QUICK START GUIDE, ARCSERVE, READ ME FIRST SHEET UDP APPLIANCE
- ♦ ASSEMBLY, ARCSERVE SOPHOS 2U BEZEL WITH 2 COLOR BUBBLE BADGE
- ♦ Dell Safety Documentation
- ♦ Power Cords (qty 2) US or Country Specific, if ordered
- ♦ Rack Mount Slide Rail Kit
- ♦ Cable Management Arm
- ♦ Optional components, if ordered:
 - SFPs
 - SAS cable
 - DAC cable

Note: The following will be attached to the front of the Array: Arcserve ME4084 painted bezel and bubble badge assembly.

- **Appliance X series Storage Node**

The 5U storage system box includes the following:

- ♦ Documentation
- ♦ 5U storage appliance enclosure
- ♦ Two power cables
- ♦ Separately packaged disk drives (5U enclosure only)
- ♦ Fibre Channel or iSCSI SFP+ transceivers or cables (one per host port)
- ♦ Host cables (1 per controller module host port)
- ♦ Expansion cables (1 per expansion module)
- ♦ Optional enclosure bezel set with key (1 per 5U enclosure)
- ♦ Appropriate rackmount kit for 5U storage system enclosure

ME4084 Accessory boxes:

- ♦ HARDWARE SETUP GUIDE, ARCSERVE ME4084
- ♦ Rack Mount Slide Rail Set
- ♦ C19 to C20, PDU Style, 2.5M Power Cord (qty 2)
- ♦ Serial Cable
- ♦ 12Gb HD-Mini to HD-Mini SAS Cable, 2M (qty 4)
- ♦ Storage Array Regulatory Info doc
- ♦ Setting Up Your Storage Array doc
- ♦ Safety and Environmental Info doc
- ♦ Bezel Removal Wrench
- ♦ Unused drive number labels

Note: The Hard Drives are in a separate box under the Array.

Note: Inspect the box that the appliance was shipped in and ensure that no items are missing from the box and that there are no visible signs of damage. If any items are missing or damaged, retain all packaging materials and contact [Arcserve Support](#).

What is Not Included in the Box

The following items are not included in the box and may be needed for installation and configuration of the appliance:

- Monitor
- Keyboard
- External Storage Device (if needed)

Available Models

The Arcserve Appliance 9000 series and X series are available in a variety of different models designed to meet your specific needs:

- [Models 9012 - 9504 DR](#)
- [Model X Series](#)

Models 9012 - 9504DR

Arcserve Appliance Models 9012 - 9504DR

Arcserve Appliance 9000 Series Specifications											
Appliance Model	9012	9024	9048	9072-DR	9096-DR	9144-DR	9192-DR	9240-DR	9288-DR	9360-DR	9504DR
Usable capacity	4 TB	8 TB	16 TB	24 TB	32 TB	48 TB	64 TB	80 TB	96 TB	120 TB	168 TB
Source Backup	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 drive	480GB SSD			2 x 1.9 TB SSD (RAID1)							
Processor	Intel Xeon Silver 4108, 8-CORE, 1.8 GHz			Intel Xeon Silver 4114, 10-CORE, 2.2 GHz							
Number of Processors	1			2							
RAID Card	PERC H730P Low Profile, adaptor, 2 GB NV Cache			PERC H730P, MiniCard, 2 GB NV Cache							
RAID Configuration	RAID-5			RAID-6							
Drive Bays	4			16							
Expansion	NA			11	10	8	6	4	6	4	NA

Kit												
RAID 2	NA			6								
Drives	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 Cards	On-Board Broadcom 5720 Dual Port 1Gb LOM			Broadcom 5720 QP 1Gb Network Daughter Card SAS 12Gbps HBA External Controller							Broadcom 5720 QP 1Gb SAS 12Gbps HBA External Dual Port 10G Base-T Copper	
PCIe Cards (Factory Option)	SAS 12Gbps HBA External Controller Broadcom 5719 Quad-Port 1G NIC Dual-Port 10G Copper Dual-Port 10G SFP+ Dual-Port FC 16G HBA			Dual-Port 10G Copper Dual-Port 10G SFP+ Dual-Port FC 16G HBA							Dual-Port 10G SFP+ Dual-Port FC 16G HBA	
Power Supplies	Dual, Hot-Plug, Redundant Power Supply (1+1), 550 W			Dual, Hot-Plug, Redundant Power Supply (1+1), 750 W								
iDRAC Enterprise	1											

Model X Series

Arcserve Appliance Model X Series

Arcserve Appliance X Series Specifications					
Appliance Model	X1000DR	X1500DR	X2000DR	X2500DR	X3000DR
Effective Capacity (TB) ¹	1,056	1,584	2,112	2,640	3,168
Maximum Effective Capacity with Expansion Kits (TB) ¹	3,168				
Note: Effective capacity takes global source deduplication into account and is approximately 3x the usable capacity of the HDDs and does not include SSDs. The actual backup capacity may vary based on factors such as data types, backup type, schedule, and so on.					
Disk Imaging and Disaster Recovery Software	Arcserve UDP Premium Edition included				
Tape Integration Software	Arcserve Backup included				
Cybersecurity Software	Sophos Intercept X Advanced for Server included				
Continuous Availability with Automated Failover	Arcserve Continuous Availability optional				
Optional Cloud Backup and Disaster Recovery Add-on	Arcserve UDP Cloud Hybrid Secured by Sophos				
Compute Node					
CPU	Dual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)				
Default 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) and 6 x 4TB (RAID-5)				
Drive Bays	24x 2.5” Enterprise NVMe SSD				
SAS 12Gbps HBA External Controller	2x Included				
Intel X550 Quad Port 10G Base-T Adapter	Included				
Broadcom 57414 Dual Port 25Gb SFP28 Adapter	Optional				
Intel X710 Dual Port 10G SFP+ FC Adapter	Optional				
QLogic 2692 Dual Port 16Gb Fibre Channel HBA	Optional				
Remote Hardware Management	iDRAC Enterprise Included				
Power Supplies	Dual, Hot-plug, Redundant Power Supply (1+1), 1100W				

Heat Dissipation	4100 BTU/hr				
Weight	75lbs (34kg)				
Form Factor	2U				
In-rack Dimensions (excludes bezel, front panel, and power supply handles)	26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)				
Outer Dimensions (includes bezel, front panel, and power supply handles)	29.6" x 19.0" x 3.4" (75.1 cm x 48.2 cm x 8.7cm)				
Packaging Dimensions	38" x 26" x 12" (97cm x 66cm x 30cm)				
Storage Node					
16TB SAS 12G Hot-Plug HDD	28	42	56	70	84
Minimum Usable Capacity	352	528	704	880	1056
Linear Expansion Capability with Optional Kits	✓	✓	✓	✓	
RAID Level	RAID-ADAPT				
RAID Controller	Dual 8-port SAS 12Gb Controller				
Hot-spare space on HDDs	Up to 64 TB				
Power Supplies	Dual, Redundant (1+1), 2200W				
Heat Dissipation	7507 BTU				
Weight	From 141lbs (64kg) to 298lbs (135kg)				
Form Factor	5U				
Outer Dimensions (includes bezel, front panel, and power supply handles)	38.31" x 19.01" x 8.75" (97.47cm x 48.30cm x 22.23cm)				

Controls and Indicators



The Arcserve Appliance contains several controls and indicators (LEDs) on the front and rear panels and on each drive carrier. These controls and indicators provide the capability to control various functions and a quick-view reference of the status of the appliance and components:

Front Panel of 9012-9048

The front panel of the Arcserve Appliance contains control panel buttons, control panel LEDs, and drive carrier LEDs. The following table describes these items:



Number	Control / Indicator	Icon	Description
1	Left control panel	NA	<p>Contains the system health and system ID, status LED, and the iDRAC Quick Sync 2 (wireless) indicator.</p> <p>NOTE: The iDRAC Quick Sync 2 indicator is available only on certain configurations.</p> <ul style="list-style-type: none"> • Status LED: Enables you to identify any failed hardware components. There are up to five status LEDs and an overall system health LED (Chassis health and system ID) bar. For more information, see link. • Quick Sync 2 (wireless): Indicates a Quick Sync enabled system. The Quick Sync feature is optional. This feature allows management of the system by using mobile devices. This feature aggregates hardware or firmware inventory and various system level diagnostic and error information that can be used in troubleshooting the system. For

			more information, see link .
2	Drive slots	NA	Enable you to install drives that are supported on your system. For more information about drives, see link .
3	Optical drive (optional)	NA	One optional slim SATA DVD-ROM drive or DVD+/-RW drive.
4	VGA port		Enables you to connect a display device to the system.
5	USB port (optional)		The USB port is USB 2.0 compliant.
6	Right control panel	NA	Contains the power button, USB port, iDRAC Direct micro port, and the iDRAC Direct status LED.
7	Information Tag	NA	The Information Tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on. If you have opted for the secure default access to iDRAC, the Information tag also contains the iDRAC secure default password.

Front Panel of 9072DR - 9504DR

The front panel of the Arcserve Appliance contains control panel buttons, control panel LEDs, and drive carrier LEDs. The following table describes these items:



Number	Control / Indicator	Icon	Description
1	Left control panel	NA	Contains system health and system ID, status LED or optional iDRAC Quick Sync 2 (wireless).
2	Drive slots	NA	Enable you to install drives that are supported on your system. For more information, see link .

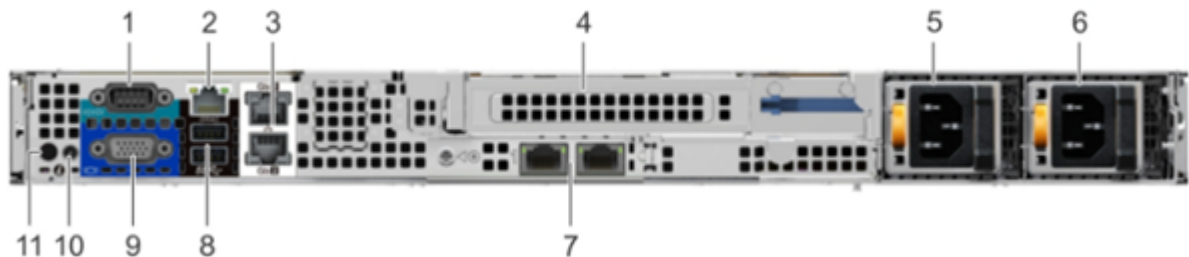
3	Right control panel	NA	Contains the power button, VGA port, iDRAC Direct micro USB port and two USB 2.0 ports.
4	Information tag	NA	The Information Tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on. If you have opted for the secure default access to iDRAC, the Information tag also contains the iDRAC secure default password.


Front Panel of X Series





For more information about the Front Panel, see [Appliance Installation of X Series - Compute Node](#) and [Appliance Installation of X Series - Storage Node](#).

Rear Panel of 9012-9048

The rear panel of the Arcserve Appliance contains the power supplies, cable connections, and ports for the appliance. The following table describes these items:

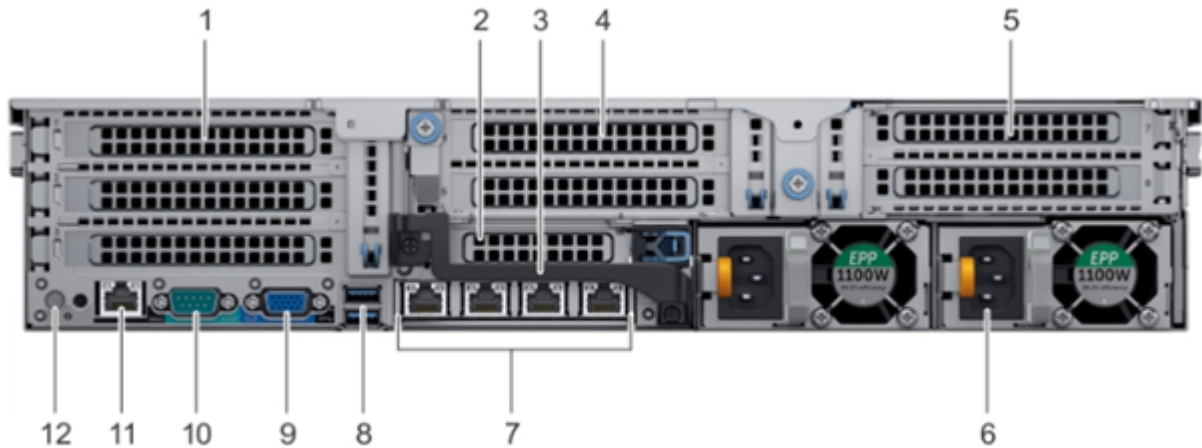



Number	Control / Indicator	Icon	Description
1	Serial port	IOIOI	Use the serial port to connect a serial device to the system. For more information, see link .
2	iDRAC9 dedicated network port		Use the iDRAC9 dedicated network port to securely access the embedded iDRAC on a separate management network. For more information, see link .
3	Ethernet ports (2)		Use the Ethernet ports to connect Local Area Networks (LANs) to the system. For more information, see link .
4	Full height riser slot		Use the card slots to connect full-height PCIe expansion cards on full height riser.
5	Power supply unit		For more information about the PSU con-






	(PSU)		figurations, see link .
6	Power supply unit (PSU)		For more information about the PSU configurations, see link .
7	LOM riser ports (2)		For more information about the PSU configurations, see link .
8	USB 3.0 port (2)		Use the USB 3.0 port to connect USB devices to the system. These ports are 4-pin, USB 3.0-compliant.
9	VGA port		Use the VGA port to connect a display to the system.
10	CMA power port		The Cable Management Arm (CMA) power port enables you to connect to the CMA.
11	System identification button		<p>Press the system ID button:</p> <ul style="list-style-type: none"> • To locate a particular system within a rack. • To turn the system ID on or off. <p>To reset iDRAC, press and hold the button for 15 seconds.</p> <p>Notes:</p> <ul style="list-style-type: none"> • To reset iDRAC using system ID, ensure that the system ID button is enabled in the iDRAC setup. • If the system stops responding during POST, press and hold the system ID button (for more than five seconds) to enter the BIOS progress mode.

Rear Panel of 9072DR-9504DR

The rear panel of the Arcserve Appliance contains the power supplies, cable connections, and ports for the appliance. The following table describes these items:



Number	Control / Indicator	Icon	Description
1	Full-height PCIe expansion card slot (3)	NA	The PCIe expansion card slot (riser 1) connects up to three full-height PCIe expansion cards to the system. For more information, see link .
2	Half-height PCIe expansion card slot	NA	The PCIe expansion card slot (riser 2) connects one half-height PCIe expansion cards to the system. For more information, see link .
3	Rear handle	NA	The rear handle can be removed to enable any external cabling of PCIe cards that are installed in the PCIe expansion card slot 6.
4	Full-height PCIe expansion card slot (2)	NA	The PCIe expansion card slot (riser 2) connects up to two full-height PCIe expansion cards to the system. For more information, see link .
5	Full-height PCIe expansion card slot (2)	NA	The PCIe expansion card slot (riser 3) connects up to two full-height PCIe expansion cards to the system. For more information, see link .
6	Power supply unit (2)	NA	For more information, see link .
7	NIC ports		The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity. For more information about the supported configurations, see link .

8	USB port (2)		The USB ports are 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system.
9	VGA port		Enables you to connect a display device to the system. For more information, see link .
10	Serial port		Enables you to connect a serial device to the system. For more information, see link .
11	iDRAC9 dedicated port		Enables you to remotely access iDRAC. For more information, see link .
12	System identification button		The System Identification (ID) button is available on the front and back of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step through mode.

Rear Panel of X Series

For more information about the Rear Panel, see [Appliance Installation of X Series - Compute Node](#) and [Appliance Installation of X Series - Storage Node](#).

Ports Used by the Appliance

The following topics provide information about ports that are used by Arcserve UDP, Arcserve Backup, and the Appliance for Linux Support:

- [Arcserve UDP](#)
- [Arcserve Backup](#)
- [Appliance for Linux Support](#)

Arcserve UDP

This section contains the following topics:

- [Components installed on Microsoft Windows](#)
- [Components installed on Linux](#)
- [Production node protected by UDP Linux remotely](#)

Components installed on Microsoft Windows

The following ports are required for backup and other jobs when you have a LAN environment:

Port #	Port Type	Initiated by	Listening Process	Description
1433	TCP	Remote Java	sqlservr.exe	Specifies the default communication port between the Arcserve UDP console and Microsoft SQL Server databases when they reside on different computers. Note: You can modify the default communication port when installing SQL Server.
4090	TCP	Arcserve UDP Agent	HATransServer.exe	Transfers data for Virtual Standby tasks in the proxy mode.
5000-5060	TCP	Arcserve UDP Server	GDDServer.exe	Reserved for Arcserve UDP RPS Global Deduplication datastore Service (GDD). One Arcserve UDP GDD datastore will use 3 free ports that

				start from 5000. It is needed when the datastore with GDD is enabled for backup or the restore task is used.
6052	TCP	Arcserve Backup GDB	CA.ARCserve.CommunicationFoundation.WindowsService.exe	Communication that lets the Arcserve UDP Console and the Arcserve Backup Global Dashboard Primary Server synchronize data.
6054	TCP	Arcserve Backup	CA.ARCserve.CommunicationFoundation.WindowsService.exe	Communication that lets the Arcserve UDP Console and the Arcserve Backup Primary Server synchronize data.
8006				To shut down Tomcat that is used by the Arcserve UDP console.
8014	TCP	Arcserve UDP Console	Tomcat7.exe	Specifies the default HTTP/HTTPS communication port between remote management consoles and the Arcserve UDP

				<p>Server.</p> <p>Specifies the default HTTP/HTTPS communication port between remote management consoles and the Arcserve UDP Agent.</p> <p>Note: You can modify the default communication port when you install the Arcserve UDP components.</p>
8014	TCP	Arcserve UDP Server	httpd.exe	<p>Specifies the default HTTP/HTTPS communication port between the Arcserve UDP Server and Arcserve UDP consoles.</p> <p>*Specifies the default shared port and the only port you must open when you use the Arcserve UDP Server as the replication destination.</p> <p>Do not open ports 5000-5060 which are used by datastores</p>

				that have global deduplication enabled. Note: You can modify the default communication port when you install the Arcserve UDP components.
8015	TCP	Arcserve UDP Console	Tomcat7.exe	Specifies the default HTTP/HTTPS communication port between remote management consoles and the Arcserve UDP Server. Specifies the default HTTP/HTTPS communication port between remote management consoles and the Arcserve UDP Agent. Note: You can modify the default communication port when you install the Arcserve UDP components.
8016	TCP	Arcserve UDP Server	Tomcat7.exe	Reserved for Arcserve UDP

				Server Web Services to communicate with the Arcserve UDP RPS Port Sharing Service on the same Server. Note: The port cannot be customized and can be ignored for the firewall setting.
1800-5			CA.ARCserve.CommunicationFoundation.WindowsService.exe	To shutdown Tomcat that is used by the Arcserve UDP Server or Agent.

Components installed on Linux

The following ports are required for backup and other jobs when you have a LAN environment:

Port #	Port Type	Initiated by	Listening Process	Description
22	TCP	SSH service		Arcserve UDP Linux third party dependency. Specifies the default for SSH service, however, you can change this port. This port is required for both incoming and outgoing communications.
67	UDP	Arcserve UDP Linux	bootpd	Used for the PXE boot Server. Only required if the user wants to use the PXE boot feature. This port is required for incoming communications. Note: The port number cannot be customized.
69	UDP	Arcserve UDP Linux	tftpd	Used for the PXE boot Server. Only required if the user wants to use the PXE boot feature. This port is required for incoming communications. Note: The port number cannot be customized.
8014	TCP	Arcserve UDP Linux	Java	Specifies the default HTTP/HTTPS communication ports between the remote consoles and the Arcserve UDP agent for Linux. This port is required for both incoming and outgoing communications.
18005	TCP	Arcserve UDP Linux	Java	Used by Tomcat, can be ignored for firewall set-

				tings.
--	--	--	--	--------

Node protected by UDP Linux remotely

The following port is required for backup and other jobs when you have a LAN environment:

Port #	Port Type	Initiated by	Listening Process	Description
22		SSH service		Arcserve UDP Linux 3rd party dependency. Specifies the default for the SSH service, however, you can change this port. This port is required for both incoming and outgoing communications.

*Port sharing is supported for replication jobs. All data on different ports can be forwarded to port 8014 (default port for the Arcserve UDP Server, which can be modified during installation). When a replication job runs between two recovery point Servers across WAN, only port 8014 needs to be opened.

Similarly, for remote replications, the Remote administrator needs to open or forward port 8014 (for data replication) and port 8015 (default port for the Arcserve UDP console, which can be modified during installation) for local recovery point Servers to obtain the assigned replication plan.

Arcserve Backup

The following ports are required for backup and other jobs when you have a LAN environment:

Port #	Port Type	Initiated by	Listening Process	Description
135	TCP			Microsoft Port Mapper
445	TCP		MSRPC over the 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	CAS TapeEngine	Tapeng.exe	Arcserve Tape Engine
6503	TCP	CAS JobEngine	Jobengine.exe	Arcserve Job Engine
6504	TCP	CAS DBEngine	DBEng.exe	Arcserve Database Engine
7854	TCP	CAS portmapper	Catirpc.exe	Arcserve PortMapper
41523	TCP	CAS Discovery	casdscsvc.exe	Arcserve Discovery Service
41524	UDP	CAS Discovery	casdscsvc.exe	Arcserve Discovery Service
9000-9500	TCP		For other Arcserve MS RPC services that use dynamic ports	

Appliance for Linux Support

The following ports are required for backup and other jobs when you have a LAN environment:

Port #	Port Type	Initiated by	Listening Process	Description
8017	TCP			NAT port redirection, redirects 8017 on appliance to the Linux backup server in order to backup other Linux node to Amazon S3.
8018	TCP			NAT port redirection, redirects 8018 on appliance to the Linux Backup Server Agent port 8014.
8019	TCP			NAT port redirection, redirects 8019 on appliance to the Linux Backup Server SSH port 22.
8021	TCP			NAT port redirection, redirects 8021 on appliance to Linux backup server to backup other Linux node using 8021 port.
8036	TCP			NAT port redirection, redirects 8036 on appliance to the Linux Backup Server port 8036.
50000	TCP			NAT port redirection, redirects 50000 on appliance to Linux backup server in order to backup other Linux node to cloud using 50000 port.
50001	TCP			NAT port redirection, redirects 50001 on appliance to Linux backup server in order to backup other Linux node to cloud using 50001 port.
50002	TCP			NAT port redirection, redirects 50002 on appliance to Linux backup server in order to backup other Linux node to cloud using 50002 port.
50003	TCP			NAT port redirection, redirects 50003 on appliance to Linux backup server in order to backup other Linux node to cloud using 50003 port.
50004	TCP			NAT port redirection, redirects 50004 on appliance to Linux backup server in order to backup other Linux node to cloud using 50004 port.

Chapter 3: Installing the Arcserve Appliance

This section contains the following topics:

How to Install Arcserve Backup 19.0	40
How to Install 9012-9048 Series Appliance	47
How to Install 9072-9504DR Series Appliance	48
How to Install X Series Appliance	48

How to Install Arcserve Backup 19.0

Arcserve Backup 19.0 is not pre-installed on the appliance. To install Arcserve Backup 19.0, mount the InstallASBU.iso file located on your desktop.

Follow these steps:

1. On your desktop, locate and mount the **InstallASBU.iso** file, navigate to the application Setup, and then run the setup as an administrator.

From the right column on the Product Installation Browser, click Install Arcserve Backup for Windows.

The Prerequisite Components dialog opens.

2. Click Install to install the Prerequisite Components.

Be aware of the Prerequisite Components dialog that opens only if Setup does not detect Arcserve Backup Prerequisite Components installed on the target computer.

Note: If you are installing Arcserve Backup on the active node in a cluster-aware environment, the cluster resources are transferred from the active node to the passive node while the active node restarts. After the active node restarts, you should transfer the cluster resources back to the original active node.

3. On the License Agreement dialog, accept the terms of the Licensing Agreement and click Next.
4. Follow the prompts and complete all required information on the subsequent dialogs.

The following list describes dialog-specific information about installing Arcserve Backup.

Select Install/Upgrade Type dialog

When you select the remote installation option, you can install Arcserve Backup on multiple systems.

With remote installations, the target remote systems can consist of different Arcserve server types, different Arcserve Backup agents and options, or both.

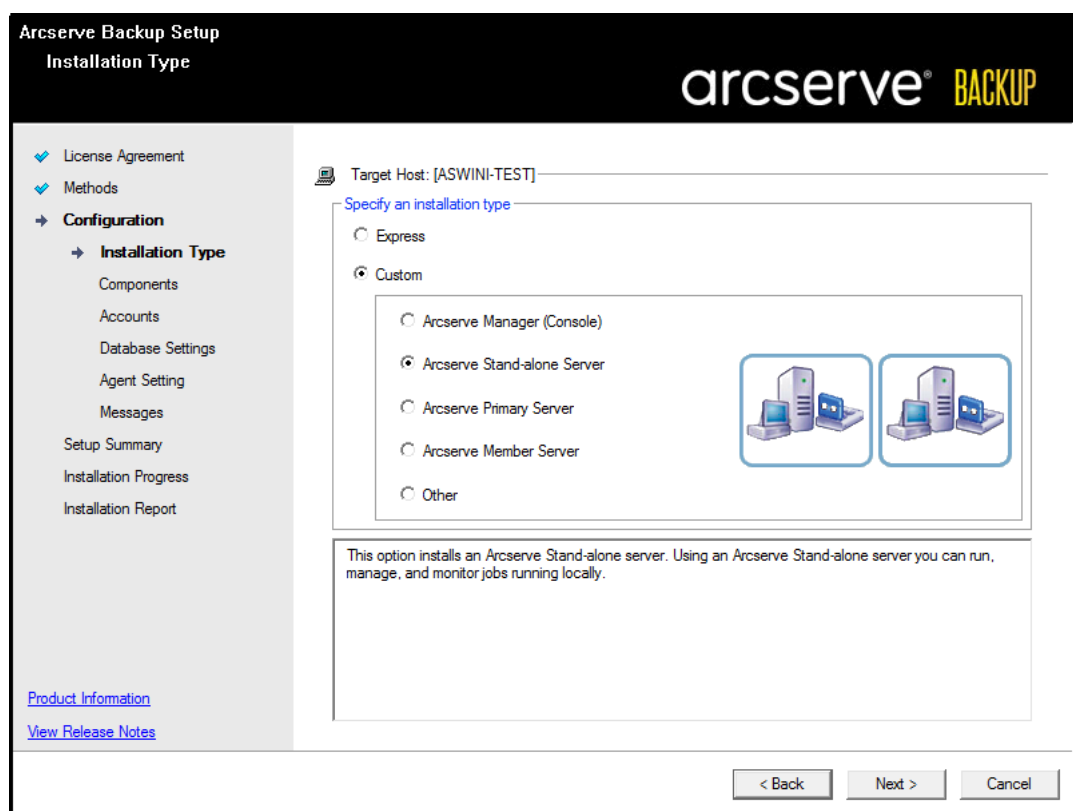
Note: The setup program for cluster machines does not support remote installation of the Arcserve Backup base product or the Arcserve Backup agents. This remote install limitation for the Arcserve Backup agents (for example, the Agent for Microsoft SQL Server and the Agent for Microsoft Exchange Server) only applies if you use a virtual host. Remote

installation of Arcserve Backup agents using the physical hosts of clusters is supported.

Installation Type dialog

Lets you specify the type of Arcserve Backup components that you want to install, by selecting either the Express or Custom installation type.

Note: When you upgrade from a previous release, the installation wizard detects your current Arcserve configuration and selects the Install-ation/Upgrade type that is appropriate for your new installation. For more information, see [Types of Arcserve Backup Server Installations](#) and [Arcserve Backup Server Options](#).



Components dialog

Lets you specify the Arcserve Backup components that you want to install on the target system.

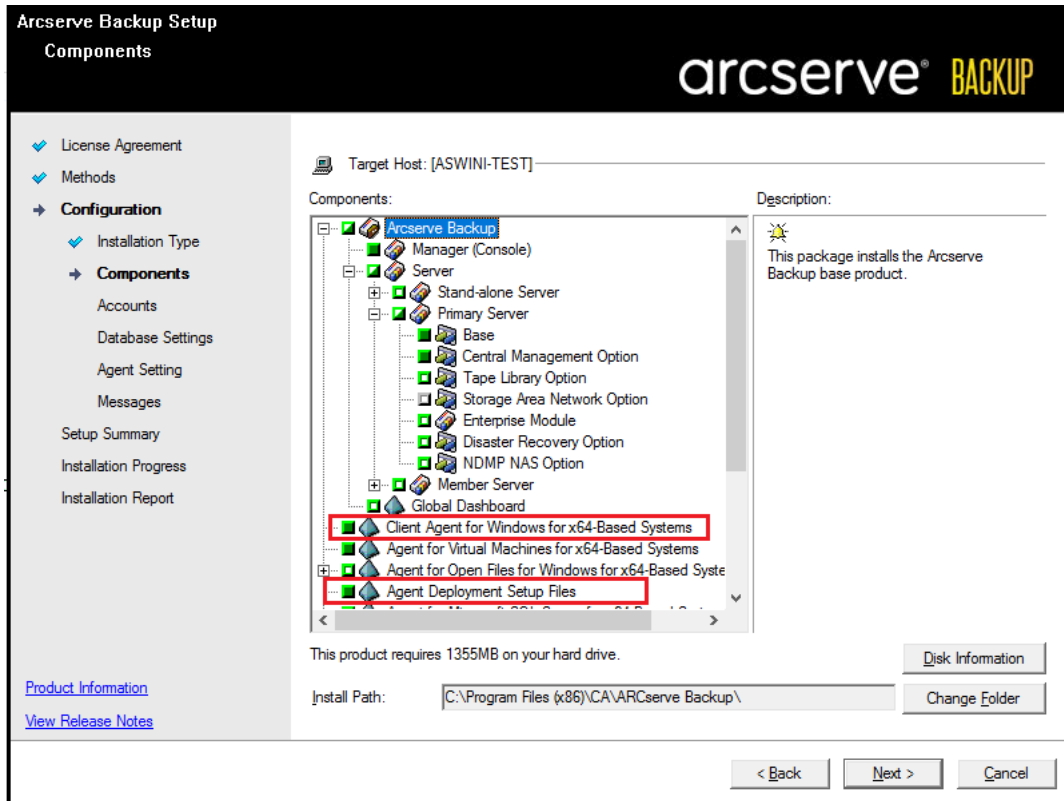
Be aware of the following considerations:

- ♦ To install a primary server, you must install the Arcserve Backup Central Management Option on the primary server.
- ♦ To install member servers, the installation wizard must be able to detect the Arcserve Backup domain name and primary server name in your network.

Therefore, you should complete at least one primary server installation before you perform member server installations.

- ♦ When you click the Arcserve Backup object or the Server object on the Select Products dialog, the installation wizard specifies the default Stand-alone Server installation components, regardless of the installation type that you specified on the Select Install/Upgrade Type dialog. To ensure that you are installing the correct components, expand the Server object, expand the object for the type of Arcserve Backup server that you want to install, and check the check boxes corresponding to the components that you want to install.
- ♦ Agent Deployment is a wizard-like application that lets you install or upgrade Arcserve Backup agents on multiple remote systems, after you install Arcserve Backup. To support this capability, Setup must copy Setup source files to the Arcserve Backup server. To copy the contents of the installation media to the Arcserve Backup server, you must select Agent Deployment on the Components dialog. When you select Agent Deployment, the length of time required to install or upgrade Arcserve Backup increases significantly.
- ♦ If you are performing a remote installation or a silent installation, do not install the Arcserve Backup Client Agent for Windows into the same directory as the Arcserve Backup base product.
- ♦ Global Dashboard can be installed on primary servers, stand-alone servers, and member servers. However, you cannot configure member servers to function as Central Primary Servers and Branch Primary Servers. For more information about Central Primary Servers and Branch Primary Servers, see the [Dashboard User Guide](#).
- ♦ On computers running Windows Server Core, you can install only the following Arcserve Backup products:
 - Member Server and supported options
 - Agent for Open Files
 - Agent for Virtual Machines
 - Client Agent for Windows
 - Disaster Recovery Option

The following diagram illustrates the default installation path for the Client Agent for Windows and Agent Deployment is specified:



Accounts dialog

Lets you set up your Arcserve Backup accounts and provides you an option to enable **Install Arcserve Backup Web Service**.

If Setup detects a cluster-aware application running in your environment, and you want to install Arcserve Backup in the cluster-aware environment, check the Cluster Environment Installation option and specify the path to the shared disk where you want to install Arcserve Backup.

Note: Arcserve Backup server names and Arcserve Backup domain names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.

Arcserve Backup Setup
Accounts
Specify the Arcserve Backup Domain you want to setup.

arcserve[®] BACKUP

Target Host: [ASWINI-TEST]

Specify a Windows administrative account

Microsoft Windows Domain: TEST

Microsoft Windows User Name: Administrator

Password:

Specify a Arcserve Backup domain account

Arcserve Backup Domain: TEST

Arcserve Backup Server: TEST

User Name: caroot

Password:

Confirm Password:

☐ Remember password

☒ Install Arcserve Backup Web Service

Web Service Settings

Port: 8020

< Back Next > Cancel

The Arcserve Backup web service works as a bridge between UDP Copy to Tape task and Arcserve Backup. By default the **Install Arcserve Backup Web Service** is enabled when you install Arcserve Backup. The default port number for the **Web Service Settings** is 8020. You can modify or the change the port number.

Clear the **Install Arcserve Backup Web Service** check box to disable the Arcserve Backup web service.

You can enable/modify the **Install Arcserve Backup Web Service** post installation of Arcserve Backup.

Note: Specify the same port number when you install Arcserve Backup web service on all servers of the Arcserve Backup domain. Arcserve UDP uses the same port number to connect to both the servers, the Arcserve Backup Primary server and the Member server in the Arcserve Backup domain.

Follow these steps:

1. Navigate to the Arcserve Backup base installation path from the command line.

- In the command prompt type the following command:

Bconfig -c

<Arcserve Backup> Accounts dialog opens.

- Configure or update the web service.

Database Settings dialog

Lets you configure the Arcserve Backup database.

After you specify a database application (Arcserve Backup Default Database or Microsoft SQL Server) complete the required fields on this dialog and click Next.

Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that Arcserve Backup can search and sort the data. To do this, click East Asian collation and then select a language from the drop-down list.

Arcserve Backup Setup
Database Settings
 The database stores critical information about Arcserve Backup and its operations.

arcserve® BACKUP

Target Host: [-TEST]

Choose a database type: [Arcserve Default Database]

Specify the installation path for Arcserve default database:

- ☒ Default installation path: C:\Program Files (x86)\Microsoft SQL Server
- ☐ Select a custom path: []

Data file path for Arcserve default database:

- ☒ Default installation path: C:\Program Files (x86)\Microsoft SQL Server\MSSQL12.ARCSEVERE_DB\MSSQL\DATA
- ☐ Select a custom path: []

SQL Language Collation Setting:

- ☒ Default collation
- ☐ East Asian collation: [Chinese_PRC]

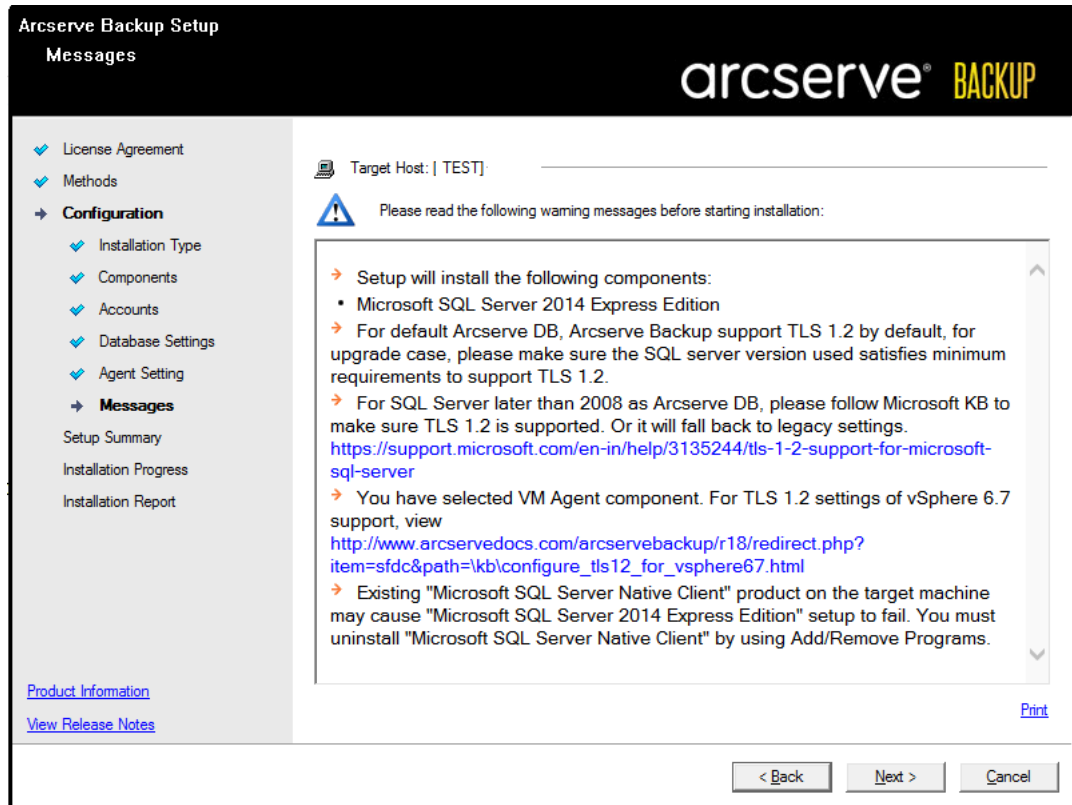
Installation Path for Catalog Files: [C:\Program Files (x86)\CA\ARCserve Backup\CATALOG.DB\]

< Back Next > Cancel

Messages dialog

As you review the messages in the Messages dialog, you should attempt to resolve the problems at this time.

The following graphic illustrates the Important Warning Messages dialog:



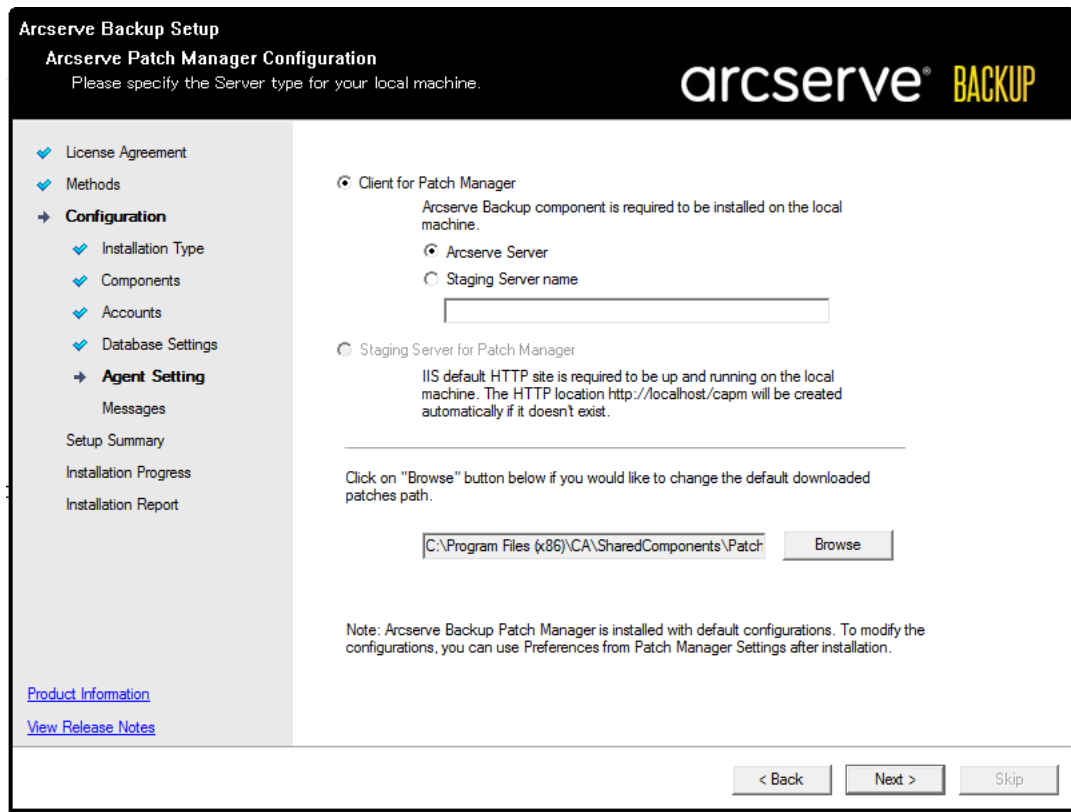
Setup Summary dialog

To modify the components that you want to install, click Back as often as necessary to return to the dialog containing the installation options that you want to change.

Installation Report dialog

If any components you select require configuration, Setup displays the necessary configuration dialogs at the end of the installation. You can configure the component immediately or configure it later using Device Configuration or Enterprise Module Configuration. For example, if you are using a single-drive autoloader that requires configuration, Setup lets you start Device Configuration by double-clicking the message for it on the Install Summary dialog.

The diagram that follows illustrates the Installation Report dialog. The Agent for Microsoft SQL Server requires configuration.



Note: You may be required to restart the server after you install Arcserve Backup. This depends on whether all of the files, services, and registry settings have been updated on the operating system level.

Installation Summary dialog

If any components you select require configuration, Setup displays the necessary configuration dialogs at the end of the installation. You can configure the component immediately or configure it later using Device Configuration or Enterprise Module Configuration. For example, if you are using a single-drive autoloader that requires configuration, Setup lets you start Device Configuration by double-clicking the message for it on the Install Summary dialog.

5. Click Finish on the Installation Summary dialog to complete the installation.

How to Install 9012-9048 Series Appliance

The appliance is intended for installation in restricted areas only. Only qualified personnel should perform Initial setup and maintenance.

For the complete installation process, see [Appliance Installation of 9012-9048](#).

How to Install 9072-9504DR Series Appliance

The appliance is intended for installation in restricted areas only. Only qualified personnel should perform Initial setup and maintenance.

For the complete installation process, see [Appliance Installation of 9072-9504DR](#).

How to Install X Series Appliance

The appliance is intended for installation in restricted areas only. Only qualified personnel should perform Initial setup and maintenance.

For the complete installation process, see [Appliance Installation of X Series - Compute Node](#) and [Appliance Installation of X Series - Storage Node](#).

Chapter 4: Upgrading Arcserve UDP on the Appliance

This section contains the following topics:

How to Apply a License After Upgrading Arcserve Software	50
Upgrade Sequence on Arcserve Appliance	51
Upgrade Sequence for UDP Console, RPS, and Agent	57

How to Apply a License After Upgrading Arcserve Software

After upgrading Arcserve UDP to 9.x or upgrading Arcserve Backup to 19.0, the original license key on the Arcserve Appliance will not work. To obtain the new license keys for Arcserve UDP 9.x and Arcserve Backup 19.0, contact your account representative.

For more details about adding a license key for Arcserve UDP, see [Arcserve Product Licensing Online Help](#).

Upgrade Sequence on Arcserve Appliance

The upgrade from Arcserve Appliance v8.1 to Arcserve UDP 9.x could involve one of the following sequences:

- Upgrade Arcserve UDP
 - ♦ [Upgrade the Arcserve Appliance Used as Arcserve Console and RPS](#)
 - ♦ [Upgrade the Arcserve Appliance Used as Arcserve UDP RPS](#)
 - ♦ [Upgrade Steps When Two or More Arcserve Appliances Are Used in the Environment](#)
- [Upgrade the Arcserve UDP Linux Agent on the Arcserve Appliance](#)
- [Upgrade the Arcserve Backup on the Arcserve Appliance](#)
- [Upgrade Sequence for UDP Console, RPS, and Agent](#)

Upgrade the Arcserve Appliance Used as Arcserve UDP Console and RPS

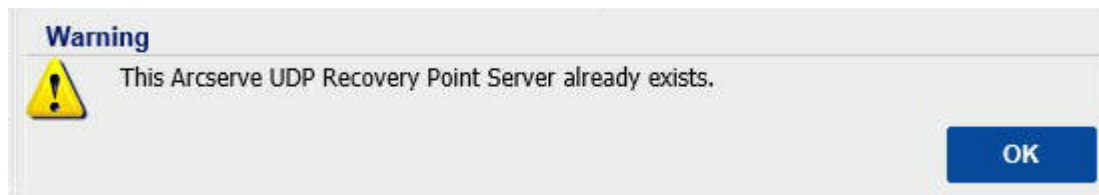
Upgrade this Arcserve Appliance, then follow up the [upgrade sequence](#) described to upgrade the environment.

Upgrade the Arcserve Appliance Used as Arcserve UDP RPS

Upgrade the complete productive environment. For details, refer to the [upgrade sequence](#).

Upgrade Steps When Two or More Arcserve Appliance Are Used in the Environment

- Upgrade the whole product environment. For details, refer to [upgrade sequence](#).
- If you see warning as displayed below when you add an Appliance as RPS from Arcserve UDP Console after upgrade, refer to the [Backing Up Arcserve Appliance from Another Appliance Reports Duplicated Nodes](#) topic in the **Troubleshooting** section.



Upgrade the Arcserve UDP Linux Agent on the Arcserve Appliance

Follow these steps:

1. Upgrade the Arcserve UDP Console that manages the Linux Backup Server environment.
2. Upgrade the Linux Backup Server on the Arcserve Appliance.

For more information, see [*Arcserve Unified Data Protection Agent for Linux Online Help*](#).

Upgrade the Arcserve Backup on the Arcserve Appliance

Refer to the [Arcserve Backup Implementation Guide](#) to complete upgrade on the Arcserve Appliance.

Upgrade Sequence for UDP Console, RPS, and Agent

Based on the Backward Compatibility Support Policy, plan your upgrade in the following sequence to ensure the upgrade works smoothly:

1. Upgrade Arcserve UDP Console.
2. Upgrade Arcserve UDP RPS (DR site).
3. Upgrade Arcserve UDP RPS (Data Center).
4. Upgrade Arcserve UDP Agentless Proxy, some Agents in Data Center.
5. Upgrade Arcserve UDP RPS (Remote site).
6. Upgrade Arcserve UDP Agentless Proxy and some Agents at the remote site.
Note: Repeat Step 5 and 6 for each remote location.
7. Upgrade Arcserve UDP Virtual Standby Monitor.

Note: According to the replication backward support policy, always upgrade the target RPS before the source RPS.

Chapter 5: Configuring the Arcserve Appliance

This section contains the following topics:

How to Configure Network Settings for Arcserve Appliance	59
How to Set Up the Arcserve Appliance	63
Configure Arcserve Appliance as Gateway	73

How to Configure Network Settings for Arcserve Appliance

To manage the Arcserve Appliance, the first step is to have the appliance in your network. For that, you need to assign a hostname to the appliance and then configure network ports.

Follow these steps:

1. After you power on the appliance, the Settings screen for the Microsoft License terms opens. Read and accept the terms.

The UDP **End User License Agreement** dialog opens.

2. Read and accept the license agreement and click **Next**.

Welcome to the Arcserve Appliance Configuration Tool screen appears.

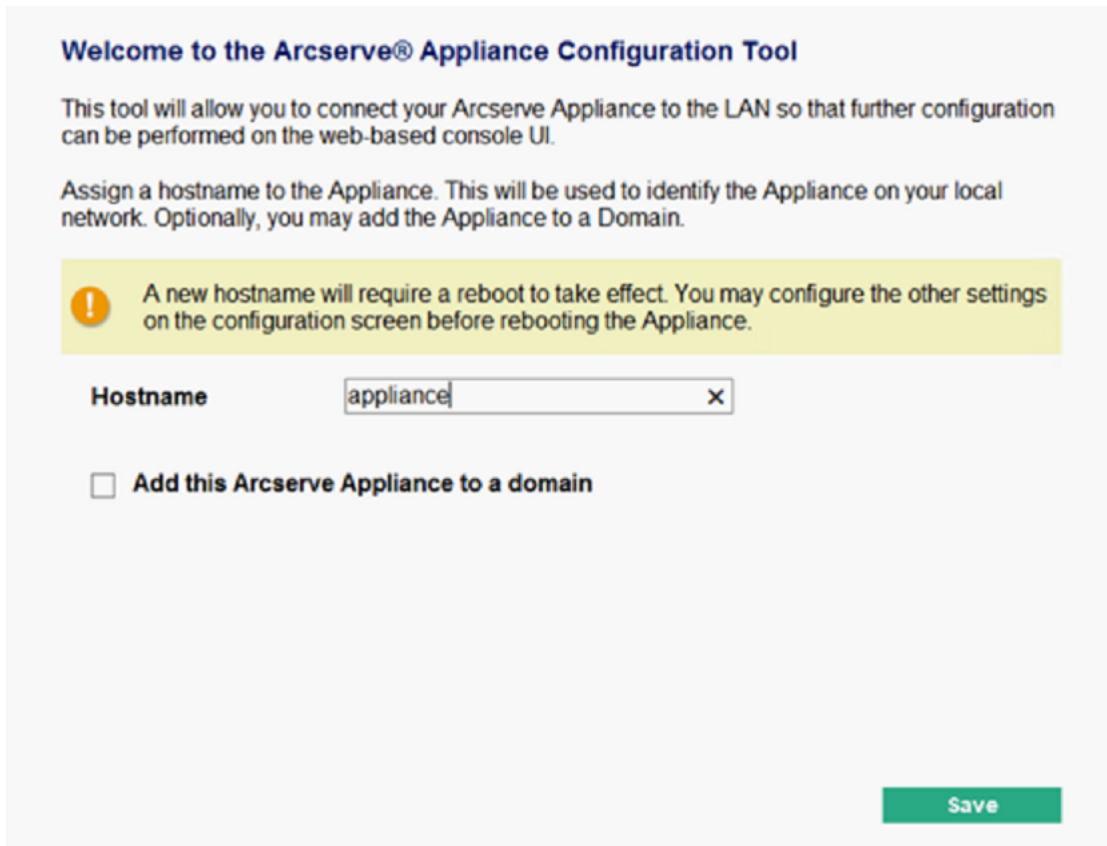
3. Enter the following details:

Hostname

Enter a host name for the appliance. Assigning a name helps identify the appliance on your network.

Add this Arcserve Appliance to a domain

Select the check-box to make your appliance a member of a domain in your network. Specify the values in Domain, Username, and Password fields that are displayed when the option is selected.




The screenshot shows the 'Welcome to the Arcserve® Appliance Configuration Tool' window. It contains introductory text about connecting the appliance to a LAN and assigning a hostname. A yellow warning box states that a new hostname requires a reboot. Below this, there is a 'Hostname' label and a text input field containing 'appliance'. A checkbox labeled 'Add this Arcserve Appliance to a domain' is unchecked. A green 'Save' button is located at the bottom right.

Welcome to the Arcserve® Appliance Configuration Tool

This tool will allow you to connect your Arcserve Appliance to the LAN so that further configuration can be performed on the web-based console UI.

Assign a hostname to the Appliance. This will be used to identify the Appliance on your local network. Optionally, you may add the Appliance to a Domain.

 A new hostname will require a reboot to take effect. You may configure the other settings on the configuration screen before rebooting the Appliance.

Hostname

☐ **Add this Arcserve Appliance to a domain**

Save

Note: To apply a new hostname, you need to restart the appliance. You can choose to reboot the appliance now or after you configure the network settings. After you reboot the appliance, you can access the appliance from any other machine using the URL - *https://<hostname>:8015*.

4. Click **Save**.

The following dialog opens. By default, Arcserve UDP discovers all network connections in a network. If some connections are not assigned, then manually edit and specify the connection details.

The screenshot shows the 'Arcserve Appliance Configuration' window. At the top, there's a yellow warning banner stating: 'Your Arcserve Appliance must be rebooted for the Hostname and Domain settings to take effect.' with a 'Reboot Appliance' button. Below this, the configuration details are listed:

- Hostname/Domain:** appliance (not assigned) [Edit]
- UDP Console URL:** https://appliance:8015
- Date and Time:** 1/24/2019 11:53:51 PM [Edit]

The 'Network Connections' section contains a table with the following data:

Connection Name	IP Address	Description	
SLOT 3 Port 1 ✗ Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	[Edit]
SLOT 3 Port 2 ✗ Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #2	[Edit]
SLOT 3 Port 3 ✗ Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #3	[Edit]
SLOT 3 Port 4 ✗ Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #4	[Edit]
NIC1 ✓ Connected	10.57.25.39 Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #5	[Edit]

5. To edit a network connection, click **Edit** from the **Network Connections** box.

The **Network Connection** dialog opens.

The 'NIC1' dialog box shows the configuration for the selected network interface. It includes the following fields and options:

- Status:** ✓ Connected
- Description:** Broadcom NetXtreme Gigabit Ethernet #5
- Connection:**
 - ☒ Use DHCP to obtain IP address automatically.
 - IP Address:** 10 . 57 . 25 . 39
 - Subnet Mask:** 255 . 255 . 255 . 0
 - Default Gateway:** 10 . 57 . 25 . 1
 - ☒ Obtain DNS server address automatically.
 - Preferred DNS Server:** 10 . 57 . 1 . 11
 - Alternate DNS Server:** 10 . 64 . 1 . 11

At the bottom right, there are 'Save' and 'Cancel' buttons.

6. Modify the IP address, subnet mask, and default gateway values as required and click **Save**.

Note: Optionally, you can also modify the hostname, domain, date, and time.

Important! Check if any script such as *acrun.bat* is running in command prompt. Before proceeding with the reboot, make sure to wait for this script to be completed.

7. To apply the changes, click **Reboot Appliance** to restart the appliance.

The appliance restarts with a new hostname. After restarting, the Login screen opens.

8. Enter the user name and password and click **Enter**.

The Arcserve Appliance Configuration screen appears.

9. When the appliance configuration screen reopens, click **Launch Wizard**.

arcserve Appliance Configuration [About the Appliance](#)

Click Launch Wizard to continue configuring your appliance with the Arcserve UDP Plan Configuration Wizard.

Launch Wizard

Hostname/Domain: **appliance (not assigned)**

UDP Console URL: **https://appliance:8015**

Date and Time: **1/25/2019 12:04:48 AM** **Edit**

Network Connections

Connection Name	IP Address	Description	
SLOT 3 Port 1 ✖ Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	Edit
SLOT 3 Port 2 ✖ Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #2	Edit
SLOT 3 Port 3 ✖ Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #3	Edit
SLOT 3 Port 4 ✖ Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #4	Edit
NIC1 ✔ Connected	10.57.25.39 Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #5	Edit

How to Set Up the Arcserve Appliance

After the appliance restarts with the new hostname, the Unified Data Protection wizard opens. The wizard lets you create a basic plan to schedule backups. The plan lets you define the nodes that you want to protect and schedule when to run backups. The backup destination is the appliance Server.

Note: If Appliance is configured in Domain, complete the Appliance wizard configuration using the Administrator login as a domain user cannot configure the appliance wizard.

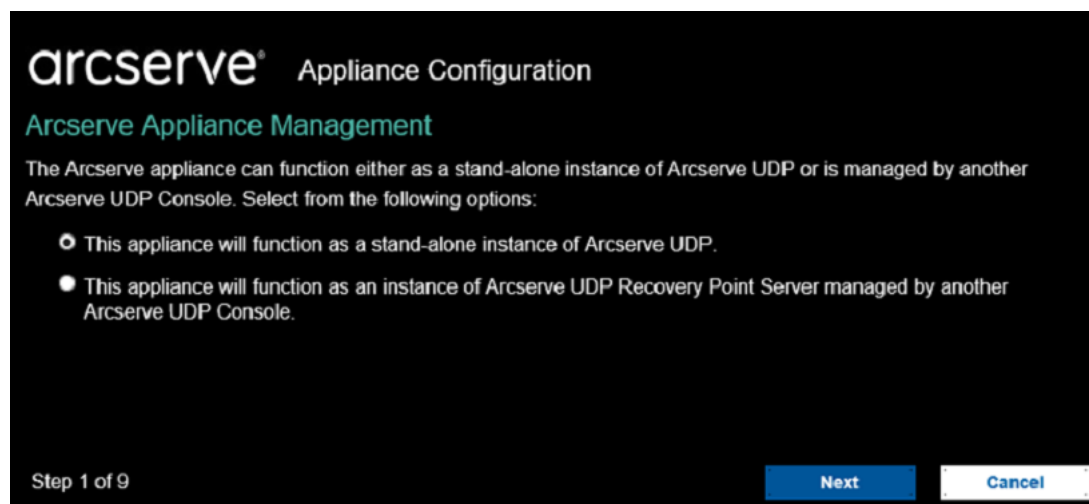
All the steps on the Arcserve Appliance Configuration wizard are optional, you can skip by clicking **Cancel** and directly open the UDP console and create plans.

Follow these steps:

1. Log into the Arcserve UDP console.

The Unified Data Protection wizard first opens and the Arcserve Appliance Management dialog appears. You can manage the UDP console either as a stand-alone instance or you can remotely manage from another UDP console. The remote console management function is useful when you are managing multiple UDP consoles.

2. On the Arcserve Appliance Management dialog, select whether you want to manage the appliance locally (default) or from another UDP console. If the appliance is managed from another UDP console, then specify the UDP console URL, username, and password.



3. Click **Next**.

The datastores dialog opens.

A datastore is a physical storage area on the appliance and is used as the destination for your backups.

By default, Arcserve UDP creates a datastore called <hostname>_data_store. This datastore is deduplication and encryption enabled.

Notes:

- The default deduplication block size is 16 KB. However, you can configure the deduplication block size based on your requirement.

To configure the deduplication block size, follow these steps:

- a. Navigate to the following location:

C:\Program Files\Arcserve\Unified Data Protection\Management\Configuration

- b. Open the **ApplianceDefaultSetting.properties** file, and then edit *deduplicationBlockSize*.

- You must configure the deduplication block size before you provide the encryption password for the datastore and click the **Next** button.

For more information about deduplication and encryption, see [Data Deduplication](#) in Arcserve UDP Solutions Guide.

Note: As the datastore is encrypted, you must specify an encryption password.


4. On the datastores dialog, type the encryption password for the datastore, retype the encryption password to confirm, and then click **Next**.

arcserve® Appliance Configuration

Data Stores

Your data store configuration is shown below. More data stores can be added from the Arcserve UDP Console.

appliance_data_store



Total Capacity
14.33 TB

Compression	Standard
Deduplication	Enabled
Encryption	Enabled
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Step 2 of 9

[Previous](#) [Next](#) [Cancel](#)

The Email and Alert dialog opens.

You can define the email Server that is used to send alerts and the recipients who would get the alerts. You can select options to get alerts based upon successful jobs, failed jobs, or both.

5. On the Email and Alert dialog, specify the following email and alert details:

Service

Specifies the email services such as Google Mail, Yahoo Mail, Live Mail, or Other.

Email Server

Specifies the email Server address. For example, for Google Server email, specify smtp.gmail.com.

Port

Species the email Server port number.

Requires Authentication

Specifies whether the email Server requires authentication. If yes, specify the account name and password for authentication.

Subject

Specifies the subject of the email that is sent to the recipients.

From

Specifies the email ID of the sender. The recipients will receive the mail from this sender.

Recipients

Specifies the recipients who will receive the alerts. You can use semicolons ";" to separate multiple recipients.

Options

Specifies the encryption method to use for the communication channel.

Connect using a proxy Server

Specifies the proxy Server user name and port number if you are connecting to the mail Server through a proxy Server. Also, specify a username and password if the proxy Server requires authentication.

Send a Test Email

Sends a test mail to the recipients. You can verify the details by sending a test mail.

arcserve® Appliance Configuration

Email and Alert

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

☒ Enable email notifications.

Service: Other

Email Server:

Port: 25

☐ Email service requires authentication.

Subject: Arcserve Unified Data Protection Alert

From:

Recipients: Separate email addresses with ;

Options:

- ☐ Use SSL
- ☐ Send STARTTLS
- ☒ Use HTML format

☐ Connect using a proxy server

Proxy Settings

Send a Test Email

Send Alerts For: ☒ Successful Jobs

Step 3 of 9

Previous Next Cancel

6. Click **Next**.

The Replication to Remote RPS dialog opens.

7. On the Replication to Remote RPS dialog, specify the following details if you want the appliance to replicate to a remotely-managed recovery point Server (RPS). For more information on a remotely-managed RPS, see *Arcserve UDP Solutions Guide*.

Arcserve UDP Console URL

Specifies the URL of the remote Arcserve UDP console.

Username and Password

Specifies the username and password to connect to the remote console.

Connect using a proxy Server

Specifies the proxy Server details if the remote console is behind a proxy Server.

Note: If you do not want the appliance to replicate to a remotely-managed RPS, select the **This appliance will not replicate to a remotely-managed RPS** option.

arcserve® Appliance Configuration

Replication to Remote RPS

Configure the settings below if you want to replicate to a remotely-managed Recovery Point Server destination.

☒ This appliance will replicate to a remotely-managed RPS.

Arcserve UDP Console URL

Username

Password

☐ Connect using a proxy server. [Proxy Settings](#)

☐ This appliance will not replicate to a remotely-managed RPS.

Step 4 of 9

[Previous](#) [Next](#) [Cancel](#)

8. Click **Next**.

The Create a Plan dialog opens. You can create a basic plan where you specify the nodes that you want to protect and the backup schedule.

Note: If you do not want to create basic plans using the wizard, perform the following steps:

- a. Click **Skip Plan Creation**.

The Next Steps dialog opens.

- b. Click **Finish** to open the UDP console and create plans.

9. On the Create a Plan dialog, specify the following details to create a plan:

Plan Name

Specifies the name of the plan. If you do not specify a Plan Name, the default name "Protection Plan <n>" is assigned.

Session Password

Specifies a session password. The session password is important and required when you restore data.

How do you want to add nodes to the plan?

Specifies the method to add nodes to the plan. Select one of the following methods:

- ♦ [Hostname/IP Address](#)
Refers to the method to manually add the nodes using host name or IP address of the node. You can add as many nodes as you want.
- ♦ [Discovering Nodes from Active Directory](#)
Refers to the method to add nodes that are in an active directory. You can first discover the nodes using the active directory details and then add the nodes.
- ♦ [Importing from a vCenter/ESX Server](#)
Refers to the method to import virtual machine nodes from ESX or vCenter Servers. This option lists all the virtual machines that are discovered on the provided host name or IP address.
- ♦ [Importing from a Hyper-V Server](#)
Refers to the method to import the virtual machine nodes from Microsoft Hyper-V Servers.

After you select a method, specify the details on each dialog.

arcserve® Appliance Configuration

Create a Plan [About Creating a Plan](#)

Next, you will need to create a protection plan for your data. In the protection plan, you will add nodes and configure a backup schedule. More than one protection plan can be created.

Skip Plan Creation

Plan Name: Protection Plan 1

Session Password: [Redacted]

Confirm Password: [Redacted]

• Retain the Session Password. You will need it to restore the data.

How do you want to add nodes to the plan?

Hostname/IP Address (for Windows machines only)

Step 5 of 9

Previous **Next** **Cancel**

10. After the nodes are added to your plan, click **Next**.

The Backup Schedule dialog opens.

11. On the Backup Schedule dialog, enter the following schedule:

- **Arcserve UDP agent install or upgrade schedule:** The latest version of the Arcserve UDP agent is installed on source nodes that do not have the agent installed. Any previous agent installations is upgraded to the latest version.
 - **Incremental backup schedule:** A full backup is performed for the first time, and then incremental backups are performed.
- Note:** If the time of backup is scheduled before the time of install/upgrade, then the backup is automatically scheduled for the next day. For example, if you schedule the agent installation for Friday at 9:00 PM and backup schedule for 8:00 PM, then the backup is performed on Saturday at 8:00 PM.
- **Cancel Plan Creation:** To cancel the plan that you just created, click **Cancel Plan Creation**.

The screenshot shows the 'arcserve® Appliance Configuration' window, specifically the 'Backup Schedule' tab. The interface is dark-themed. At the top, it says 'arcserve® Appliance Configuration'. Below that, the 'Backup Schedule' tab is selected. The instruction 'Enter criteria for the plan backup schedule.' is followed by two rows of time selection. The first row is 'Install/upgrade and reboot on' with a dropdown set to 'Friday', followed by 'at' and time selectors for '9', ':', '00', and 'PM'. The second row is 'Run Incremental Backup daily at' with time selectors for '10', ':', '00', and 'PM'. Below these is a light blue box titled 'Schedule Summary (Based upon your selections)' containing three paragraphs: 'On Friday at 9:00 PM, the latest version of the Arcserve UDP Agent will be installed on any source node that does not have the latest version already installed. Agent installation will not occur on nodes imported from Hyper-v or vCenter/ESX.', 'On Friday at 10:00 PM, the first Full Backup will be performed.', and 'On every day after the installation/upgrade is completed, at 10:00 PM an Incremental Backup will be performed.' Below the summary box is a 'Cancel Plan Creation' button. At the bottom left, it says 'Step 7 of 9'. At the bottom right, there are three buttons: 'Previous' (disabled), 'Next' (active/highlighted), and 'Cancel' (disabled).

12. Click **Next**.

The Plan Confirmation dialog opens.

13. On the Plan Confirmation dialog, review the details of your plan. If necessary, you can edit the nodes or the schedule by clicking Edit Nodes or Edit Schedule, or you can add or delete a plan.

Edit Nodes

Modifies the source nodes you want to protect.

Edit Schedule

Modifies the backup schedule.

arcserve® Appliance Configuration

Plan Confirmation

This is a confirmation of the plan that you created. You can edit plans or create a new plan.

Protection Plan 1
 + Add a Plan

Plan Name	Protection Plan 1
Nodes Protected	1
Destination	app7600
Install/Upgrade	Friday, 9:00 PM
Backup Schedule	Daily Incremental, 10:00 PM

Edit Nodes Edit Schedule Delete Plan

Step 8 of 9

Previous Next Cancel

14. After verifying the plans, click **Next**.

The Next Steps dialog opens.

You have successfully completed the configuration and you are now ready to work in the Arcserve UDP Console. You can add more nodes to protect, customize plans with features such as virtual standby, and add more destinations by including Recovery Point Servers and datastores.

15. Click **Finish** to exit the wizard and open the Arcserve UDP Console.

arcserve® Appliance Configuration

Next Steps

Configuration is complete and you are ready to open the Arcserve Unified Data Protection. With the Arcserve Unified Data Protection you can:

- + Add more nodes to protect
- + Customize plans with features such as Virtual Standby.
- + Add more destinations by including Recovery Point Servers and Data Stores.

Click Finish to open Arcserve Unified Data Protection.

Step 9 of 9

Previous Finish Cancel

Note: To log into the UDP console using domain credentials, see [Assigning Admin Privileges and Roles to a Domain User](#).

Configure Arcserve Appliance as Gateway

You can configure Arcserve Appliance as Gateway.

Follow these steps:

1. Uninstall Arcserve UDP Console from the Arcserve Appliance.
2. From the Arcserve UDP Console, click the **resources** tab.
3. From the left pane of the Arcserve UDP Console, navigate to **Infrastructures**, and click **Sites**.
4. Click **Add a Site**.
5. Follow the instructions provided in the **Add a Site** wizard to install Arcserve UDP Remote Management Gateway on the Arcserve Appliance.

Note: After installing Arcserve UDP Remote Management Gateway on the Arcserve Appliance, clicking **Launch Wizard** on the Arcserve Appliance wizard does not launch the Arcserve UDP Console. To access the Arcserve UDP Console, provide the URL of Arcserve UDP Console directly.

Chapter 6: Working with Arcserve Appliance

Using Arcserve Appliance, you can create backup plans for Windows, Linux, and virtual machines. You can also write data to a tape device and create a virtual standby machine.

This section contains the following topics:

Activate Arcserve Product on the Appliance	75
Create a Plan Using Arcserve Appliance Wizard	76
Add Nodes to a Plan	77
Create a Backup Plan for Linux Nodes	87
Create a Backup Plan to a Tape Device	88
Create an On-Appliance Virtual Standby Plan	89
Create Plan to Backup the Linux Backup Server	90
Setting-up to Perform Linux Instant VM Job to Local Appliance Hyper-V	94
Migrate Arcserve UDP Console Using ConsoleMigration.exe	95
Perform Migration between Arcserve Appliances	97
Modify the Input Source of Pre-installed Linux Backup Server	106

Activate Arcserve Product on the Appliance

For activating Arcserve product on the Appliance, see [Arcserve Product Licensing Online Help](#).

Create a Plan Using Arcserve Appliance Wizard

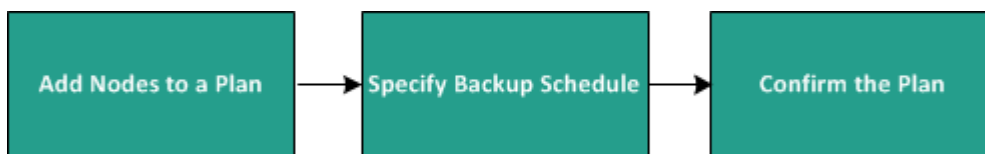
A plan is a collection of steps that defines which nodes to back up and when to back up. The Arcserve Appliance lets you create basic plans. Creating a plan using the Arcserve wizard is a three-step process:

1. Add the nodes you want to protect.

You can select Windows nodes or virtual machines from vCenter/ESX or Hyper-V Servers.

2. Define the backup schedule.

3. Review and confirm the plan.



In addition to a basic plan, Arcserve UDP lets you create complex plans and control many parameters from the UDP Console. To create complex plans from the UDP Console, see the *Arcserve UDP Solutions Guide*.

Add Nodes to a Plan

You can create a plan to protect various nodes. To protect nodes, you need to add nodes to a plan. You can add nodes from the Arcserve Appliance wizard. The wizard lets you add nodes using the following methods:

- Manually entering the node IP Address or hostname
([Add Nodes by Hostname/IP Address](#))
- Discovering nodes from an active directory
([Add Nodes by Active Directory](#))
- Importing virtual machine nodes from VMware ESX/vCenter Servers
([Add vCenter/ESX Nodes](#))
- Importing virtual machine nodes from Microsoft Hyper-V Servers
([Add Hyper-V Nodes](#))

Add Nodes by Hostname/IP Address

You can manually enter the IP address or the hostname of the address to add a node to a plan. Use this method when you have a few nodes to add, however, you can add multiple nodes one at a time. Arcserve Unified Data Protection Agent for Windows is installed on these nodes.

Follow these steps:

1. On the **Add Nodes by Hostname/IP address** dialog, enter the following details:

The screenshot shows the 'arcserve® Appliance Configuration' window. The title bar is 'arcserve® Appliance Configuration'. The main title is 'Add Nodes by Hostname/IP address' with a help icon and 'About Adding Nodes' link. Below the title is the instruction: 'Enter the hostname/IP address information for the selected Windows nodes, to add to the plan.' There are four input fields: 'Hostname/IP Address', 'Username', 'Password', and 'Description'. Below these fields is an 'Add to List' button. To the right is a panel titled 'Nodes Protected by Plan' with a 'Node Name' header and a list area. Below the list area is a 'Remove' button. At the bottom left is a 'Cancel Plan Creation' button. At the bottom right are 'Previous', 'Next', and 'Cancel' buttons. The bottom left corner indicates 'Step 6 of 9'.

Hostname/IP Address

Specifies the hostname or IP address of the source node.

User name

Specifies the user name of the node having administrator privileges.

Password

Specifies the user password.

Description

Specifies any description to identify the node.

Cancel Plan Creation

Cancels the plan that you just created.

2. Click **Add to List**.

The node is added to the right pane. To add more nodes, repeat the steps. All the added nodes are listed on the right pane.

3. (Optional) To remove the added nodes from the list on the right pane, select the nodes and click **Remove**.

4. Click **Next**.

The nodes are added to the plan.

Add Nodes by Active Directory

To add nodes that are in an active directory, provide the active directory details to discover the nodes and then add nodes to the plan.

Follow these steps:

1. On the **Add Nodes by Active Directory** dialog, enter the following details:

Username

Specifies the domain and user name in the domain\username format.

Password

Specifies the user password.

Computer Name Filter

Specifies the filter to discover node names.

Cancel Plan Creation

Cancels the plan that you just created.

The screenshot shows the 'Add Nodes by Active Directory' dialog in the Arcserve Appliance Configuration interface. The dialog has a dark blue header with the 'arcserve' logo and 'Appliance Configuration' text. Below the header, the title 'Add Nodes by Active Directory' is displayed in green, with a link for '? About Adding Nodes' to the right. The main instruction reads: 'Enter the Active Directory information to add nodes to the plan.' There are three input fields: 'Username' (containing 'domain\username'), 'Password' (empty), and 'Computer Name Filter' (containing '*'). A 'Browse' button is located below the 'Computer Name Filter' field. On the right side, there is a 'Nodes Protected by Plan' panel with a checkbox labeled 'Node Name' and a text box containing the instruction: 'Use the fields on the left to validate the node credentials and add the nodes to the plan.' A 'Remove' button is at the bottom of this panel. At the bottom left of the dialog is a 'Cancel Plan Creation' button. The bottom of the dialog shows 'Step 6 of 9' and three buttons: 'Previous', 'Next', and 'Cancel'.

2. Click **Browse**.

The discovered nodes are displayed.

arcserve® Appliance Configuration

Add Nodes by Active Directory [About Adding Nodes](#)

Enter the Active Directory information to add nodes to the plan.

Active Directory Results

Type node filter text

<input type="checkbox"/>	Name	Domain	Username	Verify
<input type="checkbox"/>	applia8400.ARCSERVE.COM	ARCserve.CC		
<input checked="" type="checkbox"/>	appliance1.ARCserve.COM	ARCserve.CC		
<input type="checkbox"/>	appliance2511.ARCserve.COM	ARCserve.CC		

Page 3 of 61

Username: administrator

Password: [masked]

Apply

Return **Add to List**

Cancel Plan Creation

Nodes Protected by Plan

☐ Node Name

Use the fields on the left to validate the node credentials and add the nodes to the plan.

Remove

Step 6 of 9 **Previous** **Next** **Cancel**

To add nodes, select the nodes and verify.

- To verify, select the nodes, enter the user name and password, and then click **Apply**.

The credentials are verified. Verified nodes are marked with green check marks. If a node fails verification, re-enter the credentials and click **Apply** again.

Note: You must verify each node before you can add it to the list.

- Click **Add to List**.

The selected node is added to the right pane.

- (Optional) To remove the nodes from the right pane, select the nodes and click **Remove**.

- Click **Next**.

The nodes are added to the plan.

Add vCenter/ESX Nodes

You can add virtual machine nodes to a VMware vCenter/ESX Server. To add these nodes, you need to discover and import nodes from the vCenter/ESX Server.

Follow these steps:

1. On the **Add Nodes by vCenter/ESX** dialog, specify the following vCenter/ESX Server details:

Hostname/IP Address

Specifies the hostname or the IP address of the vCenter/ESX Server.

Port

Specifies the port number to be used.

Protocol

Specifies the protocol to be used.

Username

Specifies a user name of the Server.

Password

Specifies the user password.

Cancel Plan Creation

Cancels the plan that you just created.

The screenshot shows the 'arcserve® Appliance Configuration' window. The main heading is 'Add Nodes by vCenter/ESX'. A link for '? About Adding Nodes' is in the top right. Below the heading, it says 'Enter the vCenter/ESX information to add nodes to the plan.' There are five input fields: 'Hostname/IP Address' (empty), 'Port' (443), 'Protocol' (HTTPS with a dropdown arrow), 'Username' (root), and 'Password' (empty). A 'Connect' button is below these fields. To the right is a 'Nodes Protected by Plan' panel with a 'Node Name' checkbox and the instruction 'Use the fields on the left to add nodes to the plan.' A 'Remove' button is at the bottom of this panel. A 'Cancel Plan Creation' button is at the bottom left. At the bottom of the window, it says 'Step 6 of 9' and has 'Previous', 'Next', and 'Cancel' buttons.

2. Click **Connect**.

The discovered hostnames are displayed.

3. Expand a hostname to see the nodes.

The screenshot shows the 'arcserve® Appliance Configuration' window. The main heading is 'Add Nodes by vCenter/ESX' with a link 'About Adding Nodes'. Below the heading is the instruction: 'Enter the vCenter/ESX information to add nodes to the plan.' The interface is divided into two main panels. The left panel, titled 'vCenter/ESX Results', contains a search bar 'Type node filter text' and a table of nodes. The table has two columns: 'Name' and 'Object Type'. The nodes listed are: 10.57.25 (Host System), IVM (Resource Pool), LinuxAgent (Resource Pool), restore (Resource Pool), Virtual Lab 1 (Resource Pool), windows (Resource Pool), LicenseTesting (Resource Pool), and agent node (Virtual Machine). The 'agent node' is selected. Below the table are buttons 'Return' and 'Add to List'. The right panel, titled 'Nodes Protected by Plan', shows a list of nodes with checkboxes: 'Node Name' and 'VM(agent node)'. Below this list is a 'Remove' button. At the bottom of the window, there is a 'Cancel Plan Creation' button and a progress indicator 'Step 6 of 9'. Navigation buttons 'Previous', 'Next', and 'Cancel' are also present.

arcserve® Appliance Configuration

Add Nodes by vCenter/ESX [About Adding Nodes](#)

Enter the vCenter/ESX information to add nodes to the plan.

vCenter/ESX Results

Name	Object Type
10.57.25	Host System
▶ IVM	Resource Pool
▶ LinuxAgent	Resource Pool
▶ restore	Resource Pool
▶ Virtual Lab 1	Resource Pool
▶ windows	Resource Pool
▶ LicenseTesting	Resource Pool
▶ agent node	Virtual Machine

Nodes Protected by Plan

☐ Node Name

☐ VM(agent node)

Step 6 of 9

4. Select the nodes that you want to add, and then click **Add to List**.

The selected nodes are added to the right pane.

5. (Optional) To remove the nodes from the right pane, select the nodes and click **Remove**.

6. Click **Next**.

The nodes are added to the plan.

Add Hyper-V Nodes

Use this method to import the virtual machine nodes from a Microsoft Hyper-V Server.

Follow these steps:

1. On the **Add Hyper-V Nodes** dialog, specify the following details.

The screenshot shows the 'Add Hyper-v Nodes' dialog in the Arcserve Appliance Configuration interface. The dialog is titled 'Add Hyper-v Nodes' and includes a subtitle 'Enter Hyper-v information to add nodes to the plan.' It features three input fields for 'Hostname/IP Address', 'Username', and 'Password', followed by a 'Connect' button. A 'Nodes Protected by Plan' section on the right contains a checkbox for 'Node Name' and a text box with the instruction 'Use the fields on the left to add nodes to the plan.' Below this is a 'Remove' button. At the bottom left, there is a 'Cancel Plan Creation' button. At the bottom right, there are 'Previous', 'Next', and 'Cancel' buttons. The bottom left corner indicates 'Step 6 of 9'.

Hostname/IP Address

Specifies the Hyper-V Server name or the IP address. To import virtual machines that are in Hyper-V clusters, specify either the cluster node name or Hyper-V host name.

Username

Specifies Hyper-V user name having the administrator rights.

Note: For Hyper-V clusters, use a domain account with administrative privilege of the cluster. For standalone Hyper-V hosts, we recommend using a domain account.

Password

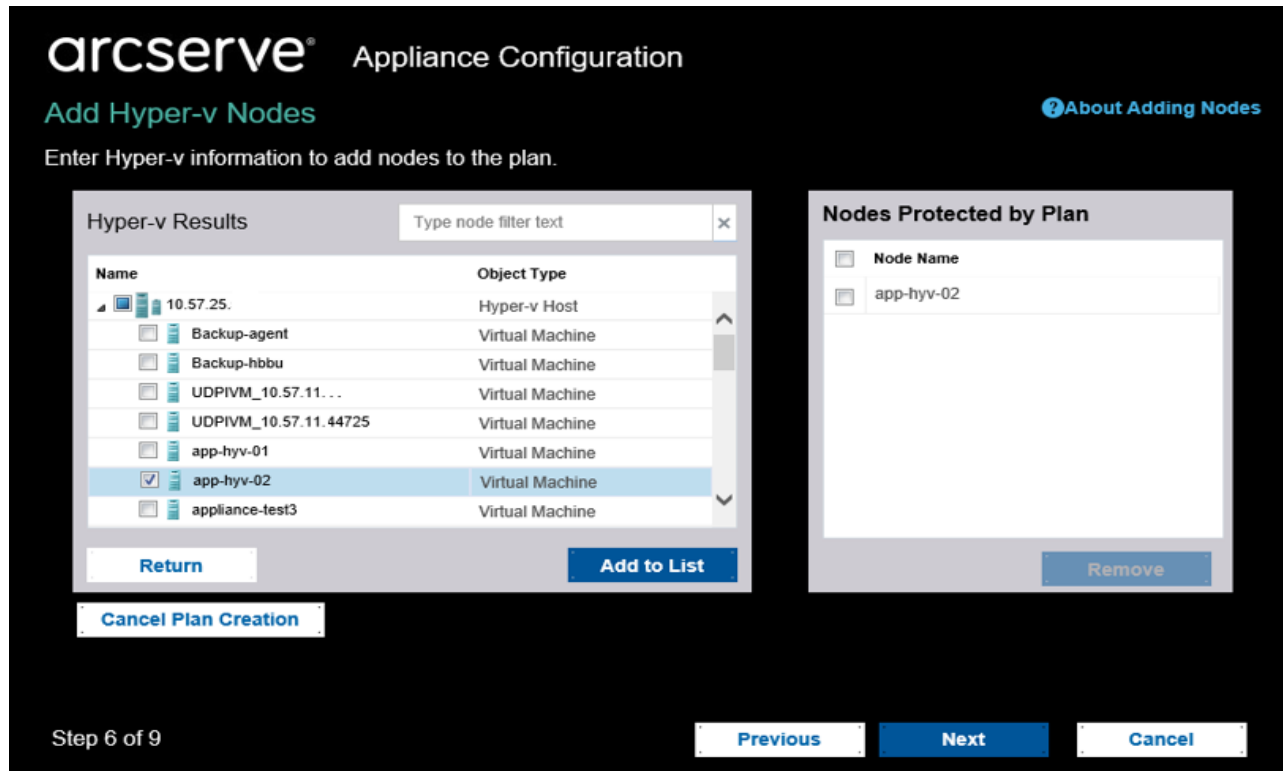
Specifies the password of user name.

Cancel Plan Creation

Cancels the plan that you just created.

2. Click **Connect**.

The discovered hostnames are displayed. Expand a hostname to see the nodes.



3. (Optional) You can type the node name in the filter field to locate the node in the tree.
4. Select the nodes, and then click **Add to List**.
The selected nodes are added to the right pane.
5. (Optional) To remove the nodes from the right pane, select the nodes and click **Remove**.
6. Click **Next**.
The nodes are added to the plan.

Create a Backup Plan for Linux Nodes

You can back up Linux nodes from the Arcserve Appliance Console. The Linux Backup Server is already added to the Console.

Follow these steps:

1. Open the Arcserve Appliance Console.
2. Click resources, Plans, All Plans.
3. Create a Linux Backup plan.
4. Specify the Source, Destination, Schedule, and Advanced configurations.

Note: For more information about each of the configurations, see [How to Create a Linux Backup Plan](#) in the Solutions Guide.

5. Run the backup plan.

Create a Backup Plan to a Tape Device

Arcserve Appliance has the capability to write data to a tape device. Typically, the source data is the recovery point that you have saved in a datastore using the UDP backup plan, and the destination is a tape device. You need to use Arcserve Backup Manager to manage your backup jobs to a tape.

The following process overview gives you an idea on how to write to a tape device using the Arcserve Appliance:

1. **Attach the tape device to the Arcserve Appliance**

Arcserve Appliance comes with a port at the rear panel to attach your tape device. Once you attach the tape device, Arcserve Appliance automatically identifies the tape device.

2. **Configure the tape device using the Backup Manager**

Open the Backup Manager and add the tape device to Backup Manager. Backup Manager is the interface that lets you manage Arcserve Backup. After you add the tape device to Backup Manager, configure the device.

Note: For more information on configuring and managing the device, see [Managing Devices and Media](#) in Arcserve Backup Administration Guide.

3. **Successfully complete at least one backup job using the UDP Console**

You need at least one successful backup that you can write to a tape device. To back up data, create a plan using the UDP Console and back up to a data-store.

Note: For more information about creating a backup plan for different nodes, see [Creating Plans to Protect Data](#) in the Solutions Guide.

4. **Initiate a backup to tape job from Backup Manager**

Open the Backup Manager and create a plan to back up data to the tape device. The source data is the destination of UDP backup plan and the destination is the tape device.

Note: For more information on creating a backup plan to tape, see [Backing Up and Recovering D2D/UDP Data](#) in *Arcserve Backup Administration Guide*.

Create an On-Appliance Virtual Standby Plan

Arcserve Appliance has the capability to serve as a virtual standby machine.

Follow these steps:

1. Verify and ensure that you have a successful backup plan.
2. Open the Arcserve Appliance Console.
3. Navigate to the plans and modify the backup plan.
4. Add a Virtual Standby task.
5. Update the Source, Destination, Virtual Machine configurations.

Note: For more information about the configurations, see [How to Create a Virtual Standby Plan](#) topic in the Arcserve UDP Solutions Guide.

6. Save and run the plan.

Create Plan to Backup the Linux Backup Server

In the Arcserve UDP Console, you can configure the Linux Backup Server to backup.

Follow these steps:

1. From Arcserve UDP Console, click the **resources** tab.
2. Click **All Nodes** in the right pane.
3. From the center pane, click **Add Nodes**.

The **Add Nodes to Arcserve UDP Console** dialog opens.

4. From the **Add Nodes by** drop-down list, select *Add Linux Node*.
5. Provide the node credentials and click **Add to List**.

Add Nodes to Arcserve UDP Console

Add nodes by: Add Linux Node

Node Name/IP Address: Linux-BackupSvr

☐ SSH Key Authentication

User Name: root

Password: *****

☐ Non-root Credential

Non-root Username:

Non-root Password:

Add Description:

Add to List

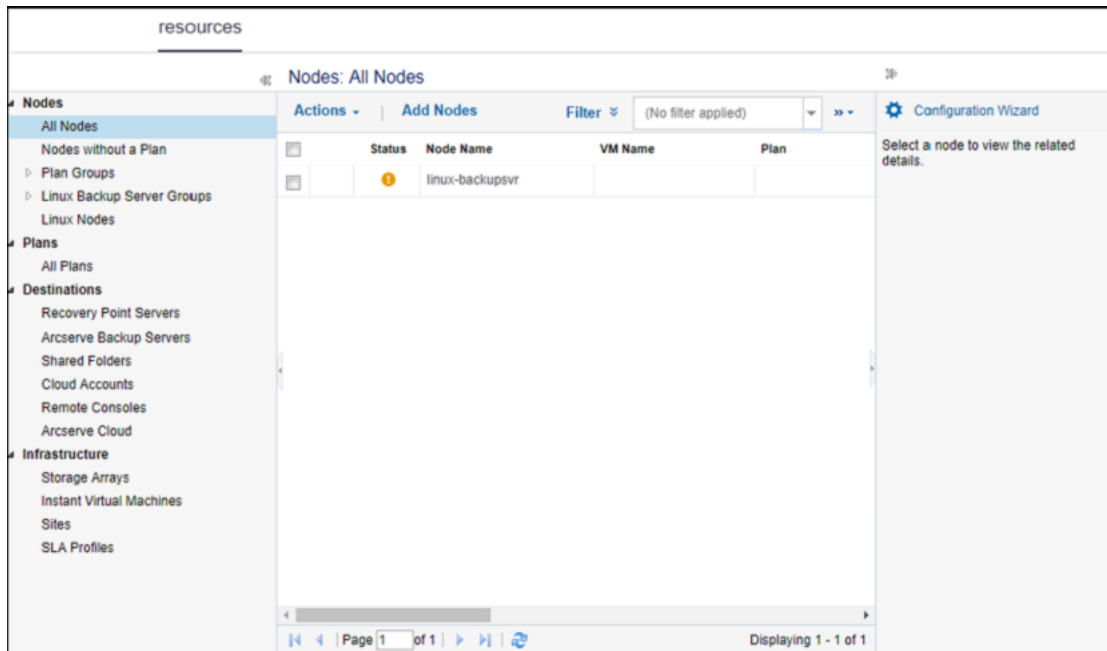
Node Name	VM Name	Hypervisor
You have not added any node to the list.		

Remove

Help **Save** **Cancel**

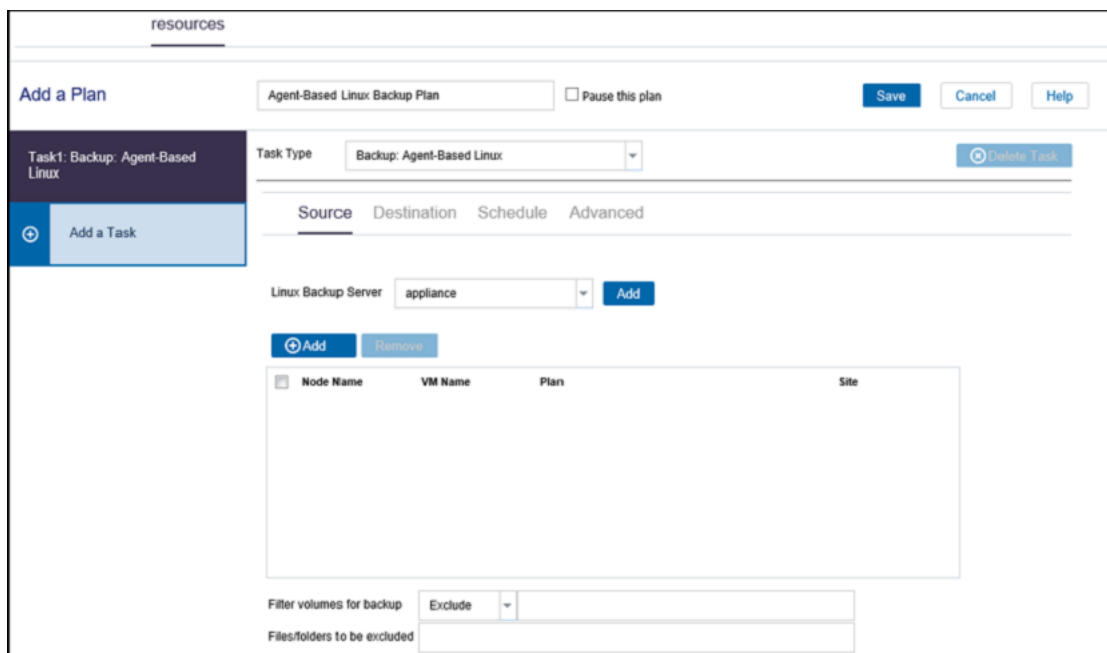
6. Click **Save**.

The added Linux node is displayed in the **All Nodes** list.

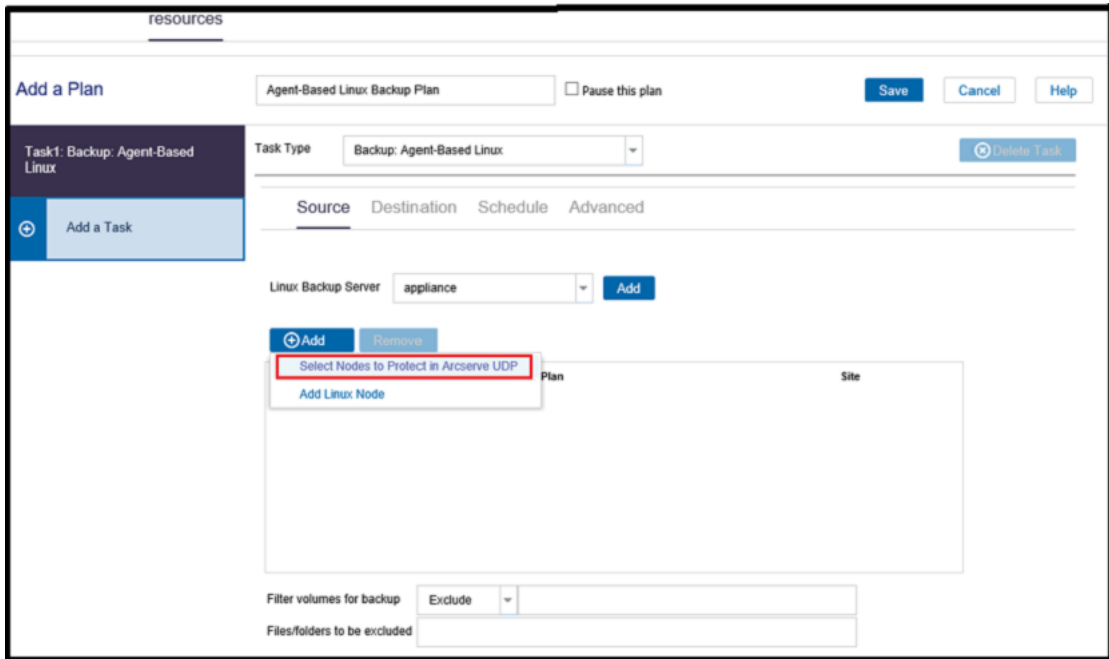


7. Navigate to **All Plans** and create an Agent-based Linux plan.

The **Source** tab appears.

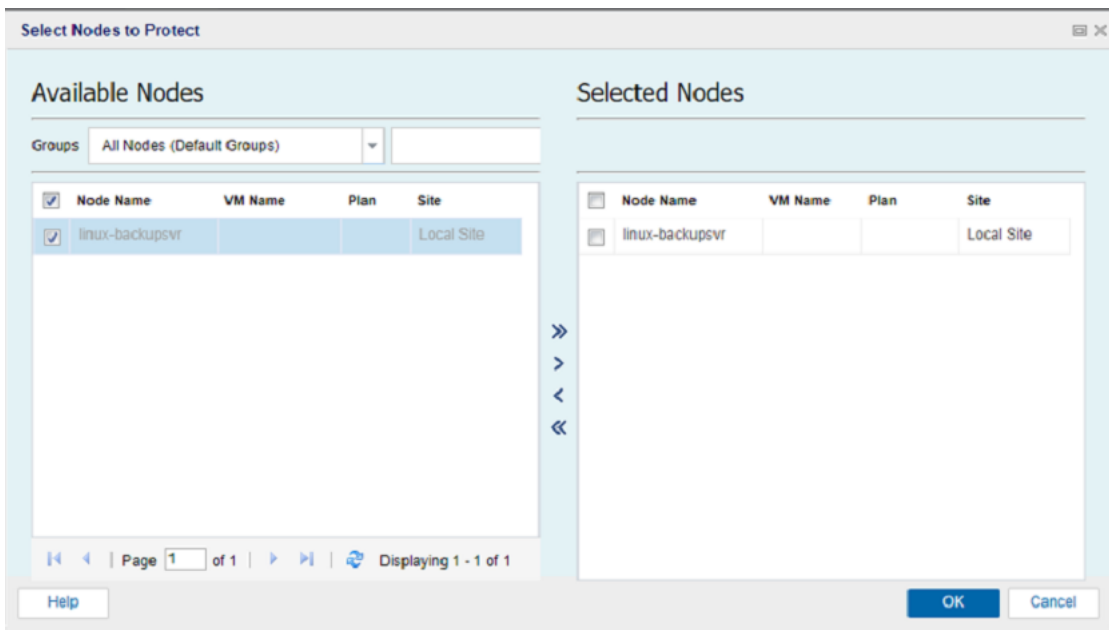


8. From the **Add** drop-down list, select *Select Nodes to Protect in Arcserve UDP*.



The **Select Nodes to Protect** dialog opens.

9. Protect the added Linux node and click **OK**.



The **Destination** tab appears.

10. The default destination displayed is the datastore created using Appliance wizard. Select Local disk or shared folder to backup the node if required.

The screenshot shows the 'Add a Plan' configuration window. At the top, there's a text input field containing 'Agent-Based Linux Backup Plan' and a checkbox labeled 'Pause this plan'. To the right are 'Save', 'Cancel', and 'Help' buttons. Below this is a 'Task Type' dropdown menu set to 'Backup: Agent-Based Linux', with a 'Delete Task' button to its right. A left sidebar contains a 'Task1: Backup: Agent-Based Linux' header and an 'Add a Task' button. The main area has tabs for 'Source', 'Destination', 'Schedule', and 'Advanced'. The 'Destination' tab is active, showing 'Destination Type' with radio buttons for 'Local disk or shared folder' and 'Arcserve UDP Recovery Point Server' (selected). Below are dropdowns for 'Recovery Point Server' (set to 'appliance') and 'Data Store' (set to 'appliance_data_store'). There's a 'Password Protection' checkbox (checked) with an information icon, and input fields for 'Session Password' and 'Confirm Session Password'.

11. After providing the settings related to plan, click **Save**.

The screenshot shows the 'Plans: All Plans' view. On the left is a navigation tree with categories: 'Nodes' (containing 'All Nodes', 'Nodes without a Plan', 'vCenter/ESX Groups', 'Hyper-V Groups', 'Linux Nodes', 'Linux Backup Server Groups', and 'Plan Groups'), 'Plans' (containing 'All Plans'), and 'Destinations' (containing 'Recovery Point Servers', 'Arcserve Backup Servers', 'Shared Folders', 'Cloud Accounts', 'Remote Consoles', and 'Arcserve Cloud'). The 'All Plans' section is selected. The main area has a table with columns: 'Plan Name', 'Nodes Protected' (with sub-columns for 'Total', a green checkmark, a yellow warning, and a red X), and 'Status'. One plan is listed: 'Agent-Based Linux Backup Plan' with a total of 1 node protected, 0 warnings, and 0 errors. The status is 'Deployment: Successful (1)'. Above the table are 'Actions' and 'Add a Plan' buttons. On the right, there's a 'Configuration Wizard' button and a note: 'Select a plan to view the related details.'

Plan Name	Nodes Protected				Status
	Total	✓	⚠	✗	
Agent-Based Linux Backup Plan	1	0	1	0	✓ Deployment: Successful (1)

You can perform backup for the added Linux Backup Server successfully.

Setting-up to Perform Linux Instant VM Job to Local Appliance Hyper-V

Using Arcserve Appliance, you can set the network to perform Linux instant VM job on local Appliance Hyper-V.

Follow these steps:

1. Open Hyper-V manger.
2. Create a new external virtual network switch.
3. Run the following command with PowerShell to reconfigure Routing and Remote Access for the newly added virtual network switch in step 1 using DOS command line:

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

Note: The Linux Backup Server *Linux-BackupSvr* is rebooted during the process.

4. To perform Linux instant VM job to local Hyper-V, select the newly added virtual network switch created.

Now, you can perform Linux instant VM job to local Appliance Hyper-V successfully.

Migrate Arcserve UDP Console Using ConsoleMigration.exe

On the Arcserve Appliance, you can migrate the Arcserve UDP Console to another Appliance using *ConsoleMigration.exe*. From Arcserve UDP v6.5 Update 2 onwards, you can migrate the Arcserve UDP Console between any two Arcserve UDP consoles, even when not belonging to Appliance.

Use *ConsoleMigration.exe* for BackupDB and RecoverDB. The following screenshot displays the usage of *ConsoleMigration.exe*:

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe
Usage: ConsoleMigration.exe <-BackupDB|-RecoverDB [-Force]>
-BackupDB: Backup UDP Console database Arcserve_APP
-RecoverDB: Recover UDP Console database Arcserve_APP
-Force (optional): Force recover UDP Console database
Your input is not valid. Please follow the usage.
```

To complete the migration process, follow these steps:

1. On old Arcserve UDP Console, perform backup for the Arcserve UDP database.

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe -backupdb
Start Backup...
Backed up DB and version files completed.
DB and version files were created at: "C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\DB_Migration".
```

The *DB_Migration* folder is created successfully.

2. On the new Arcserve UDP Console, copy the *DB_Migration* folder to the following path:

<UDP_Home> \Management\BIN\Appliance\

3. If the new Arcserve UDP Console is Arcserve Appliance then change host-name and reboot the system and finish the Appliance configuration using Appliance wizard.

Note: If the Arcserve UDP Console is not an Arcserve Appliance, skip this step.

4. On the new Arcserve UDP Console, perform the steps mentioned in the screen below to recover the Arcserve UDP Console database. When the database recovery process is completed, the nodes are updated for new Arcserve UDP Console. If any nodes are failed to get updated, the disconnected nodes are recorded in the *DisconnectedNodesInfo*-<mm-dd-

yyyy>.txt file under the path *C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\logs*. You can manually update the disconnected nodes from the new Arcserve UDP Console.

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe -recoverdb
Are you sure you want to recover the backup DB file? <y/n>: y
Stopping Arcserve UDP Management service, please wait...
Recovering backup DB file...
Updating nodes, please wait...
Please update nodes manually from UDP console if you still encounter disconnected nodes.
The disconnected nodes(if existing) will be saved at "C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\logs".
Console migration completed. Console uses DB "localhost\ARCSERVE_APP".
```

Note: In Arcserve UDP Console, if any site other than Local Site exists, follow the steps mentioned in *NewRegistrationText.txt* file to register the site again.

You have completed migration of Arcserve Appliance Console to the new Arcserve UDP Console successfully.

You can use this tool to perform console migration for Arcserve UDP Console connected with remote SQL database. After the migration is complete, the migrated Arcserve UDP Console is configured to connect with the same remote SQL database.

Note: From Arcserve UDP v6.5 Update 4 onwards, **-force** option is introduced in **ConsoleMigration.exe** command to force the recovery backup database file migration to the target console under the following conditions:

1. When you want to perform console migration between two consoles where the source console uses SQL Server Enterprise edition and the target console uses SQL Server Express edition. In this case, the minimum required Database size of the source UDP console is 4000 MB.
2. When you want to perform console migration from a console that uses an advanced version of SQL Server database to a console that uses an older version of SQL Server database. For example, migrating from a console using SQL Server 2016 to a console using SQL Server 2014.

Perform Migration between Arcserve Appliances

This topic provides two solutions for user to perform migration from existing Arcserve Appliance to another fresh Arcserve Appliance.

For example, let us migrate the Arcserve Appliance 8200 to Arcserve Appliance 8400. The prerequisites are listed as follows:

- Ensure that you can connect to both Appliance 8200 and Appliance 8400.
- Capacity of the new Appliance should have enough memory to hold all the data on the original Appliance.
- In the Arcserve Appliance 8200, ensure that no job runs.

For more information on Console migration, refer the [How to Migrate Arcserve UDP Console Using ConsoleMigration.exe](#) topic.

To migrate from any Appliance to a fresh Appliance, you have two solutions as listed below.

- [Solution 1](#)
- [Solution 2](#)

Solution 1

Bare Metal Recovery (BMR) solution

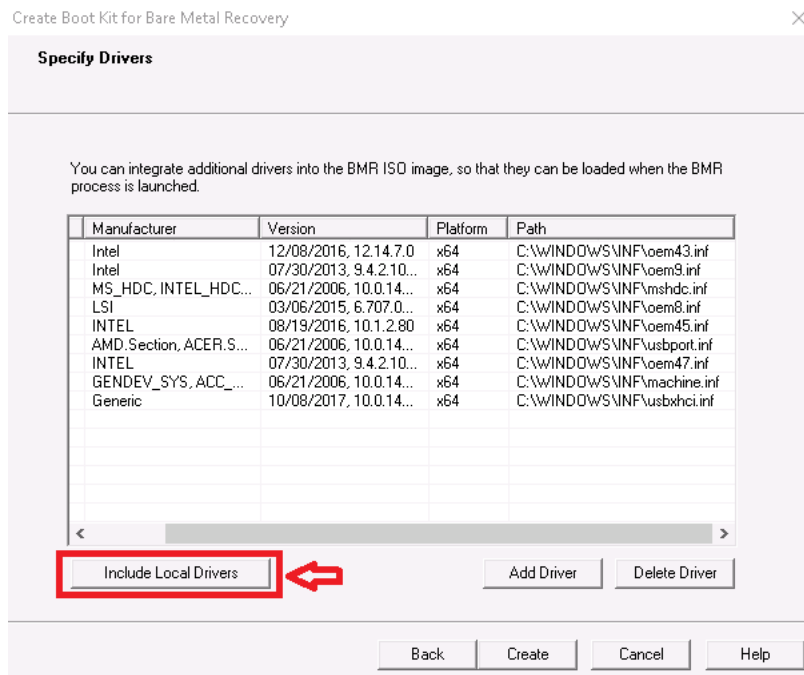
To perform BMR from existing Arcserve Appliance to another fresh Arcserve Appliance, follow these steps:

1. Create a datastore on the fresh Arcserve Appliance 8400 and backup Arcserve Appliance 8200 to this datastore.

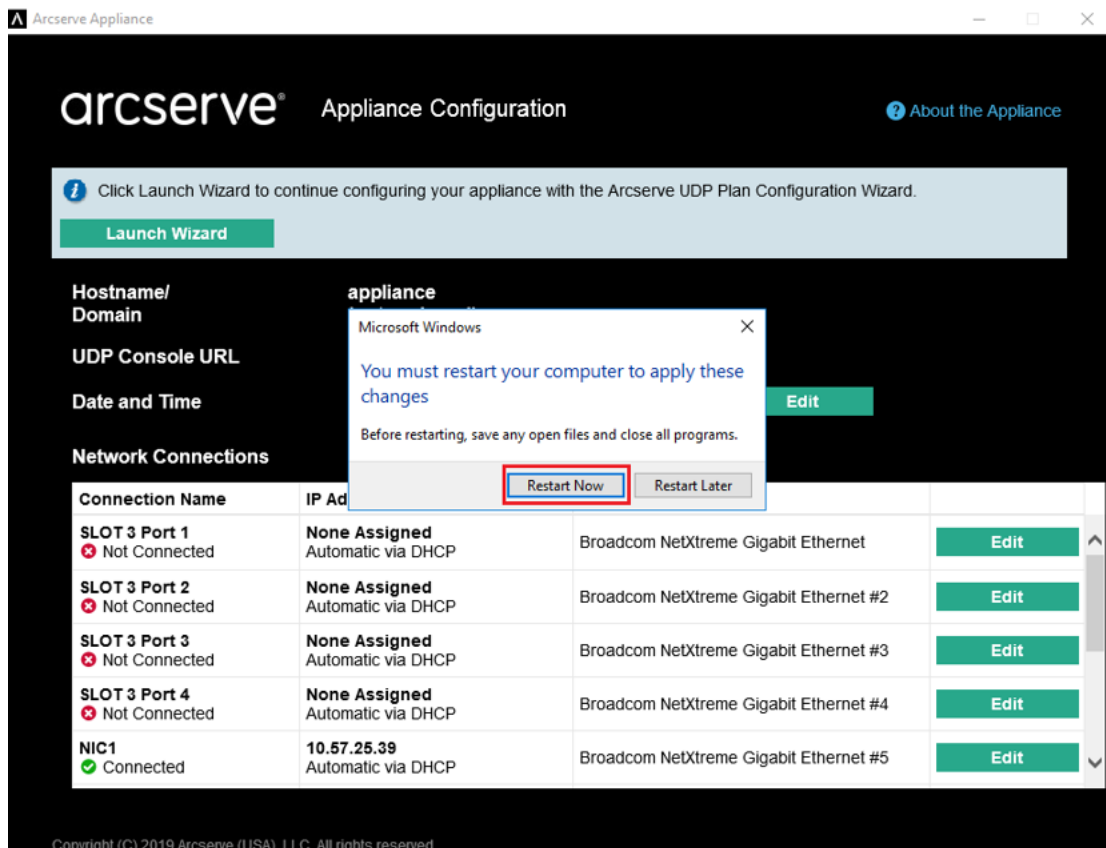
Note: You can just ignore the following warning:

The Arcserve UDP Recovery Point Server datastore is configured on volume X:,Y:. This volume will not be backed up.

2. After the backup, perform BMR on the Appliance 8400 using the recovery point you get on the step above and select driver *megasas.inf* manually.



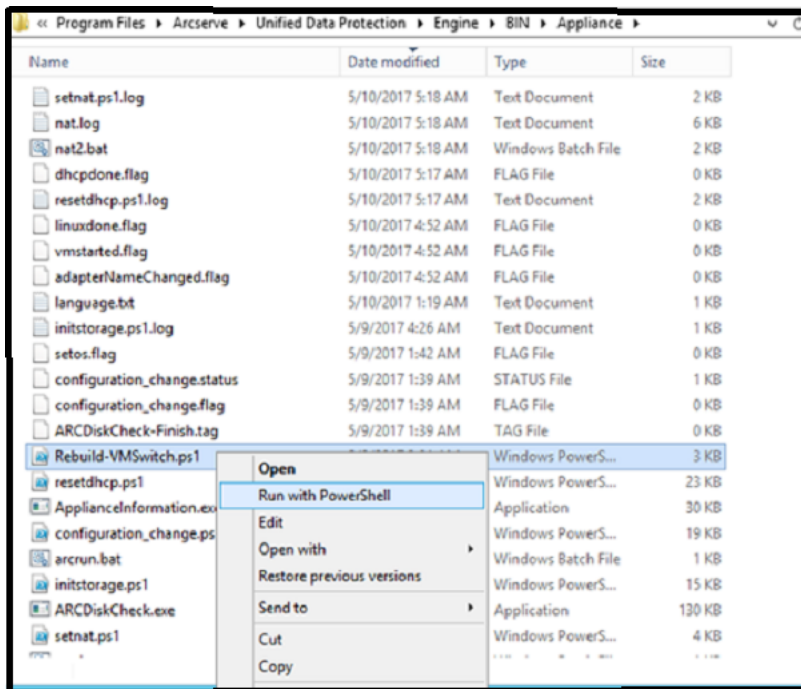
3. After the BMR, restart the Appliance 8400 according to the system prompt.



4. Now, rebuild the network switch on 8400 Appliance.

Run the following command with PowerShell:

```
C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Rebuild-VMSwitch.ps1
```

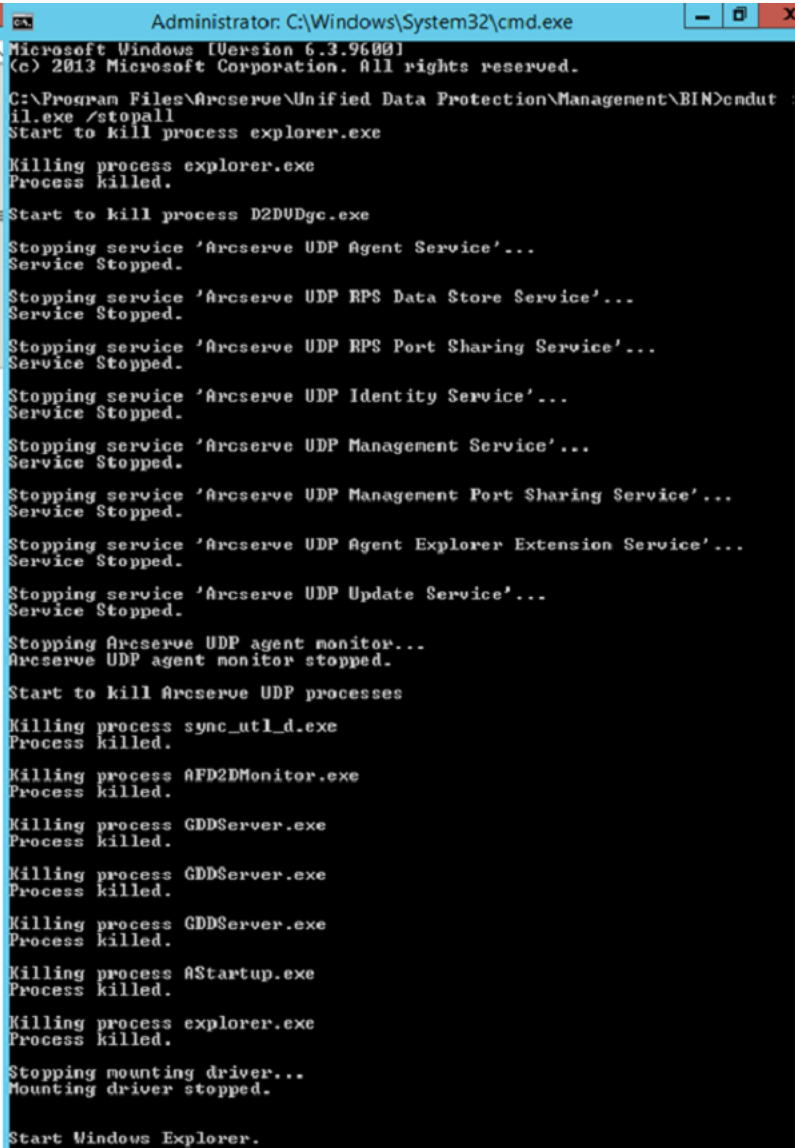


5. Now, follow these steps to copy the data on 8200 Appliance to 8400 Appliance and import the data on to 8400 Appliance:

- a. Stop all the UDP services on Arcserve Appliance 8200 using the following command in the command line:

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

- b. Copy all the data on disk X and Y from Arcserve Appliance 8200 to 8400 manually.



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>cndut
il.exe /stopall
Start to kill process explorer.exe

Killing process explorer.exe
Process killed.

Start to kill process D2DUDgc.exe

Stopping service 'Arcserve UDP Agent Service'...
Service Stopped.

Stopping service 'Arcserve UDP RPS Data Store Service'...
Service Stopped.

Stopping service 'Arcserve UDP RPS Port Sharing Service'...
Service Stopped.

Stopping service 'Arcserve UDP Identity Service'...
Service Stopped.

Stopping service 'Arcserve UDP Management Service'...
Service Stopped.

Stopping service 'Arcserve UDP Management Port Sharing Service'...
Service Stopped.

Stopping service 'Arcserve UDP Agent Explorer Extension Service'...
Service Stopped.

Stopping service 'Arcserve UDP Update Service'...
Service Stopped.

Stopping Arcserve UDP agent monitor...
Arcserve UDP agent monitor stopped.

Start to kill Arcserve UDP processes

Killing process sync_utl_d.exe
Process killed.

Killing process AFD2DMonitor.exe
Process killed.

Killing process GDDServer.exe
Process killed.

Killing process GDDServer.exe
Process killed.

Killing process GDDServer.exe
Process killed.

Killing process AStartup.exe
Process killed.

Killing process explorer.exe
Process killed.

Stopping mounting driver...
Mounting driver stopped.

Start Windows Explorer.
```

- c. On 8400 Appliance, start all UDP services and then import the data copied from 8200 Appliance.

resources

Import a Data Store

Recovery Point Server

appliance

Data Store Folder

X:\Arcserve\data_store\common

Browse

Encryption Password

Next

Save

Cancel

Help

Solution 2

Migrate Arcserve Appliance solution

Important! If the existing Appliance works as both Arcserve UDP Console and Arcserve UDP RPS, we can use this solution.

Prerequisites:

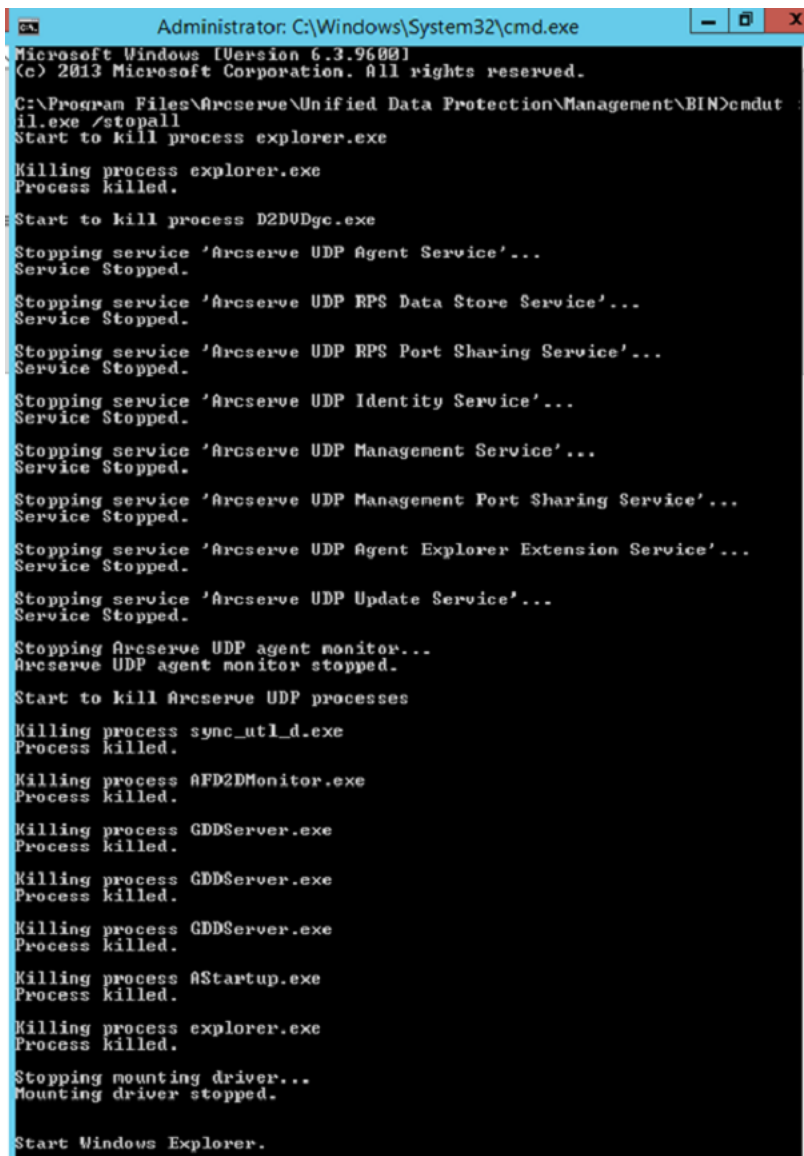
- On Arcserve Appliance 8200, ensure that no job runs.
- You have migrated the Arcserve UDP Console from Arcserve Appliance 8200 to 8400.

Note: For more information about how to migrate the Arcserve UDP Console from Appliance 8200 to 8400, refer [How to Migrate Arcserve UDP Console Using ConsoleMigration.exe](#).

Follow these steps:

1. Stop all the Arcserve UDP services on Arcserve Appliance 8200 using the following command in the command line:

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



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>cndut
il.exe /stopall
Start to kill process explorer.exe

Killing process explorer.exe
Process killed.

Start to kill process D2DUDgc.exe

Stopping service 'Arcserve UDP Agent Service'...
Service Stopped.

Stopping service 'Arcserve UDP RPS Data Store Service'...
Service Stopped.

Stopping service 'Arcserve UDP RPS Port Sharing Service'...
Service Stopped.

Stopping service 'Arcserve UDP Identity Service'...
Service Stopped.

Stopping service 'Arcserve UDP Management Service'...
Service Stopped.

Stopping service 'Arcserve UDP Management Port Sharing Service'...
Service Stopped.

Stopping service 'Arcserve UDP Agent Explorer Extension Service'...
Service Stopped.

Stopping service 'Arcserve UDP Update Service'...
Service Stopped.

Stopping Arcserve UDP agent monitor...
Arcserve UDP agent monitor stopped.

Start to kill Arcserve UDP processes

Killing process sync_utl_d.exe
Process killed.

Killing process AFD2DMonitor.exe
Process killed.

Killing process GDDServer.exe
Process killed.

Killing process GDDServer.exe
Process killed.

Killing process GDDServer.exe
Process killed.

Killing process AStartup.exe
Process killed.

Killing process explorer.exe
Process killed.

Stopping mounting driver...
Mounting driver stopped.

Start Windows Explorer.
```

2. Copy all the data on disk X and Y from Arcserve Appliance 8200 to 8400 manually.
3. On 8400 Appliance, start all Arcserve UDP services and then import the datastores copied from 8200 Appliance.

The screenshot shows a software window titled 'resources' with a sub-header 'Import a Data Store'. It contains three input fields: 'Recovery Point Server' with the value 'appliance', 'Data Store Folder' with the value 'X:\Arcserve\data_store\common' and a 'Browse' button to its right, and 'Encryption Password' with a masked input field and a 'Next' button below it. At the bottom right are 'Save', 'Cancel', and 'Help' buttons.

Note: The Arcserve UDP log files are not migrated to the new fresh Appliance.

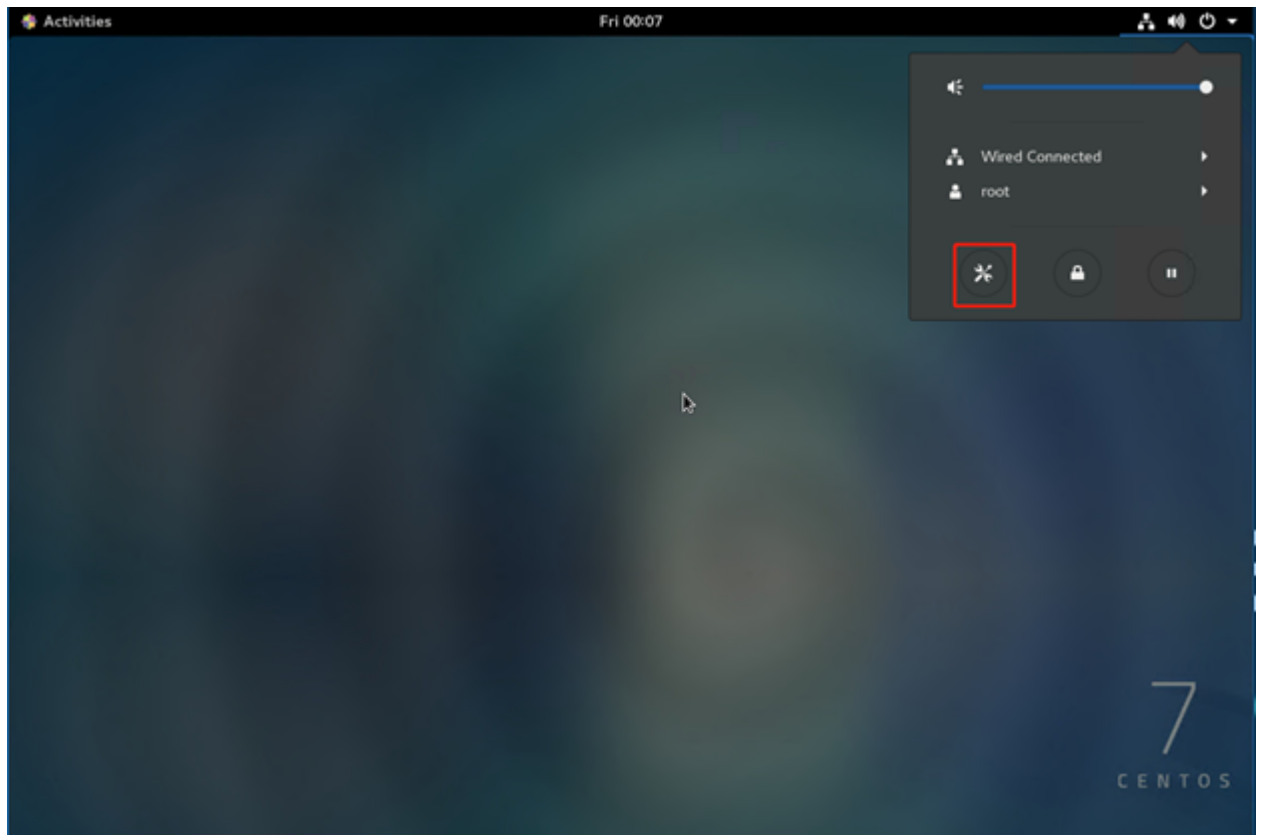
You have migrated the existing Arcserve Appliance to another fresh Arcserve Appliance successfully.

Modify the Input Source of Pre-installed Linux Backup Server

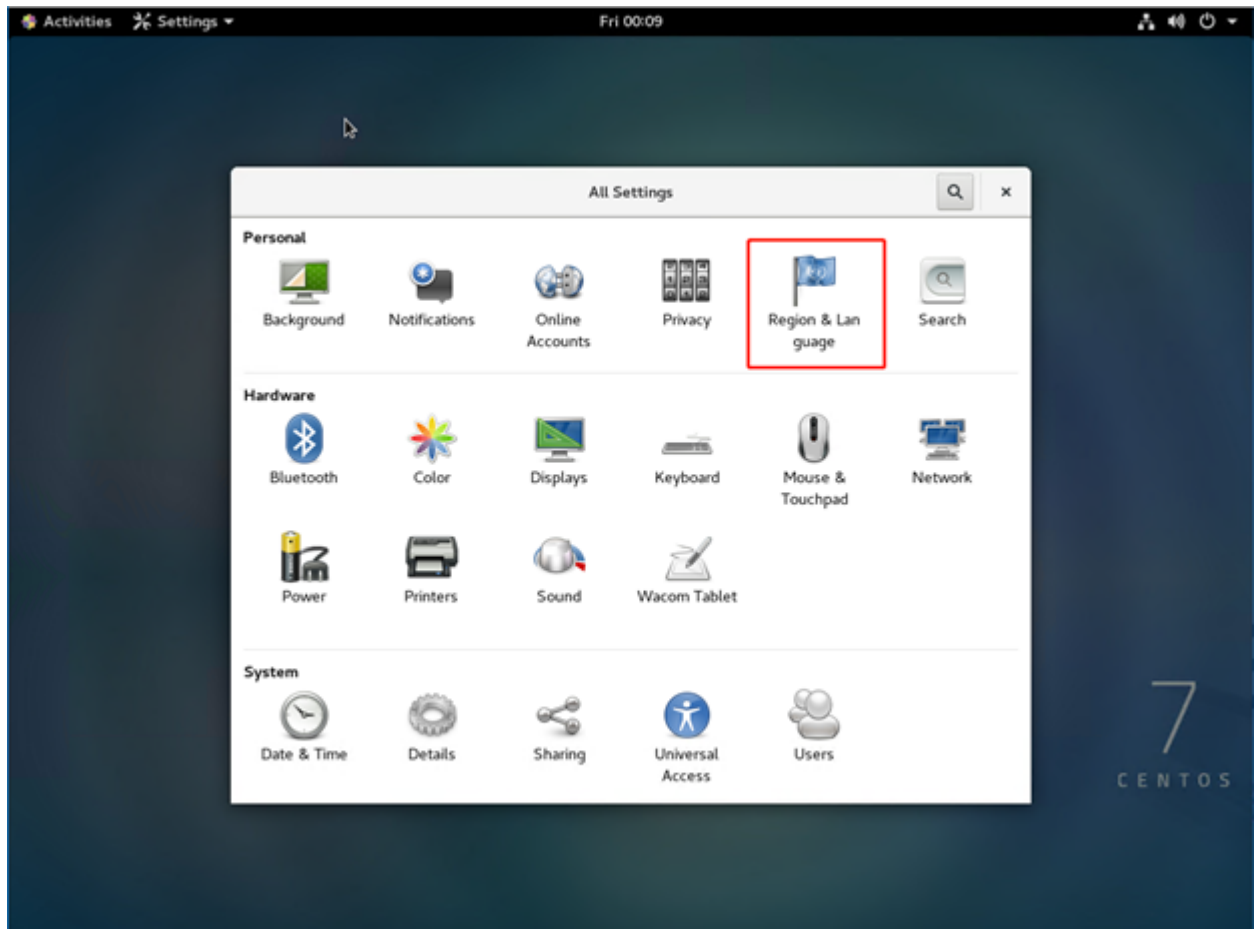
You can change the Keyboard of pre-installed Linux Backup Server.

Follow these steps:

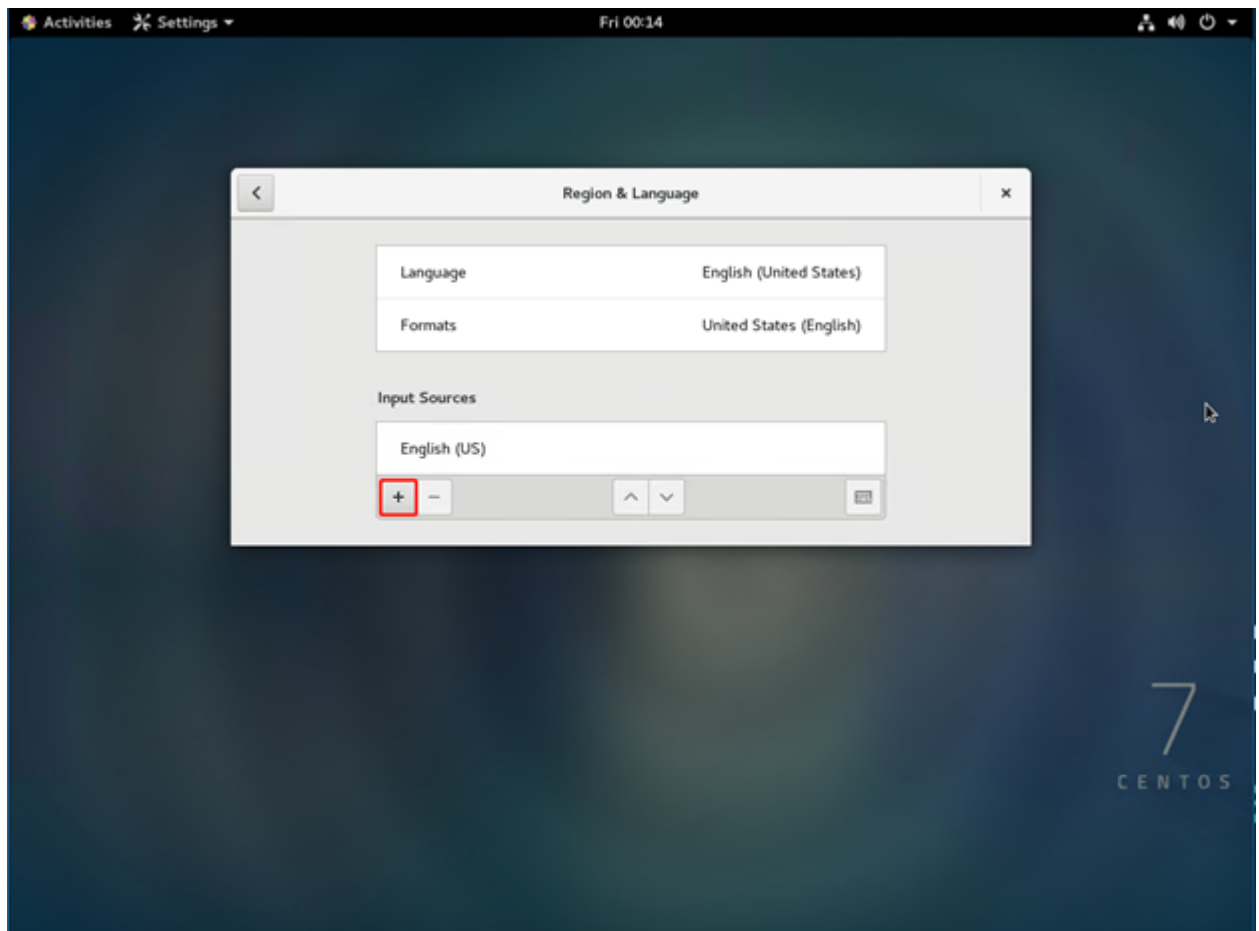
1. Log into Arcserve Appliance as administrator.
2. Click **Settings**.



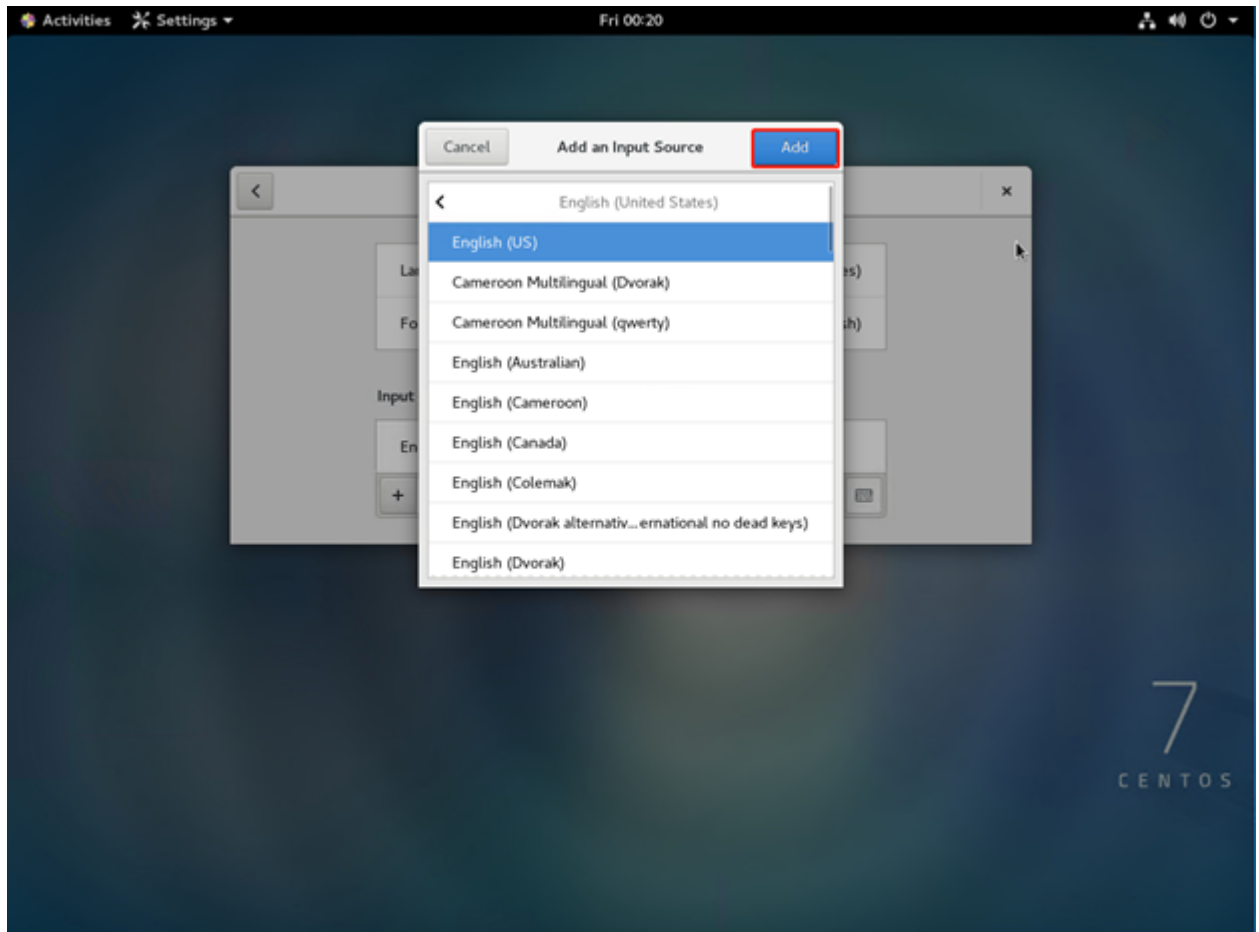
3. Click **Region & Language**.



4. Click + to select a new input source.



5. Select the language and keyboard layout.



6. Click **Add**.

Input source is successfully added.

Chapter 7: Monitoring the Appliance Server Remotely

You can monitor Arcserve Appliance remotely.

This section contains the following topics:

Working with Integrated Dell Remote Access Controller (iDRAC)	111
---	-----

Working with Integrated Dell Remote Access Controller (iDRAC)

This section contains the following topics:

Monitor and Manage Integrated Dell Remote Access Controller (iDRAC)

Arcserve Appliance 9012-9504DR series models are installed with Integrated Dell Remote Access Controller 9 (iDRAC9). iDRAC9 lets the server administrators improve the overall availability of Arcserve Appliance. iDRAC provides the alerts to administrators about server issues, allows to perform remote server management, and reduces the need for physical access to the server.

You must log into iDRAC to monitor system status, manage system information and launch virtual console.

Follow these steps:

Log into iDRAC:

1. Launch a browser and navigate to *https://<iDRAC-IP-address>*.
iDRAC login page displays.
2. Enter the following information:
User Name: root
Password: ARCADMIN
3. Click **Login**.

Monitor System Status and Manage System Information:

You can monitor iDRAC system status and manage the following system information:

- System health
- System properties
- Hardware and firmware inventory
- Sensor health
- Storage devices
- Network devices
- View and terminate user sessions

Launch Virtual Console:

1. Log into *https://<iDRAC-IP-address>*
2. Navigate to Dashboard and click **Launch Virtual Console**.

The Virtual Console page displays.

The Virtual Console Viewer displays the remote system desktop. You can take the control of remote system and run the operations using keyboard and mouse.

Find the IP address of Integrated Dell Remote Access Controller for 9000 Series (iDRAC)

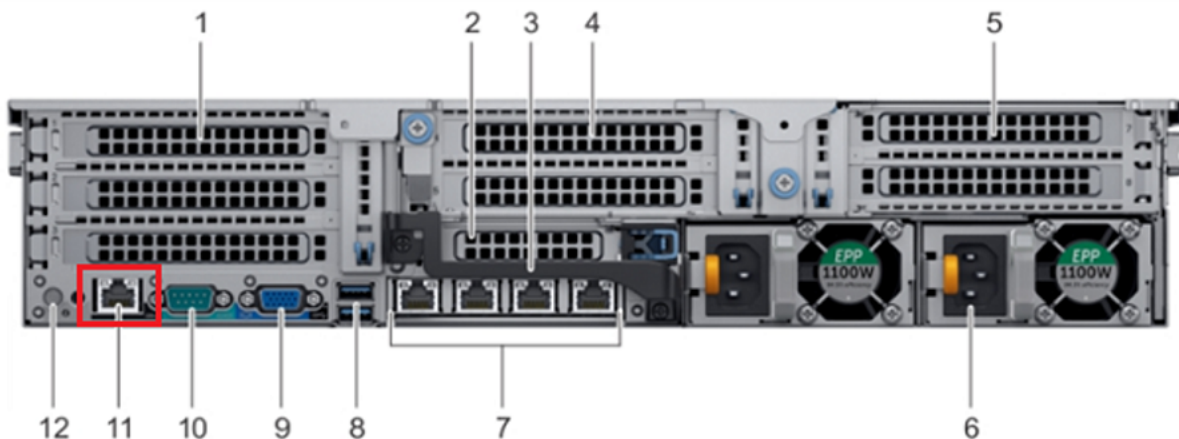
Arcserve Appliance 9012-9504DR series models are configured to use DHCP for iDRAC by default. To access iDRAC, ensure that you connect the ethernet cable to the iDRAC9 dedicated network port. For information about rear panel and iDRAC9 dedicated network port of Arcserve Appliance 9012-9504DR series models, see [Rear Panel of 9012-9048](#), [Rear Panel of 9072DR-9504DR](#).

View Rear Panel of 9012-9048 for iDRAC9



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

View Rear Panel of 9072DR-9504DR for iDRAC9

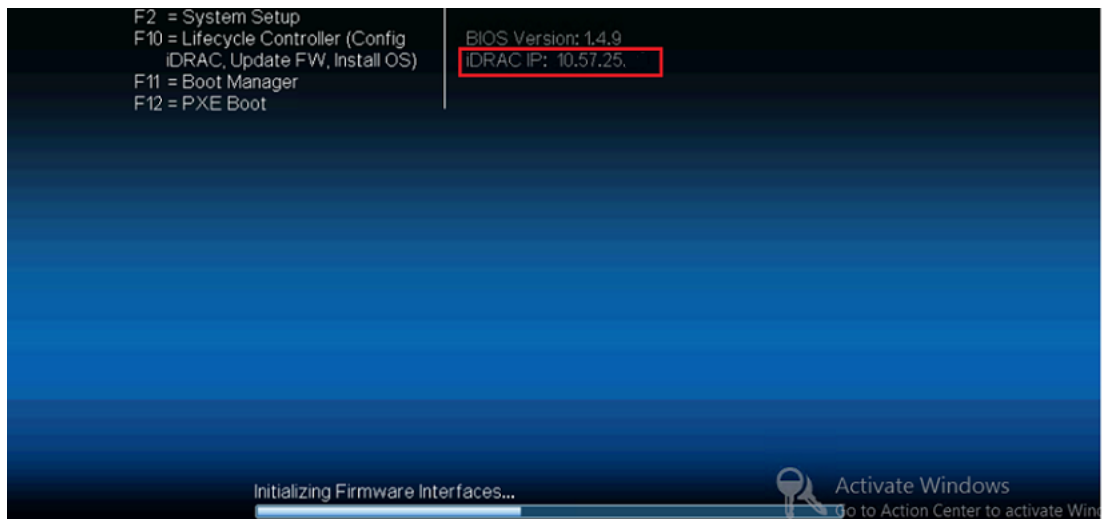


iDRAC9 dedicated network port on |
rear panel of Arcserve Appliance 9072DR-9504DR series models

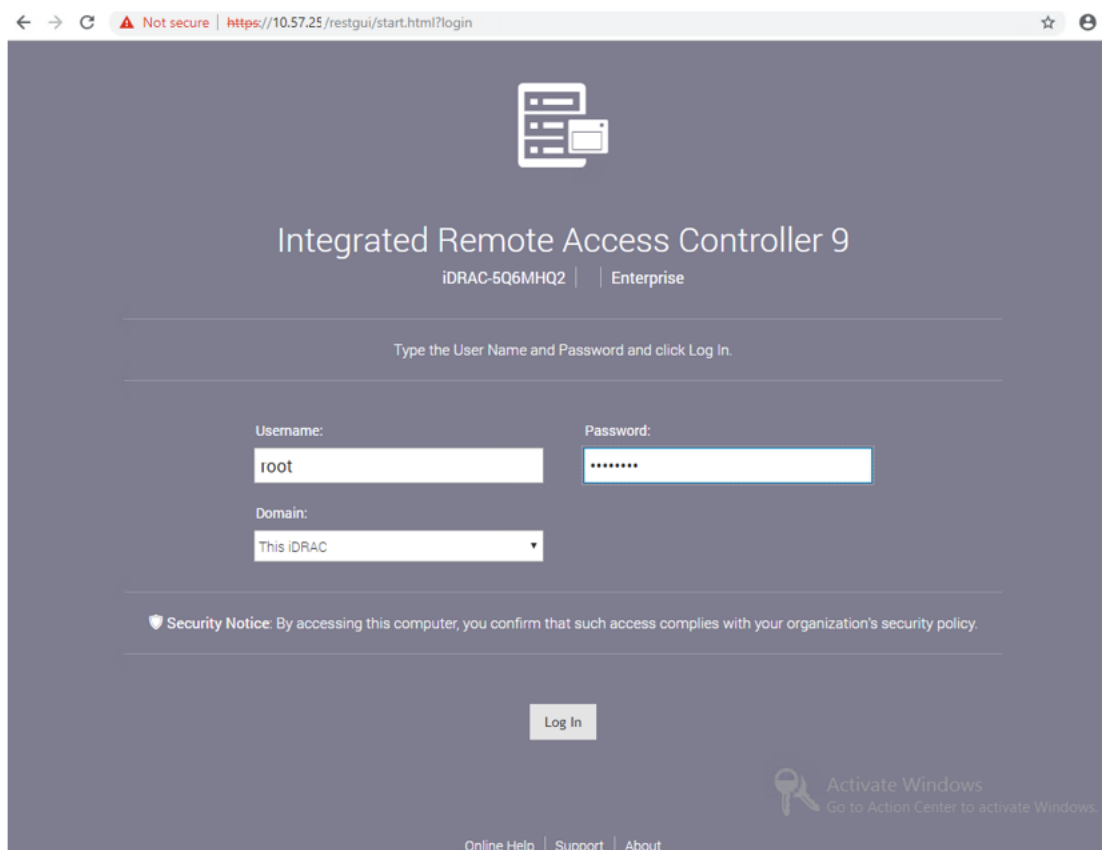
You can find the IP address of iDRAC from appliance.

Follow these steps:

1. Make a note of iDRAC IP while starting Arcserve Appliance.



2. Launch a browser and navigate to <https://<iDRAC-IP-address>>.



iDRAC login page is displayed.

Find the IP address of Integrated Dell Remote Access Controller for X Series (iDRAC)

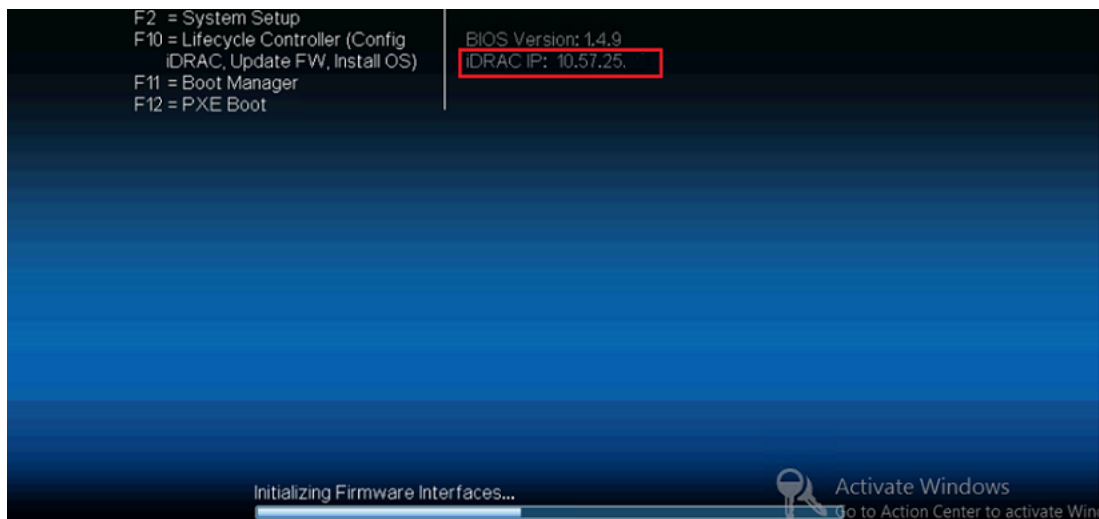
Arcserve Appliance X series model is configured to use DHCP for iDRAC by default. To access iDRAC, ensure that you connect the ethernet cable to the iDRAC9 dedicated network port. For information about rear panel and iDRAC9 dedicated network port of Arcserve Appliance X Series model, see [Rear Panel of X Series](#).

View Rear Panel of X Series

You can find the IP address of iDRAC from appliance.


Follow these steps:

1. Make a note of iDRAC IP while starting Arcserve Appliance.



2. Launch a browser and navigate to *https://<iDRAC-IP-address>*.

← → ↻ ⚠ Not secure | https://10.57.25/restgui/start.html?login ☆ ⓘ



Integrated Remote Access Controller 9

iDRAC-5Q6MHQ2 | Enterprise


Type the User Name and Password and click Log In.

Username:

Password:

Domain:

🛡 Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

 Activate Windows
Go to Action Center to activate Windows.

[Online Help](#) | [Support](#) | [About](#)

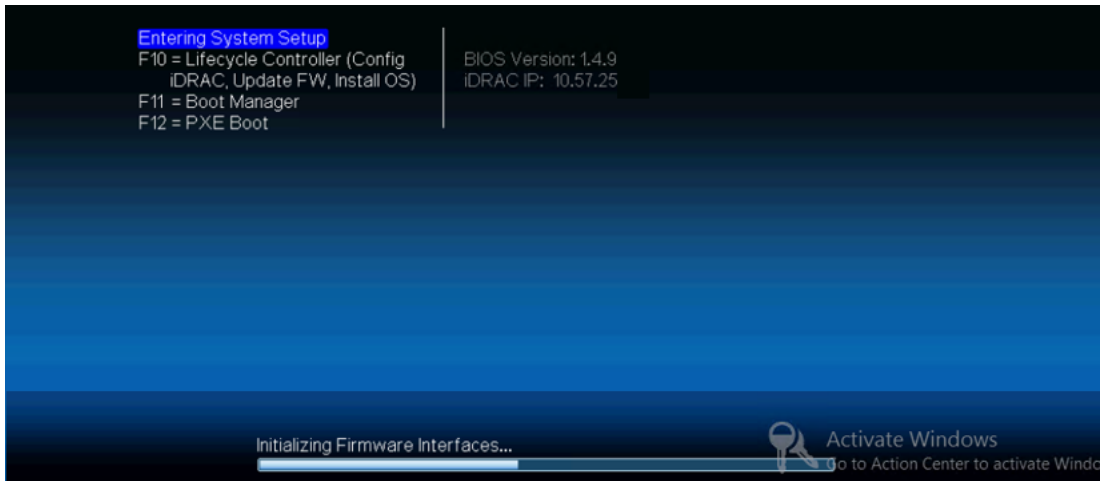
iDRAC login page is displayed.

Configure DHCP or Static IP address of iDRAC

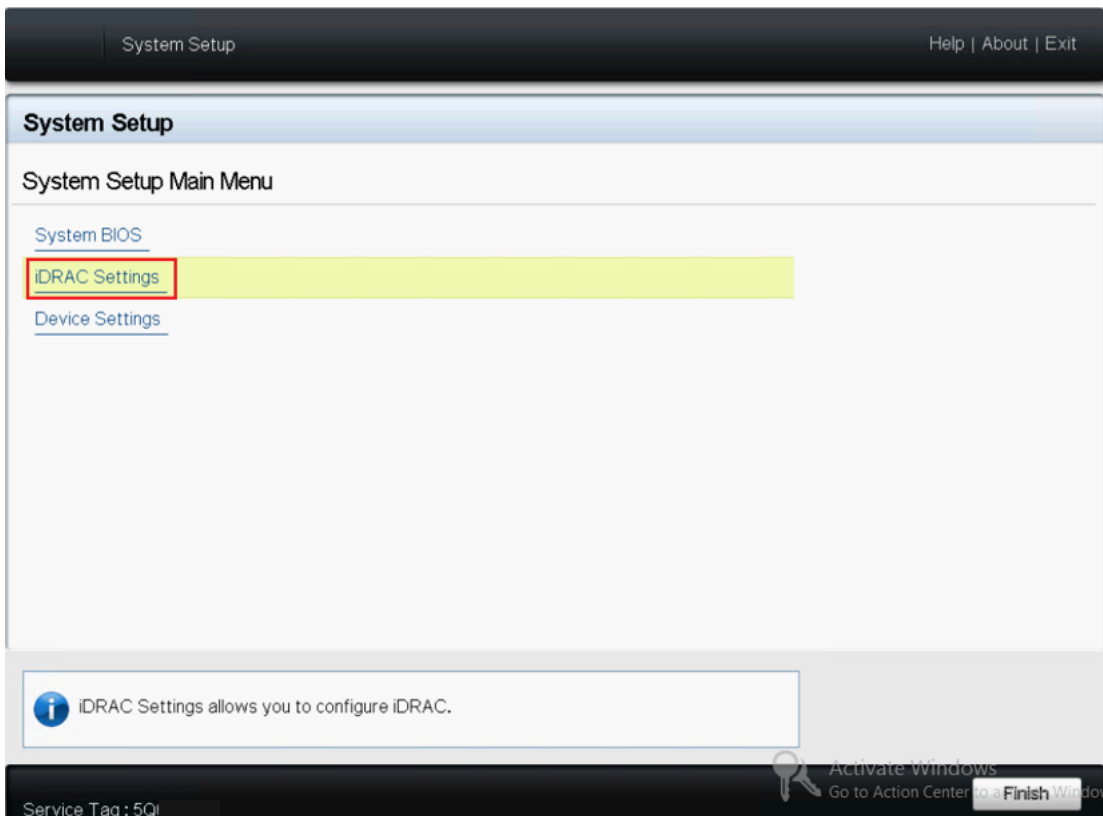
You can set DHCP network mode for iDRAC.

Follow these steps:

1. Press F2 while starting Arcserve Appliance and enter System Setup.

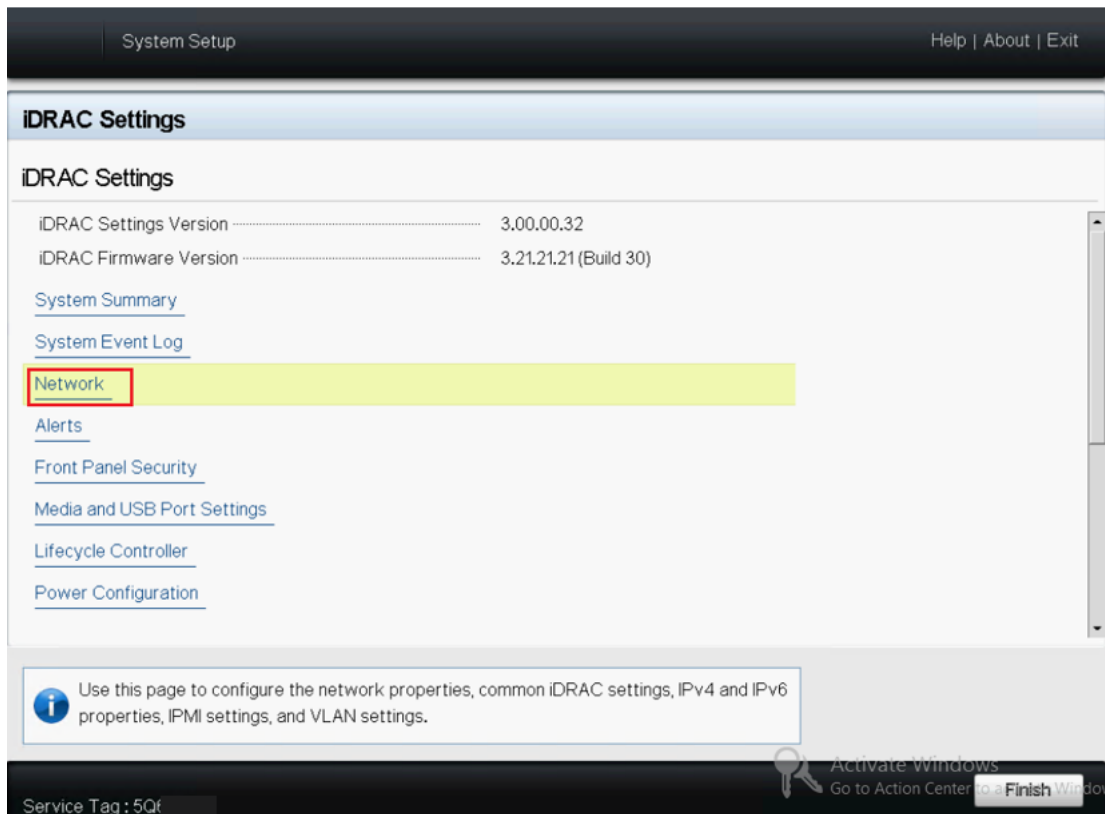


2. From the System Setup Main Menu screen, click **iDRAC Settings**.

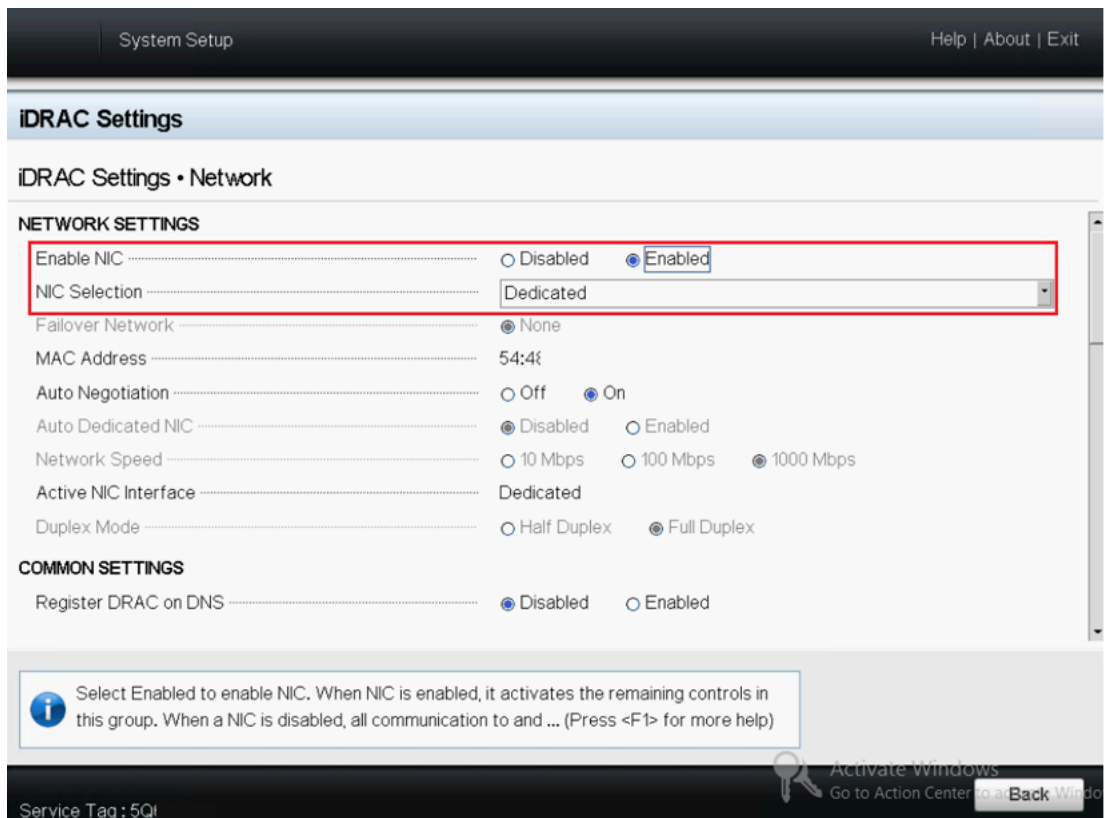


3. From the options of iDRAC Settings, click **Network**.

The Network Settings fields are displayed.



4. Select **Enabled** for **Enable NIC setting**, and select **Dedicated** for **NIC Selection** to use the dedicated network interface.



5. To set DHCP mode, from IPV4 Settings select the **Enabled** option for **Enable IPv4** and **Enable DHCP**.

System Setup Help | About | Exit

iDRAC Settings

iDRAC Settings • Network

Auto Config Domain Name ☒ Disabled ☐ Enabled

Static DNS Domain Name

IPV4 SETTINGS

Enable IPv4 ☐ Disabled ☒ Enabled

Enable DHCP ☐ Disabled ☒ Enabled

IP Address

Gateway

Subnet Mask

Use DHCP to obtain DNS server addresses ☒ Disabled ☐ Enabled

Preferred DNS Server

Alternate DNS Server

IPV6 SETTINGS

Info Select Enabled to enable NIC. When NIC is enabled, it activates the remaining controls in this group. When a NIC is disabled, all communication to and ... (Press <F1> for more help)

Service Tag: 50L...

Activate Windows
Go to Action Center to activate Windows
[Back](#)

Note: If you want to set Static IP for iDRAC dedicated network, set **Enable IPv4** as **Enabled** and **Enable DHCP** as **Disabled**. Set IP Address, Gateway, and Subnet Mask according to the network configuration.

System Setup Help | About | Exit

iDRAC Settings

iDRAC Settings • Network

Auto Config Domain Name ☒ Disabled ☐ Enabled

Static DNS Domain Name

IPv4 SETTINGS

Enable IPv4 ☐ Disabled ☒ Enabled

Enable DHCP ☒ Disabled ☐ Enabled

IP Address

Gateway

Subnet Mask

Use DHCP to obtain DNS server addresses ☒ Disabled ☐ Enabled

Preferred DNS Server

Alternate DNS Server

IPv6 SETTINGS

Select Enabled to enable NIC. When NIC is enabled, it activates the remaining controls in this group. When a NIC is disabled, all communication to and ... (Press <F1> for more help)

Service Tag: 5QL... Activate Windows
Go to Action Center to activate Windows

- Click **Back**, click **Finish**, and then click **Yes** on the **Warning** dialog.

The network information is saved.

System Setup Help | About | Exit

iDRAC Settings

iDRAC Settings

iDRAC Settings Version 3.00.00.32

iDRAC Firmware Version 3.21.21.21 (Build 30)

[System Summary](#)

[System Event Log](#)

[Network](#)

[Alerts](#)

[Front Panel Security](#)

[Media and USB Port Settings](#)

[Lifecycle Controller](#)

[Power Configuration](#)

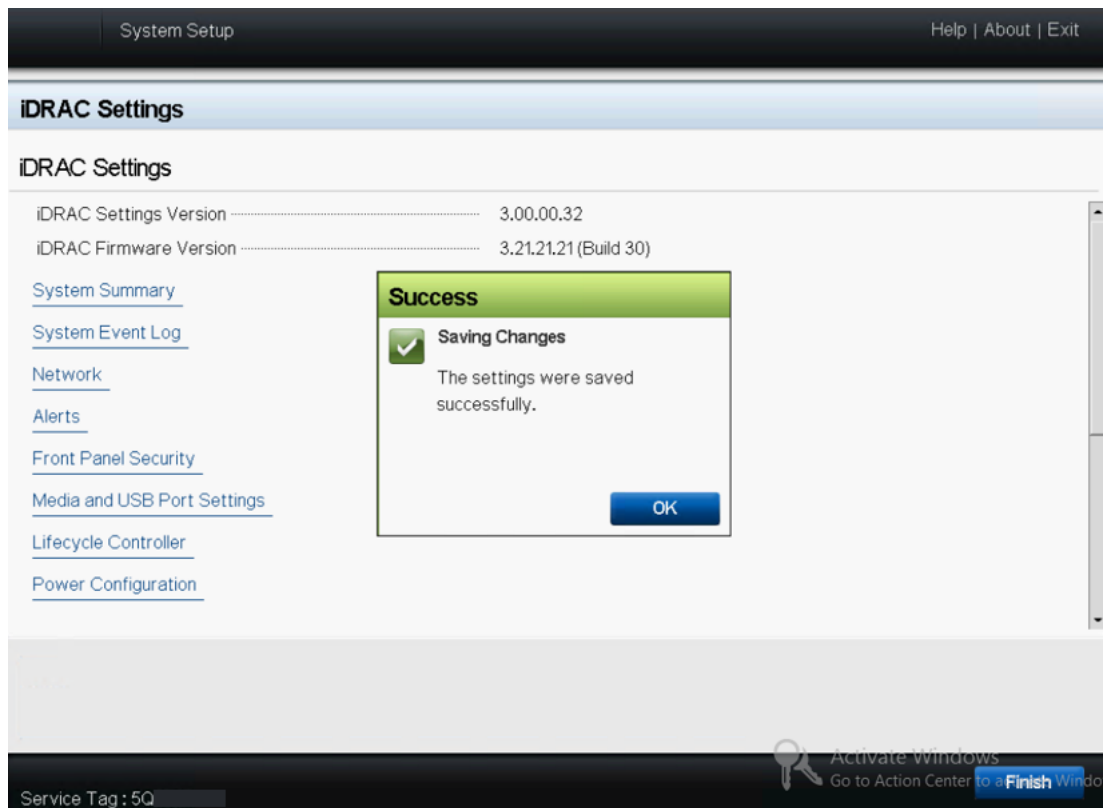
Warning

Saving Changes

Settings have changed. Do you want to save the changes?

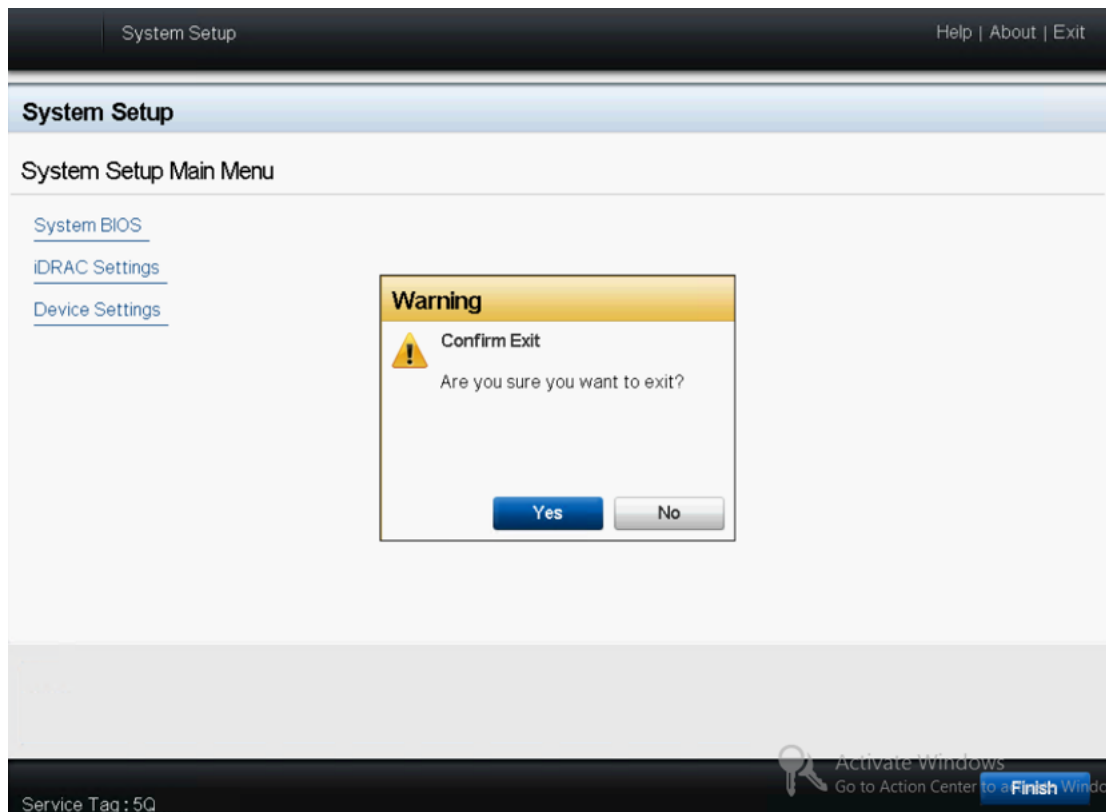
Service Tag: 5C... Activate Windows
Go to Action Center to activate Windows

7. From the **Success** dialog, Click **OK**.



You have completed configuration of iDRAC DHCP.

8. Click **Finish** and then click **Yes** to exit the Setup and boot the system.



The DHCP network mode for iDRAC is configured.

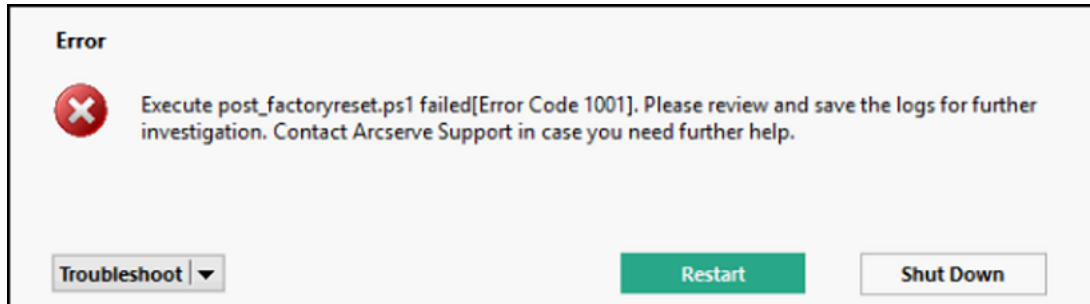
Chapter 8: Restoring or Repairing the Arcserve Appliance

This section contains the following topics:

Debug Factory Reset	125
Apply Arcserve UDP Factory Reset Using Boot Option in 9012-9504DR Series Appliance	127
Apply Arcserve UDP Factory Reset Using Boot Option in X Series Appliance	129
Clear Configuration and Apply Appliance Factory Reset	132
Replace Factory Reset Image Using Set Appliance Image Utility	134
Remove and Replace a Hard Drive	137
Perform Bare Metal Recovery (BMR) without Preserving Data	139
Perform Bare Metal Recovery (BMR) and Preserving Data	155

Debug Factory Reset

The topic describes how to debug factory reset when you receive the following Error message:



To resolve the issue, perform the following steps:

1. From the Error message, click the drop-down option of **Troubleshoot**.

The following options are displayed:

Command Prompt

The CMD (command prompt) dialog box lets you perform some basic operation. For example, verify if a file exists in the folder, copy files, delete files, and get the disk layout information.

View Logs

View logs option lets you view the logs in Notepad. You can check the logs and save the logs for further help by clicking *File, Save As*.

Restart Factory Reset

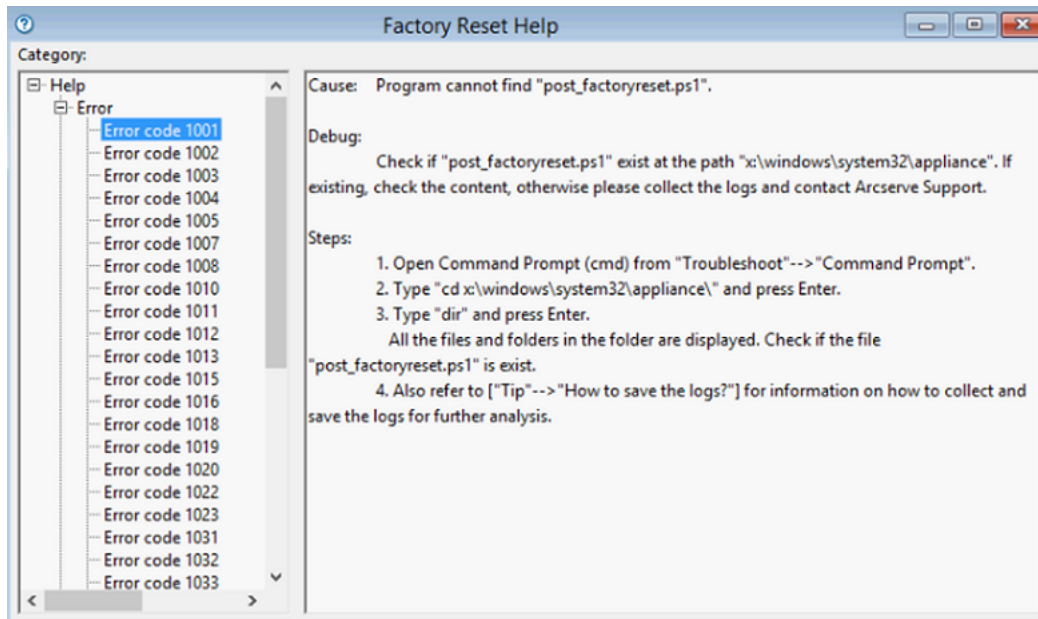
This option lets you restart Factory Reset when the issue is resolved.

Help

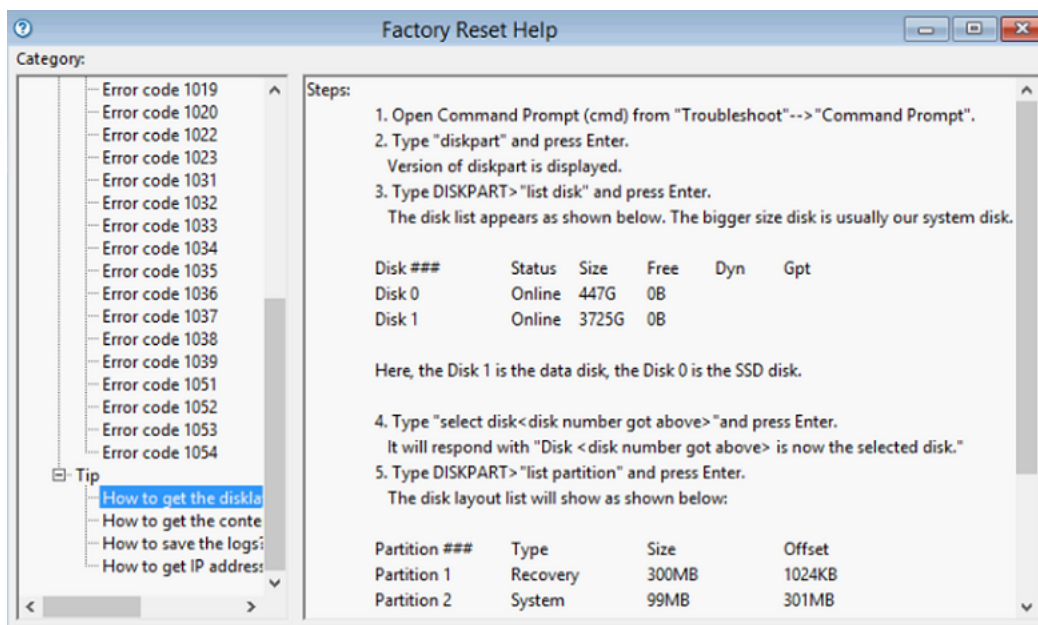
The Help Dictionary dialog box provides information about the cause, basic analysis, and solutions for the error. Follow the steps to resolve the issue. Some tips about common operations are also displayed. For example, how to get the disk layout, how to get the content of factory reset property file, how to save the logs.

2. From the options displayed, click **Help**.

The screen displays multiple Error Code with details.



3. Navigate to **Tip** of the Error code displayed in Error message and follow the instructions as displayed in the right panel below.



Selecting the right error and following the instructions displayed in tip helps to resolve Factory Reset.

Apply Arcserve UDP Factory Reset Using Boot Option in 9012-9504DR Series Appliance

You can apply UDP factory reset from the Boot Menu of the Arcserve Appliance 9012-9504DR series. Using UDP factory reset, you can return your Arcserve Appliance 9012-9504DR series to clean and non-configured status.

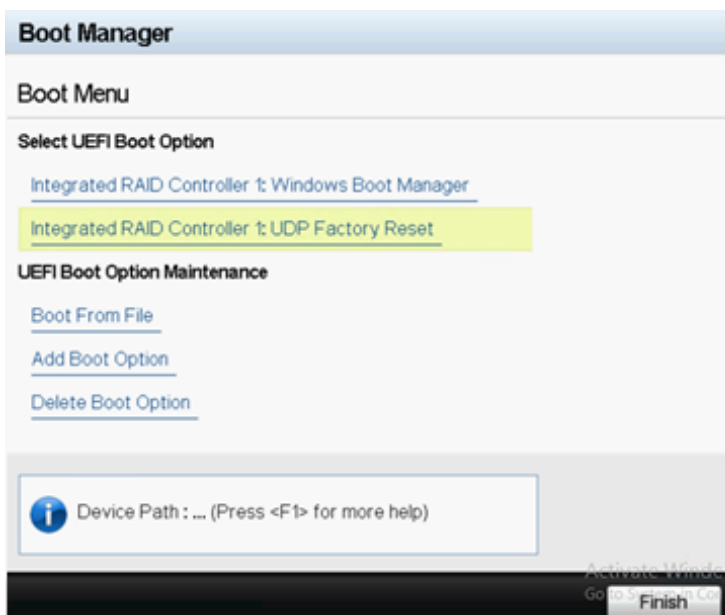
Note: You can also select the Preserve the backup data option while running UDP factory reset.

Follow these steps:

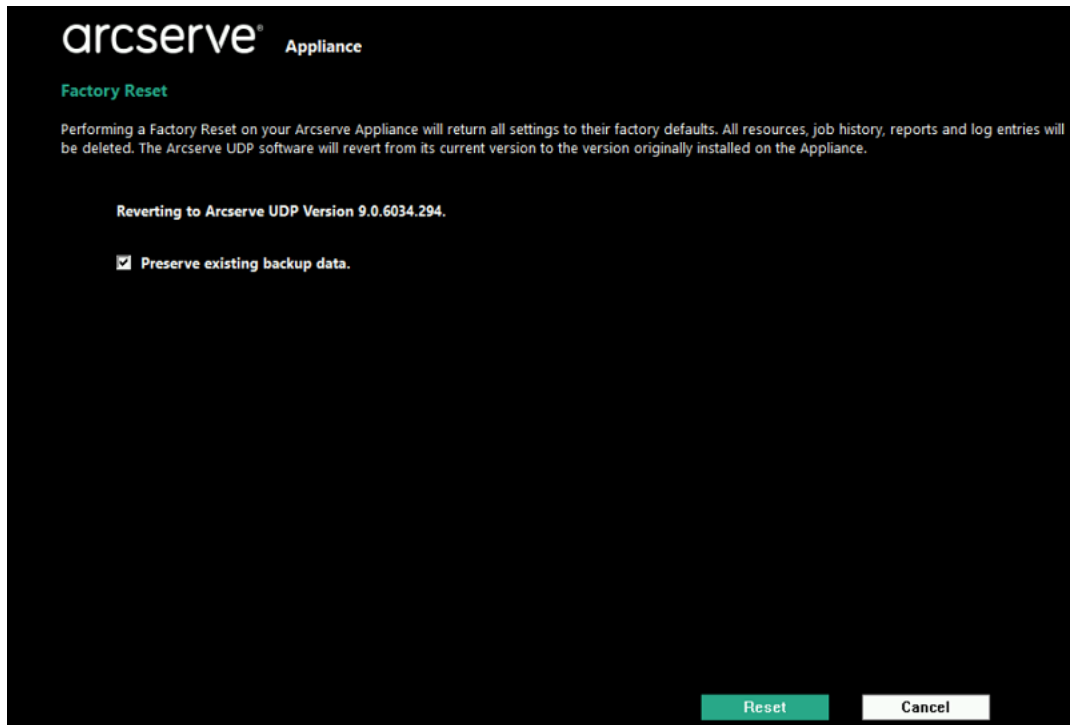
1. Press F11 on the keyboard to invoke Boot Menu.



2. Select the boot option **Integrated RAID Controller 1: UDP Factory Reset**.



A page about factory reset is displayed.

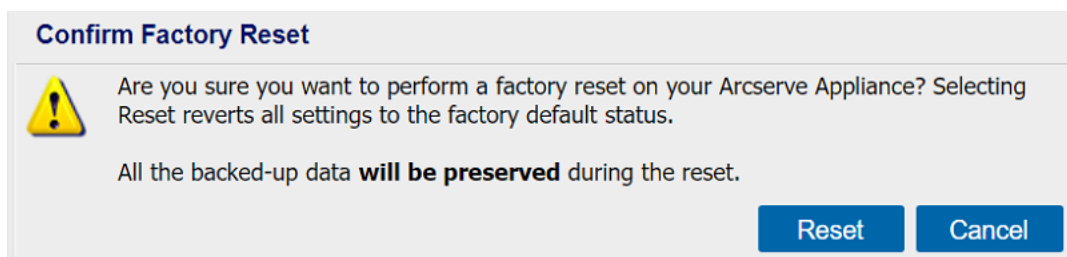


Notes:

- The **Preserve existing backup data** option is selected by default. Only C:\ volume in the original operating system is rebuilt. Data at X:\ volume and Y:\ volume remain unchanged.
- If you clear the selection of the Preserve existing backup data option, all the data on the respective volumes of C:\, X:\, and Y:\ in the original operating system is rebuilt.

3. Click **Reset**.

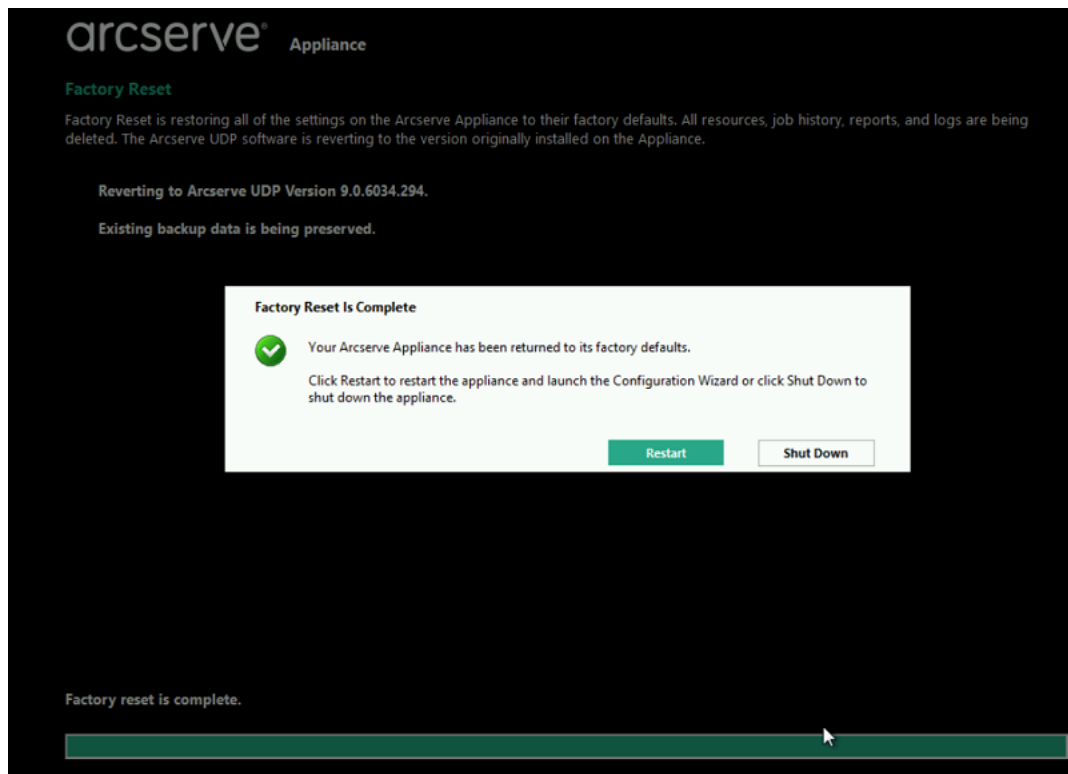
A confirmation dialog appears.



You can click **Cancel** to reboot the Arcserve Appliance unit.

4. After factory reset finishes, you can perform either of the following actions:

- ♦ Click **Restart** to reboot the appliance.
- ♦ Click **Shut Down** to close the appliance.



Apply Arcserve UDP Factory Reset Using Boot Option in X Series Appliance

You can apply UDP factory reset from the Boot Menu of the Arcserve Appliance X series. Using UDP factory reset, you can return your Arcserve Appliance X series to clean and non-configured status.

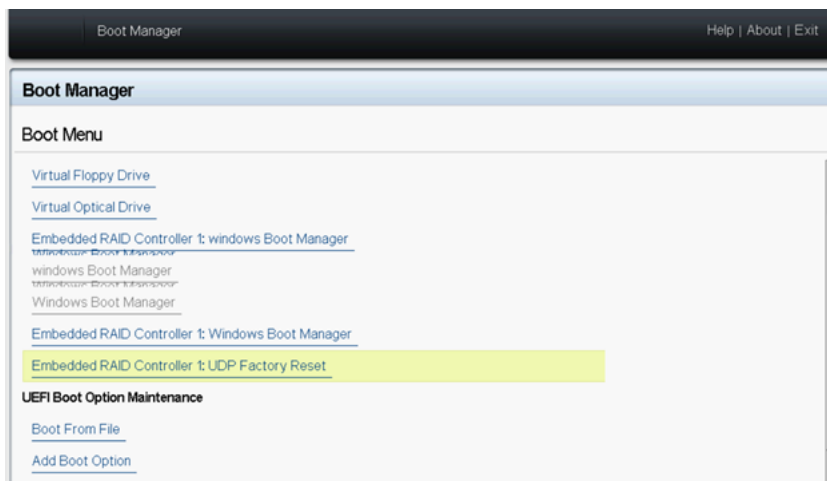
Note: You can also select the Preserve the backup data option while running UDP factory reset.

Follow these steps:

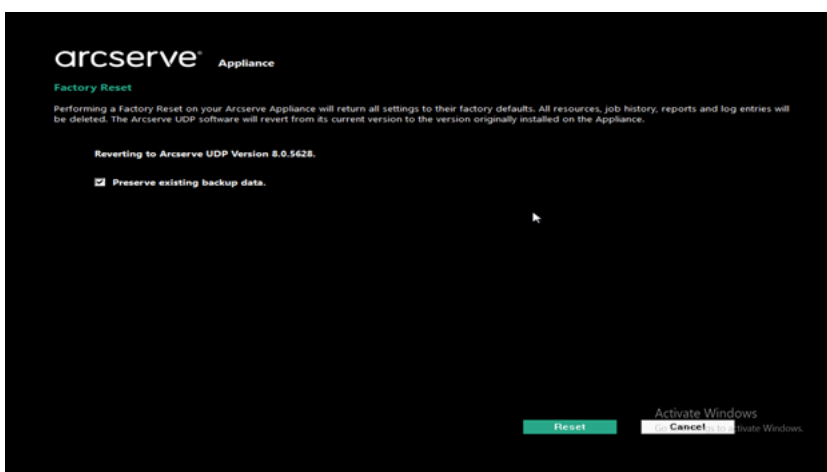
1. Press F11 on the keyboard to invoke Boot Menu.



2. Select the boot option **Embedded RAID Controller 1: UDP Factory Reset**.



A page about factory reset is displayed.

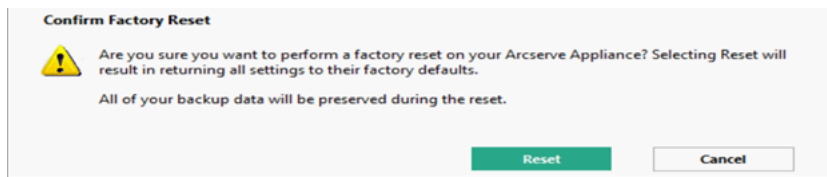


Notes:

- The **Preserve existing backup data** option is selected by default. Only C:\ volume in the original operating system is rebuilt. Data at X:\ volume and Y:\ volume remain unchanged.
- If you clear the selection of the Preserve existing backup data option, all the data on the respective volumes of C:\, X:\, and Y:\ in the original operating system is rebuilt.

3. Click **Reset**.

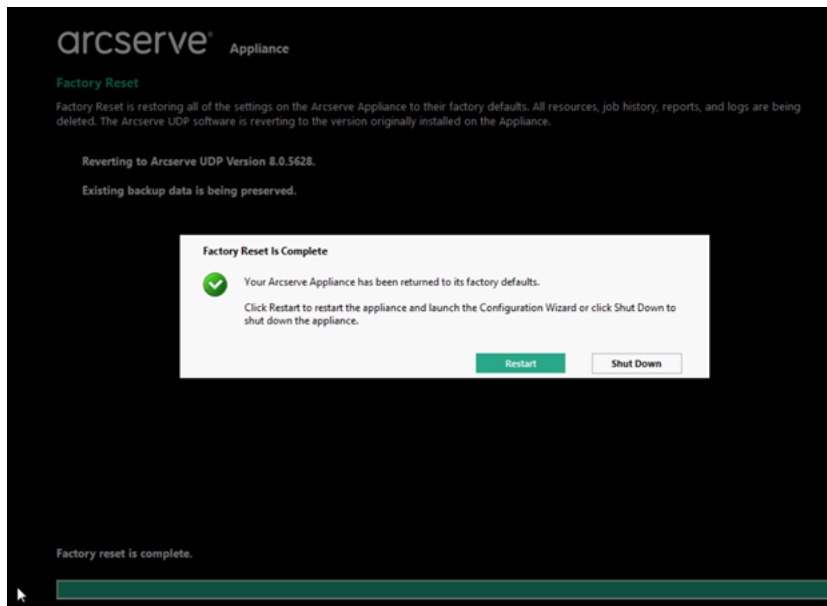
A confirmation dialog appears.



You can click **Cancel** to reboot the Arcserve Appliance unit.

4. After factory reset finishes, you can perform either of the following actions:

- ✦ Click **Restart** to reboot the appliance.
- ✦ Click **Shut Down** to close the appliance.

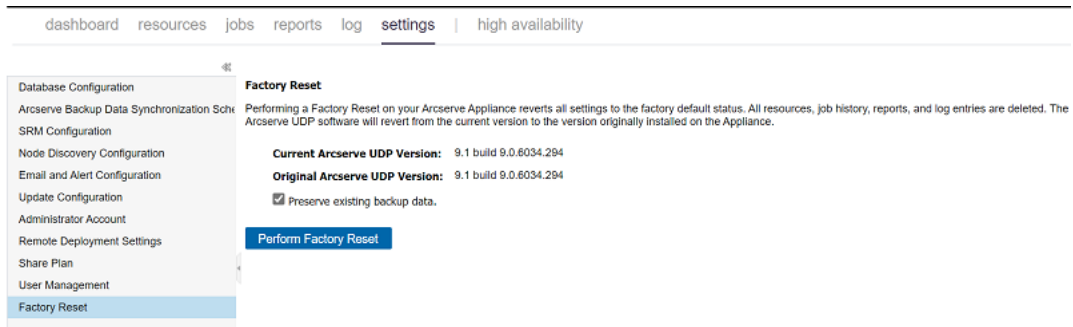


Clear Configuration and Apply Appliance Factory Reset

Using Factory Reset, you can return your Arcserve Appliance back to clean and non-configured status. You can apply factory reset from the Arcserve UDP Console.

Follow these steps:

1. Click **Factory Reset** on the **settings** tab from the Arcserve UDP Console.



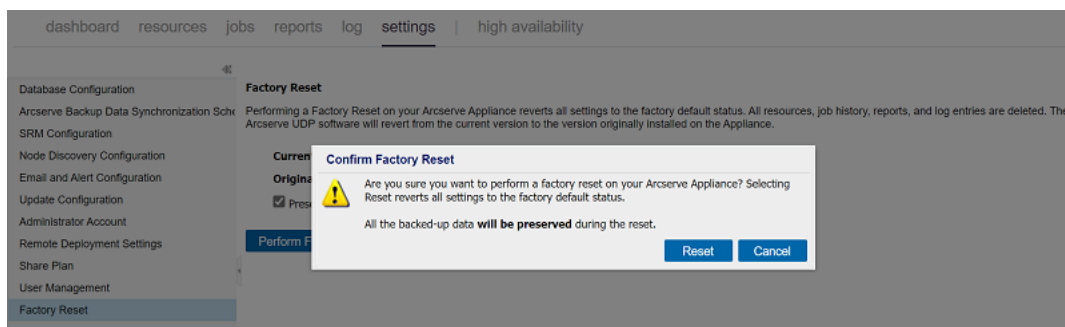
All the backed up data is preserved by default.

Note: Arcserve UDP provides the **Preserve existing backup data** option to help you preserve the existing datastore.

- ♦ If you select the **Preserve existing backup data** option, only *C:\ volume* is rebuilt. Data at *X:\ volume* and *Y:\ volume* remain unchanged.
- ♦ If you do not select the **Preserve existing backup data** option, all the data on the respective volumes of *C:* , *X:* and *Y:* is rebuilt.

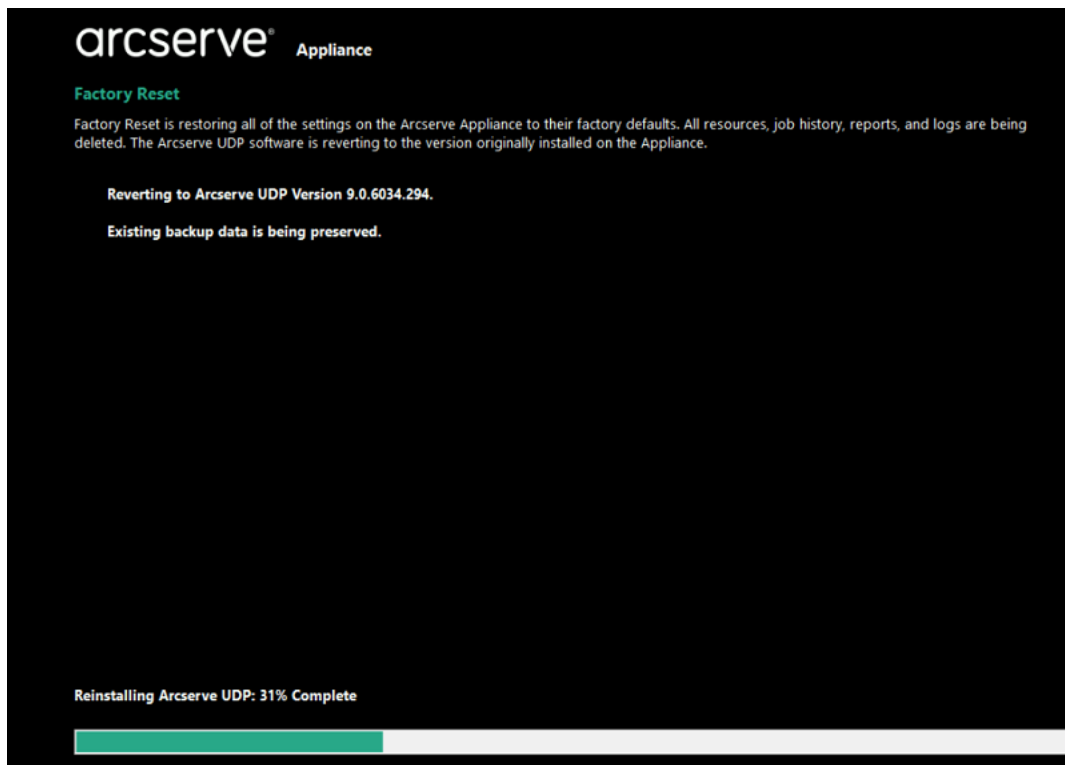
2. Click **Perform Factory Reset**.

A confirmation dialog appears.



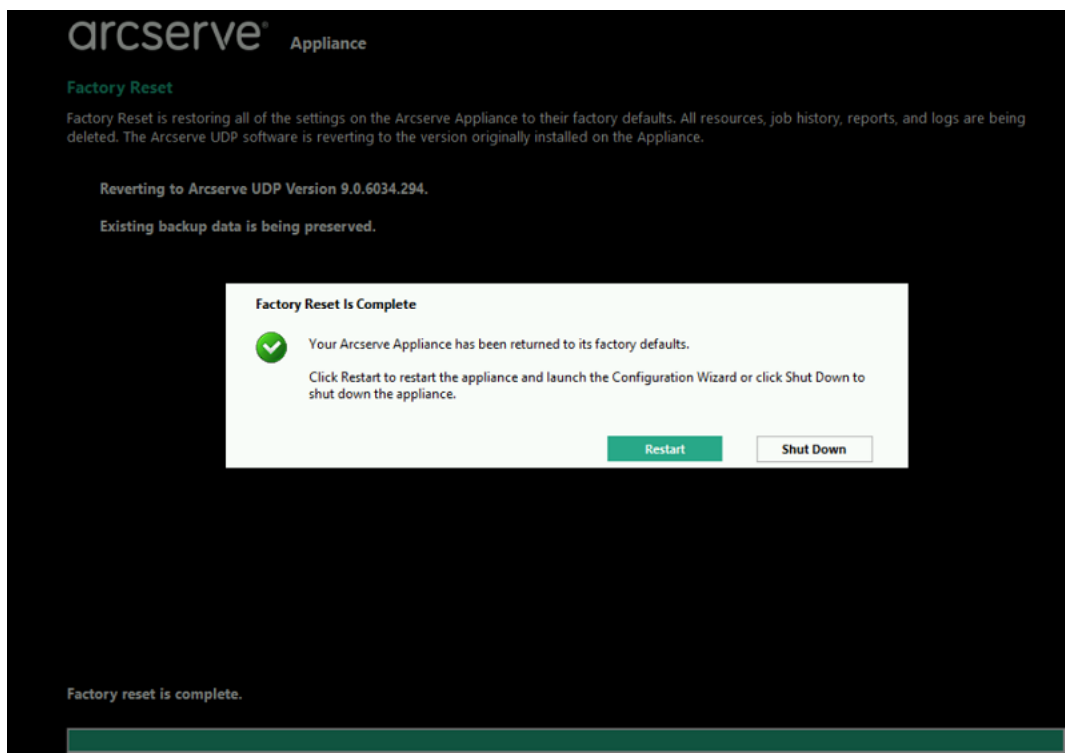
3. From the confirmation dialog, click **Reset** to launch the factory reset.

The Appliance machine is rebooted, and the factory reset runs as follows:



Completion of factory reset displays a confirmation dialog.

4. On the confirmation dialog, perform one of the following options:
 - ♦ Click **Restart** to reboot the appliance.
 - ♦ Click **Shut Down** to close the appliance.



Replace Factory Reset Image Using Set Appliance Image Utility

Set Appliance Image Utility tool helps you to replace the original Appliance image in current system with desired Appliance image of Arcserve Appliance available versions.

After executing the utility, perform factory reset which is available in the Arcserve UDP Console to revert Appliance to desired released version of Arcserve Appliance in factory default setting. Set Appliance Image utility is available for Arcserve Appliance v6.5 Update 1 or later releases.

Note: The Appliance image used for replacement should have higher version than the *Original Arcserve UDP version* installed on the Arcserve Appliance. Replacing the Arcserve Appliance image with a different Windows operating system version is not supported.

To verify the original Arcserve UDP version, log into Arcserve UDP Console, navigate to **settings** and select **Factory Reset** for the version details.

Factory Reset

Performing a Factory Reset on your Arcserve UDP Appliance will return all settings to their factory defaults. All resources, job history, reports, and log entries will be deleted. The Arcserve UDP software will revert from its current version to the version originally installed on the Appliance.

Current Arcserve UDP Version: 6.5.4175 update 4 build 1223

Original Arcserve UDP Version: 6.5.4175 update 4 build 1223

☒ Preserve existing backup data.

Perform Factory Reset

Note: The above screen refers to Arcserve Appliance v6.5 Update 4 and may vary from other release versions of Arcserve Appliance.

Example scenario to replace factory reset image for Arcserve Appliance v6.5 Update 4 with Appliance 7.0 factory reset image of Appliance 9000 series

The example below describes the process to replace factory reset image. You can follow the same process for other versions also.

How to Use Set Appliance Image Utility to revert from Arcserve Appliance v6 Update 4 to Arcserve Appliance 7.0

Follow these steps:

1. Download the Appliance factory reset image of Arcserve Appliance 9000 series, and execute the Set Appliance Image Utility. Perform the following steps to use set Appliance Image Utility:

- a. To download the 7.0 factory reset image, [contact Arcserve Support](#).
- b. Open the Windows command line and run the following command:

```
C:\Program Files\Arcserve\Unified Data Protection\Management\bin\Appliance\SetImage.exe -applianceimage <Fullpath of the appliance image just downloaded>
```

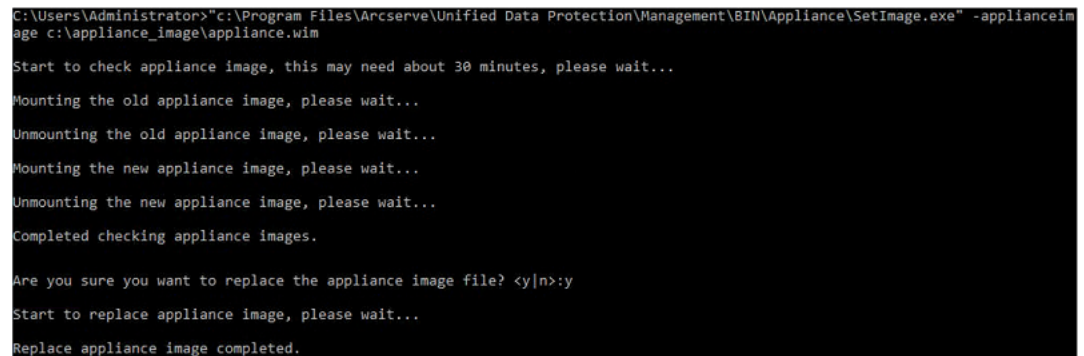
After checking appliance images finished step is complete, you can view the following query:

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

- c. Enter *y* or *yes* to replace the image or enter *n* or *no* to exit the execution.

When the image replication is complete, the command line displays the following message:

Replace appliance image completed.



```
C:\Users\Administrator>"C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\SetImage.exe" -applianceimage c:\appliance_image\appliance.wim
Start to check appliance image, this may need about 30 minutes, please wait...
Mounting the old appliance image, please wait...
Unmounting the old appliance image, please wait...
Mounting the new appliance image, please wait...
Unmounting the new appliance image, please wait...
Completed checking appliance images.
Are you sure you want to replace the appliance image file? <y|n>:y
Start to replace appliance image, please wait...
Replace appliance image completed.
```

2. Perform the following steps to revert to Arcserve Appliance 7.0:

Note: After replacing Appliance factory reset image in Arcserve UDP Console, the Original Arcserve UDP version is changed to the desired Appliance release version.

- a. From Arcserve UDP Console, navigate to **Settings** and select **Factory Reset**.

Factory Reset

Performing a Factory Reset on your Arcserve UDP Appliance will return all settings to their factory defaults. All resources, job history, reports, and log entries will be deleted. The Arcserve UDP software will revert from its current version to the version originally installed on the Appliance.

Current Arcserve UDP Version: 6.5.4175 update 4 build 1223

Original Arcserve UDP Version: 7.0.4455

☒ Preserve existing backup data.

Perform Factory Reset

The *Original Arcserve UDP Version* changes to Arcserve Appliance 7.0.

Note: Reload the page if desired Appliance release version is not displayed in *Original Arcserve UDP version* after replacing the Appliance image.

- b. Click **Perform Factory Reset** to revert from current version of Appliance to the new Arcserve Appliance 7.0 version.

For more information about Factory Reset, refer the [link](#).

Remove and Replace a Hard Drive

With the Arcserve Appliance, if one hard drive fails, the rest of the drives will kick in immediately to ensure no data is lost and the appliance continues to work normally. Therefore, to guard against any problems associated with multiple hard drive failures, it is important to replace a hard drive as soon as possible to minimize potential loss of data.

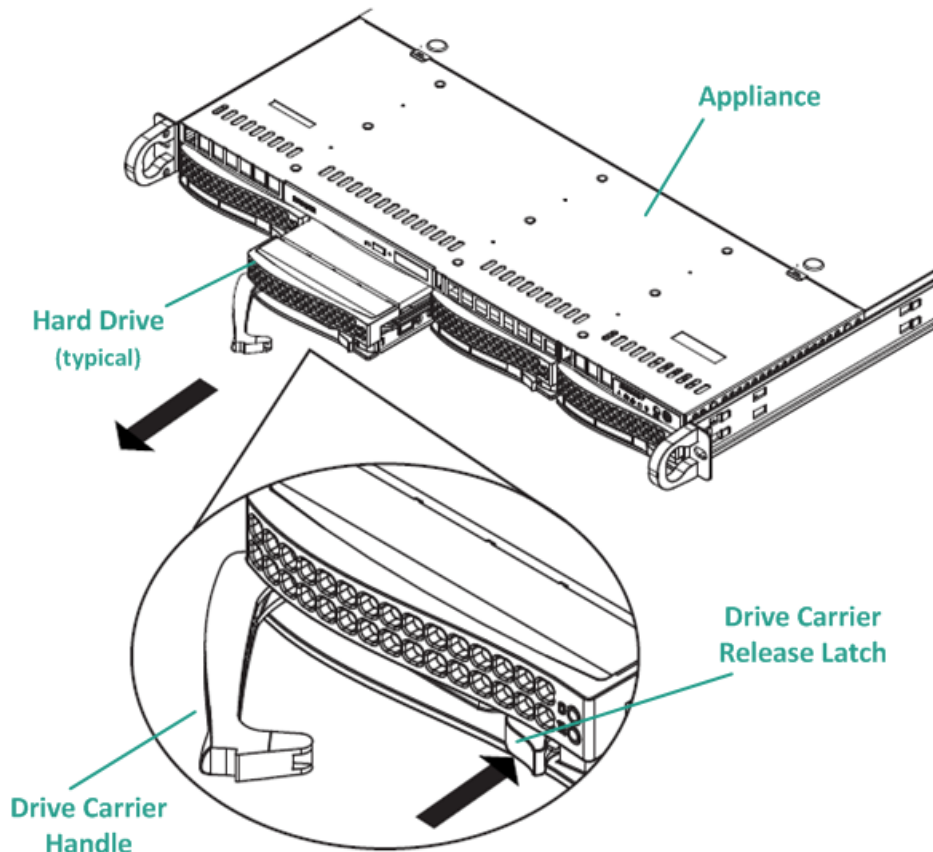
The Arcserve Appliance contains four hard drive carriers which are labeled 0, 1, 2 and 3 from left to right. If you replace more than one hard drive at a time, you should label the replacement hard drives so that you know which drive is placed into each drive carrier. You should also label the hard drives that you remove from the appliance so that you know which drive carrier they occupied.

Important! Take proper safety precautions when handling the hard drives because they are static-sensitive devices and can be easily damaged.

- Wear a wrist strap to prevent any static discharge.
- Touch a grounded object before removing the replacement hard disk from the antistatic shipping bag.
- Always handle a hard drive by the edges only and do not touch any of the visible components on the bottom.

Follow these steps:

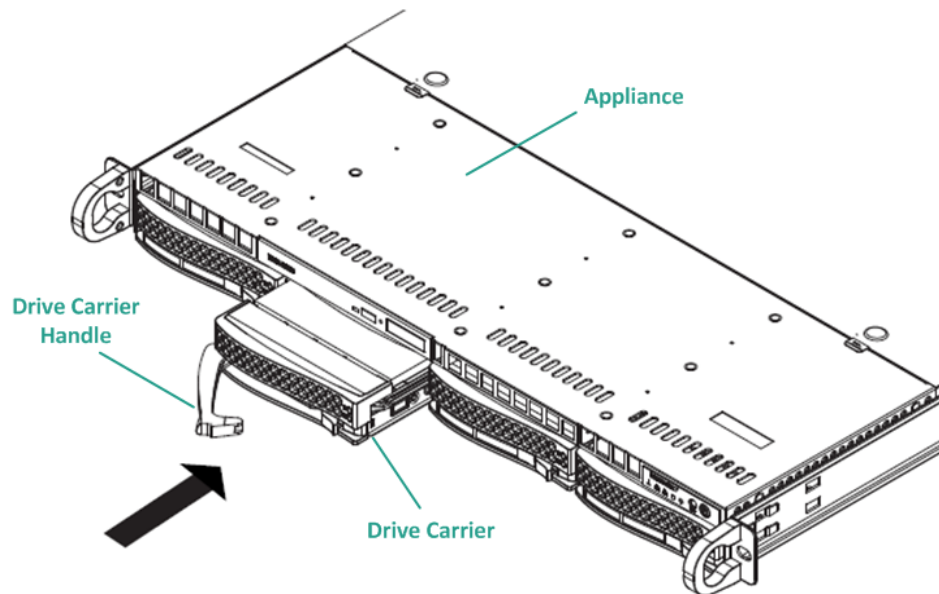
1. To gain access to the drive holders, you first need to remove the faceplate:
 - a. Unlock the faceplate lock.
 - b. Press the release knob to retract the faceplate pins.
 - c. Carefully remove the faceplate (using two hands).
2. Press the release latch on the drive carrier. This extends the drive carrier handle.



3. Using the handle, pull the drive carrier out from the front of the appliance. The hard drives are mounted in drive carriers to simplify their removal and replacement from the appliance. These carriers also help promote proper air-flow for the drive bays.

Important! Except for short periods of time (swapping of the hard drives), do not operate the appliance without the drive carriers fully installed.

4. Remove the old hard drive from the drive carrier and install the new hard drive being careful to properly orient the replacement hard drive with the label on top and the visible components on the bottom.
5. Slide the drive tray into the appliance until it is fully installed and secure by closing the drive carrier handle.



6. Obtain return instructions from Arcserve Support to return a defective drive.

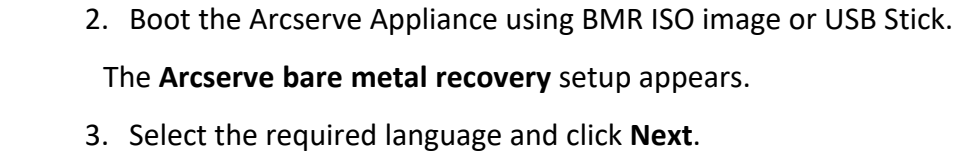
Perform Bare Metal Recovery (BMR) without Preserving Data

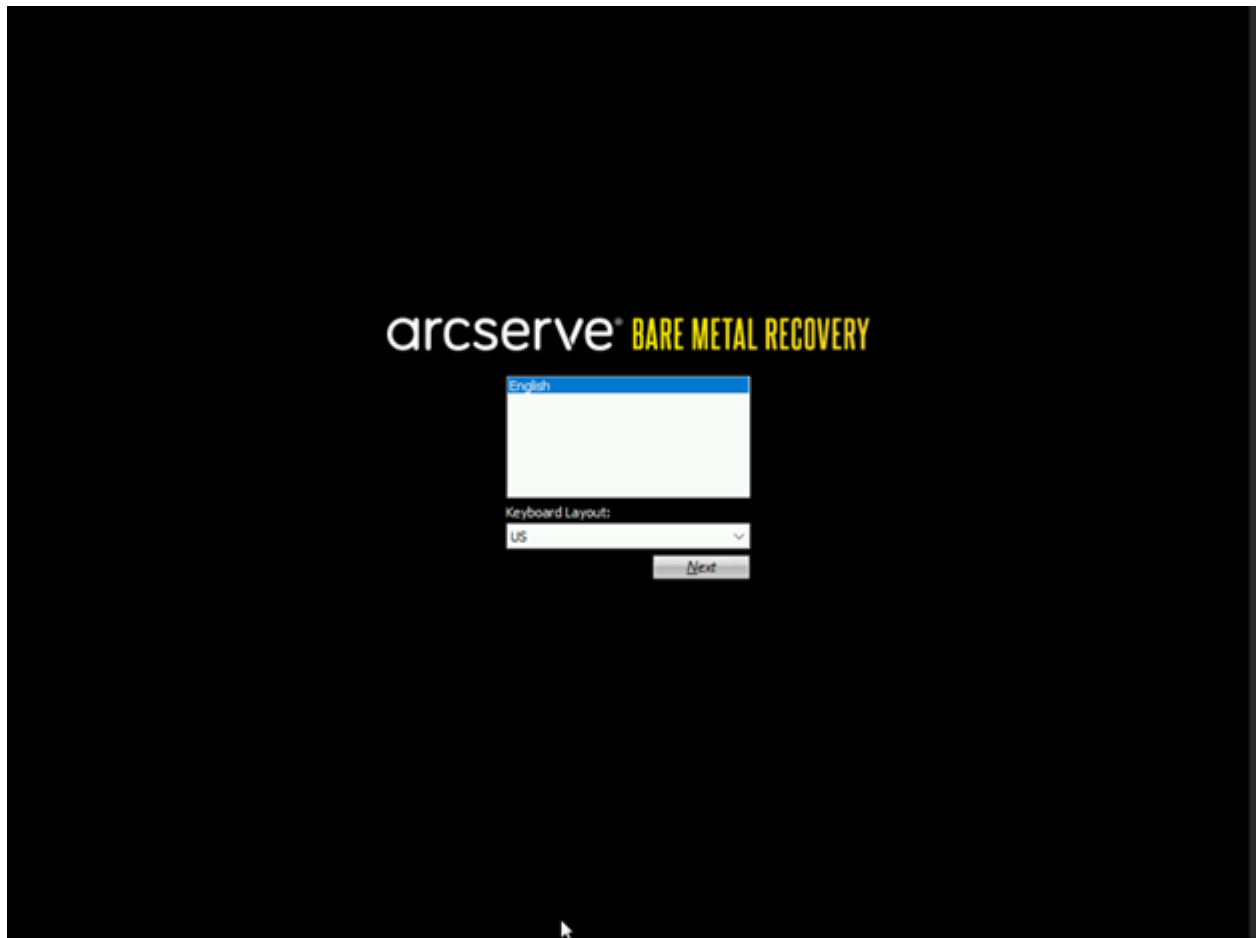
On Arcserve Appliance, you can perform the Bare Metal Recovery using the Arcserve UDP Boot Kit.

Follow these steps:

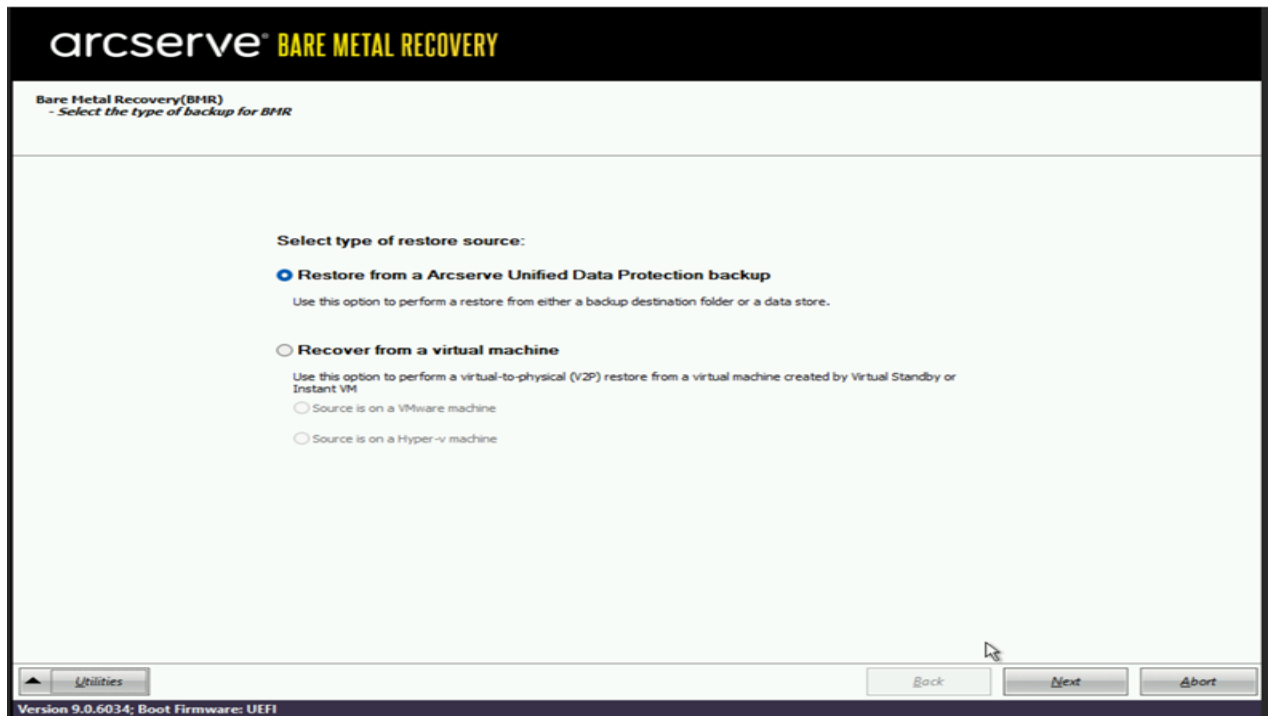
1. Run the *Create Arcserve UDP Boot Kit* application in the Appliance and generate the bootable BMR ISO image or USB stick for x64 platform.

Note: You need to include the local drivers for the ISO image. To include the local drivers, select the **Include Local Drivers** option in the **Create Boot Kit for Bare Metal Recovery** window. For more information on how to create boot kit, refer [link](#).





4. Select the **Restore from a Arcserve Unified Data Protection backup** option and click **Next**.



The **Select a Recovery Point wizard** window appears.

5. Click **Browse** and select **Browse from Recovery Point Server**.

Bare Metal Recovery(BMR)
- *Select a Recovery Point*

The top pane displays all backed up machines and their backup destinations. If you click on a machine, you can then see the associated recovery points on the bottom pane. Select a recovery point to continue.

Note: By default, only the backed up machines that are detected from local volumes are listed here. After a new removable disk is attached or detached, you can click "Refresh" the machine list. You can also click "Browse" to add any backed up machines from the remote shared folder or the data store.

If you fail to browse the remote shared folder, it may be because the NIC driver is not installed or the IP address is incorrect. If necessary, you can perform the following:
[Click here](#) to launch the load driver utility
[Click here](#) to launch the network configuration utility

The following backed up machines are detected:

Backed up Information

Host Name:

Operating System:

DNS Suffix:

Source:

Browse from network/local path

The following recovery points are detected for the specified machine. Select a recovery point at

6 Network Adapter(s) Detected

Intel(R) 1350 Gigabit Network Connection
- IP Address: 10.10.255.255
- Status: Connected

Intel(R) 1350 Gigabit Network Connection #2
- IP Address: 0.0.0.0
- Status: Disconnected

The **Select Node** window appears.

6. Enter the Recovery Point Server Host Name, User Name, Password, Port, and Protocol.
7. Click **Connect**.
8. Once the connection is established, click **OK**.

Select Node


Enter the Recovery Point Server credentials and click "Connect" to connect to the server and retrieve the data store and node list.

Host Name: Port:

User Name: Protocol: ☐ HTTP ☒ HTTPS

Password:

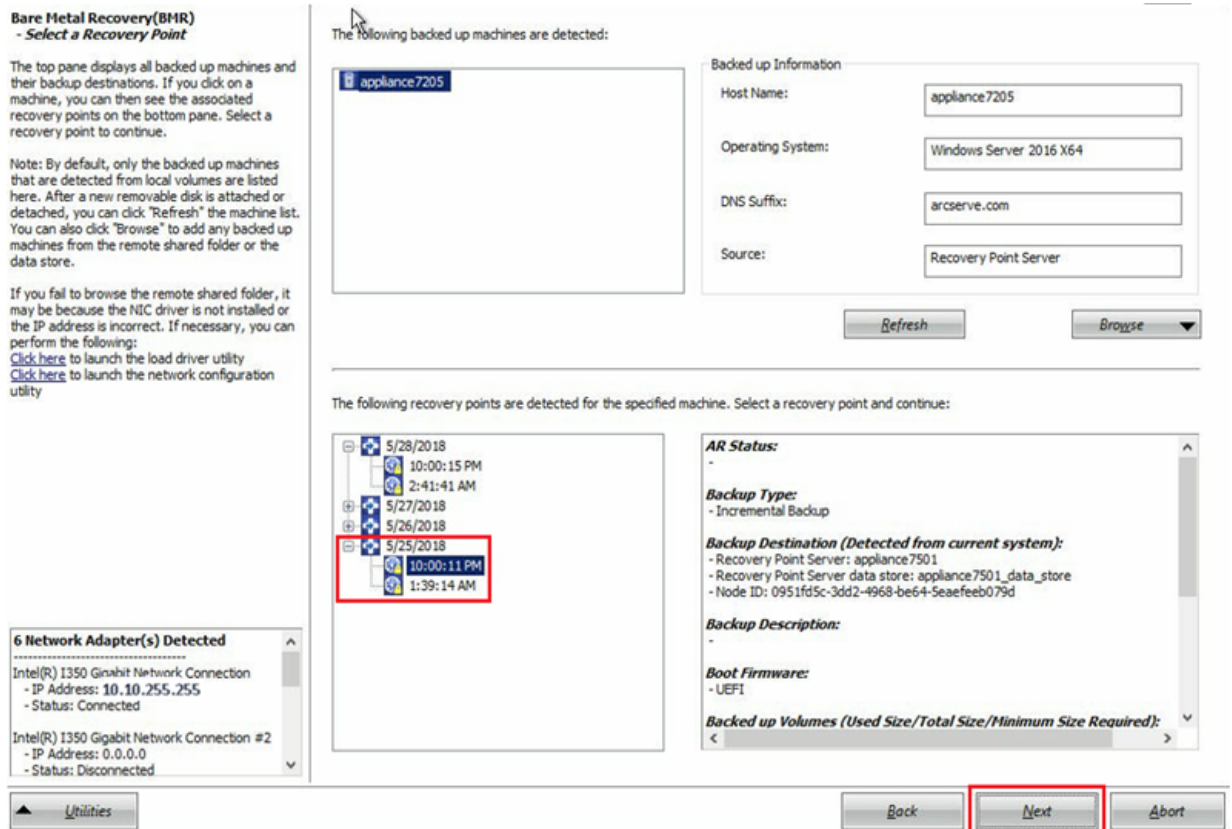
Data stores and nodes protected on this server:



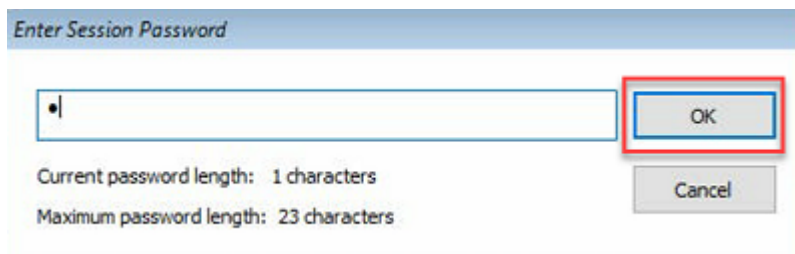
Property	Description
Node	appliance7205
DNS Suffix	arcserve.com
Node ID	0951fd5c-3dd2-4968-be64-5eae...

The **Bare Metal Recovery(BMR)- Select a Recovery Point** dialog appears.

9. Select the recovery point to restore and click **Next**.

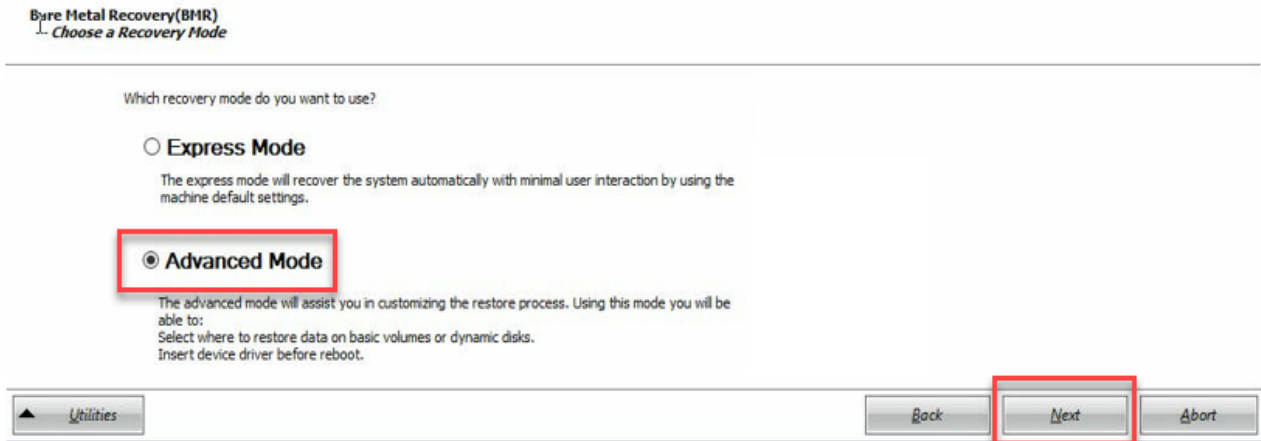


10. (Optional) Enter the session password if prompted, and click **OK**.



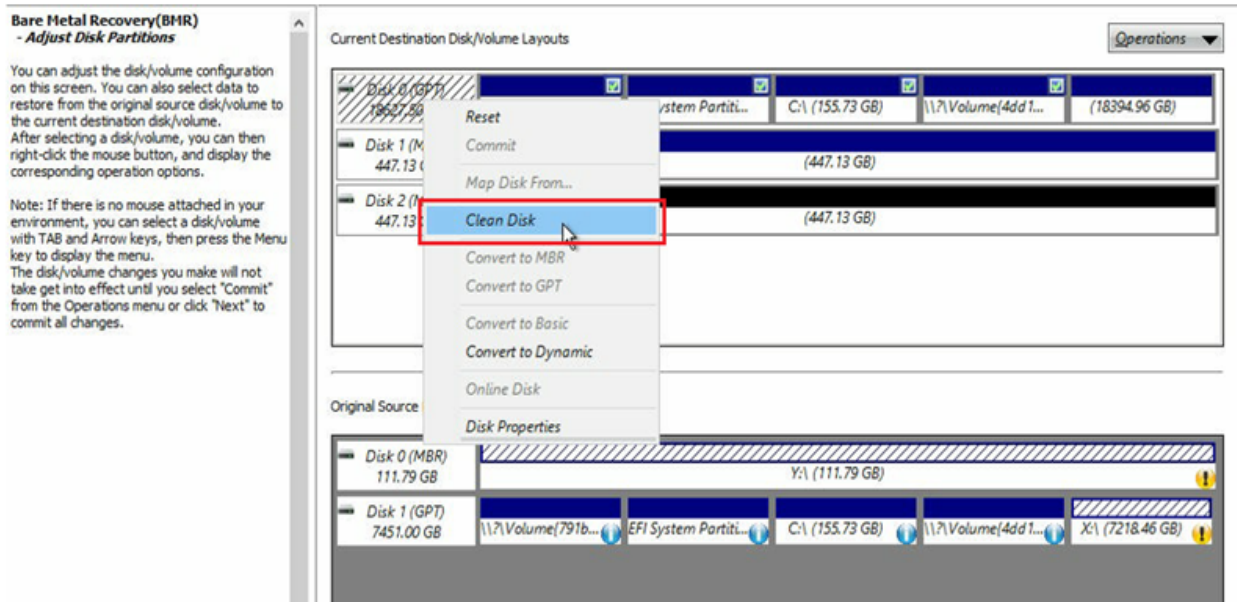
The **Bare Metal Recovery(BMR)- Choose a Recovery Mode** dialog appears.

11. Select **Advanced Mode** and click **Next**.

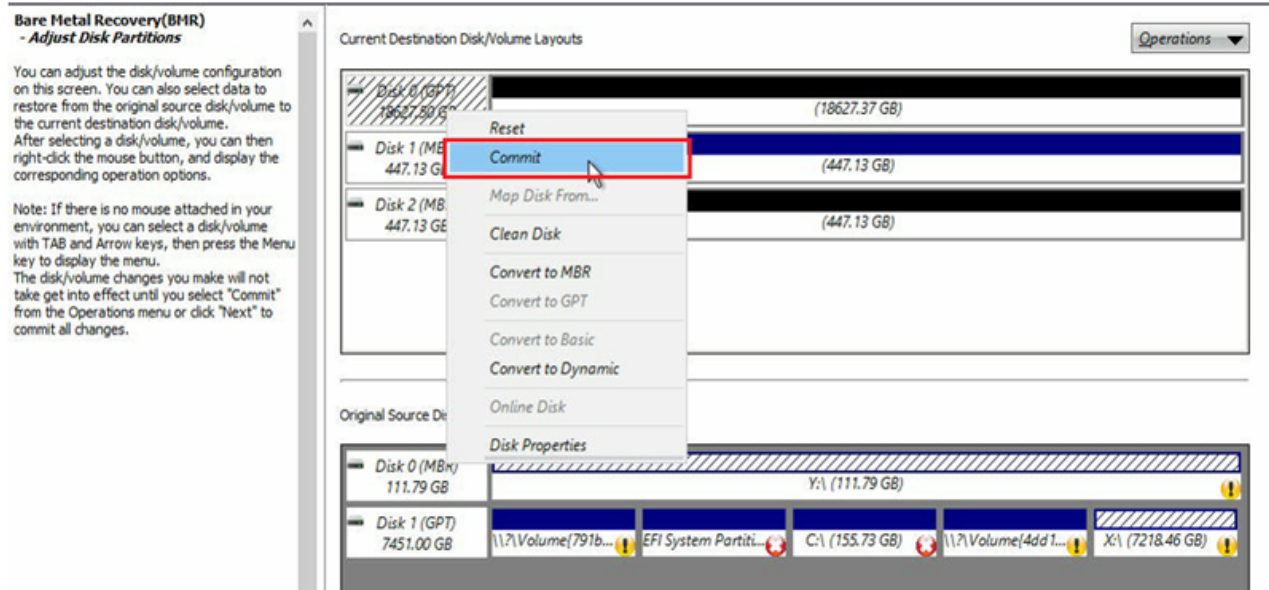


The **Bare Metal Recovery(BMR)- Adjust Disk Partitions** dialog appears.

12. Right click on the largest GUID Partition Table(GPT) disk available and click **Clean Disk**.

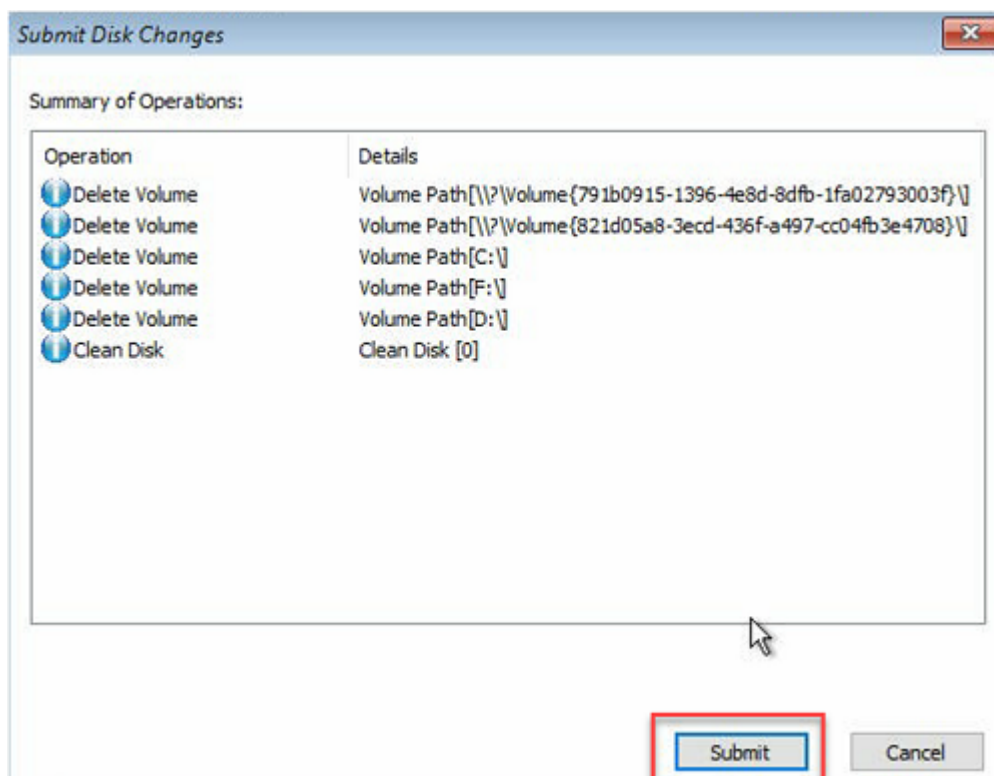


13. After cleaning the disk, right click on the same disk and click **Commit**.

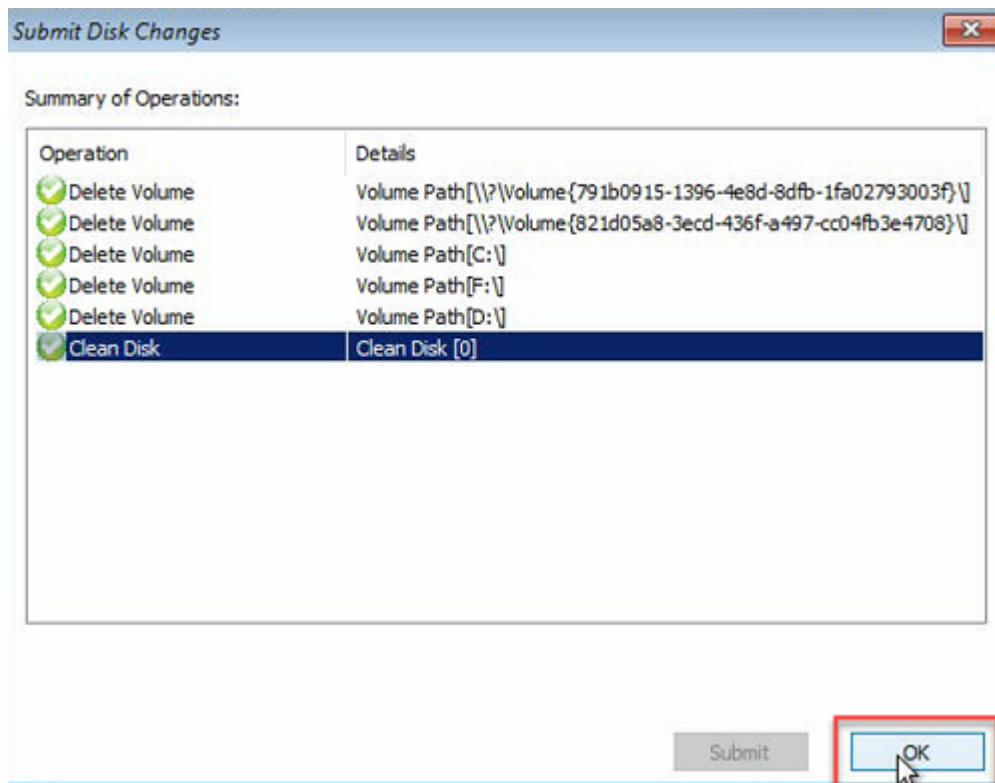


The **Submit Disk Changes** window appears.

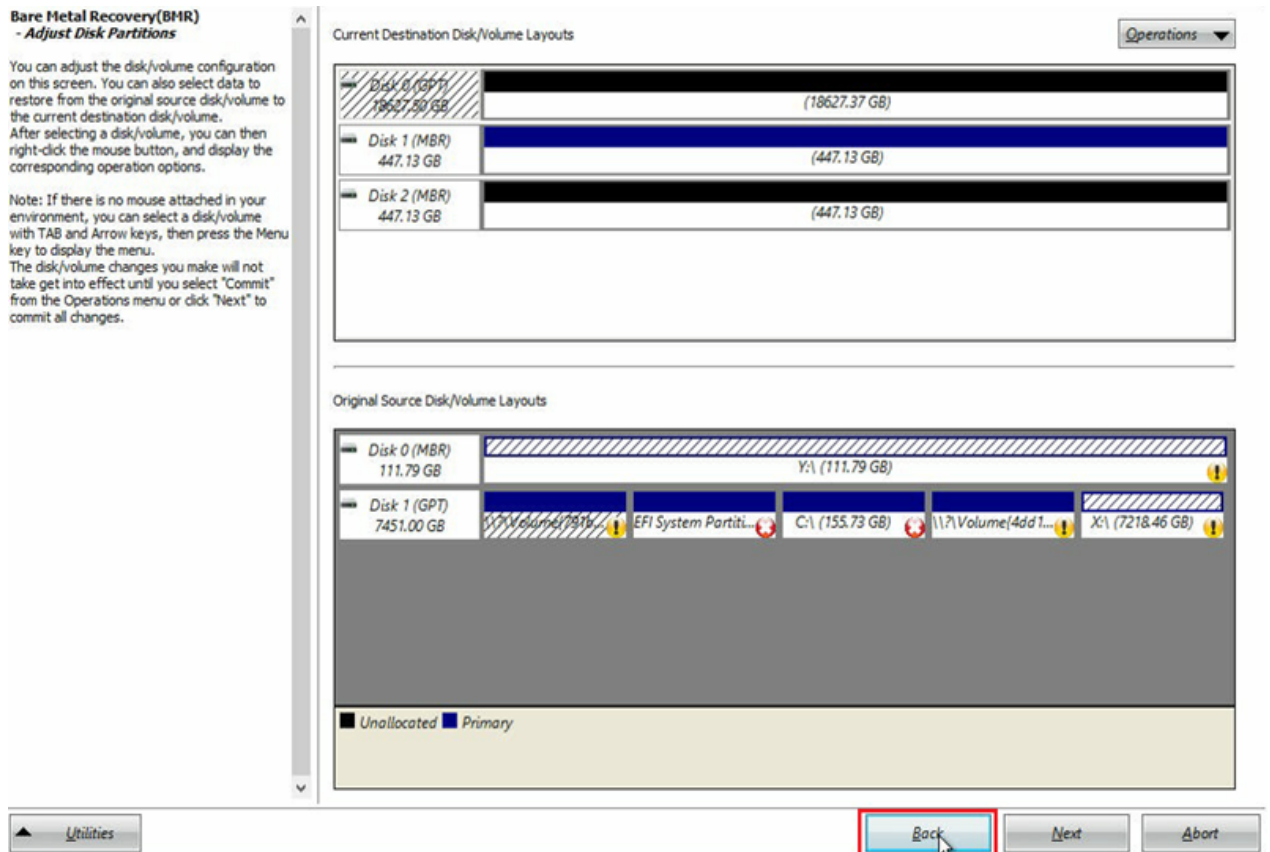
14. Click **Submit**.



15. After the cleaning of disk is completed, click **OK**.

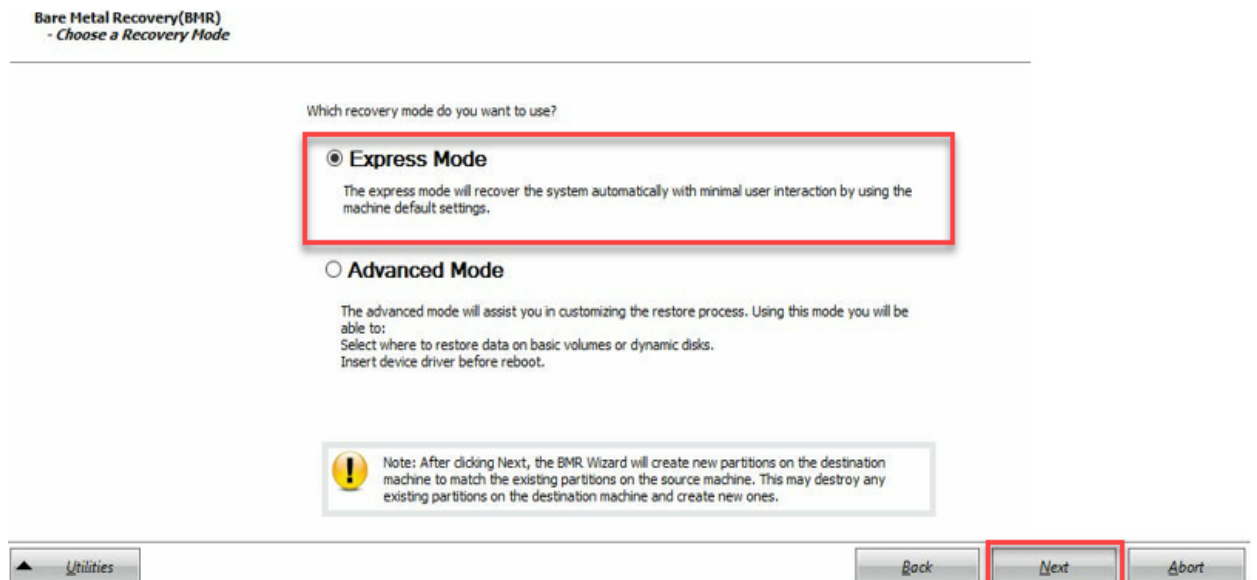


16. From the **Bare Metal Recovery(BMR)- Adjust Disk Partitions** dialog, click **Back**.



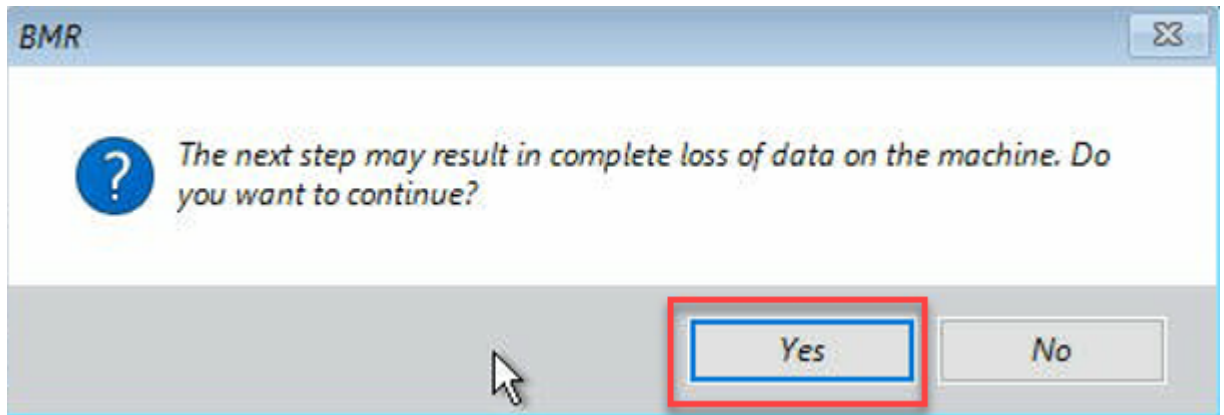
The **Bare Metal Recovery(BMR)- Choose a Recovery Mode** dialog appears.

17. Select **Express Mode** and click **Next**.



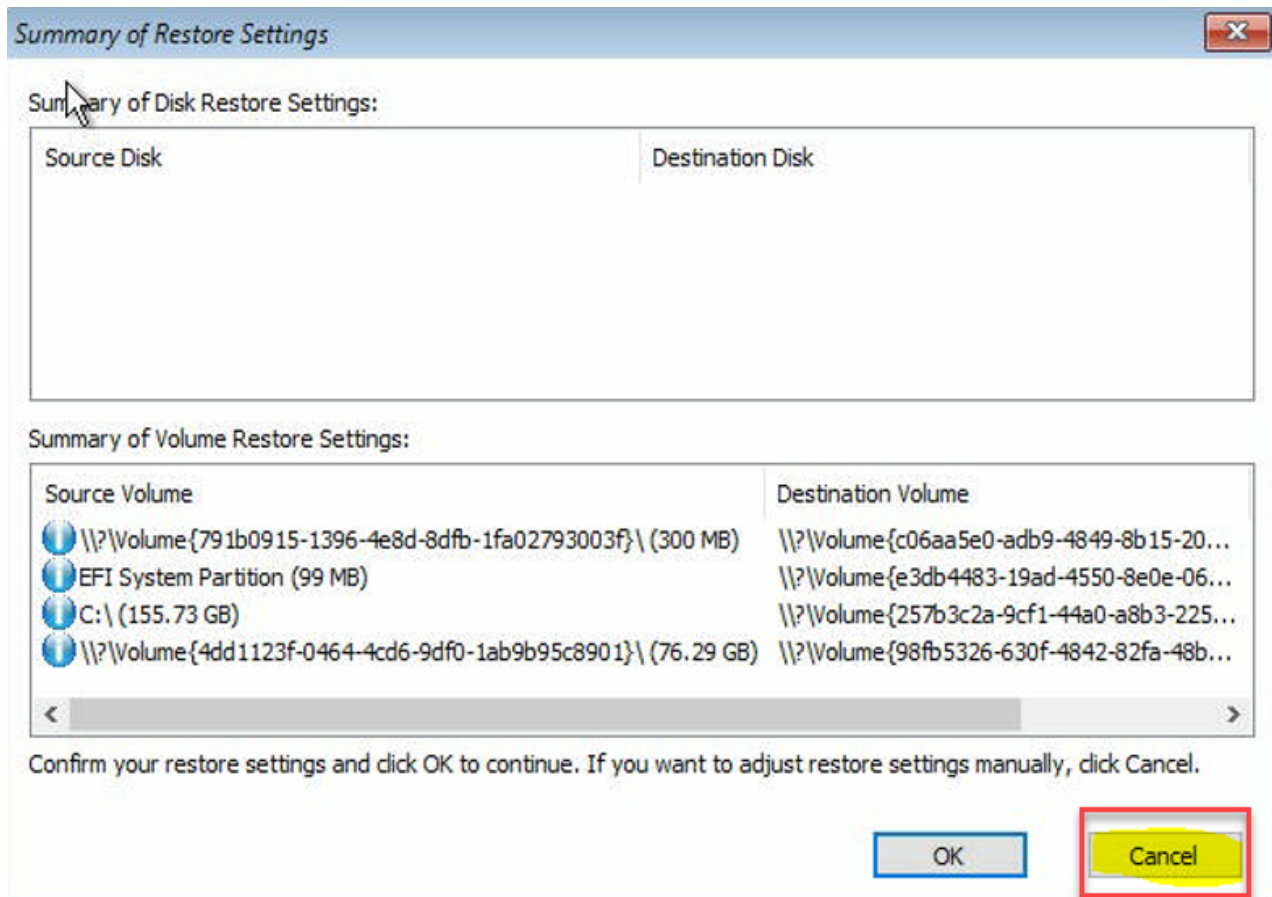
The **BMR** dialog appears.

18. Click **Yes**.



The **Summary of Restore Settings** dialog appears.

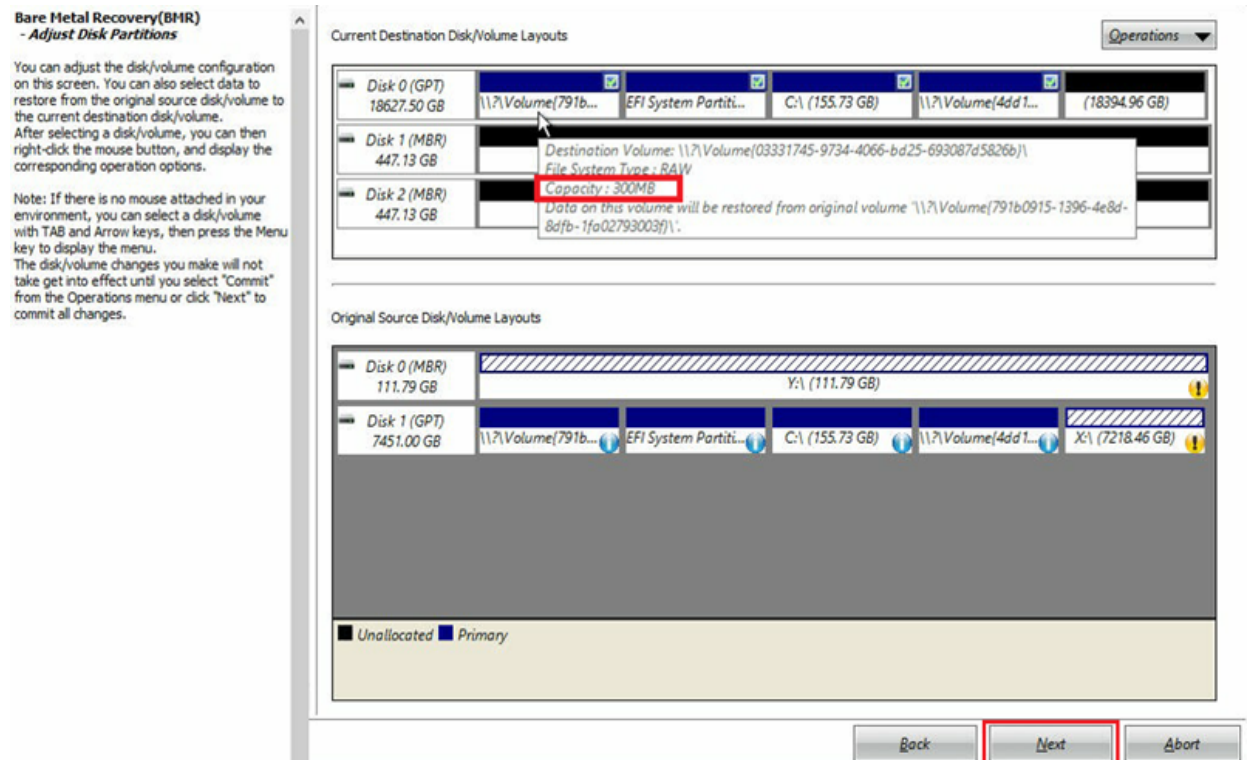
19. Click **Cancel**.



The **Bare Metal Recovery(BMR)- Adjust Disk Partitions** dialog appears.

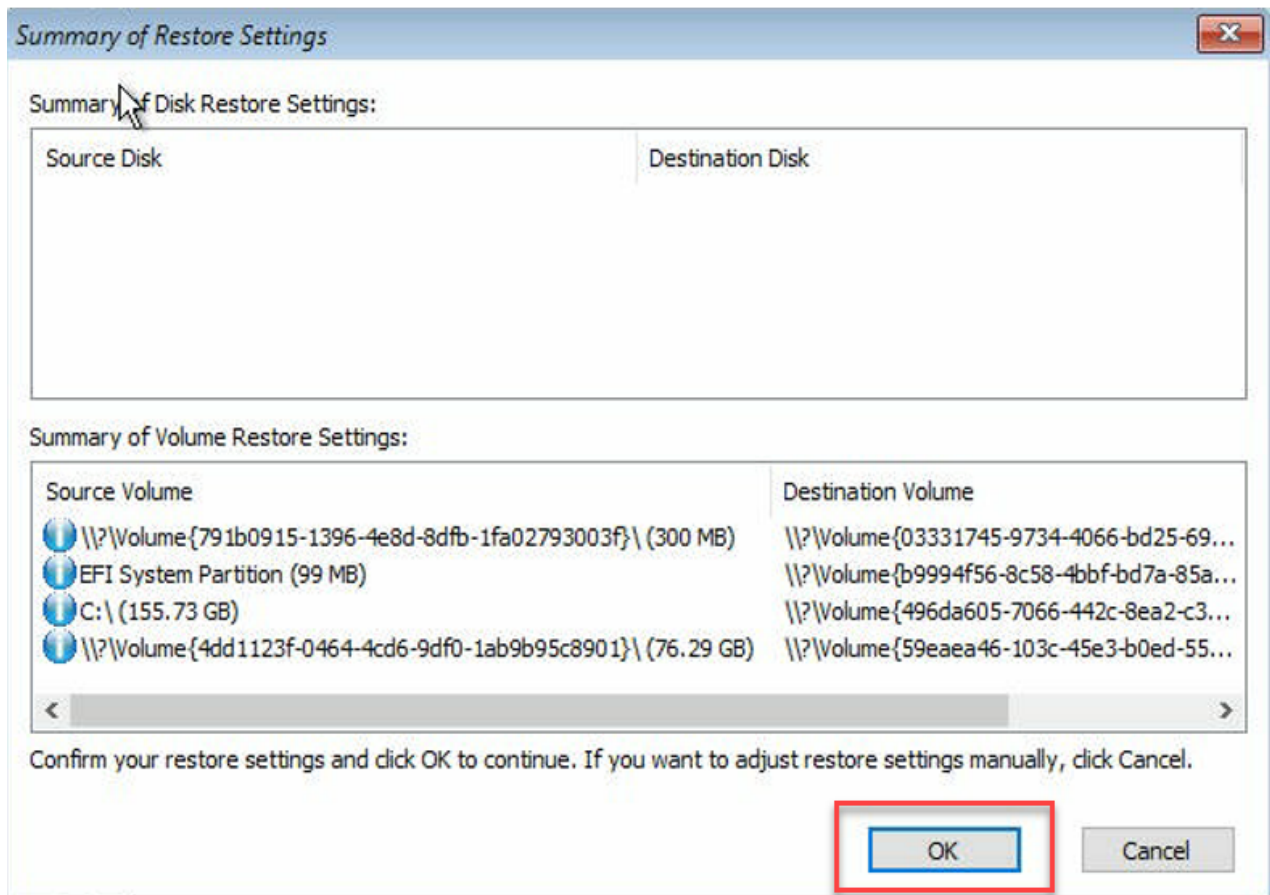
20. Compare and verify if the capacity of the first four partitions available in the **Current Destination Disk/Volume Layouts** tab matches with the largest GPT disk available in the **Original Source Disk/Volume Layouts** tab and click **Next**.

Note: To view the size of partition, hover the mouse to the disk to display the disk properties.



The **Summary of Restore Settings** dialog appears.

- Click **OK**.



The **Bare Metal Recovery(BMR)- Start Recovery Process** dialog appears.

22. Clear selection of the **Do not start Agent service automatically after reboot** option and wait for restore to complete.

Bare Metal Recovery(BMR)
- Start Restore Process

This page displays a summary of the disk/volume restore settings that you have made.

Note: After the BMR process is complete and server has been rebooted, you may not want to perform backup jobs from this server. If you are just testing the BMR functionality, we recommend that you select the "Do not start Agent service automatically after reboot" option.

When you select this option, you can manually start the Agent service (and the Recovery Point Server service, if installed) after reboot if you want to perform backup jobs.

Enable Windows F8 boot option helps user perform further recovery or troubleshooting after BMR. For example, press F8 and boot into Active Directory Service Restore mode to perform Active Directory authoritative restore.

Summary of Restore Settings

Restore Item	Status	Progress	Throughput
Restore source volume '\\?\Volume{791b0915-1396-4e8d-8dfb-1fa02793003f}\ ...	Completed	100.0%	367.44 MB/Minute
Restore source volume 'EFI System Partition' to current destination disk 0	Completed	100.0%	967.90 MB/Minute
Restore source volume 'C:\' to current destination disk 0	Restoring	0.8%	2705.50 MB/Minute
Restore source volume '\\?\Volume{4dd1123f-0464-4cd6-9df0-1ab9b95c8901}\ ...	Not Started		

☒ Automatically reboot your system after recovery.

☐ Do not start Agent service automatically after reboot.

☐ Boot the system to Advanced Boot Options (F8) Menu on the next boot for Windows 8 / Windows Server 2012 and later OS.

Elapsed Time: 00 : 00 : 24

Estimated Time Remaining: 01 : 30 : 50

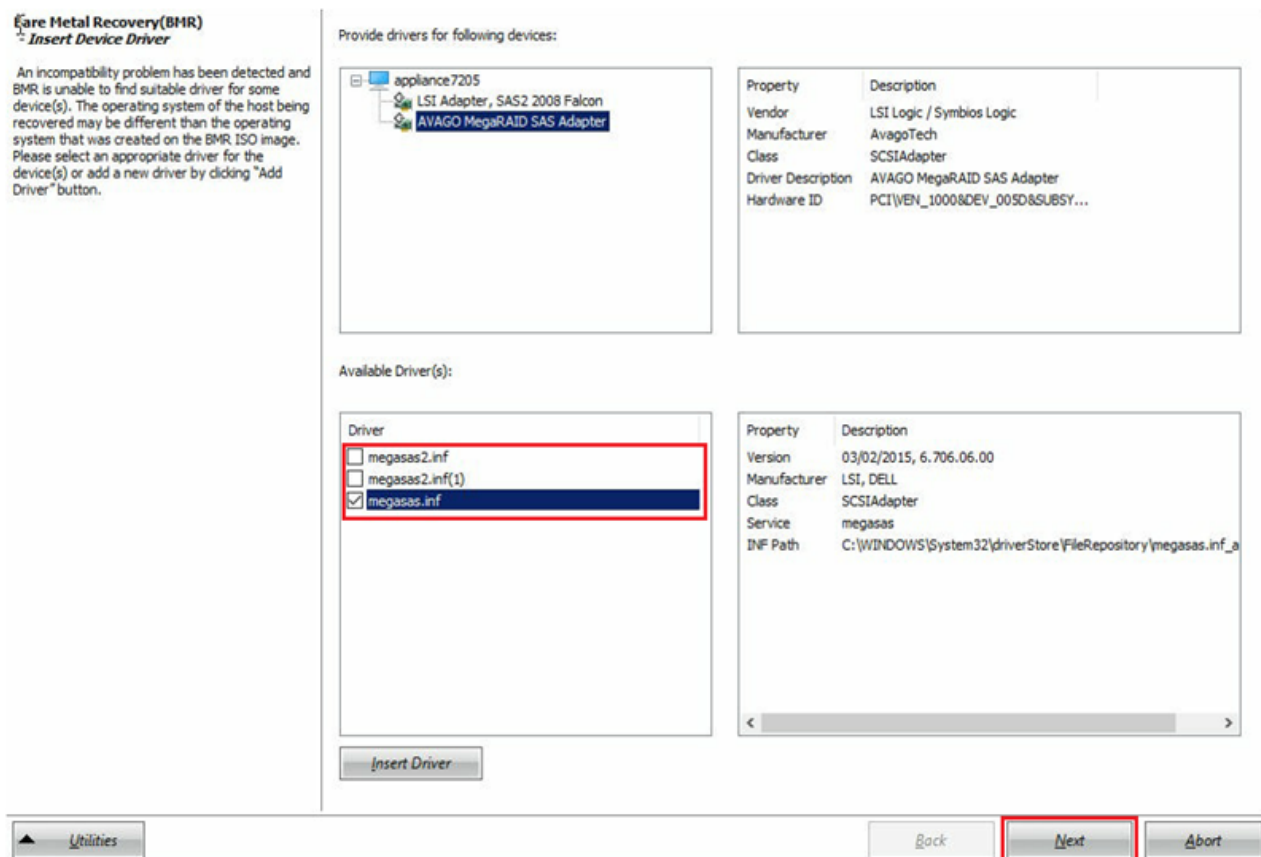
[0.8%] [576MB/76631MB] Restoring basic source volume 'C:\' to current destination disk 0

Utilities

BackNextAbort

The **Bare Metal Recovery(BMR)- Insert Device Driver** dialog appears.

23. Select the required driver for raid controller and click **Next**.



The Reboot pop up appears and the Arcserve Appliance is rebooted automatically.

Click **ReBoot** to automatically reboot your system at this time. If you want to collect all BMR log files you can use the Activity log utility.
[Click here](#) to launch the Activity Log utility.

Your system will reboot in 11 second(s).



Boot volume was restored to current destination disk 0. Please boot your system from this disk.

The BMR process is completed successfully.

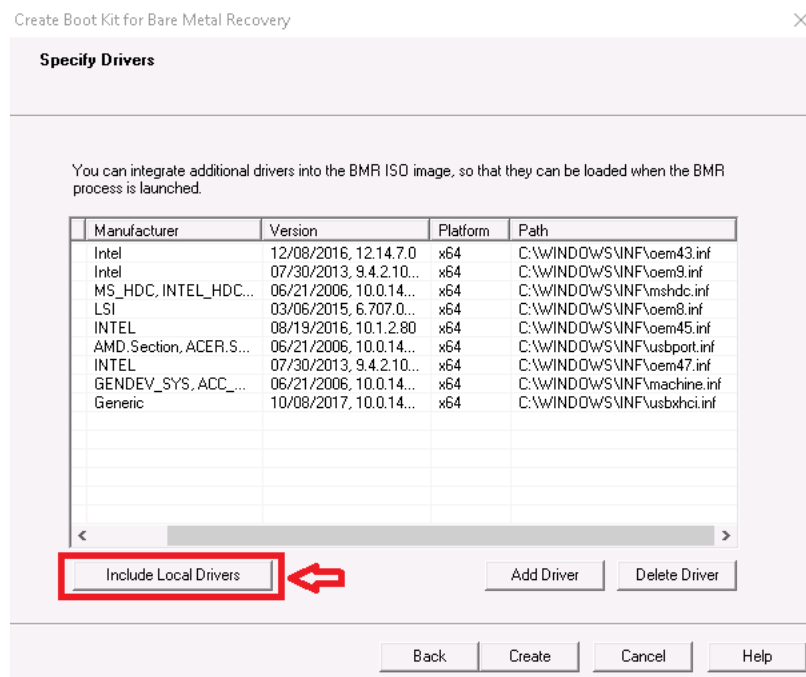
Perform Bare Metal Recovery (BMR) and Preserving Data

On Arcserve Appliance, you can perform the Bare Metal Recovery using the Arcserve UDP Boot Kit.

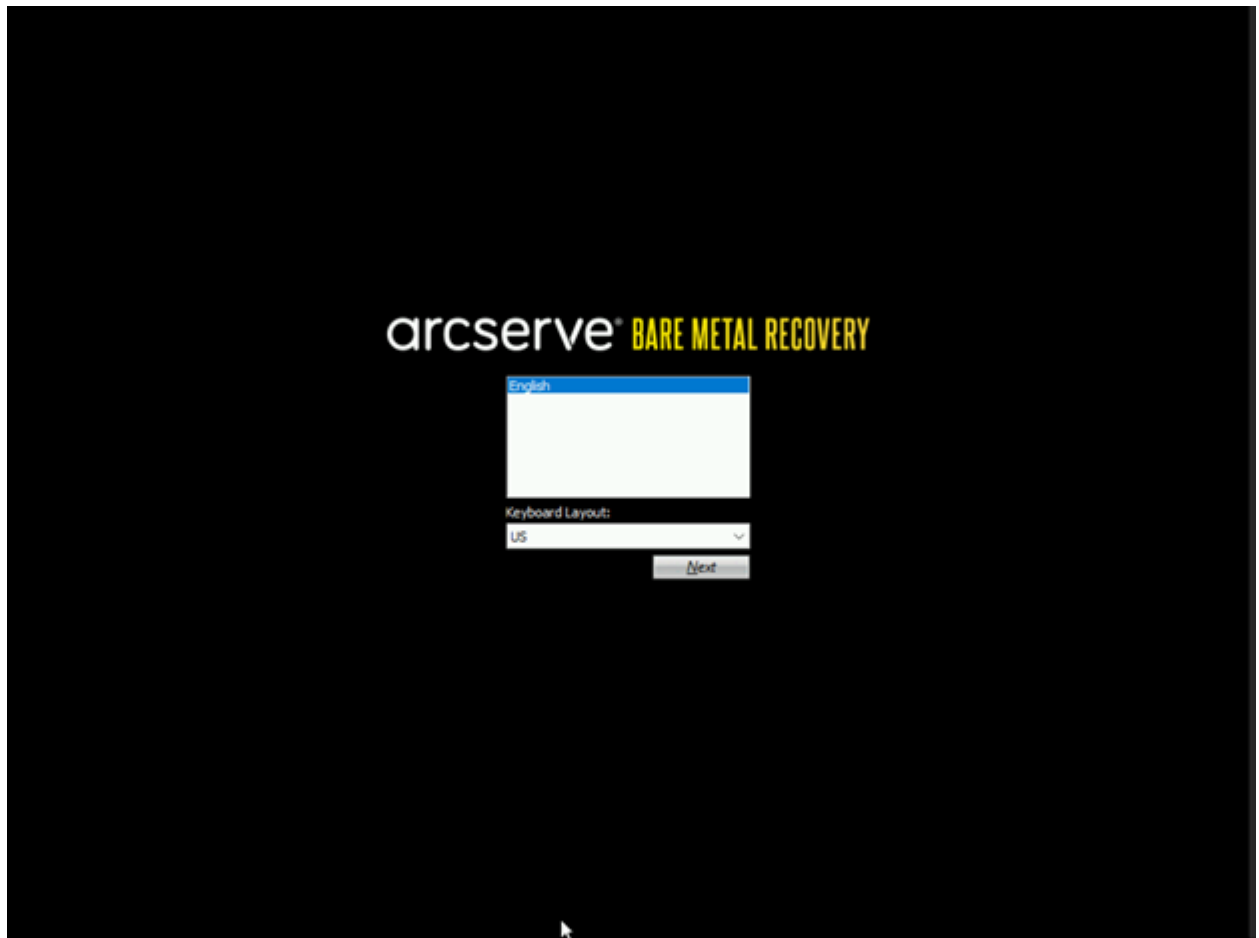
Follow these steps:

1. Run the *Create Arcserve UDP Boot Kit* application in the Appliance and generate the bootable BMR ISO image or USB stick for x64 platform.

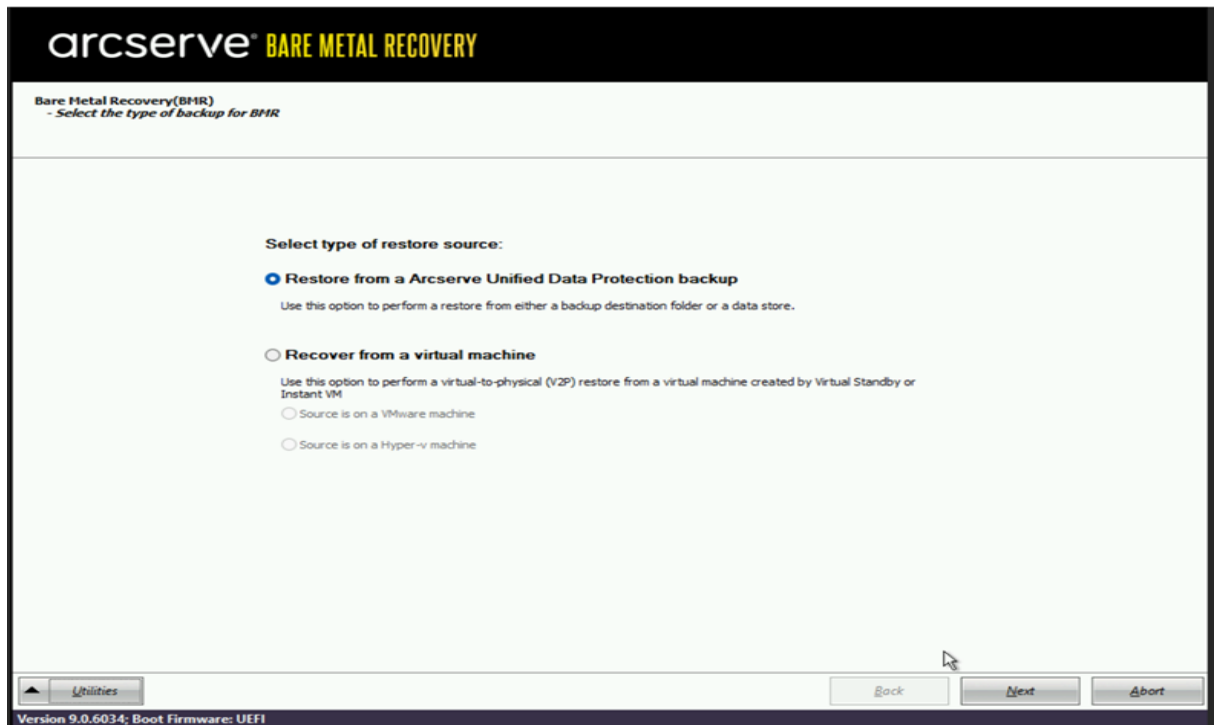
Note: You need to include the local drivers for the ISO image. To include the local drivers, select the **Include Local Drivers** option in the **Create Boot Kit for Bare Metal Recovery** window. For more information on how to create boot kit, refer [link](#).



2. Boot the Arcserve Appliance using BMR ISO image or USB Stick.
The **Arcserve bare metal recovery** setup appears.
3. Select the required language and click **Next**.

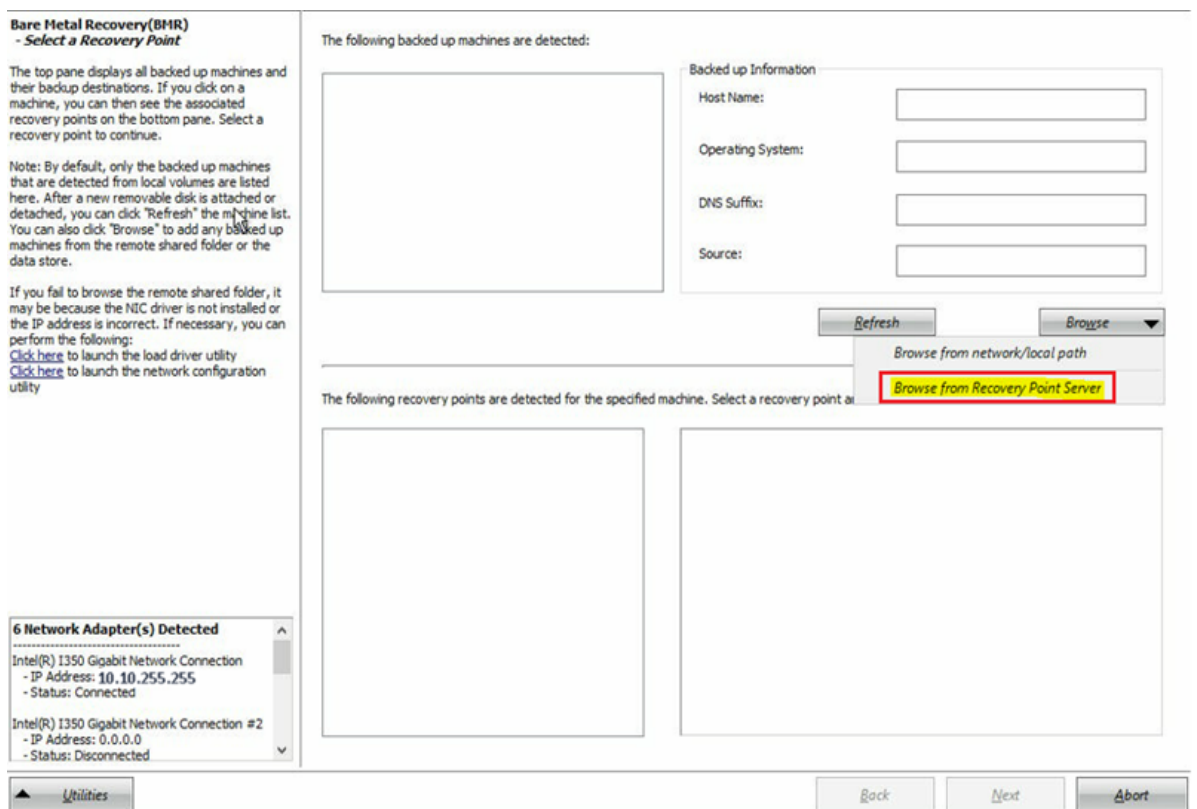


4. Select the **Restore from a Arcserve Unified Data Protection backup** option and click **Next**.



The **Select a Recovery Point wizard** window appears.

5. Click **Browse** and select **Browse from Recovery Point Server**.



The **Select Node** window appears.

6. Enter the Recovery Point Server Host Name, User Name, Password, Port, and Protocol.
7. Click **Connect**.
8. Once the connection is established, click **OK**.

Select Node

Enter the Recovery Point Server credentials and click "Connect" to connect to the server and retrieve the data store and node list.

Host Name: Port:

User Name: Protocol: ☐ HTTP ☒ HTTPS

Password:

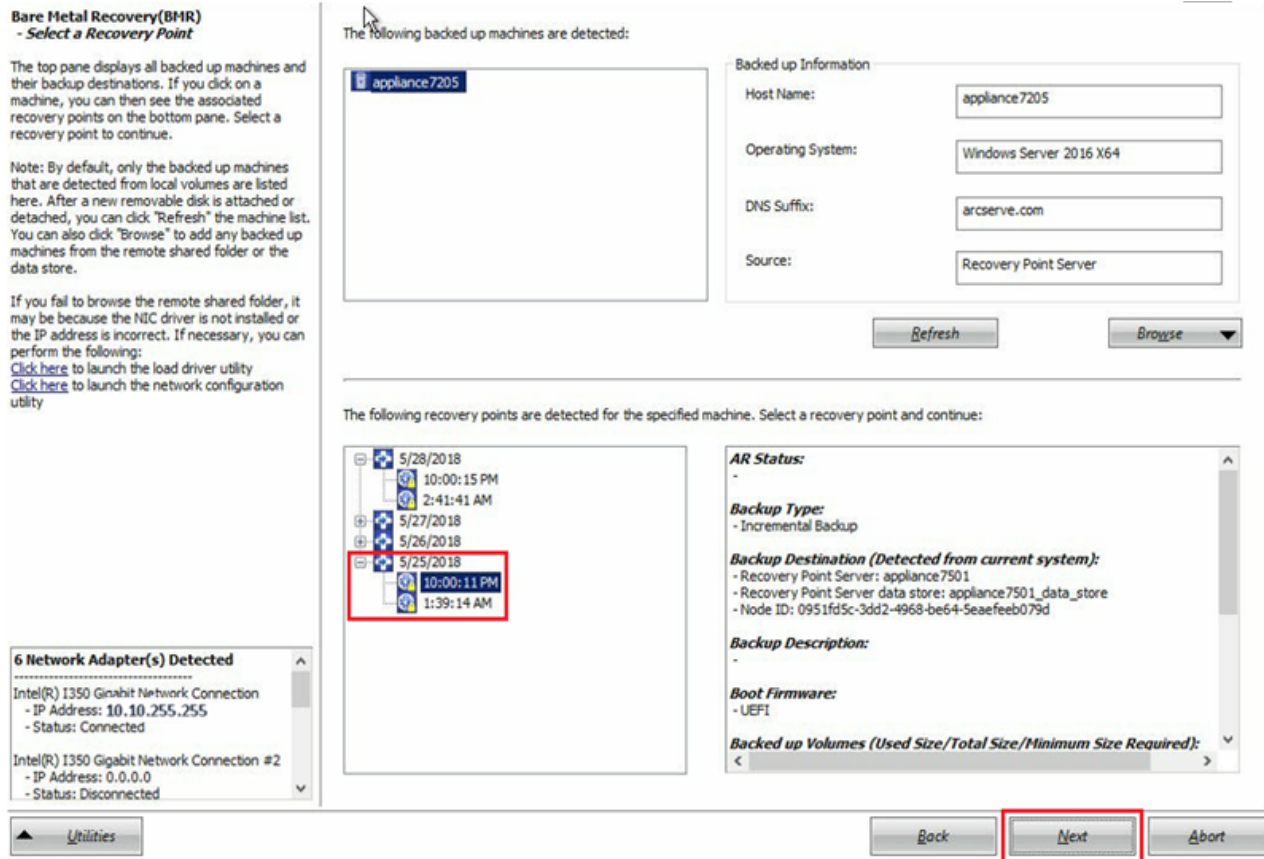
Data stores and nodes protected on this server:

appliance7501_data_store
 appliance7205

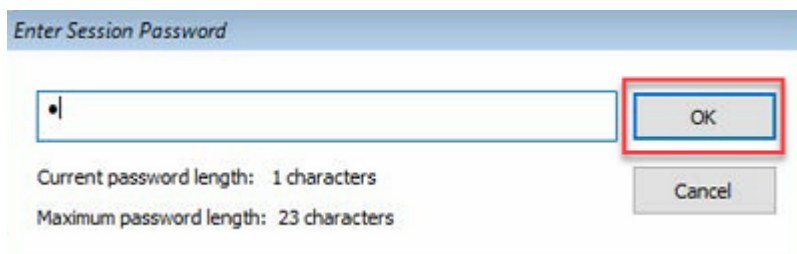
Property	Description
Node	appliance7205
DNS Suffix	arcserve.com
Node ID	0951fd5c-3dd2-4968-be64-5eaf...

The **Bare Metal Recovery(BMR)- Select a Recovery Point** dialog appears.

9. Select the recovery point to restore and click **Next**.

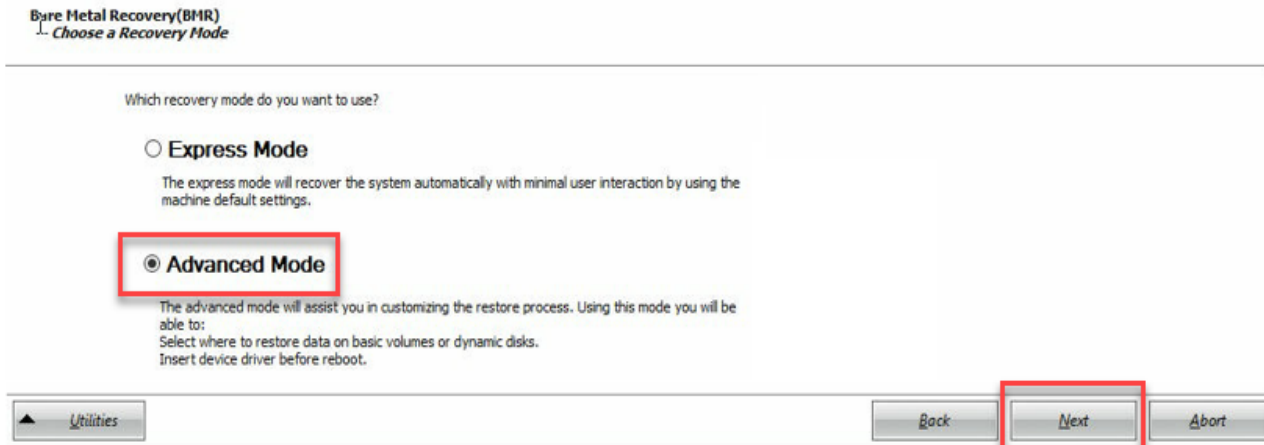


10. (Optional) Enter the session password if prompted, and click **OK**.

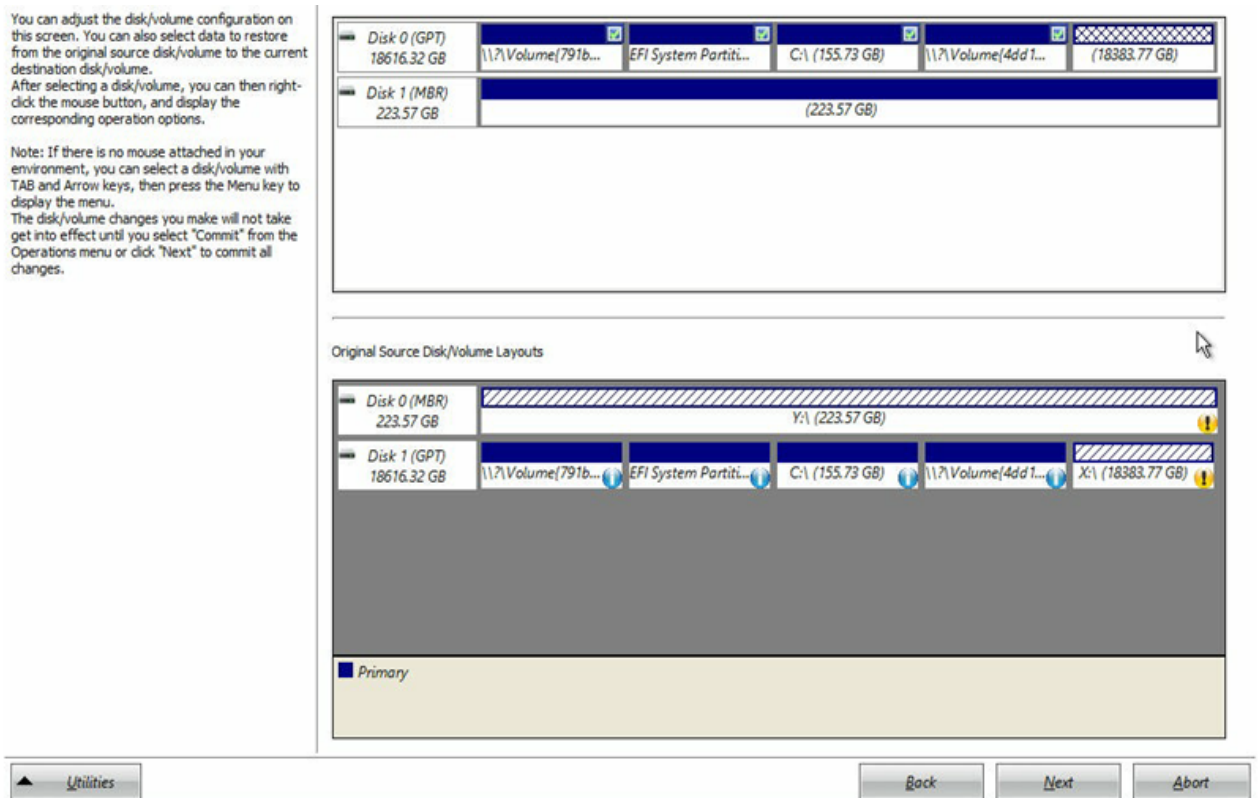


The **Bare Metal Recovery(BMR)- Choose a Recovery Mode** dialog appears.

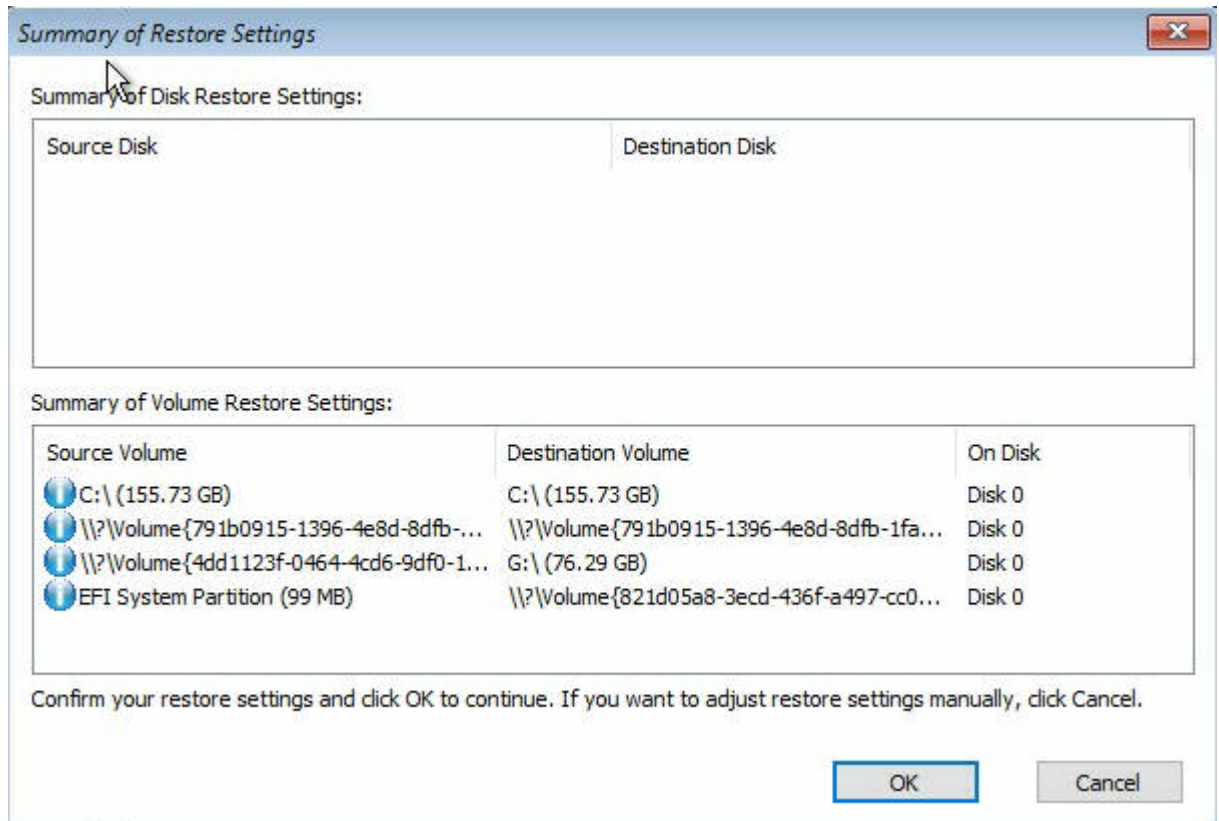
11. Select **Advanced Mode** and click **Next**.



12. On the **Bare Metal Recovery(BMR)- Adjust Disk Partitions** dialog, click **Next**.



13. On the **Summary of Disk Restore Settings** screen, click **OK**.



14. On the **Bare Metal Recovery(BMR)- Start Recovery Process** dialog, clear selection of the **Do not start Agent service automatically after reboot** option and wait for restore to complete and machine reboot.

Bare Metal Recovery(BMR)
- Start Restore Process

This page displays a summary of the disk/volume restore settings that you have made.

Note: After the BMR process is complete and server has been rebooted, you may not want to perform backup jobs from this server. If you are just testing the BMR functionality, we recommend that you select the "Do not start Agent service automatically after reboot" option.

When you select this option, you can manually start the Agent service (and the Recovery Point Server service, if installed) after reboot if you want to perform backup jobs.

Enable Windows F8 boot option helps user perform further recovery or troubleshooting after BMR. For example, press F8 and boot into Active Directory Service Restore mode to perform Active Directory authoritative restore.

Summary of Restore Settings

Restore Item	Status	Progress	Throughput
Restore source volume 'C:\' to current destination disk 0	Restoring	1.8%	3115.69 MB/Minute
Restore source volume '\\?\Volume{791b0915-1396-4e8d-8dfb-1fa02793003f}\ ...	Not Started		
Restore source volume '\\?\Volume{4dd1123f-0464-4cd6-9df0-1ab9b95c8901}\ ...	Not Started		
Restore source volume 'EFI System Partition' to current destination disk 0	Not Started		

☒ Automatically reboot your system after recovery.

☐ Do not start Agent service automatically after reboot.

☐ Boot the system to Advanced Boot Options (F8) Menu on the next boot for Windows 8 / Windows Server 2012 and later OS.

Elapsed Time: 00 : 00 : 33

Estimated Time Remaining: 00 : 52 : 55

[1.8%] [1632MB/90738MB] Restoring basic source volume 'C:\' to current destination disk 0

Utilities

BackNextAbort

The BMR process is completed successfully.

Chapter 9: Performing Appliance Capacity Expansion

This section contains the following topics:

Working with Arcserve Appliance Expansion Kit - X Series Models	163
Working with SSD Flash Expansion Kit in Arcserve X Series Appliance	167
Working with Expansion Kit in Arcserve Appliance 9072-9504 DR Models	177
Working with SSD Flash Expansion Kit in Arcserve Appliance 9072-9504 DR Models	182

Working with Arcserve Appliance Expansion Kit - X Series Models

Arcserve Expansion Kit lets you expand the data capacity in Arcserve Appliance X Series models.

Follow these steps:

1. For X series Expansion Kit - Capacity of any model (except X3000DR), you can perform a linear expansion with optional Expansion Kits as many times as required till you reach the largest model X3000DR.
2. Perform the following steps to insert HDDs in the empty disk slots:
 - a. From the Arcserve UDP Console verify and ensure that no jobs are running on the Appliance Server. If any jobs are running, pause the corresponding plans.
 - b. Insert the HDDs in the empty disk slots of Storage Unit - ME4084 Value Array. Each kit in the X series Expansion kit consists of 14 x

16TB disks.



3. Log into the ME unit - Value Array Storage Manager, go to Pools, and then select the disk group that you want to expand.

VA084
Value Array Storage Manager

System: Uninit
Version: GT28

Home

System

Hosts

Pools

Volumes

Mapping

Action

Clear Filters

Export to CSV

Show All

Name	Health	Size
Arc01	OK	5

Related Disk Groups

Clear Filters

Export to CSV

Show All

Name	Health	Pool	RAID
Arc01	OK	Arc01	ADAPT

Related Disks

Clear Filters

Export to CSV

Show All

Location	Health	Description	Size
0.0	OK	SAS MDL	16
0.1	OK	SAS MDL	16
0.2	OK	SAS MDL	16
0.3	OK	SAS MDL	16

4. Right-click the selected disk group, and the select **Expand Disk Group**.

The Expand Disk Group panel opens and displays the disk group information and disk tables.

Chapter 9: Performing Appliance Capacity Expansion 165

Expand Disk Group

Name: Arc01 Type: Linear
Owner: A Data Protection: ADAP

Disk Selection Sets, Complete: Yes

Type	Disk Description	Selected	Maximum	Size
ADAPT	SAS MDL	0	128	672.0TB

Add disks to the disk group by entering a range of disks or by selecting disks from the table below.

Enter Range of Disks: ⓘ

☐ Select All ⓘ

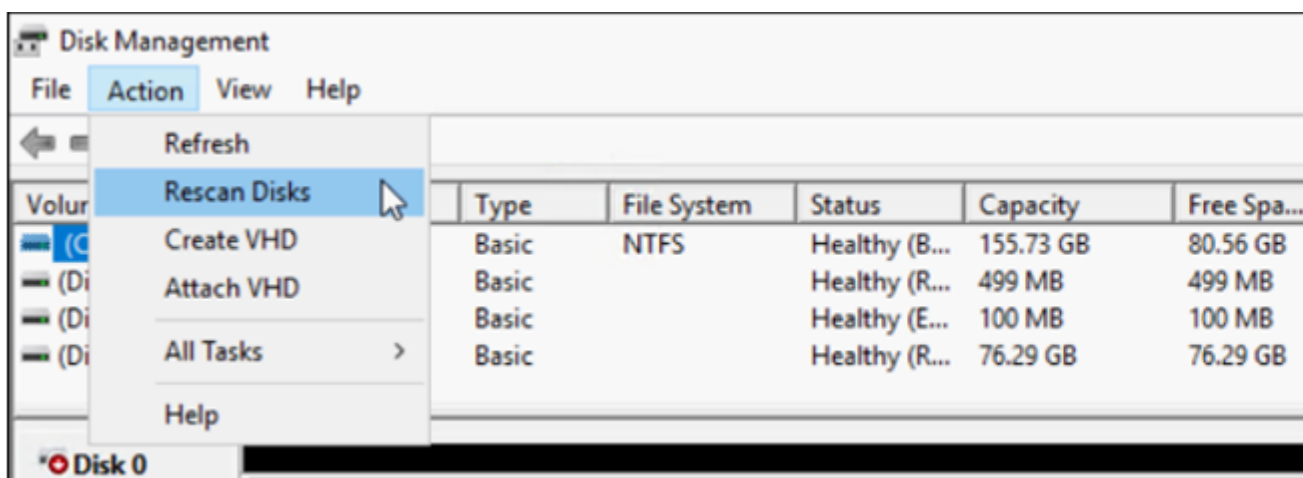
Showing 1 to 0 of 0 entries

Description	Enclosure ID	Slot	Size
No data available in the table			

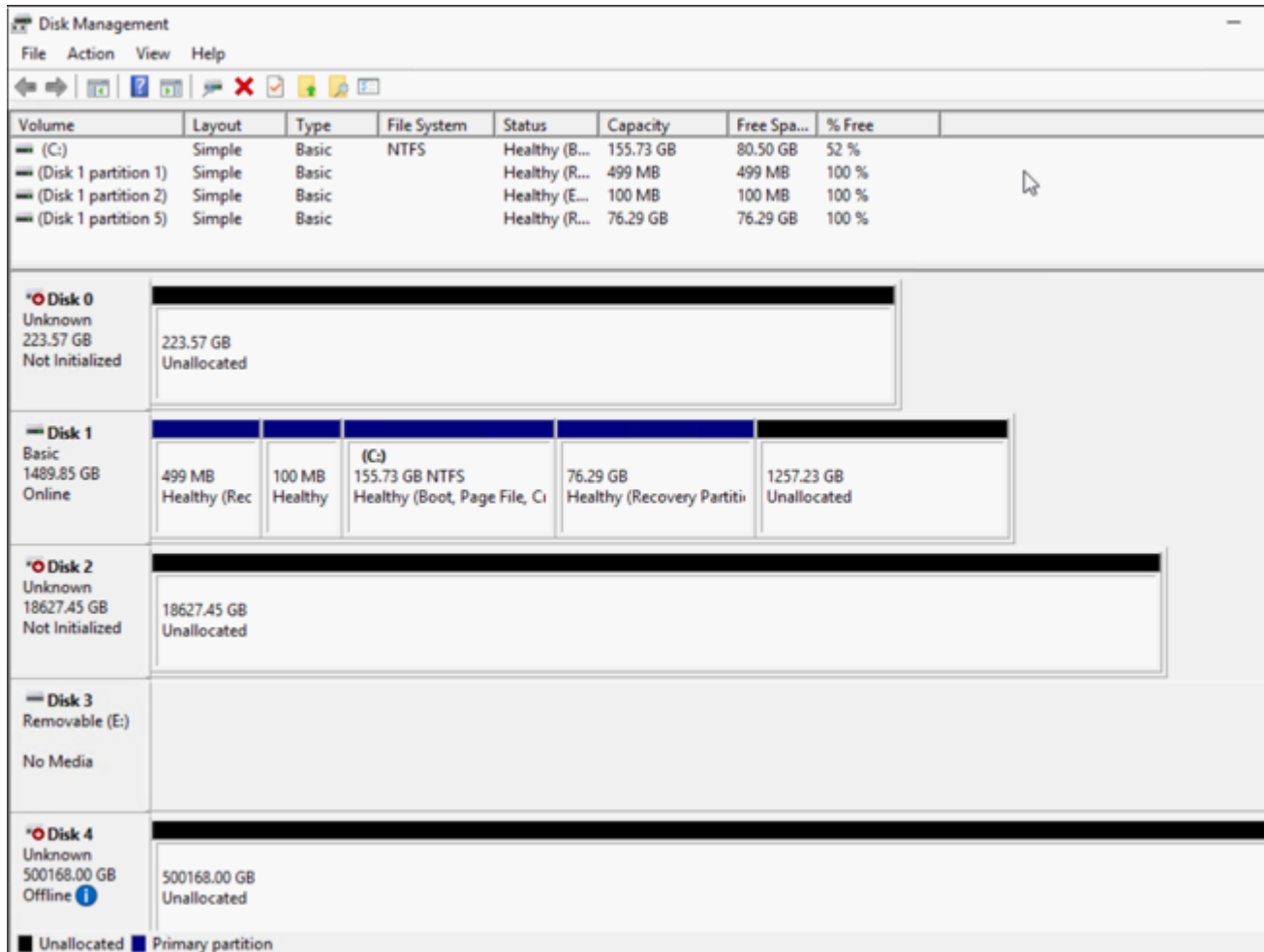
- To add additional disks to the disk group, enter a range of disks in the **Enter Range of Disks** field or select the disks from the table.
- Click **Modify**.
- On the confirmation panel, click **Yes** to start the group expansion, and then click **OK** to close the panel.

Note: After the Expand job is completed, a rebalance job is triggered on the disk group.

- After the Expand and Rebalance jobs are completed, open **Disk Management** from the compute unit, and then select **Action > Rescan Disks**.



After Rescan, the disk from the Storage Unit appears with the expanded storage.



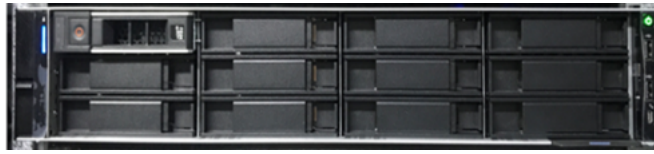
Working with SSD Flash Expansion Kit in Arcserve X Series Appliance

Arcserve SSD Flash Expansion Kit lets you expand the data capacity by creating a secondary datastore and performing DR-related operations (IVM /VSB/Continuous Availability) in the Arcserve Appliance X-Series.

Follow these steps:

1. Perform the following steps to insert SSDs in the empty disk slots:
 - a. From the Arcserve UDP Console, verify and make sure that no jobs are running on the Appliance Server. If in case any jobs are running, pause the corresponding plans.

- b. Insert SSDs in the empty disk slot.



2. Perform the following steps to configure Raid-5 from the BIOS Boot Manager option:

- a. To launch the Virtual Console dashboard, log in to iDRAC, and then click **Start the Virtual Console**.
- b. In the Virtual Console page, click **Boot**, and then select the **BIOS Boot Manager** option.

On the confirmation window, click **Yes** to restart the BIOS Boot Manager.

- c. Click **Power**, and then select **Reset system (warm boot)**.

The appliance boots and relaunched the Boot Manager setup page.

- d. In the Boot Manager Main Menu, click **Launch System Setup**, and then navigate to **Device Settings > Dell EMC PERC S140 Controller > Virtual Disk Management > Create Virtual Disk**.
- e. From the Select RAID Level drop-down list, select **RAID 5**.

Note: The RAID 5 Virtual Disk is used for expansion kit and includes newly attached disks of 3.63 TB for each physical disk.

System Setup Help | About | Exit

DELL EMC PERC S140 Configuration Utility

Configuration Options • Virtual Disk Management • Create Virtual Disk

Create Virtual Disk

Select RAID Level: Volume

Select Physical Disks From: Volume

Select Physical Disks

Configure Virtual Disk Parameters:

Virtual Disk Size: 0

Virtual Disk Size Unit: ☐ MB (MegaBytes) ☒ GB (GigaBytes) ☐ TB (TeraBytes)

Read Cache Policy: No Read Ahead

Write Cache Policy: Write Through

Physical Disk Write Cache: ☒ Default ☐ Enable ☐ Disable

Selects the desired RAID level. The configuration utility supports RAID levels 0, 1, 5 and 10. (Press <F1> for more help)

Service Tag : G19CR53 Back

- f. Select the **Select Physical Disks** option.

System Setup Help | About | Exit

DELL EMC PERC S140 Configuration Utility

Configuration Options • Virtual Disk Management • Create Virtual Disk

Create Virtual Disk

Select RAID Level: RAID 5

Select Physical Disks From: ☒ Unconfigured Capacity

Select Physical Disks

Configure Virtual Disk Parameters:

Virtual Disk Size: 0

Virtual Disk Size Unit: ☐ MB (MegaBytes) ☒ GB (GigaBytes) ☐ TB (TeraBytes)

Read Cache Policy: No Read Ahead

Write Cache Policy: Write Through

Physical Disk Write Cache: ☒ Default ☐ Enable ☐ Disable

Active when creating a virtual disk using unconfigured capacity; selects physical disks for the virtual disk.

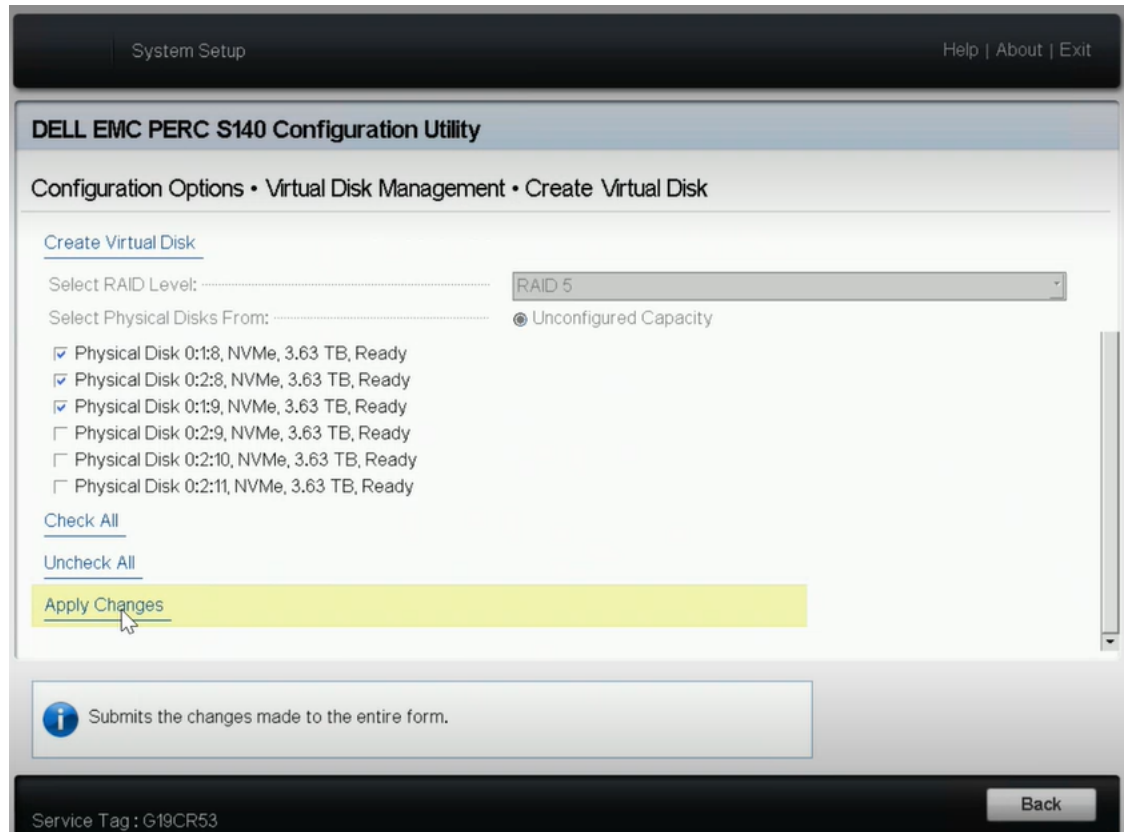
Service Tag : G19CR53 Back

The Select Physical Disk Operation window opens.

- g. For the Select Interface Type option, click **NVMe**.

A list of physical disks is displayed.

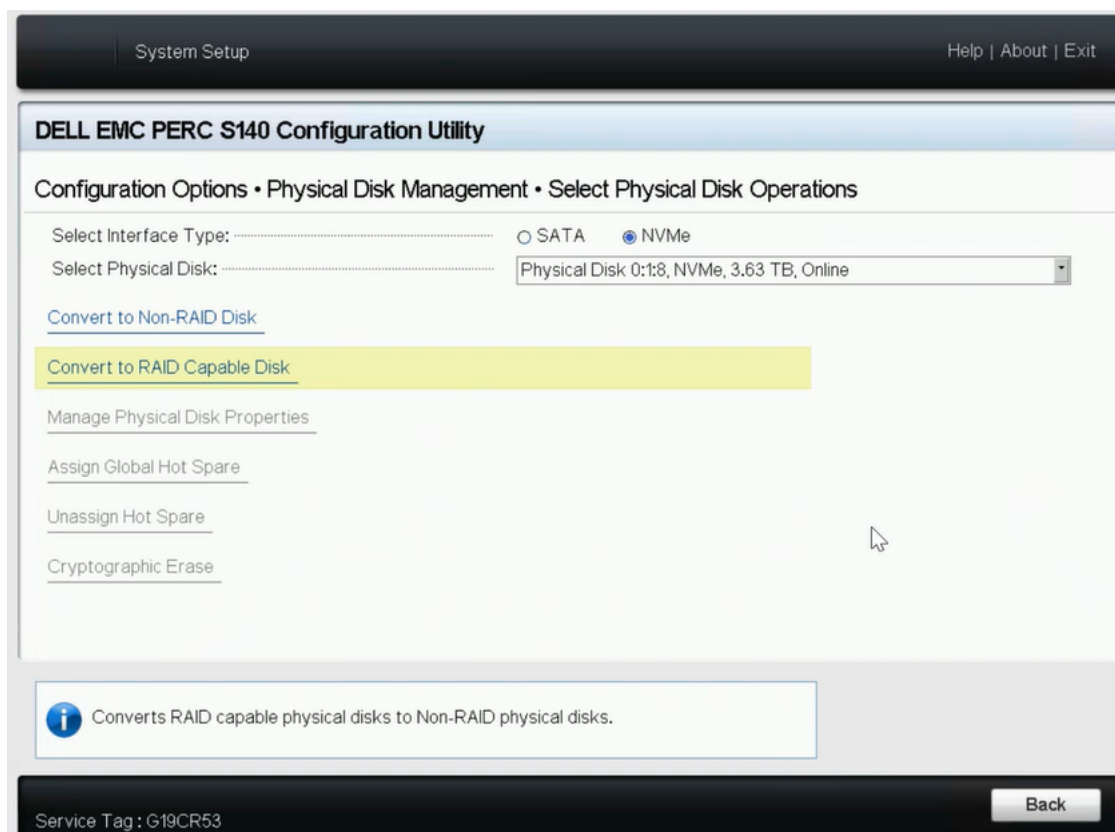
- h. From the list of physical disks, select the disks as needed, and then click **Apply Changes**.



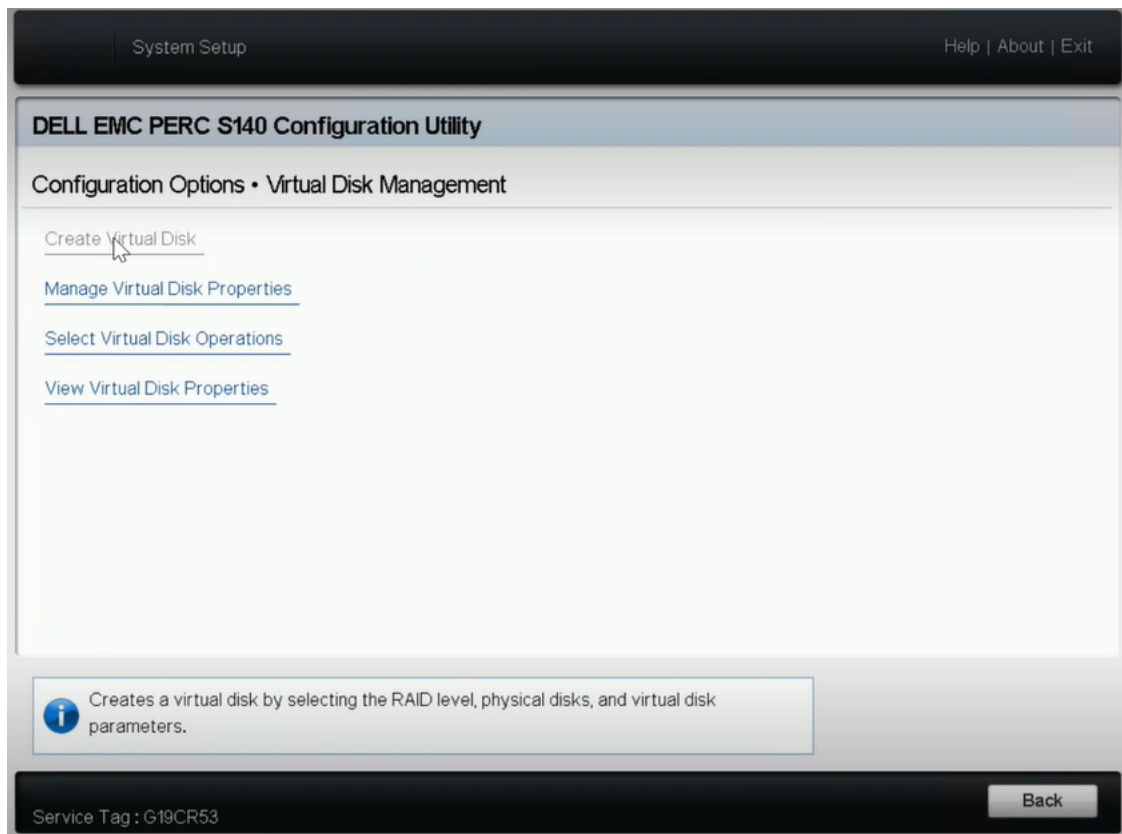
Notes: Select a minimum of three disks and a maximum of 16 disks.

- i. After the changes are applied, click the **Create Virtual Disk** option again to complete the process of creating the virtual disk.
3. Navigate to **Configuration Options > Physical Disk Management > Select Physical Disk Operations**.
 - a. For Select Interface Type, click **NVMe**.
 - b. From the Select Physical Disk drop-down list, select the option as needed, and then click **Convert to RAID Capable Disk**.

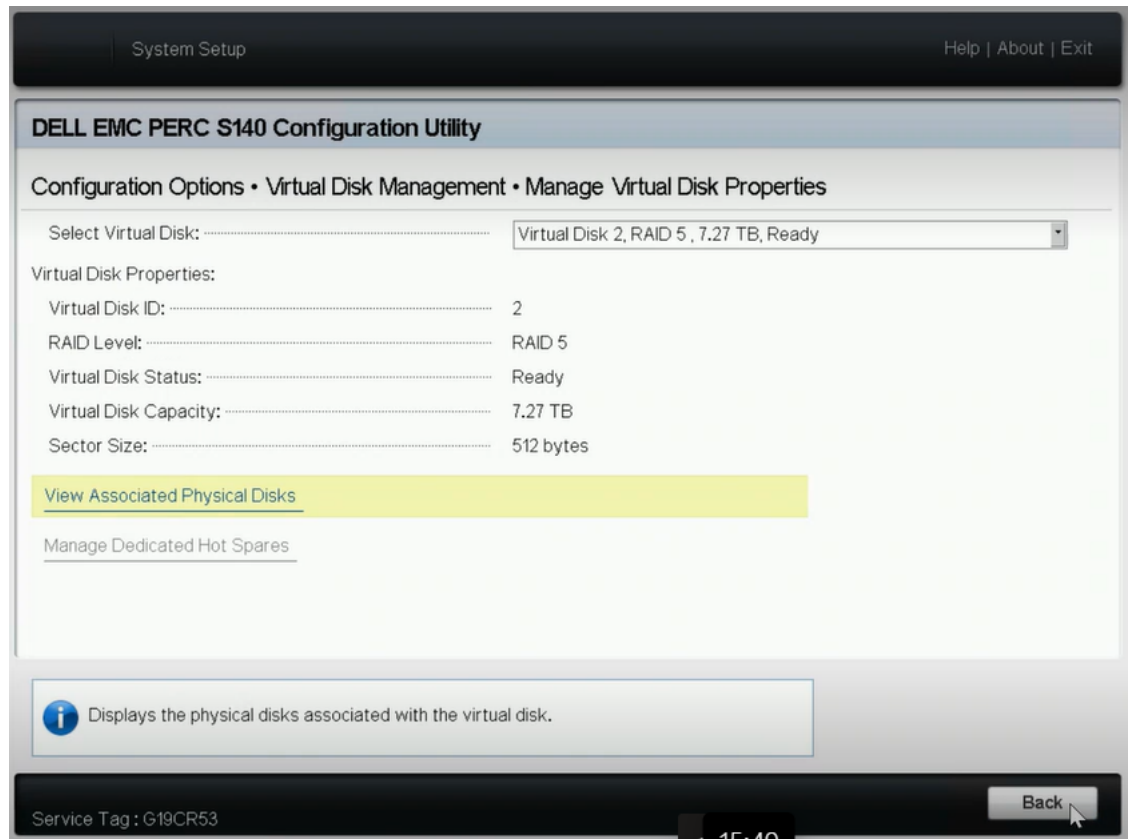
Note: You can apply the Convert to RAID Capable Disk option to all the physical disks one by one.



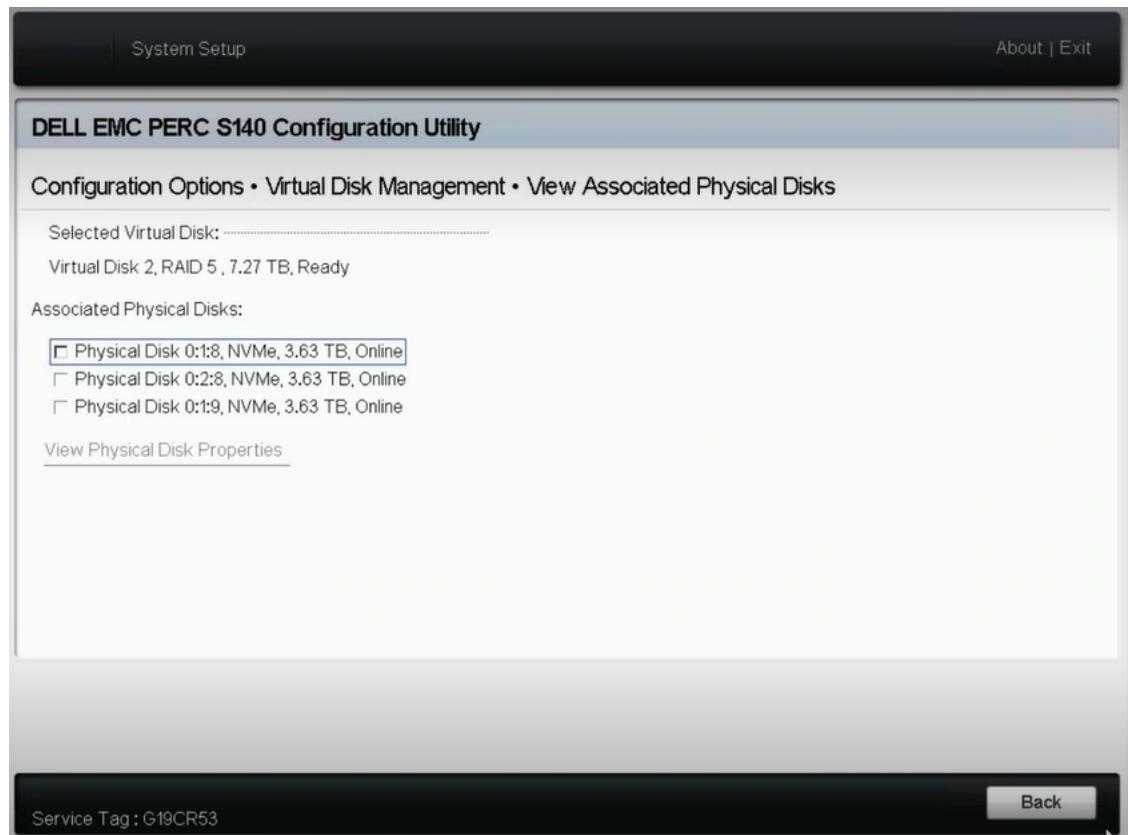
- c. When the following warning message is displayed, do the following:
- RAC0516: Converting physical disk drives to RAID-compatible will over-write any OS-created RAID arrays.
1. Verify that there are no OS-configured RAID arrays, and then click OK.
 2. Click OK.
4. Navigate to **Configuration Options > Virtual Disk Management**, and then do the following:



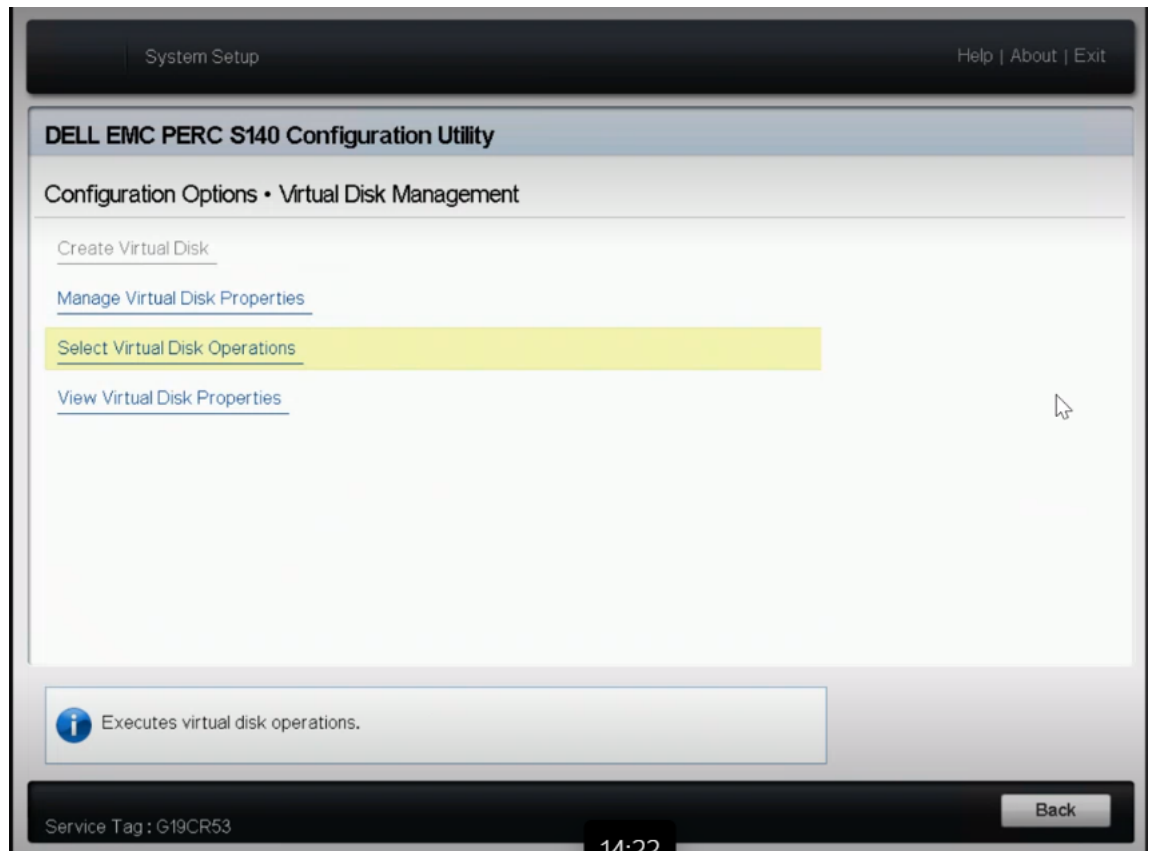
- a. To manage your virtual disks, click **Manage Virtual Disk Properties**.
From the Select Virtual Disks drop-down list, select any RAID 5 disk,
and then click **View Associated Physical Disks**.



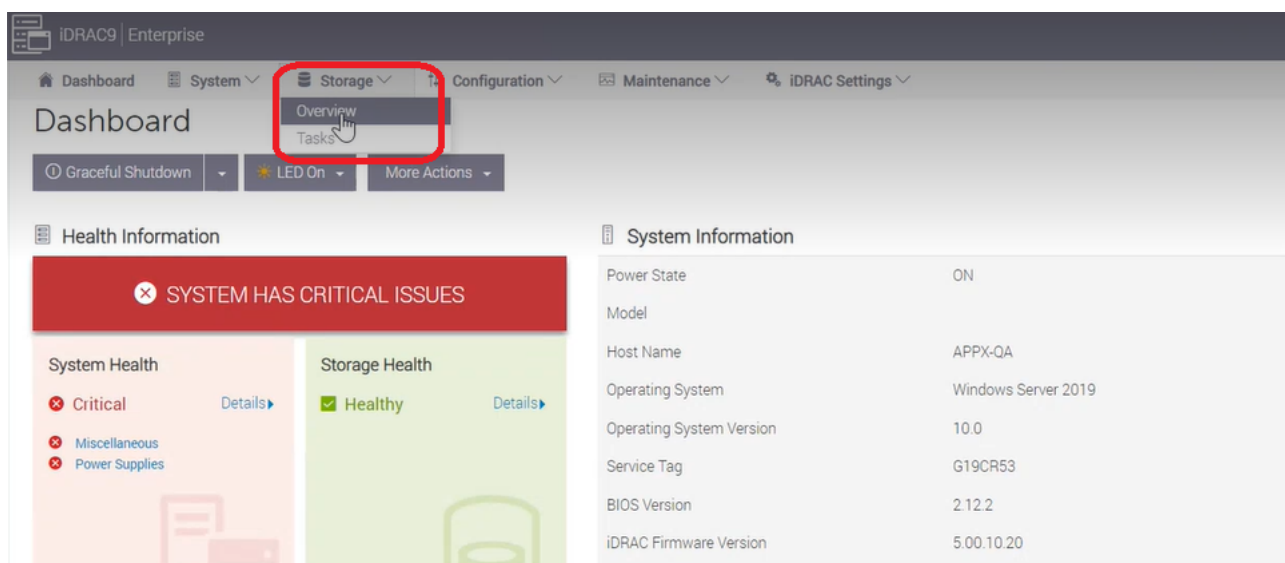
The associated disks are displayed.



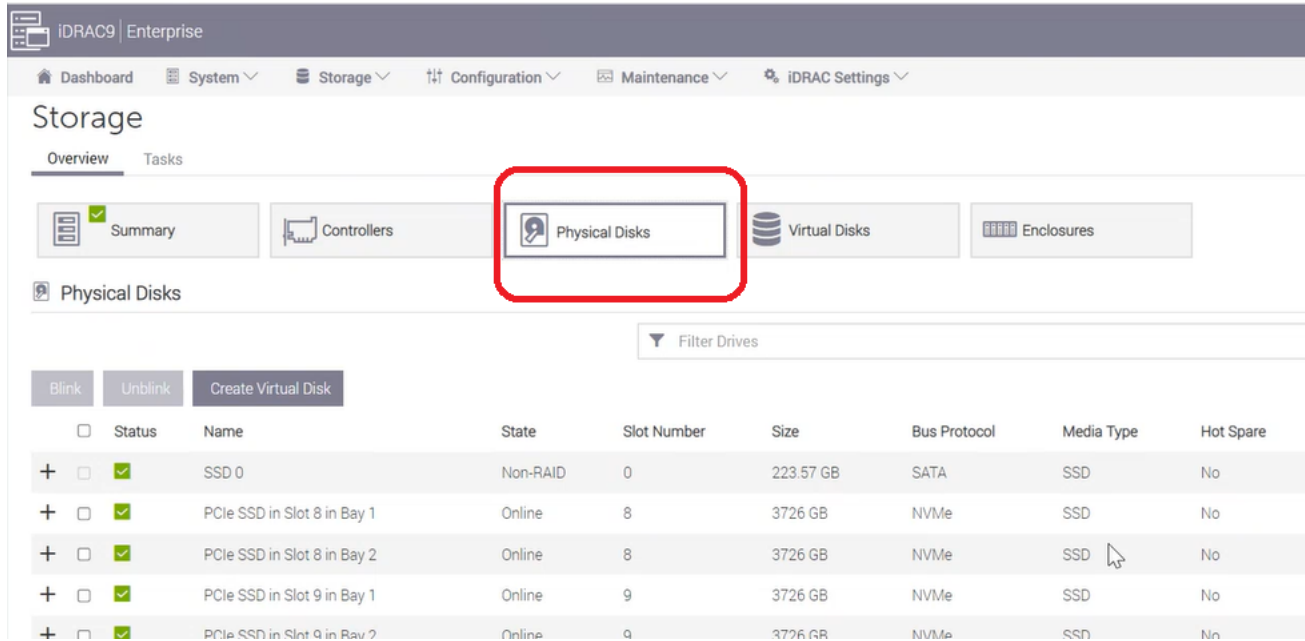
- b. To select the virtual disk operations, click **Select Virtual Disk Operations**.



- c. To view the virtual disk properties in the Boot Manager, click **View Virtual Disk Properties**.
5. To view the disk information in iDRAC, log into iDRAC, and then click **Storage > Overview**.



In the Overview section, click **Physical Disks** to view the list of physical disks that you have created.



6. To initialize and format the newly added Virtual Disk, do the following:

a. Navigate to **Computer Management and Disk Management**.

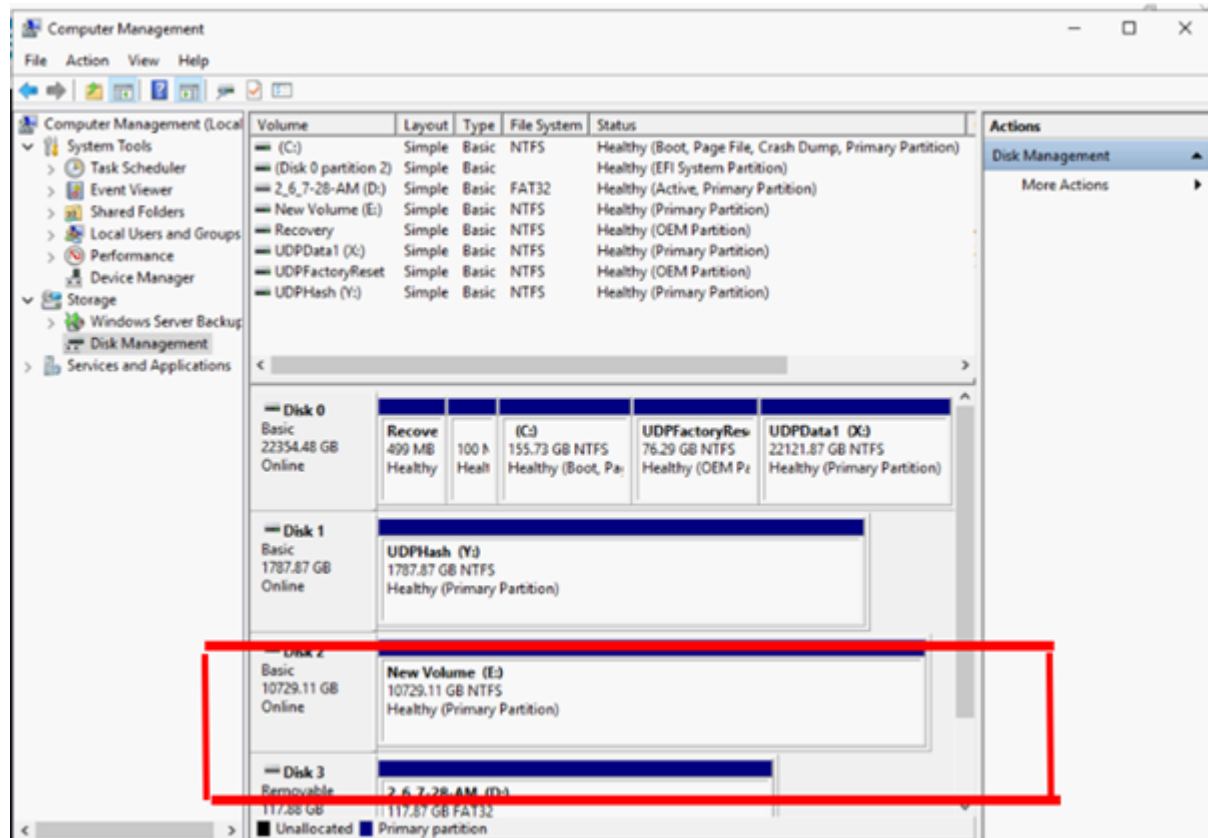
b. Double click the new virtual disk that you added.

The Initialize Disk window appears.

c. Select the **GPT (GUID Partition Table)** option and click **OK**.

d. From the Disk Management window, select the virtual disk and apply the following properties:

- ♦ Assign a Drive Letter
- ♦ Specify NTFS as File System
- ♦ Format the disk



The virtual disk is created.

Working with Expansion Kit in Arcserve Appliance 9072-9504 DR Models

Arcserve Expansion Kit lets you expand the data capacity in Arcserve Appliance 9072-9504DR models.

Follow these steps:

1. Perform the following steps to insert HDDs in the empty disk slots:
 - a. From the Arcserve UDP Console verify and ensure that no jobs are running on the Appliance Server. If any jobs are running, Pause the corresponding plans.
 - b. Insert HDD in the empty disk slot.



2. Perform the following steps to configure Raid-6 from iDRAC:
 - a. Log into iDRAC and navigate to Configuration, Storage Configuration and Physical Disk Configuration.
 - b. Under **Physical Disk Configuration** section, select **Convert to RAID** option from **Actions** drop-down for each new disk.

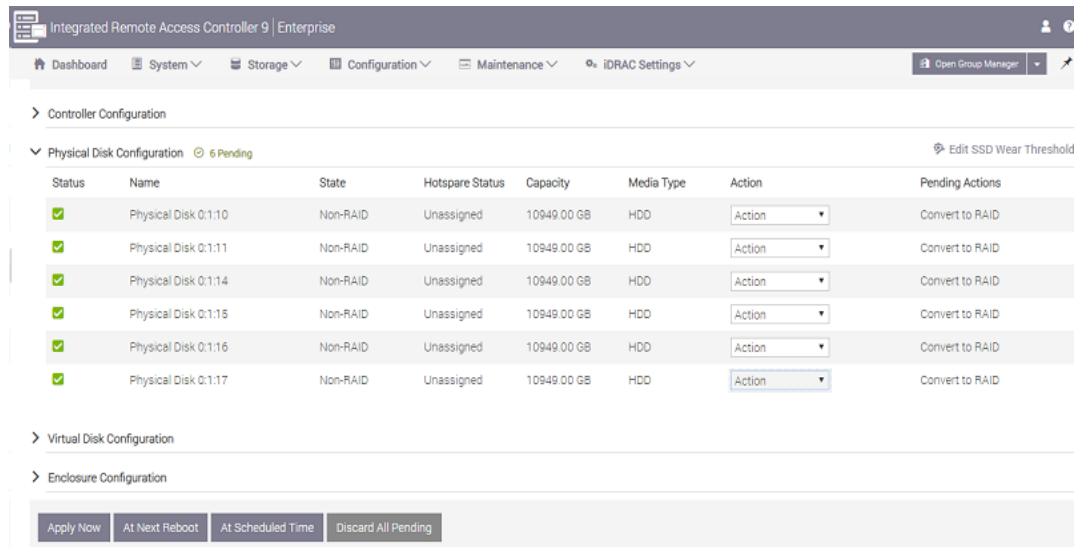
A dialog appears to display the following warning message:

RAC0516: Converting physical disk drives to RAID-compatible will overwrite any OS-created RAID arrays.

Make sure that there are no OS-configured RAID arrays, and then click OK.

- c. Click **OK**.

The Convert to Raid status appears under Pending Actions.



- d. Click one of the following options to complete the pending actions:

Apply Now

Starts the convert to Raid action immediately.

At Next Reboot

Starts the convert to Raid action at the time of next reboot.

At Scheduled Time

Starts the convert to Raid action at the scheduled time.

Discard All Pending

Discards the convert to Raid action for all the disks.

- e. Navigate to **Maintenance, Job Queue**.

The list of jobs running to convert the disks to Raid appears. When convert to RAID job is completed the status changes to **Completed (100%)**.

3. Perform the following steps to create virtual disk:

- Navigate to Configuration, Storage Configuration and Virtual Disk Configuration.
- Under **Virtual Disk Configuration** section, click **Create Virtual Disk**.
- Select **RAID-6** as **Layout**.
- Under **Select Physical Disks** section, select the disks that are converted to RAID.
- Click **Add to Pending Operations**.

Create Virtual Disk

Name	<input type="text" value="Enter or use auto-name"/>
Layout	RAID-6 ▾
Media Type	HDD ▾
Stripe Element Size	64 KB ▾
Capacity*	<input type="text" value="14.55"/> TB ▾
Read Policy	Read Ahead ▾
Write Policy	Write Back ▾
Disk Cache Policy	Default ▾
T10 PI Capability	Disabled ▾
Span Count	1 ▾

- f. Navigate to Configuration and Storage Configuration.
- g. Click one of the following options to complete the pending operations:

Apply Now

Starts the create virtual disk operation immediately.

At Next Reboot

Starts the create virtual disk operation at the time of next reboot.

At Scheduled Time

Starts the create virtual disk operation at the scheduled time.

Discard All Pending

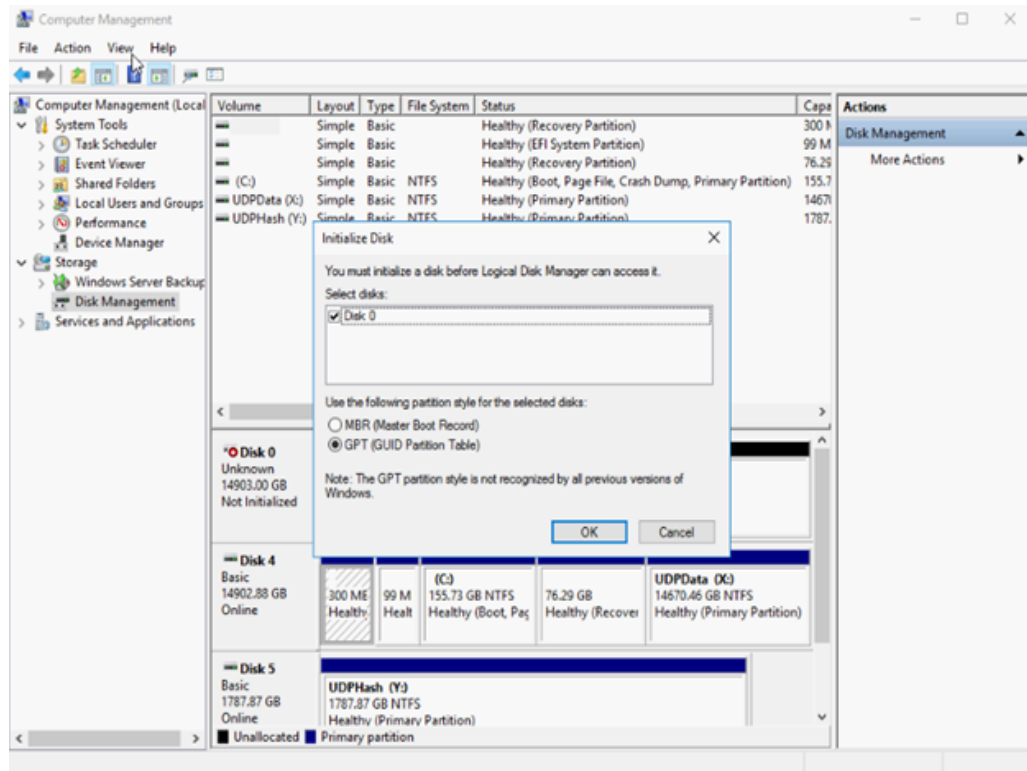
Discards the create virtual disk operation for all the disks.

- h. Navigate to **Maintenance, Job Queue**.

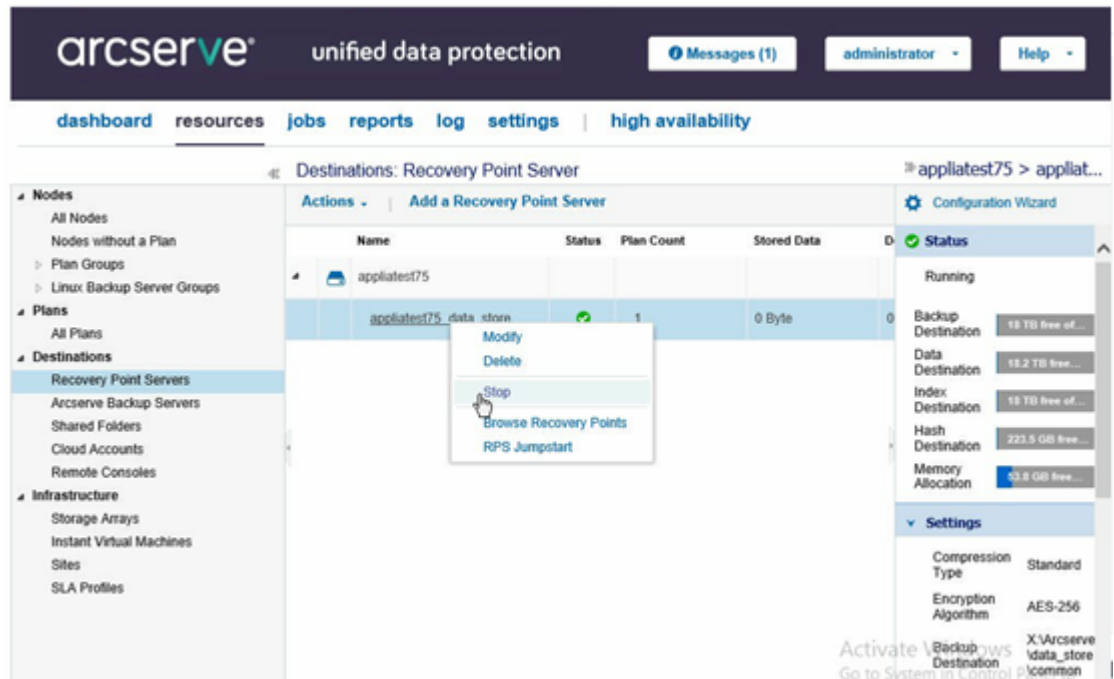
The list of jobs running to create virtual disk appears. When create virtual disk job is completed the status changes to **Completed (100%)**.

- i. Navigate to **Computer Management and Disk Management**.
- j. Double click the new virtual disk that you added.
The Initialize Disk window appears.
- k. Select the **GPT (GUID Partition Table)** option and click **OK**.

- I. From the **Disk Management** window, select the virtual disk and apply the following properties:
 - Assign a Drive Letter
 - Specify NTFS as File System
 - Format the disk



4. Perform the following steps to expand the datastore:
 - a. Navigate to the Drive that you added and create a folder.
 - b. From the Arcserve Appliance desktop, launch the **Arcserve Appliance** wizard.
Arcserve Appliance Configuration page opens.
 - c. Click **Launch UDP Console**.
Arcserve UDP Console login page appears.
 - d. Log into UDP Console as Administrator.
 - e. Navigate to **resources**, **Destinations**, and **Recovery Point Servers**.
 - f. Right click the datastore and click **Stop**.



- g. From the command line, navigate to `C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN` and run the following command:

```
as_gddmgr.exe -DataPath Add <datastore name> -NewDataPath <new data folder>
```

The following example screen shows the details such as Volume capacity, Used space, Free space for Primary data path, Expanded data path and the total values. The total value is the sum of primary data path and expanded data path.

To view the data path details, you can also run the following command:

```
as_gddmgr.exe -DataPath Display <datastore name>
```

```
C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN>as_gddmgr.exe -Data
path Add appliatest75_data_store -NewDataPath Y:\data
Successfully load data store configuration information.
Successfully added new expanded data path for the data store.
The data store has 1 expanded data path(s) now:

          Volume capacity      Used space      Free space
Primary data path : X:\Arcserve\data_store\data\
                  18384 GB          1 GB          18383 GB
Expanded data path1: Y:\data
                  224 GB            1 GB          223 GB
Total              18608 GB          2 GB          18606 GB
Success to add data path Y:\data.
C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN>
```

Successfully added new expanded data path to the datastore.

- h. In UDP Console, navigate to **resources**, **Destinations**, and **Recovery Point Servers**.
- i. Right click the datastore and click **Start**.
- j. Resume the plans that you paused before from UDP Console.

Data capacity of the Arcserve Appliance is successfully expanded.

Working with SSD Flash Expansion Kit in Arcserve Appliance 9072-9504 DR Models

Arcserve SSD Flash Expansion Kit lets you expand the data capacity by creating secondary datastore and performing DR related operations (IVM /VSB/Continuous Availability) in the Arcserve Appliance 9072-9504DR models.

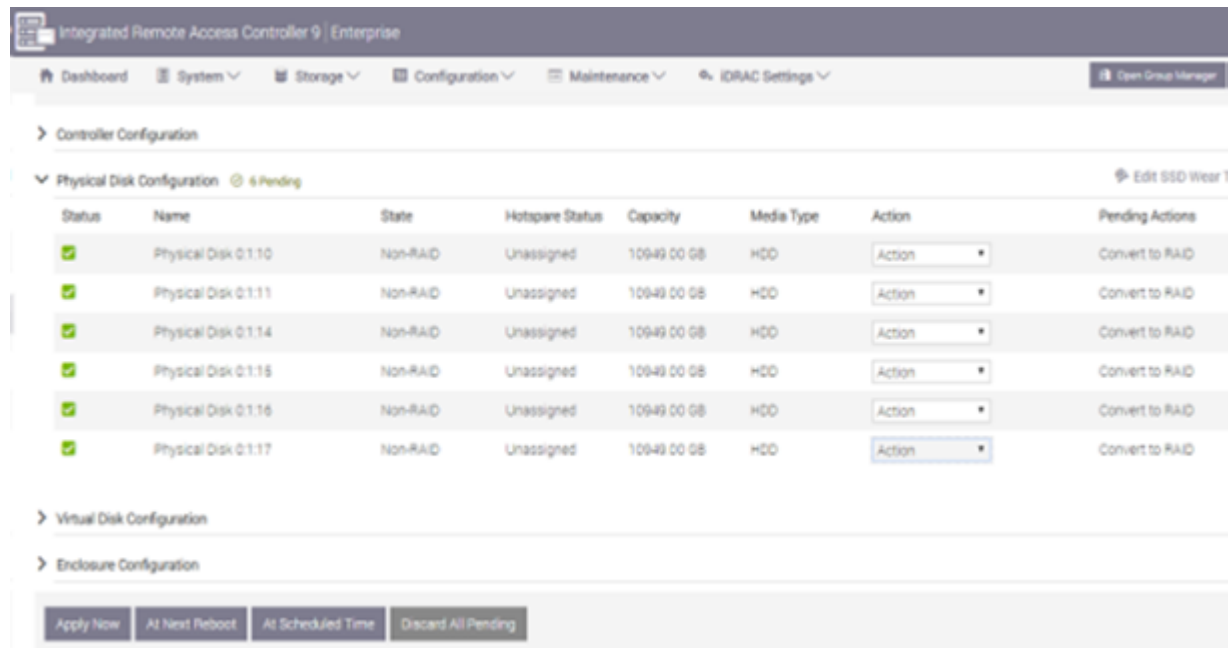
Follow these steps:

1. Perform the following steps to insert SSDs in the empty disk slots:
 - a. From the Arcserve UDP Console, verify and make sure that there are no jobs are running on the Appliance Server. If in case any jobs are running, pause the corresponding plans.
 - b. Insert SSDs in the empty disk slot.



2. Perform the following steps to configure Raid-5 from iDRAC:
 - a. Log into iDRAC, and then navigate to **Configuration > Storage Configuration > Physical Disk Configuration**.
 - b. Under the Physical Disk Configuration section, from the **Actions** drop-down list of each new SSD DISK, select the **Convert to RAID** option.
A dialog appears to display the following warning message:
RAC0516: Converting physical disk drives to RAID-compatible will overwrite any OS-created RAID arrays.
Make sure that there are no OS-configured RAID arrays, and then click **OK**.
 - c. Click **OK**.

As the media type is SSD, the Convert to Raid status appears under the Pending Actions column.



- d. Click one of the following options to complete the pending actions:

Apply Now

Starts the convert to Raid action immediately.

At Next Reboot

Starts the convert to Raid action at the time of next reboot.

At Scheduled Time

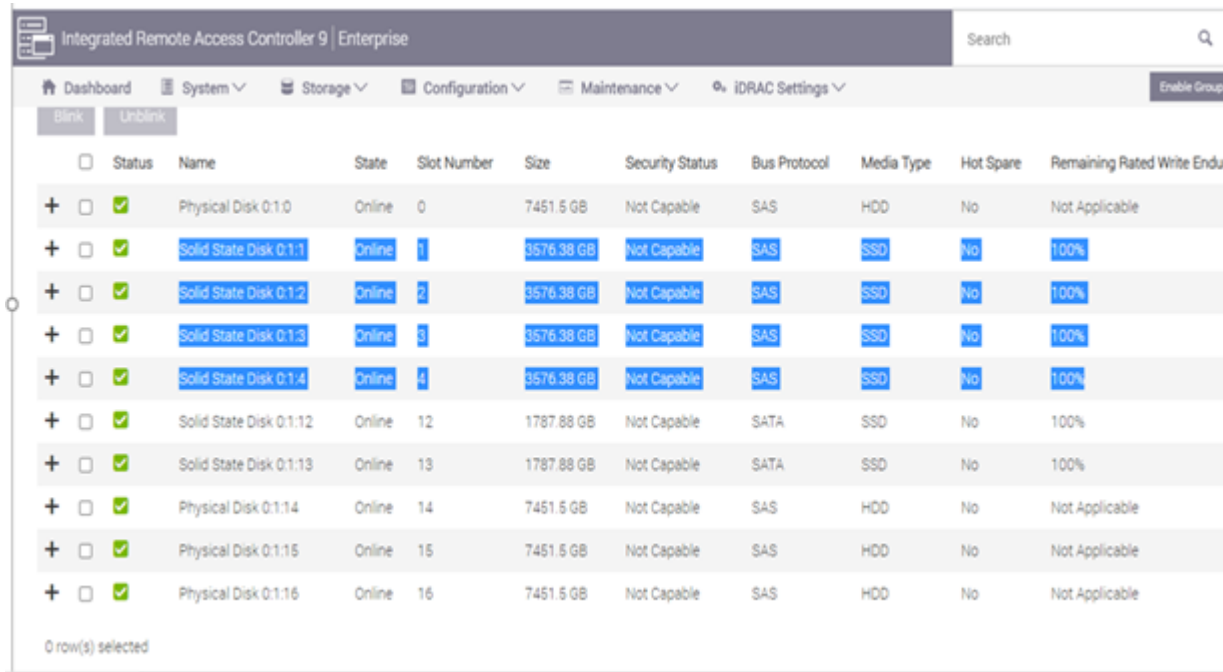
Starts the convert to Raid action at the scheduled time.

Discard All Pending

Discards the convert to Raid action for all the disks.

- e. Navigate to Maintenance, Job Queue.

The list of jobs running to convert the disks to Raid appears. When converting to RAID job is completed, the status displays as 100%.



	Status	Name	State	Slot Number	Size	Security Status	Bus Protocol	Media Type	Hot Spare	Remaining Rated Write Endurance
+	<input checked="" type="checkbox"/>	Physical Disk 0:1:0	Online	0	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable
+	<input checked="" type="checkbox"/>	Solid State Disk 0:1:1	Online	1	3576.38 GB	Not Capable	SAS	SSD	No	100%
+	<input checked="" type="checkbox"/>	Solid State Disk 0:1:2	Online	2	3576.38 GB	Not Capable	SAS	SSD	No	100%
+	<input checked="" type="checkbox"/>	Solid State Disk 0:1:3	Online	3	3576.38 GB	Not Capable	SAS	SSD	No	100%
+	<input checked="" type="checkbox"/>	Solid State Disk 0:1:4	Online	4	3576.38 GB	Not Capable	SAS	SSD	No	100%
+	<input checked="" type="checkbox"/>	Solid State Disk 0:1:12	Online	12	1787.88 GB	Not Capable	SATA	SSD	No	100%
+	<input checked="" type="checkbox"/>	Solid State Disk 0:1:13	Online	13	1787.88 GB	Not Capable	SATA	SSD	No	100%
+	<input checked="" type="checkbox"/>	Physical Disk 0:1:14	Online	14	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable
+	<input checked="" type="checkbox"/>	Physical Disk 0:1:15	Online	15	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable
+	<input checked="" type="checkbox"/>	Physical Disk 0:1:16	Online	16	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable

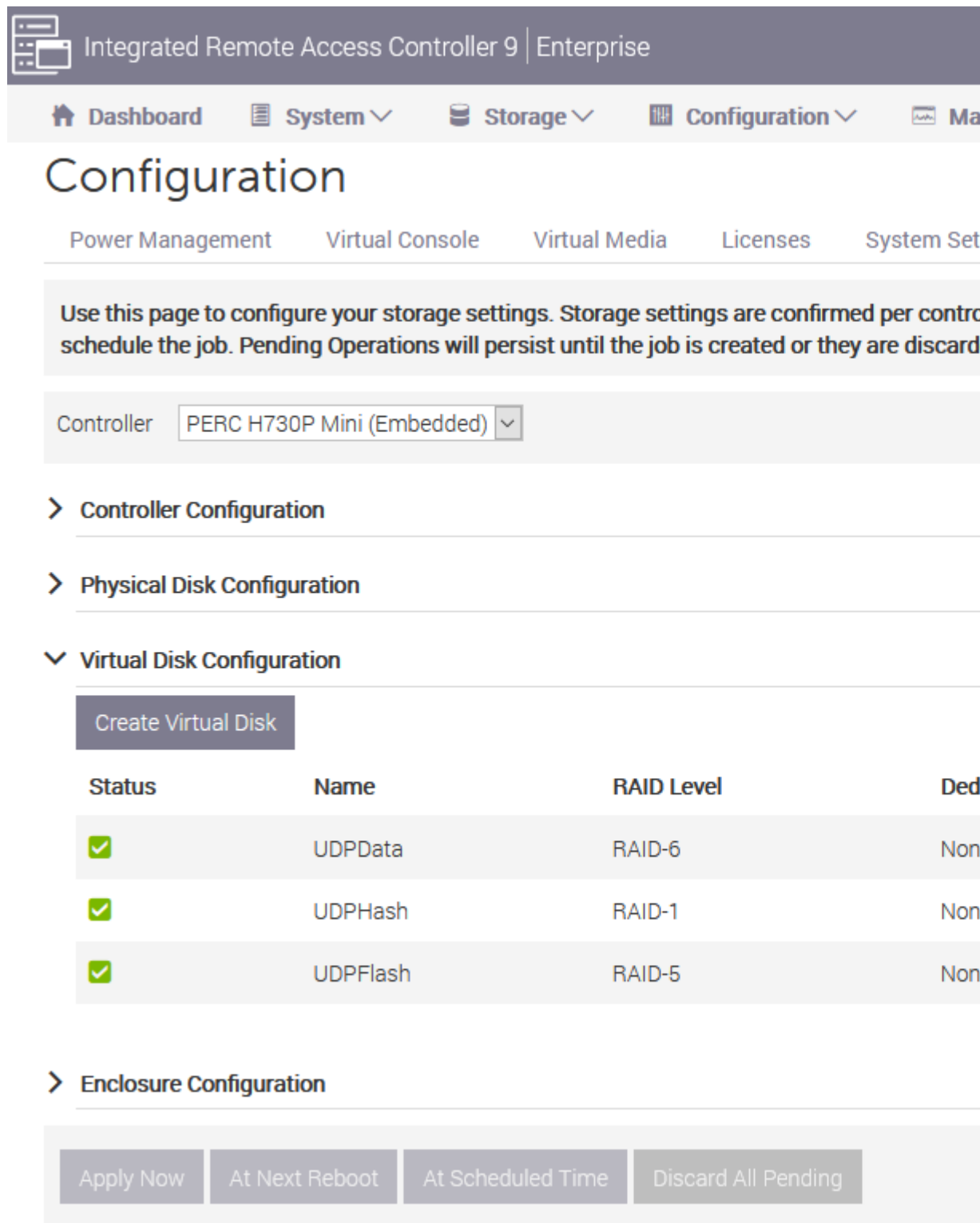
0 row(s) selected

3. Perform the following steps to create virtual disk:
 - a. Navigate to **Configuration > Storage Configuration > Virtual Disk Configuration**.
 - b. Under Virtual Disk Configuration section, click **Create Virtual Disk**.
 - c. In the Create Virtual Disk window, do the following and retain defaults for the remaining:
 - **Layout** - From the drop-down list, select RAID-5.
 - **Media Type** - From the drop-down list, select SSD.
 - d. Under Select Physical Disks section, scroll down and select all the SSD disks that are converted to RAID.
 - e. Click **Add to Pending Operations**.

Create Virtual Disk

Name	<input type="text" value="UDPFash"/>		
Layout	<input type="text" value="RAID-5"/> ▼		
Media Type	<input type="text" value="SSD"/> ▼		
Stripe Element Size	<input type="text" value="64 KB"/> ▼		
Capacity*	<input type="text" value="10.48"/>	TB	▼
Read Policy	<input type="text" value="Read Ahead"/> ▼		
Write Policy	<input type="text" value="Write Back"/> ▼		
Disk Cache Policy	<input type="text" value="Default"/> ▼		
T10 PI Capability	<input type="text" value="Disabled"/> ▼		
Span Count	<input type="text" value="1"/> ▼		

- f. Navigate to **Configuration > Storage Configuration**.
- g. To create the virtual disk operation immediately, click **Apply Now**.



Integrated Remote Access Controller 9 | Enterprise

Dashboard System Storage Configuration Maintenance

Configuration

Power Management Virtual Console Virtual Media Licenses System Settings

Use this page to configure your storage settings. Storage settings are confirmed per controller and schedule the job. Pending Operations will persist until the job is created or they are discarded.

Controller PERC H730P Mini (Embedded) ▼

- > Controller Configuration
- > Physical Disk Configuration
- ▼ Virtual Disk Configuration
 - Create Virtual Disk

Status	Name	RAID Level	Deduplication
✓	UDPData	RAID-6	Non-Deduped
✓	UDPHash	RAID-1	Non-Deduped
✓	UDPFlash	RAID-5	Non-Deduped
- > Enclosure Configuration

Apply Now At Next Reboot At Scheduled Time Discard All Pending

- h. Navigate to **Maintenance > Job Queue**.

The list of jobs running to create virtual disk appears. When virtual disk job is created, the status changes to **100%**.

- i. Navigate to **Computer Management and Disk Management**.

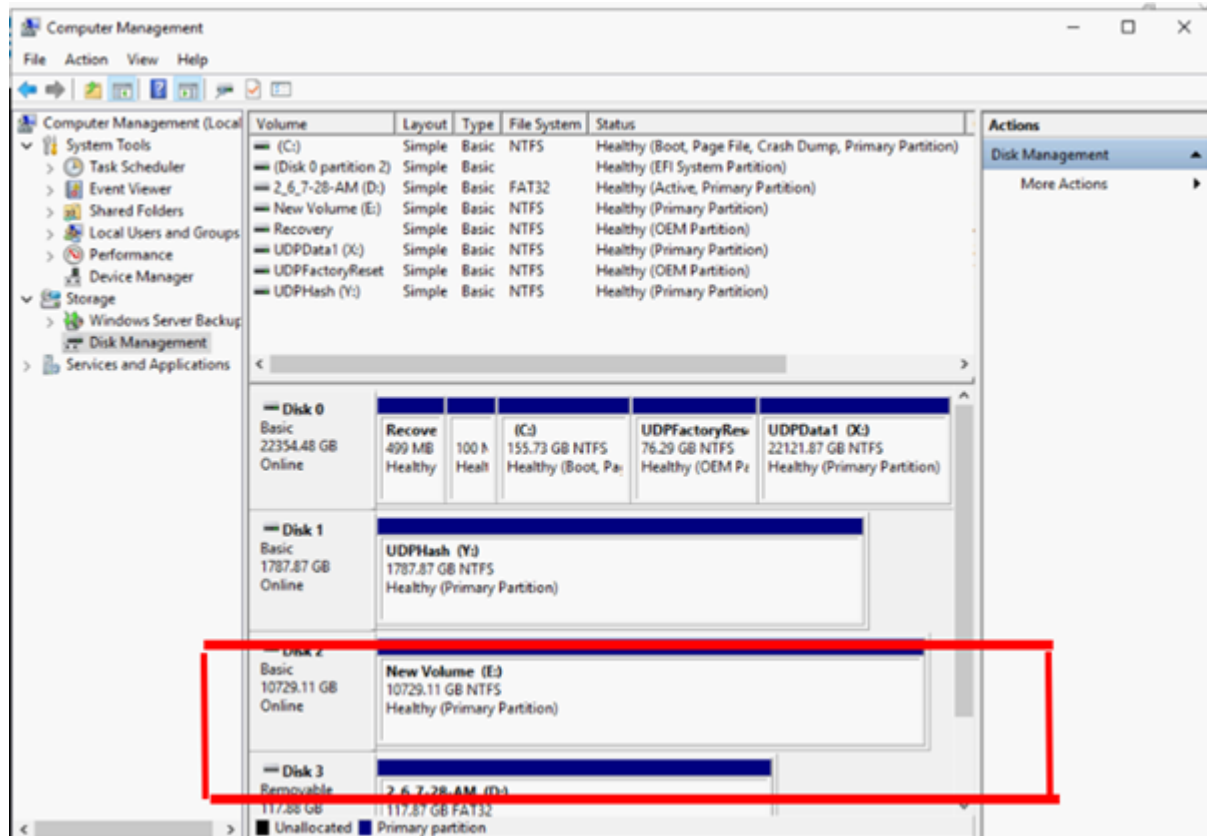
j. Double click the new virtual disk that you added.

The Initialize Disk window appears.

k. Select the **GPT (GUID Partition Table)** option and click **OK**.

l. From the Disk Management window, select the virtual disk and apply the following properties:

- ♦ Assign a Drive Letter
- ♦ Specify NTFS as File System
- ♦ Format the disk



The virtual disk is created.

Chapter 10: Working with Network Configuration

This section contains the following topics:

Understanding the Network Configuration Details	190
How to Disable DHCP Server	195
How to Configure IP Address for the Preinstalled Linux Backup Server	196
How to Enable Round Robin on the DNS Server to Balance Load	198
How to Check Network Status on Appliance	199

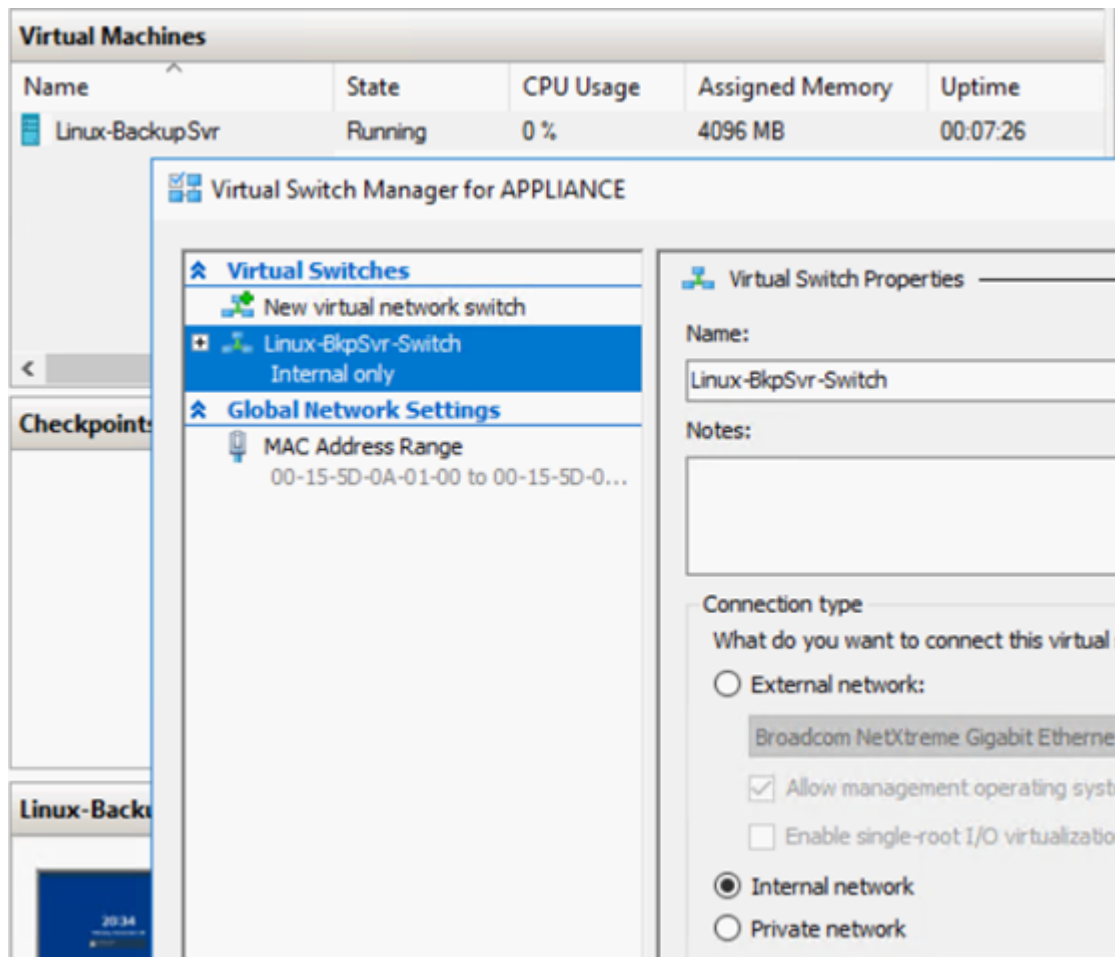
Understanding the Network Configuration Details

The network configuration on Appliance enables the built-in Linux Backup Server (virtual name in Hyper-V Manager: Linux-BackupSvr) to work behind NAT and provides the following advantages:

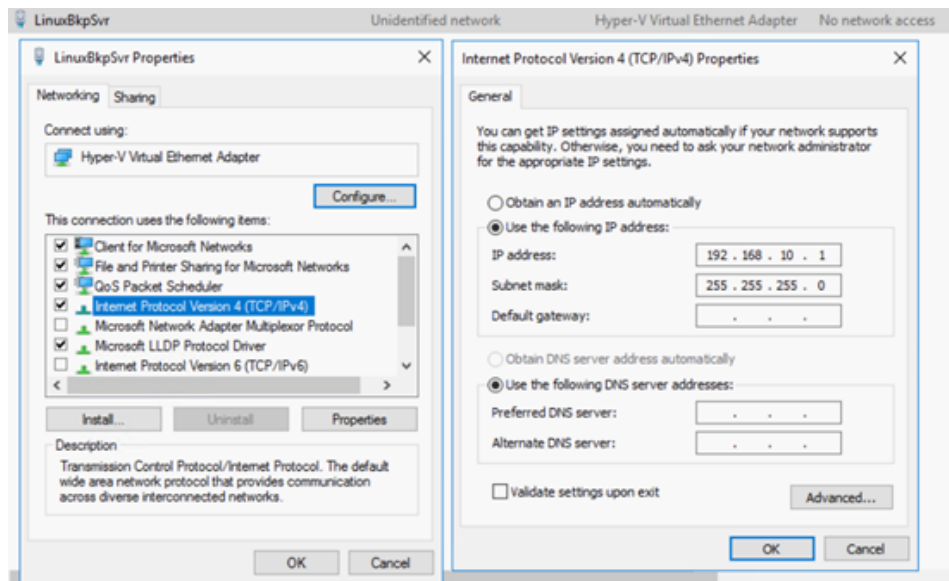
- User does not need to change the host name of the built-in Linux.
- User saves an IP on the network for the Linux Backup Server.
- The Linux Backup Server can connect to any machine on the public network.
- Any machine on the public network can connect to the Linux Backup Server through the special port of Appliance Server only.

Network Configuration Details:

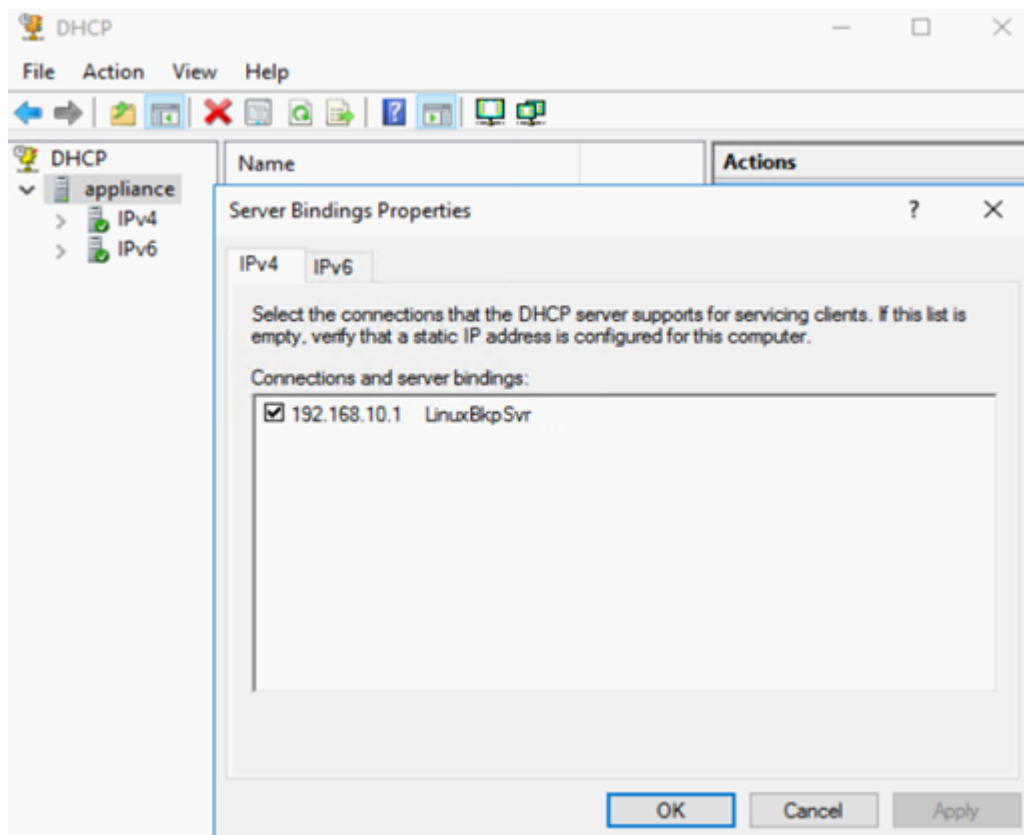
- On the Hyper-V Manager, an internal only virtual switch – *Linux-BkpSvr-Switch* is available that is used only by Linux-BackupSvr.



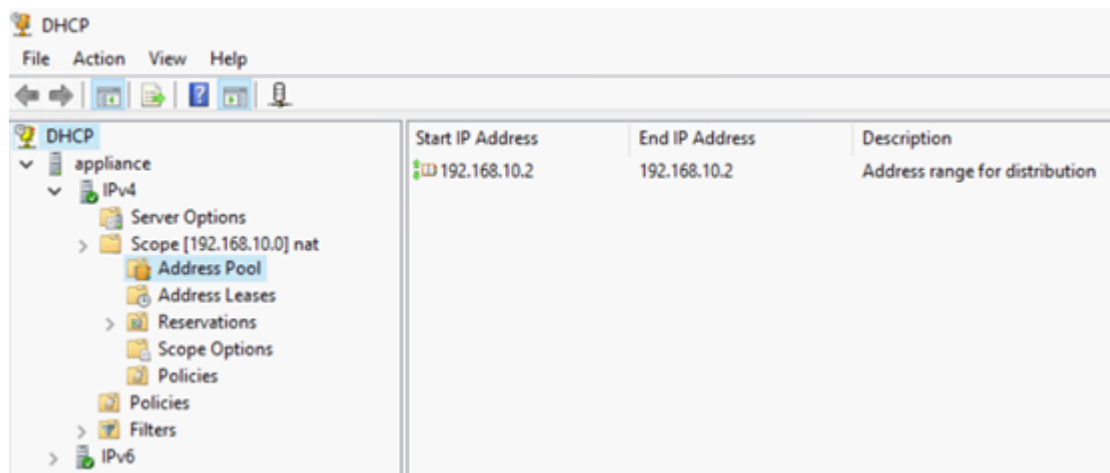
- In the *Control Panel\Network and Internet\Network Connections*, you can see “Hyper-V Virtual Ethernet Adapter” named as “LinuxBkpSvr”. You have configured the IPv4 for this switch as “192.168.10.1” by default as below.



- You have configured DHCP Server on the appliance machine by default. The DHCP Server works only on the Hyper-V virtual adapter.



- By default, only one 192.168.10.2 in the Address Pool to ensure the built-in Linux Backup Server can get the IP 192.168.10.2.



- We have configured NAT on the Appliance machine.

Name	Status	Device Name	Connectivity	Network Category
NIC1	Disabled	Broadcom NetXtreme Gigabit Et...		
NIC2	Disabled	Broadcom NetXtreme Gigabit Et...		
NIC3	Disabled	Broadcom NetXtreme Gigabit Et...		
NIC4	ARCserve.COM	Broadcom NetXtreme Gigabit Et...	Internet access	Public network
LinuxBkpSvr	Unidentified network	Hyper-V Virtual Ethernet Adapter	No network access	Public network

```
Administrator: Command Prompt
c:\Windows\System32>netsh routing ip nat dump

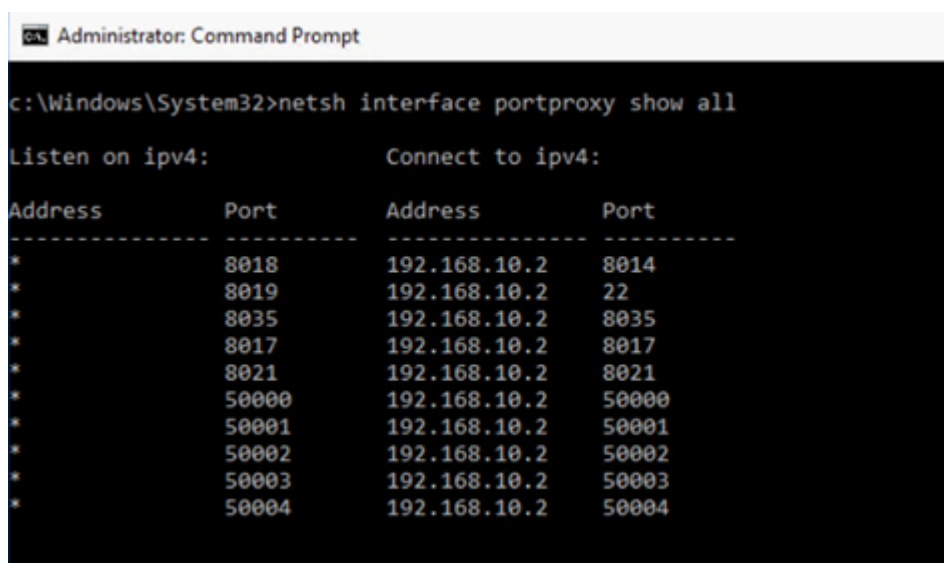
# -----
# NAT configuration
# -----
pushd routing ip nat
install
set global tcptimeoutmins=1440 udptimeoutmins=1 loglevel=ERROR

#
#NAT Configuration For Interface NIC4
#
add interface name="NIC4" mode=FULL

#
#NAT Configuration For Interface LinuxBkpSvr
#
add interface name="LinuxBkpSvr" mode=PRIVATE

popd
```

- We have configured port redirection on the appliance for the Linux Backup Server.



```
Administrator: Command Prompt

c:\Windows\System32>netsh interface portproxy show all

Listen on ipv4:          Connect to ipv4:
Address      Port      Address      Port
-----
*            8018      192.168.10.2 8014
*            8019      192.168.10.2 22
*            8035      192.168.10.2 8035
*            8017      192.168.10.2 8017
*            8021      192.168.10.2 8021
*            50000     192.168.10.2 50000
*            50001     192.168.10.2 50001
*            50002     192.168.10.2 50002
*            50003     192.168.10.2 50003
*            50004     192.168.10.2 50004
```

- Linux Backup Server gets the IP address 192.168.10.2 from the DHCP Server. After getting the IP, the backend script (*C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\resetdhcp.ps1*) communicates with Linux to change the system locale of the Linux to make it consistent with the system locale of the Appliance Windows OS.

```
[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
```


How to Disable DHCP Server

DHCP Server is enabled by default on the Appliance. The DHCP Server works only on Hyper-V Virtual Ethernet Adapter – *LinuxBkpSvr* on the Appliance to make sure that the preinstalled Linux Backup Server can get the IP and communicate with the Appliance and does not impact the production network environment.

To disable DHCP Server, follow these steps:

1. Open file *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Configuration\Appliance.properties*
2. Modify the file to *DHCP_ENABLE=false*. The *Appliance.properties* appears as below:

```
DHCP_ENABLE=false
AdapterName=LinuxBkpSvr
Appliance_IPAddress=192.168.10.1
Linux_IPAddress=192.168.10.2
```

3. Save the file.
4. Delete the file *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\dhcpdone.flag*.
5. Run *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\resetdhcp.ps1* to disable the DHCP Server service as below from dos command line:

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

How to Configure IP Address for the Preinstalled Linux Backup Server

Note: This method is applicable to Arcserve Appliance for 9000 series and above.

For the preinstalled Linux Backup Server, by default, the backup server uses IP 192.168.10.2 to communicate with the Appliance Server. To understand how the preinstalled Linux Backup Server communicates with Appliance Server, refer to the network configuration introduction for the preinstalled Linux Backup Server.

To specify the IP address for the preinstalled Linux Backup Server, follow these steps:

1. Open the *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Configuration\Appliance.properties* file.
2. Change the IP address of *Appliance_IPAddress* and *Linux_IPAddress*. For example, set *Appliance_IPAddress* as 192.168.100.1 and *Linux_IPAddress* as 192.168.100.2.

Notes:

- ♦ The IP address of *Appliance_IPAddress* sets to the network interface LinuxBkpSvr (Hyper-V Virtual Ethernet Adapter) used to communicate with this preinstalled Linux Backup Server.
- ♦ The IP address of *Linux_IPAddress* is set to the preinstalled Linux Backup Server.
- ♦ Ensure that *Appliance_IPAddress* and *Linux_IPAddress* use the IP address of the same sub network.

After modifications, the content in the file looks as follows:

```
DHCP_ENABLE=true
AdapterName=LinuxBkpSvr
Appliance_IPAddress=192.168.100.1
Linux_IPAddress=192.168.100.2
```

3. Save the file.
4. Delete the *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\dhcpcdone.flag* file.
5. Run *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\User_Uutilities\UpdateIcsHostAdapter.ps1* to

reset the IP address for the network interface LinuxBkpSvr and the pre-installed Linux Backup Server.

Notes:

- The preinstalled Linux Backup Server gets shut down and restarts during the process if you change *Linux_IPAddress*.
- To share Internet from the production NIC adapter to the LinuxBkpSvr adapter, run the *UpdateIcsHostAdapter.ps1* file. In case you want a specific NIC adapter to share its internet with the LinuxBkpSvr adapter, use the following registry tweak.

Create the following registry key to provide the name of network adapter through which an Internet must be shared

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

Value Type: "*String*"

Value Name: "*IcsHostAdapter*"

Value Data: "<*Adapter Name*>"

6. After the above registry is changed, run the following command:

```
C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\User_Utilities >powershell .\ UpdateIcsHostAdapter.ps1
```

How to Enable Round Robin on the DNS Server to Balance Load

The Microsoft DNS Server supports round robin, which is a technique used for balancing the load between servers. This feature enables DNS to send both IP addresses when a query is received for *myserver.mydomain.com*. The client (or Resolver) always uses the first one. The next time when DNS receives a query for this name, the order of the IP address list is changed using round robin method (the address that was first in the previous list is last in the new list). Round Robin of name records is not supported because only one canonical name is allowed for any one alias.

In the Appliance, you can add record(s) for all the IPv4 address to the Domain Name Service(DNS) Server to get load balance among the network interfaces.

For more information on load balancing between servers, refer to [RFC 1794](#).

How to Add a Record for Additional IP Addresses to Domain Name Service Server

When a server has two or more network interface cards (NICs), or more than one IP address for an NIC, you can add a record for the additional IP address(es) to the DNS server by creating an "A" record for each IP address.

Example:

Consider that a server's DNS host name is <myserver> and DNS domain name is <mydomain.com>. This server has following two IP addresses assigned:

- IPAddress1
- IPAddress2

To add these IP addresses to the DNS Server, create two "A" records in the <mydomain.com> zone as below:

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

For the Resolver to get the same IP address every time, create two more "A" records assigning a unique name to each address as below:

- Alname1 A <IPAddress1>
- Alname2 A <IPAddress2>

Using this method, a Resolver always obtains IPAddress1 when sending a query for Alname1 and always obtains IPAddress2 when sending a query for Alname2.

How to Check Network Status on Appliance

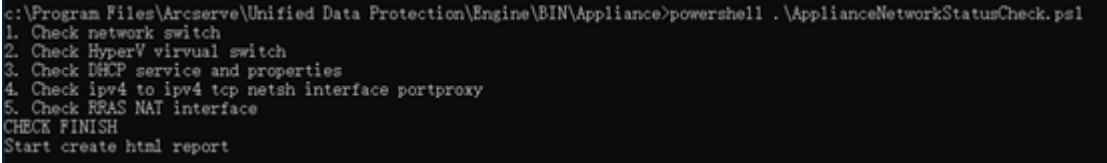
The ApplianceNetworkStatusCheck.ps1 tool is used to gather information about the current overall network status of the Arcserve Appliance Server and generate a report in an XML format. The report includes information about the network adapter, network switch, Hyper-V virtual switch, DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), RRAS (Route and Remote Access Service) and other key configurations on the server.

The ApplianceNetworkStatusCheck.ps1 tool is available in Arcserve Appliance Server UDP V7.0 Update1.

To generate the network status report of the Appliance Server using this tool, follow these steps:

1. Log into the Arcserve Appliance Server as an administrator.
2. Open the command prompt and enter the folder location:
C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance
3. Run ApplianceNetworkStatusCheck.ps1 to generate report:

#Powershell .\ApplianceNetworkStatusCheck.ps1



```
c:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance>powershell .\ApplianceNetworkStatusCheck.ps1
1. Check network switch
2. Check HyperV virtual switch
3. Check DHCP service and properties
4. Check ipv4 to ipv4 tcp netsh interface portproxy
5. Check RRAS NAT interface
CHECK FINISH
Start create html report
```

The browser opens and displays the overall network status report of the Appliance server.

Chapter 11: Understanding Safety Precautions

This section contains the following topics:

General Safety Precautions	201
Electrical Safety Precautions	203
FCC Compliance	204
Electrostatic Discharge (ESD) Precautions	205

General Safety Precautions

You must adhere to the following general safety precautions to protect yourself and to protect the appliance from damage or malfunction:

- For EMI Class A Equipment (Business equipment), this equipment is registered for Electromagnetic Conformity Registration as business equipment (A) and not home equipment. Sellers or users are required to take caution in this regard.

A급기기(업무용방송통신기자재)

이기는업무용(A급)으로전자파적합기기로서판매자또는사용자는이점을주의하시기바라며,가정외의지역에서사용하는것을목적으로합니다

Note: This safety precaution only applies to South Korea. For more details, contact Arcserve Support at <https://www.arcserve.com/support> or call 0079885215375 (South Korea).

- Inspect the box in which the appliance was shipped and ensure that there are no visible signs of damage. If there is evidence of damage, please retain all packaging materials and contact Arcserve Support immediately at: <https://www.arcserve.com/support>.
- Decide on a suitable location for the rack unit that will hold the appliance. It should be situated in a clean, dust-free area that is well ventilated and free of clutter. Avoid areas where heat, electrical noise, and electromagnetic fields are generated.
- You will also need it placed near at least one grounded power outlet. Depending on the model, the appliance includes either one power supply or a redundant power supply and will then require two grounded outlets.
- The appliance is only for use in a restricted location.
 - Access can only be gained by service persons or by users who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken; and
 - Access is through the use of a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location.
- Place the appliance top cover and any components that are removed from the appliance on a table so that you do not accidentally step on the components.

- While working on the appliance, do not wear loose clothing such as neckties and unbuttoned shirt sleeves, which can come into contact with electrical circuits or be pulled into a cooling fan.
- Remove any jewelry or metal objects from your body, which are excellent metal conductors that can create short circuits and harm you if they come into contact with printed circuit boards (PCBs) or areas where power is present.
- After accessing the inside of the appliance, close the appliance and secure it to the rack unit with the retention screws after ensuring that all connections have been made.

Electrical Safety Precautions

You must adhere to the following electrical safety precautions to protect yourself and to protect the appliance from damage or malfunction:

- Be aware of the locations of the power on/off switch on the appliance as well as the room's emergency power-off switch, disconnection switch, or electrical outlet. If an electrical accident occurs, you can then quickly remove power from the appliance.
- Do not work alone when working with high-voltage components.
- Power should always be disconnected from the appliance when removing or installing main system components, such as the Serverboard, memory modules and the DVD-ROM and floppy drives (not necessary for hot swappable drives). When disconnecting power, you should first power down the appliance with the operating system and then unplug the power cords from all the power supply modules in the appliance.
- When working around exposed electrical circuits, another person who is familiar with the power-off controls should be nearby to switch off the power, if necessary.
- Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage any electrical components or circuit boards they come into contact with.
- Do not use mats designed to decrease electrostatic discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- The power supply power cord must include a grounding plug and must be plugged into grounded electrical outlets.
- Serverboard Battery: **CAUTION** - There is a danger of explosion if the onboard battery is installed upside down, which will reverse its polarities. This battery must be replaced only with the same or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.
- DVD-ROM laser: **CAUTION** - this Server may have come equipped with a DVD-ROM drive. To prevent direct exposure to the laser beam and hazardous radiation exposure, do not open the enclosure or use the unit in any unconventional way.

FCC Compliance

This appliance complies with part 15 of the FCC Rules. Operation is subject to the following conditions:

- This appliance may not cause harmful interference, and
- This appliance must accept any interference received, including interference that may cause undesired operation

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

Electrostatic Discharge (ESD) Precautions

Electrostatic Discharge (ESD) is generated by two objects with different electrical charges coming into contact with each other. An electrical discharge is created to neutralize this difference, which can damage electronic components and printed circuit boards. Devices that are sensitive to ESD, such as Serverboards, motherboards, PCIe cards, drives, processors, and memory cards require special handling. Use the following precautions to help neutralize the difference of electrical charges coming into contact with each other, before contact is made, to protect your equipment from ESD:

- Use a rubber mat that has been specifically designed as an electrical insulator. Do not use a mat designed to decrease electrostatic discharge as protection from electrical shock.
- Use a grounded wrist strap designed to prevent static discharge.
- Use antistatic or electrostatic discharge (ESD) preventive clothing or gloves.
- Keep all components and printed circuit boards (PCBs) in their antistatic bags until ready for use.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Do not let components or PCBs come into contact with your clothing, which may retain a charge even if you are wearing a wrist strap.
- Handle a board by its edges only. Do not touch its components, peripheral chips, memory modules, or contacts.
- When handling chips or modules, avoid touching their pins.
- Put the Serverboard and peripherals back into their antistatic bags when not in use.
- For grounding purposes, verify your appliance provides excellent conductivity between the power supply, the case, the mounting fasteners, and the Serverboard.

Chapter 12: Activating Sophos on the Arcserve Appliance for 9000 Series

This section provides information about how to activate Sophos on the Arcserve Appliance.

Important!

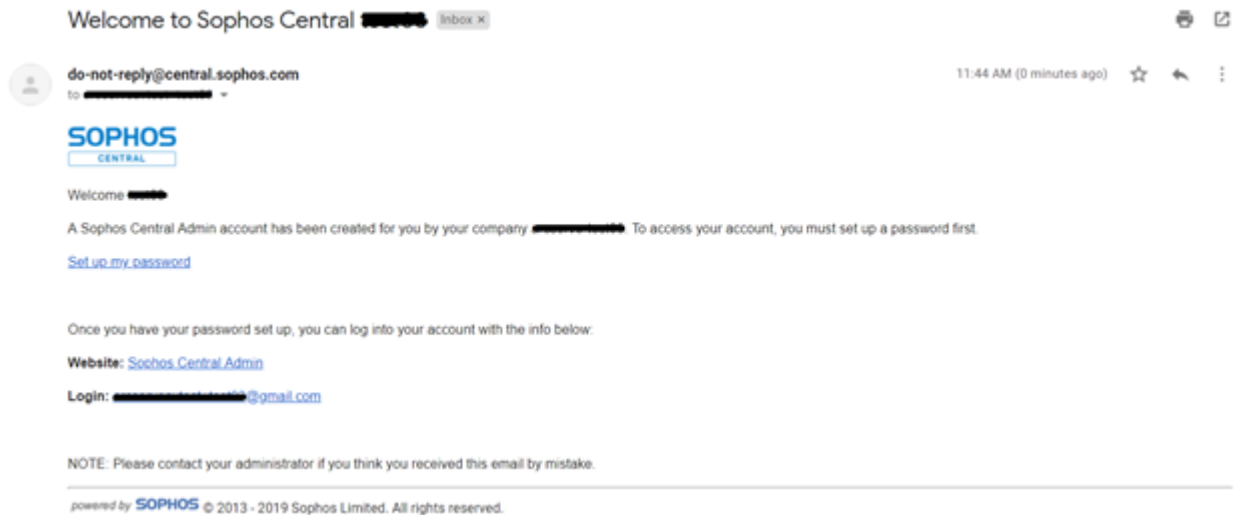
- If you are a new customer of Arcserve Appliances with Sophos Intercept X preinstalled as part of the delivery process, an email is sent with simple activation instructions. Please follow the given methods to complete the activation process. If you are an existing customer, the Arcserve Appliances have no Sophos Intercept X preinstalled. It is recommended to download and install Sophos Intercept X manually.
- Activation of Sophos using the email not applicable for Appliance X Series, and you need to install Sophos manually. For information about the complete installation process, see [Manually Installing Sophos Intercept X Advanced for Server on Arcserve Appliances](#).

Follow these steps:

1. After you receive a Welcome email from Sophos, to set your password, click the **Set up my password** link.

Note: If you apply for more than one customer accounts, you will receive the corresponding number of Welcome emails for each account separately from Sophos to setup password accordingly.

If you already have an existing customer account and want to continue using the same customer account to activate one more Arcserve Appliance Sophos, then you will not get such Welcome emails at email address associated with this customer account. You will receive an email from Arcserve that contains a Zip file and instructions for activating Sophos.



2. To activate Sophos on Arcserve Appliance, see [Activate Sophos on the Arcserve Appliance using the email from Arcserve](#).

Activate Sophos on the Arcserve Appliance using Email

Arcserve sends you a Zip file through email for activating Sophos. Unzip the file. The folder “Arcserve_Appliance_Sophos_Activation_YYYY-MM-DD-HH-MM-SS” contains the following files:

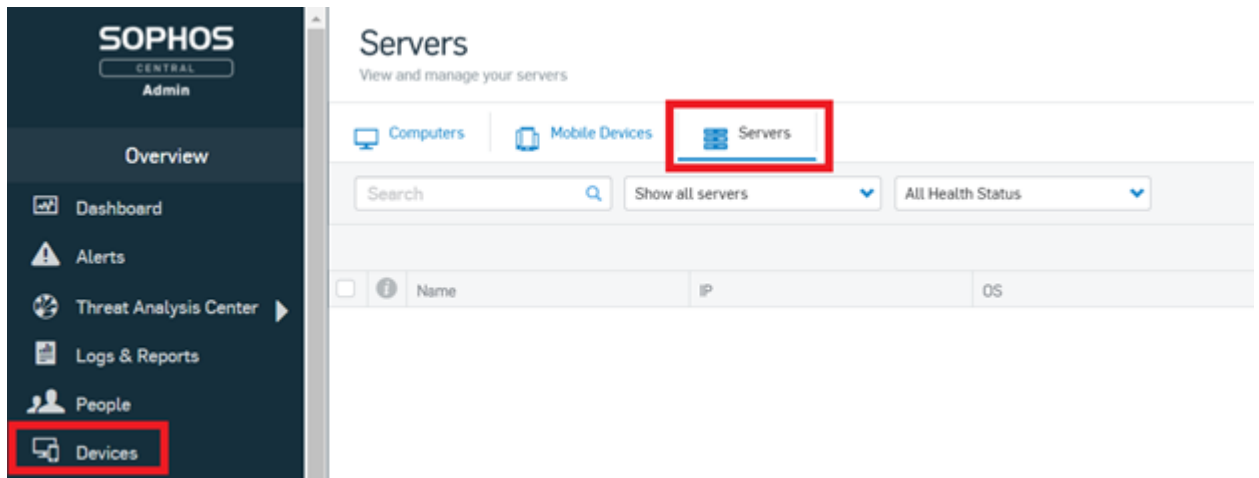
- **Config.xml:** The configuration file.
- **Registration.txt:** The registration file.
- **Arcserve_Appliance_Sophos_Activation.ps1:** Powershell script to run to activate Sophos.

Follow these steps to activate Sophos:

1. Log into Arcserve Appliance as a system administrator.
2. Copy the zip file to Arcserve Appliance, and unzip and extract the file a location as needed.
3. Open the command prompt, and enter the location that contains the extracted files.
4. Run **Arcserve_Appliance_Sophos_Activation.ps1**.

```
#powershell .\ Arcserve_Appliance_Sophos_Activation.ps1
```
5. To view the protected Arcserve Appliance, log into the Sophos Central page with your email address and password, then navigate to Devices > Servers.

Note: The email address where you received the zip file is the the same email address you must use for login.



Sophos is activated on the Appliance.

Manually Installing Sophos Intercept X Advanced for Server on Arcserve UDP

The installation of Sophos Intercept X Advanced for Server on Arcserve UDP enables the following:

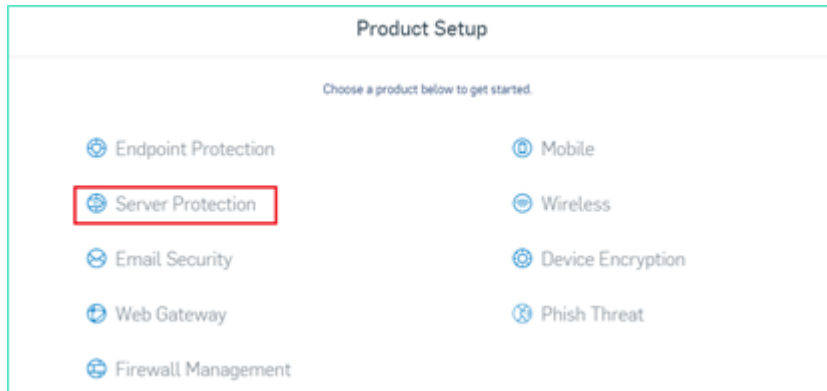
- Protect data and system backups from ransomware and other attacks
- Endpoint protection that combines signature-based and signatureless malware detection.
- Deep learning neural network
- Anti-exploit technology
- CyptoGuard anti-ransomware and WipeGuard technologies, and more to stop the widest range of endpoint threats

Follow these steps:

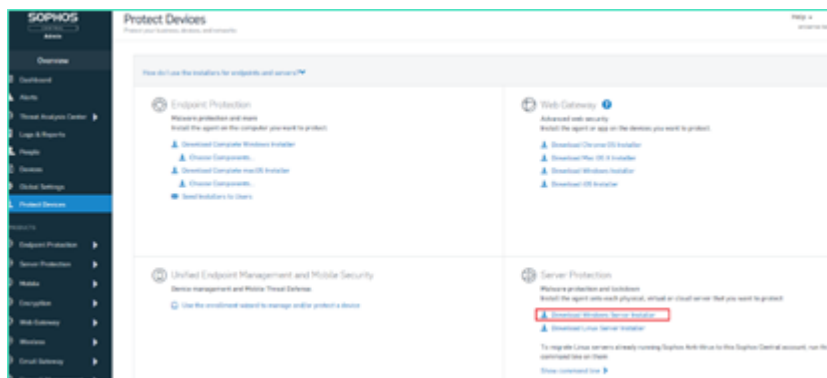
1. On the Arcserve Support Website, create an account.
2. To request for a free copy of Sophos Intercept X Advanced, provide all relevant details in the [Sophos Request form](#) and submit it to Arcserve Support. It is mandatory to share the details of Email ID and Order ID. You will receive an auto-generated email confirmation.

After you confirm your email ID, Arcserve processes your request and creates an account on the Sophos Central and sends an email with instructions on how to create a password.

3. To create a password for your new account on Sophos Central, follow the instructions in the email.
4. Log into Sophos Central.
5. Open the Product Setup dialog, then select **Server Protection**.



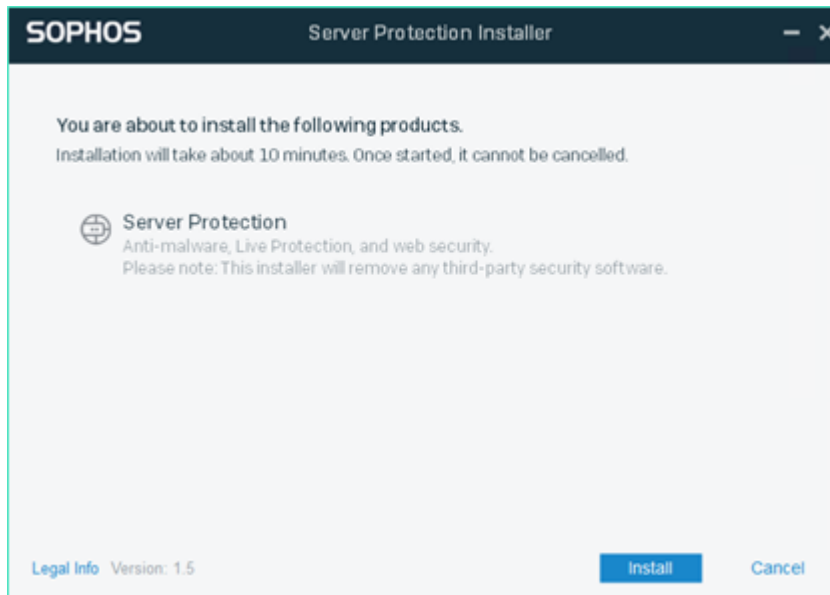
6. From the Server Protection section, click **Download Windows Server Installer**, and then save **SophosSetup.exe** installer to a folder on UDP.



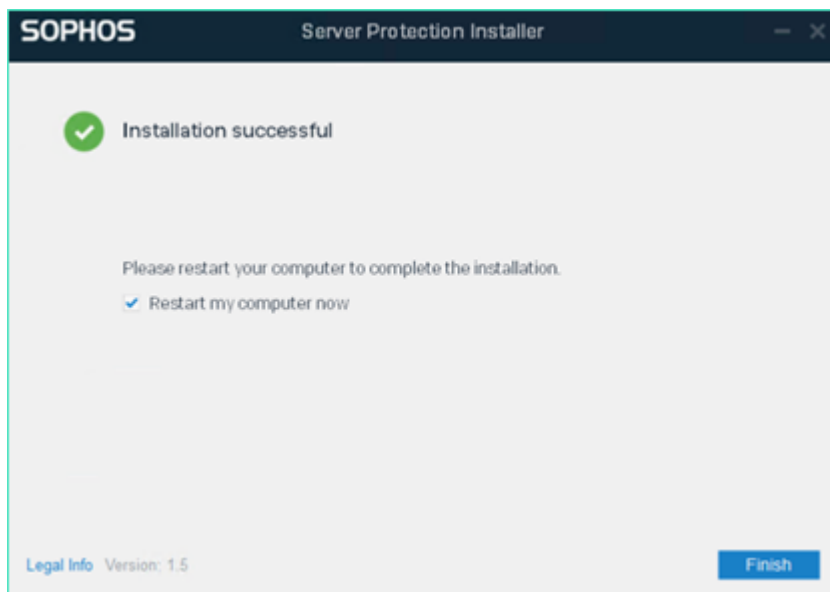
7. To start the installer, open the folder, and then double-click **SophosSetup.exe**.

Note: To avoid unexpected behavior while installing the Sophos Intercept-X, disable the Windows Defender and/or other antivirus software from the server. Sophos will remove some non-Sophos security products from the Windows servers. For more information, see [Sophos CRT: List of third-party security software removed by Sophos](#).

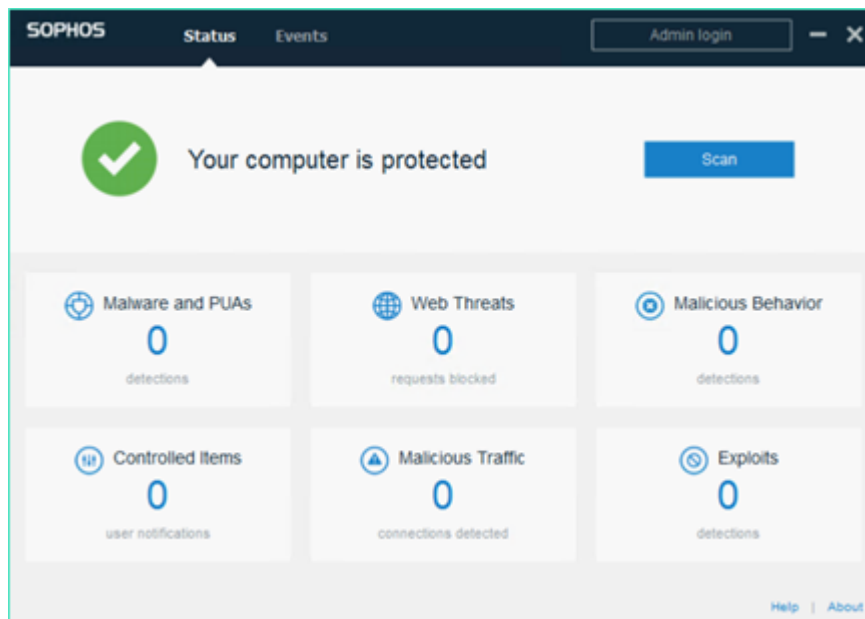
8. Click **Install**.



9. To restart your system immediately, click **Finish**. To restart later, uncheck the **Restart my computer now** option.



10. To view the protection status, open the **Sophos Intercept X** interface.



The status indicates that Arcserve UDP 9.x is secured from ransomware attacks, malware, web threats, and zero-day exploits.

11. To access Sophos Central, click **Admin Login**. It allows you to manage Sophos Intercept X Advanced Server, set alerts and policies, and so on.

Notes:

- It is mandatory to have Internet access in Arcserve UDP to install *Sophos Intercept X Advanced* and any related updates. Sophos Intercept X Advanced is cloud based and there are no offline installers available.
- If you have already purchased another UDP previously and have a Sophos account through Arcserve, use the same account for all your Arcserve UDP 9.x.
- If you already have a Sophos account through any other purchase, such as directly from Sophos, provide a different email address for a separate account on Sophos Central.
- If the Sophos installation fails for any reason, follow the on-screen or email instructions that are provided along with the error message.
- To receive the Sophos Intercept X Advanced for Server updates such as malware definition updates and version upgrades, you must have a valid and active maintenance or subscription for your Arcserve UDP.

For further assistance, please contact Arcserve Technical Support on phone (+1.844.765.7043) or [online](#), or contact your local Arcserve support office.

Chapter 12: Activating Sophos on the Arcserve Appliance for X Series

This section provides information about how to activate Sophos on the Arcserve Appliance manually.

Manually Installing Sophos Intercept X Advanced for Server on Arcserve UDP

The installation of Sophos Intercept X Advanced for Server on Arcserve UDP enables the following:

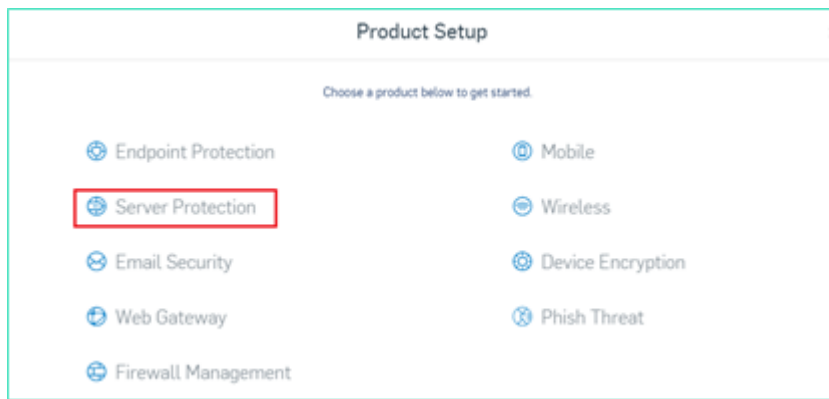
- Protect data and system backups from ransomware and other attacks
- Endpoint protection that combines signature-based and signatureless malware detection.
- Deep learning neural network
- Anti-exploit technology
- CyptoGuard anti-ransomware and WipeGuard technologies, and more to stop the widest range of endpoint threats

Follow these steps:

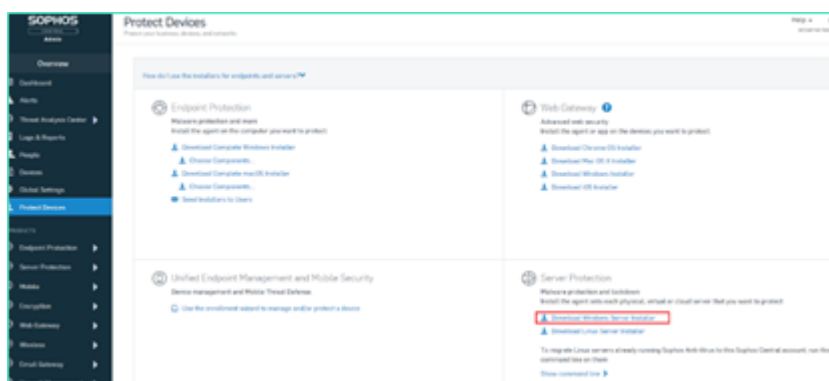
1. On the Arcserve Support Website, create an account.
2. To request for a free copy of Sophos Intercept X Advanced, provide all relevant details in the [Sophos Request form](#) and submit it to Arcserve Support. It is mandatory to share the details of Email ID and Order ID. You will receive an auto-generated email confirmation.

After you confirm your email ID, Arcserve processes your request and creates an account on the Sophos Central and sends an email with instructions on how to create a password.

3. To create a password for your new account on Sophos Central, follow the instructions in the email.
4. Log into Sophos Central.
5. Open the Product Setup dialog, then select **Server Protection**.



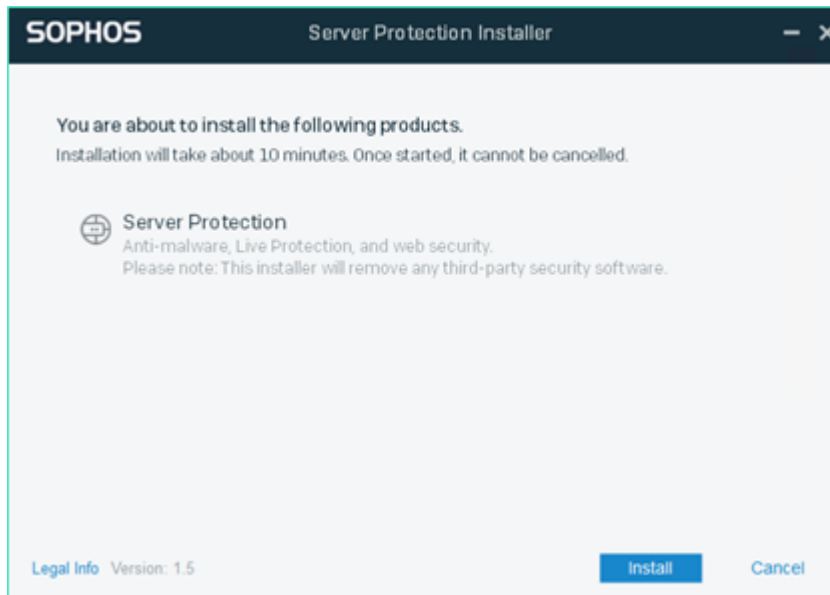
- From the Server Protection section, click **Download Windows Server Installer**, and then save **SophosSetup.exe** installer to a folder on UDP.



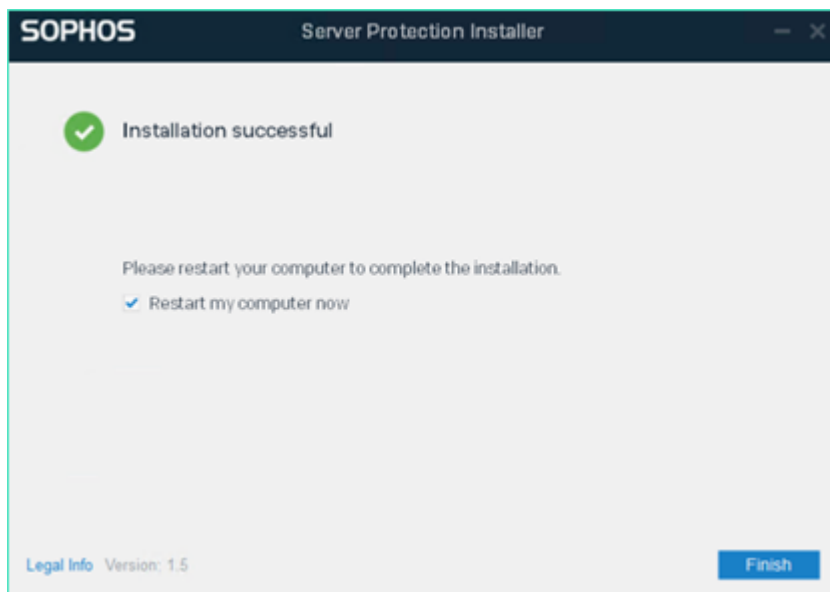
- To start the installer, open the folder, and then double-click **SophosSetup.exe**.

Note: To avoid unexpected behavior while installing the Sophos Intercept-X, disable the Windows Defender and/or other antivirus software from the server. Sophos will remove some non-Sophos security products from the Windows servers. For more information, see [Sophos CRT: List of third-party security software removed by Sophos](#).

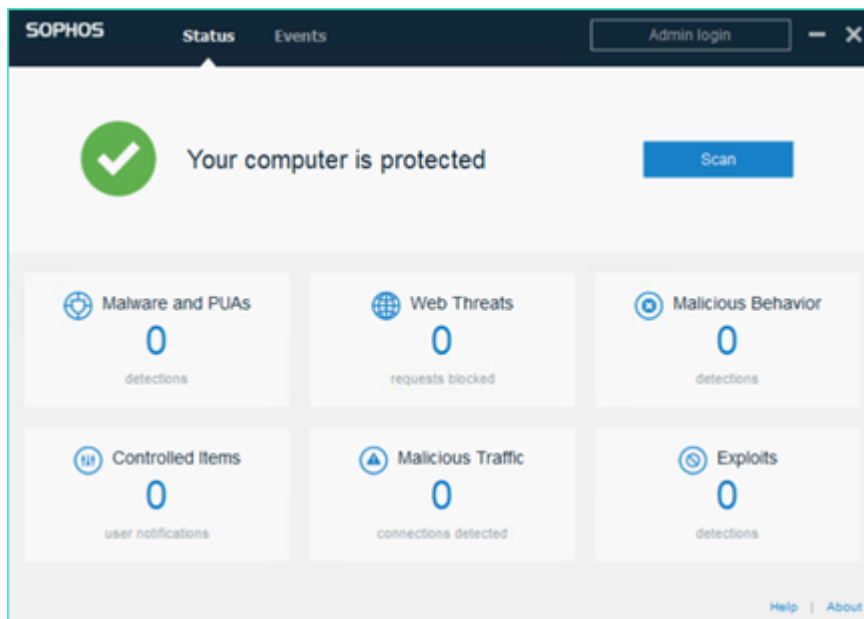
- Click **Install**.



9. To restart your system immediately, click **Finish**. To restart later, uncheck the **Restart my computer now** option.



10. To view the protection status, open the **Sophos Intercept X** interface.



The status indicates that Arcserve UDP 8.0 is secured from ransomware attacks, malware, web threats, and zero-day exploits.

11. To access Sophos Central, click **Admin Login**. It allows you to manage Sophos Intercept X Advanced Server, set alerts and policies, and so on.

Notes:

- It is mandatory to have Internet access in Arcserve UDP to install *Sophos Intercept X Advanced* and any related updates. Sophos Intercept X Advanced is cloud based and there are no offline installers available.
- If you have already purchased another UDP previously and have a Sophos account through Arcserve, use the same account for all your Arcserve UDP 8.0.
- If you already have a Sophos account through any other purchase, such as directly from Sophos, provide a different email address for a separate account on Sophos Central.
- If the Sophos installation fails for any reason, follow the on-screen or email instructions that are provided along with the error message.
- To receive the Sophos Intercept X Advanced for Server updates such as malware definition updates and version upgrades, you must have a valid and active maintenance or subscription for your Arcserve UDP.

For further assistance, please contact Arcserve Technical Support on phone (+1.844.765.7043) or [online](#), or contact your local Arcserve support office.

Chapter 12: Upgrading Firmware for Arcserve Appliance 9000 Series

This section contains the following topics:

Upgrade BIOS Firmware for Arcserve Appliance 9000 Series	216
Upgrade iDRAC Firmware for Arcserve Appliance 9000 Series	220

Upgrade BIOS Firmware for Arcserve Appliance 9000 Series

This section describes how to do the following:

Viewing BIOS Firmware Version

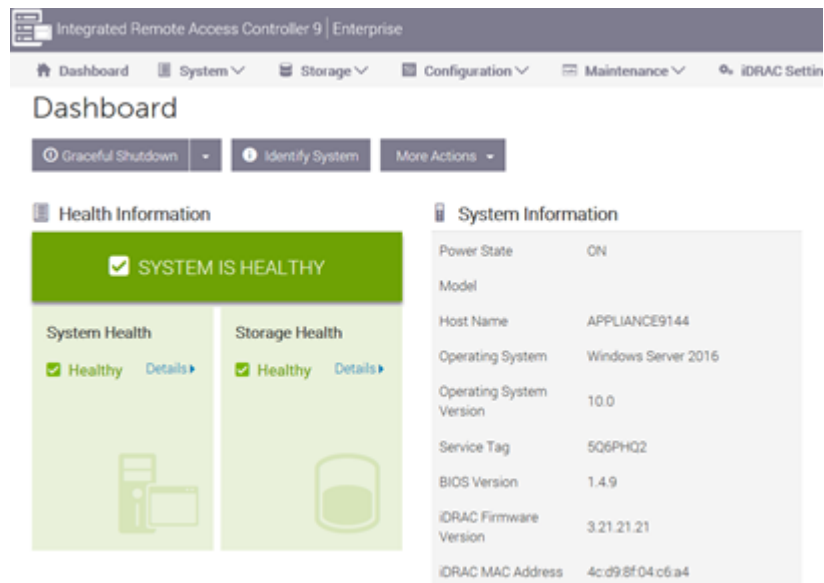
Use one of the following methods to view the BIOS firmware version:

- [Method 1: View BIOS Firmware Version from iDRAC Web Interface](#)
- [Method 2: View BIOS Firmware Version from BIOS Arcserve Appliance 9000 Series](#)

Method 1: View BIOS firmware version from iDRAC Web Interface

Follow these steps:

1. Navigate to the iDRAC web interface.
2. To log in, enter the following:
 - **Username:** root
 - **Password:** ARCADMIN

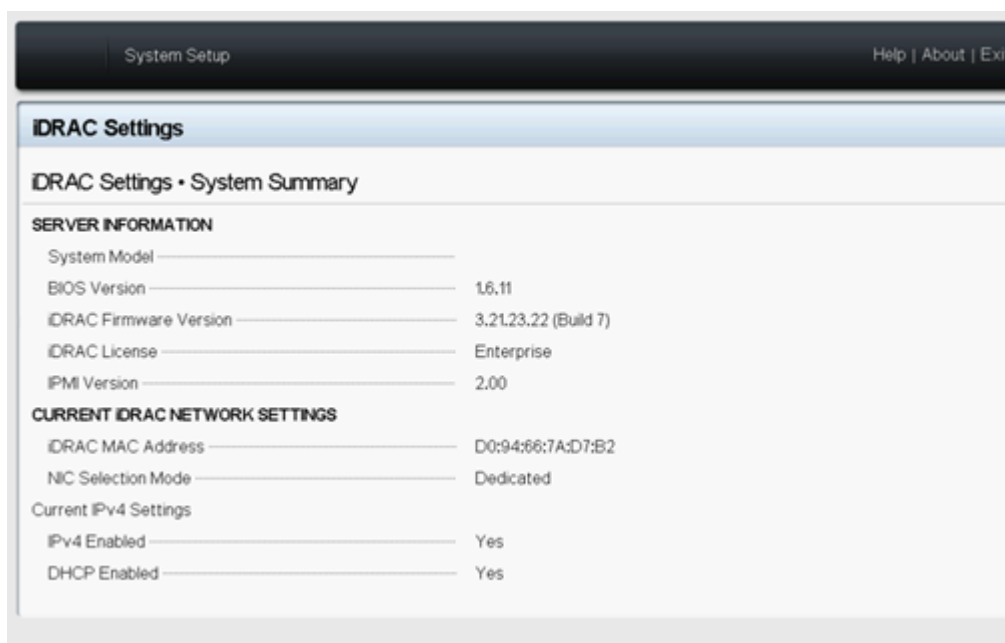


The iDRAC Dashboard page displays the System information, which contains the BIOS firmware version.

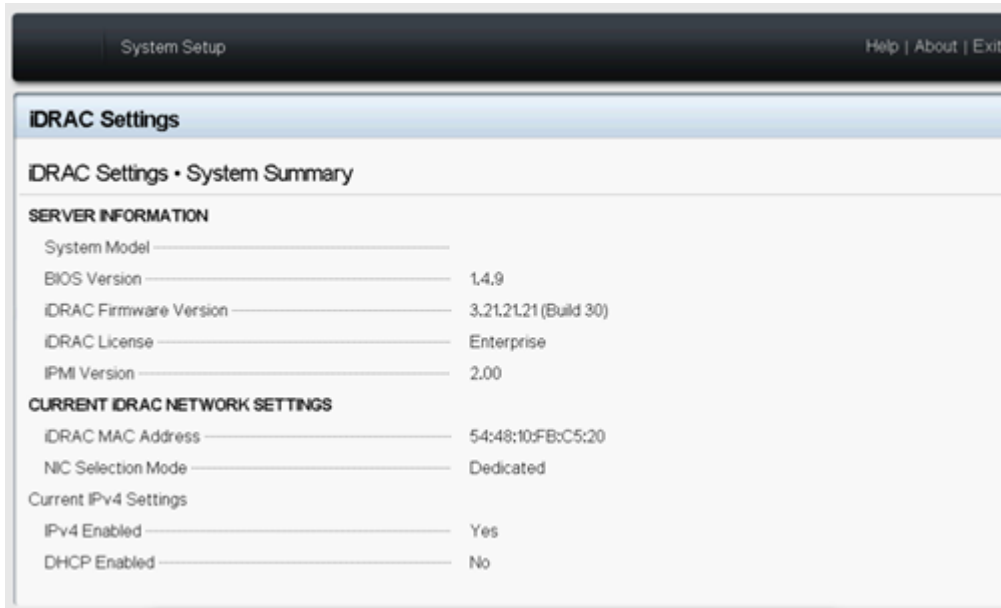
Method 2: View BIOS firmware version from BIOS Arcserve Appliance 9000 series

Follow these steps:

1. When the system starts, press **F11** to enter Setup.
2. To view the BIOS Version, navigate to **System Setup > iDRAC Settings** or **System BIOS**.



The page displays the firmware version.



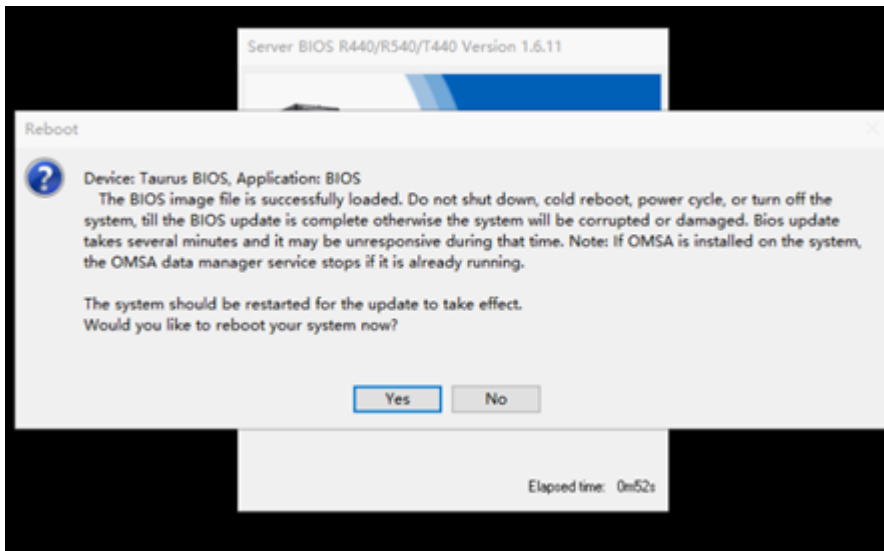
Download the Updated Package for BIOS

You can download the latest BIOS firmware package of specific Arcserve Appliance 9000 Series model from the [Dell](#) website or contact Arcserve support.

Upgrade BIOS

Follow these steps:

1. Copy the upgrade package to local disk of Arcserve Appliance 9000 Series.
2. Start the upgrade package, and then follow the prompts to complete the upgrade.
3. To complete the update, restart the system.



Note: Make sure all applications are closed before starting the upgrade process.



Verify Updated BIOS

Use one of the following methods:

- [Verify the updated BIOS using System Logs](#)
- [Verify the updated BIOS from iDRAC Web Interface or BIOS](#)

Verify Updated BIOS using System Logs

Follow these steps:

1. Log into iDRAC, and then navigate to **Maintenance >SupportAssist > Start a Collection**.
2. Review the log and verify that there are no errors during the updated process.

5CTNHQ2 2019-09-03 21:12:55 > Hardware > Logs > Lifecycle Log			
2019-08-29 15:40:34	USR0032	The session for root from 10.57.12.37 using GUI is logged off.	
2019-08-29 15:10:35	SRV068	The SupportAssist Save to Local operation is successfully completed.	
2019-08-29 15:10:34	SRV002	The SupportAssist Save to Local operation is started.	
2019-08-29 15:10:20	SRV108	The SupportAssist job JID_670625874264 is completed.	
2019-08-29 15:10:20	SRV068	The SupportAssist Collection operation is successfully completed.	
2019-08-29 15:10:20	SRV096	The SupportAssist Collection TSR20190829021014_5CTNHQ2.zip is successfully created.	
2019-08-29 15:10:13	SRV007	The SupportAssist System Information collection operation is successfully completed.	
2019-08-29 15:10:13	LOG009	The current Lifecycle Log is successfully created for the view or export operation.	
2019-08-29 15:10:07	LOG008	The complete Lifecycle Log was successfully created for an export operation.	
2019-08-29 15:09:47	SRV006	The SupportAssist System information collection operation is started.	
2019-08-29 15:09:47	SRV001	The SupportAssist Collection operation is started by iDRAC_GUI.	
2019-08-29 15:09:47	SRV106	The Debug Logs are excluded from the SupportAssist collection because the Collection data is being filtered for personally identifiable information.	
2019-08-29 15:09:47	SRV107	The Storage Logs are excluded from the SupportAssist collection because the Collection data is being filtered for personally identifiable information.	
2019-08-29 15:09:47	SRV067	The SupportAssist Collection Job JID_670625874264 is successfully created.	
2019-08-29 15:09:25	RAC1195	User root via IP 10.57.12.37 requested state / configuration change to SupportAssist using GUI.	
2019-08-29 15:08:53	SEL9901	OEM software event.	
2019-08-29 15:08:53	OSE1002	C: boot completed.	
2019-08-29 15:08:46	PR36	Version change detected for BIOS firmware. Previous version:1.6.11, Current version:2.2.11	

Verify Updated BIOS from iDRAC Web Interface or BIOS

Log into the iDRAC web interface or enter system BIOS to see the updated BIOS firmware version.

Upgrade iDRAC Firmware for Arcserve Appliance 9000 Series

This section describes how to do the following:

Viewing iDRAC Firmware Version

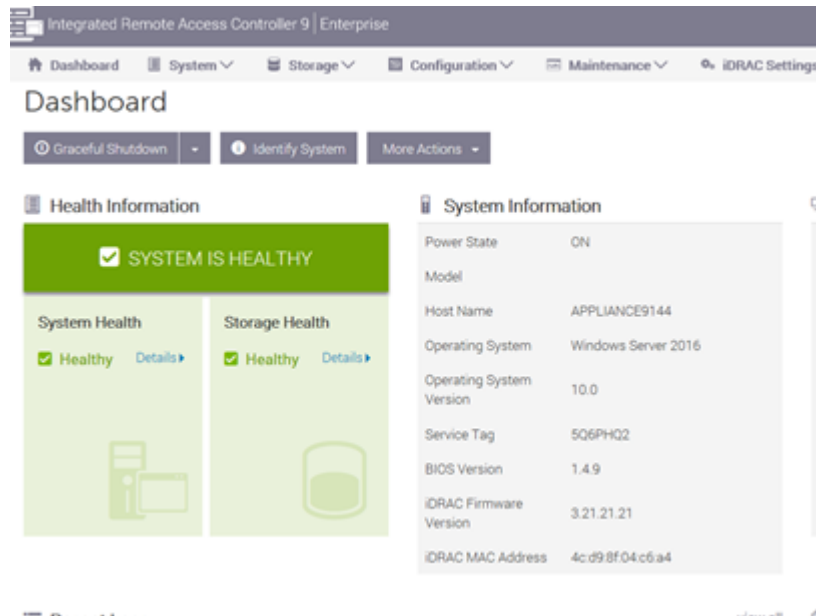
Use one of the following methods to view the iDRAC firmware version:

- [Method 1: View iDRAC Firmware Version from iDRAC Web Interface](#)
- [Method 2: View iDRAC Firmware Version from BIOS Arcserve Appliance 9000 Series](#)

View iDRAC Firmware Version from iDRAC Web Interface

To view the iDRAC firmware version from the iDRAC web interface, log into the iDRAC web interface.

Note: We strongly recommend you change the default password immediately. To change the default password, see [How to Change the iDRAC Password](#).

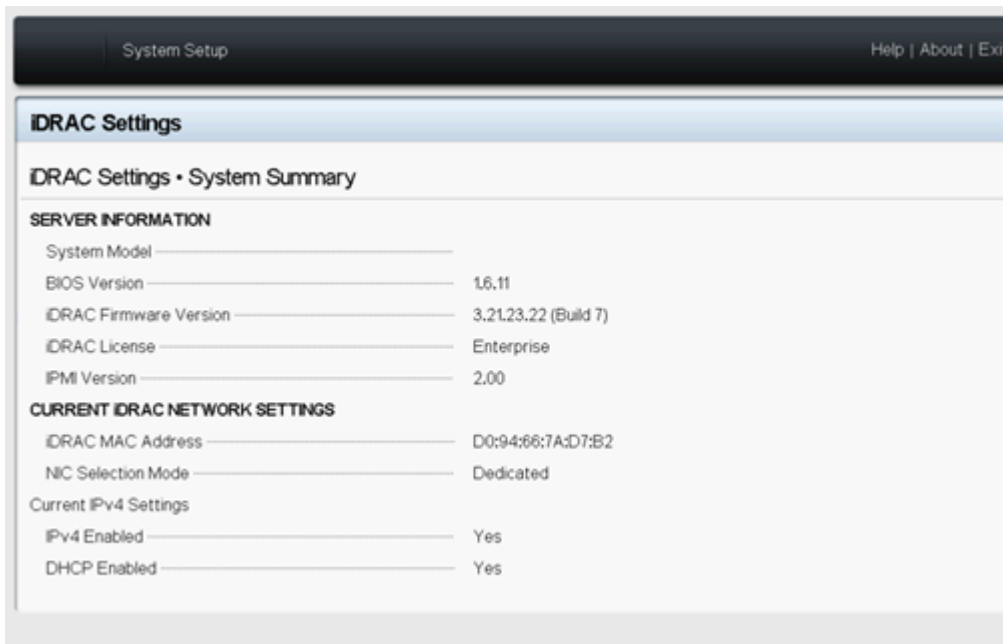


The iDRAC dashboard displays the system information, which contains iDRAC firmware version.

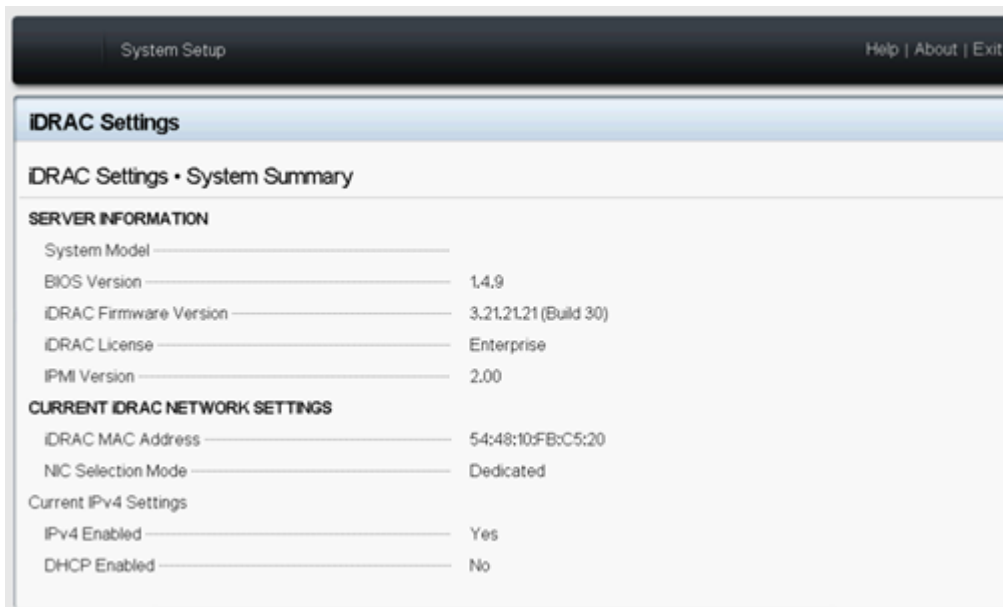
Method 2: View iDRAC Firmware Version from BIOS Arcserve Appliance 9000 series

Follow these steps:

1. When the system starts, press **F11** to enter Setup.
2. To view the iDRAC Version, navigate to **System Setup > iDRAC Settings** or **System BIOS**.



The page displays the firmware version.

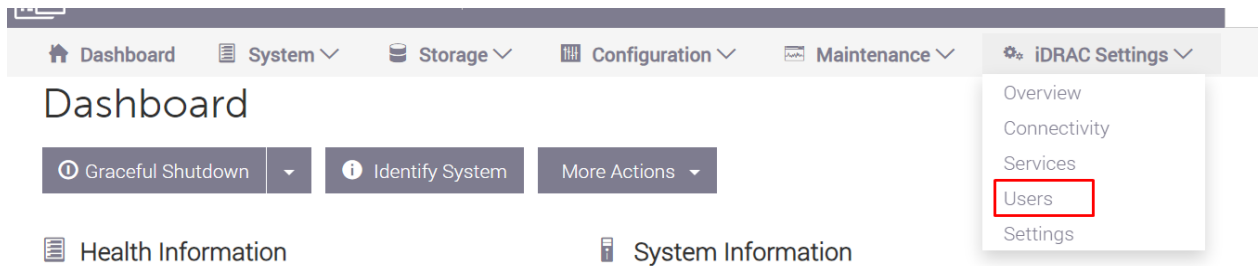


How to Change the iDRAC Password

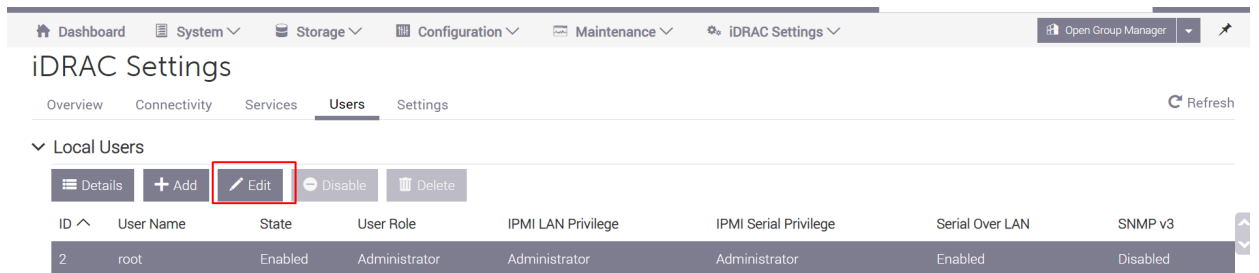
This section provides information about how to change the iDRAC password.

Follow these steps:

1. Log into iDRAC with the current password.
2. Go to **iDRAC Settings**, and then select **Users**.



3. On the iDRAC Settings page, click the **Local Users** drop-down, and then click the **Edit** button.



The Edit User dialog appears.

4. Under the User Configuration tab, type the new password, retype the new password to confirm, and then click **Save**.

Note: We recommend that you keep the User Role as Administrator.

The screenshot shows the 'Edit User' dialog box. The 'User Configuration' tab is active. The 'User Account Settings' section contains the following fields:

- ID: 2
- User Name*: admin
- Password*: [masked]
- Confirm Password*: [masked]

The 'User Privileges' section shows the 'User Role' set to 'Administrator'. Below this, there are three columns of checkboxes, all of which are checked:

- Login to iDRAC
- Clear Logs
- Access Virtual Media
- Configure iDRAC
- Control and Configure System
- Test Alerts
- Configure Users
- Access Virtual Console
- Execute Debug Commands

The iDRAC password is changed successfully.

Download the Updated Package for iDRAC

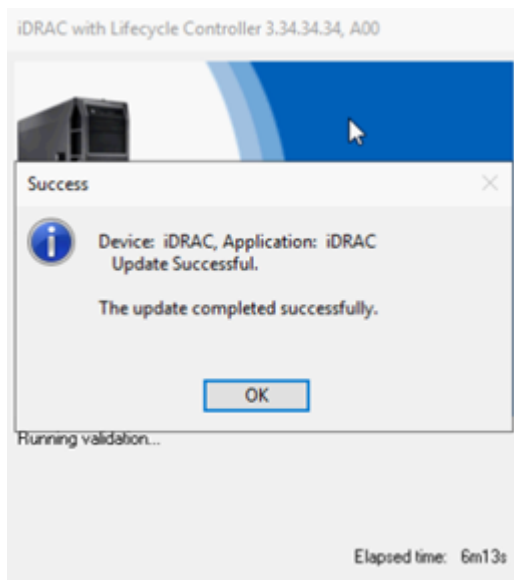
You can download the latest iDRAC firmware package of specific Arcserve Appliance 9000 Series model from the [Dell](#) website or contact Arcserve support.

Upgrade iDRAC

Follow these steps:

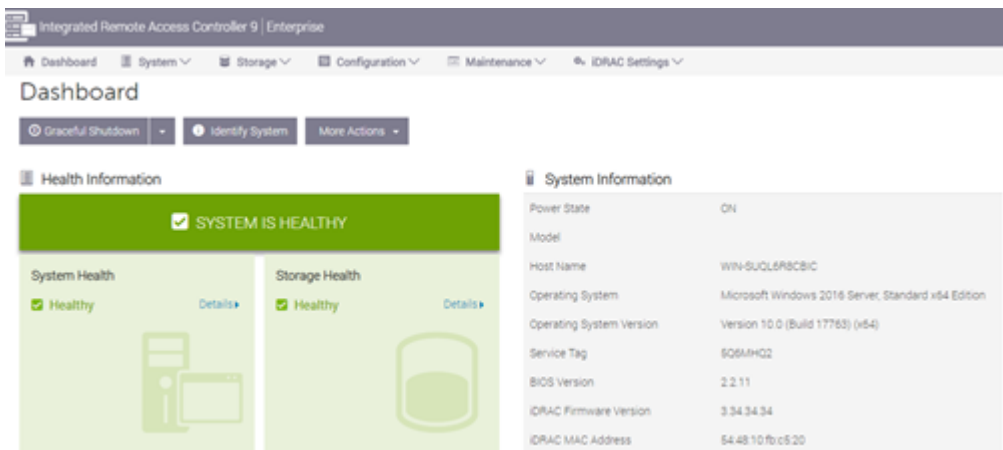
1. Copy the upgrade package to local disk of Arcserve Appliance 9000 Series.
2. Start the upgrade package, and then follow the prompts to complete the upgrade.

Note: Make sure all applications are closed before starting the upgrade process.



3. During the upgrade process, iDRAC and virtual console gets disconnected for a few minutes. Log into iDRAC and restart the virtual console. The

upgrade completes now.



Verify Updated iDRAC

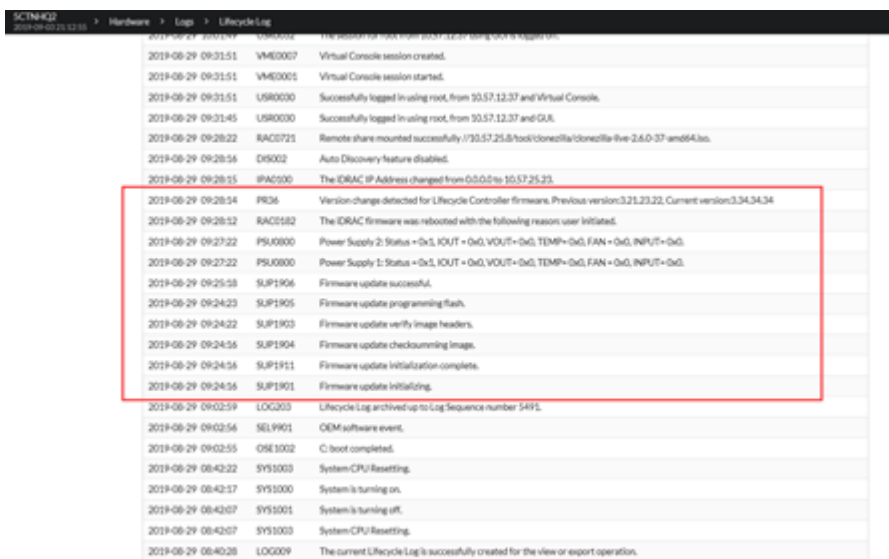
Use one of the following methods:

- [Verify the updated iDRAC using System Logs](#)
- [Verify the updated iDRAC from iDRAC Web Interface or BIOS](#)

Verify Updated iDRAC using System Logs

Follow these steps:

1. Log into iDRAC, and then navigate to **Maintenance > SupportAssist > Start a Collection**.
2. Review the log and verify that there are no errors during the updated process.



Verify Updated iDRAC from iDRAC Web Interface or BIOS

Log into the iDRAC web interface or enter system BIOS to see the updated BIOS firmware version.

Upgrade Firmware for Arcserve Appliance X Series

This section describes how to do the following:

Upgrade BIOS Firmware for Arcserve Appliance X Series

This section describes how to do the following:

Viewing BIOS Firmware Version

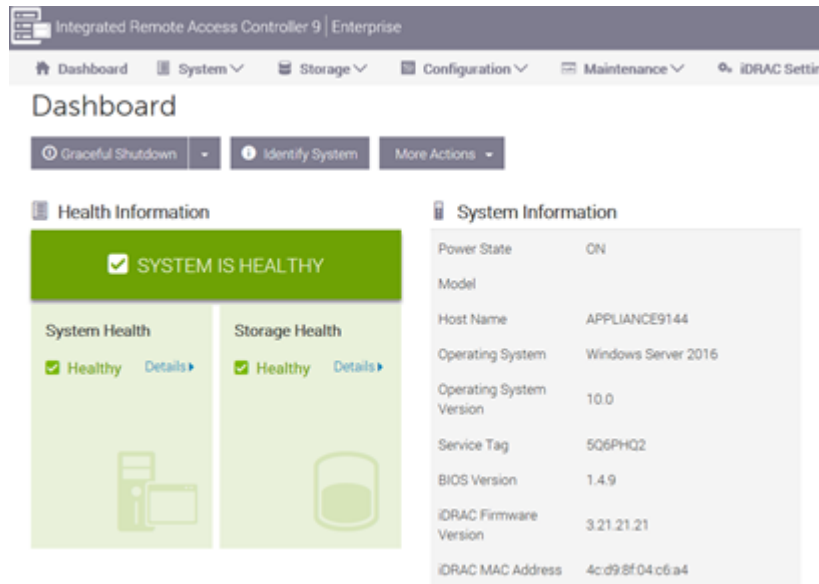
Use one of the following methods to view the BIOS firmware version:

- [Method 1: View BIOS firmware version from iDRAC Web Interface](#)
- [Method 2: View BIOS firmware version from BIOS Arcserve Appliance X Series](#)

Method 1: View BIOS firmware version from iDRAC Web Interface

Follow these steps:

1. Navigate to the iDRAC web interface.
2. To log in, enter the following:
 - **Username:** root
 - **Password:** ARCADMIN

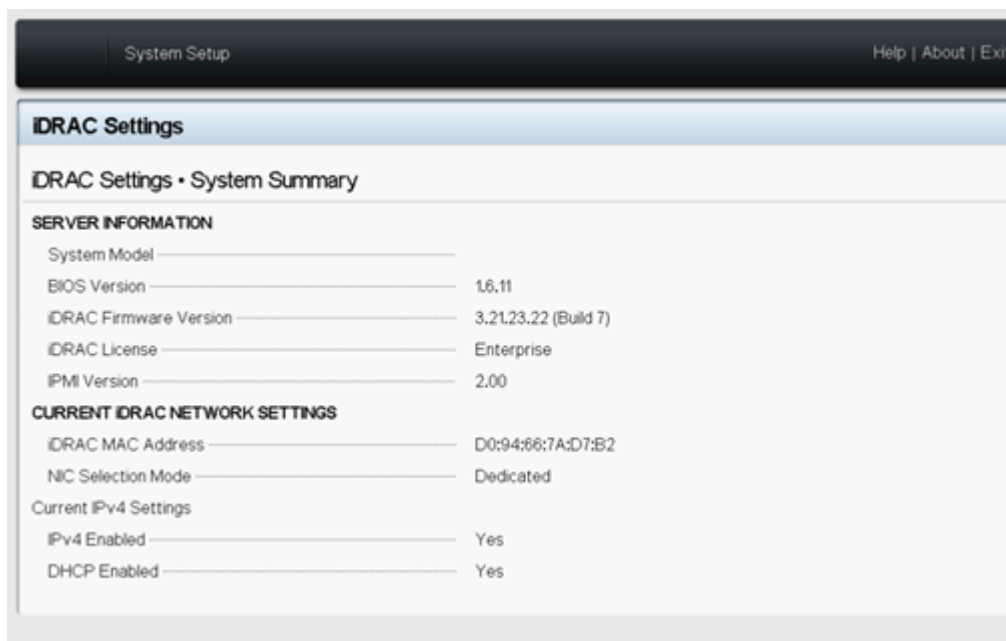


The iDRAC Dashboard page displays the System information, which contains the BIOS firmware version.

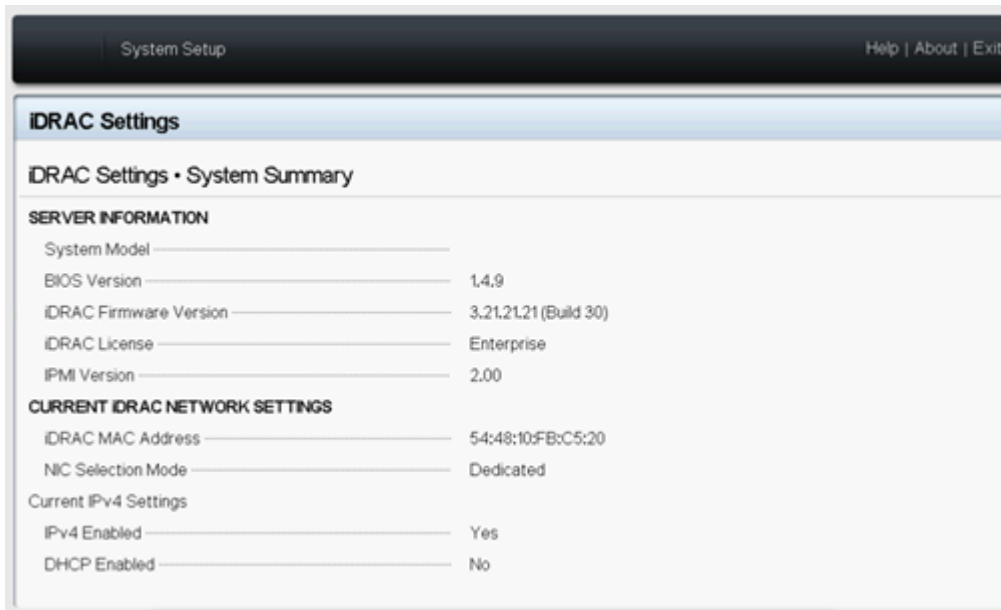
Method 2: View BIOS firmware version from BIOS Arcserve Appliance X series

Follow these steps:

1. When the system starts, press **F11** to enter Setup.
2. To view the BIOS Version, navigate to **System Setup > iDRAC Settings** or **System BIOS**.



The page displays the firmware version.



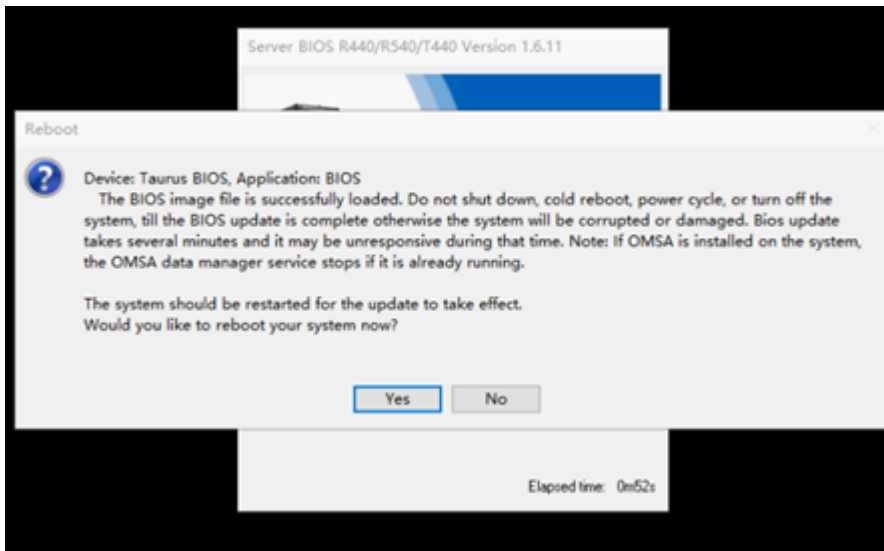
Download the Updated Package for BIOS

You can download the latest BIOS firmware package of specific Arcserve Appliance X Series model from the [Dell](#) website or contact Arcserve support.

Upgrade BIOS

Follow these steps:

1. Copy the upgrade package to local disk of Arcserve Appliance X Series.
2. Start the upgrade package, and then follow the prompts to complete the upgrade.
3. To complete the update, restart the system.



Note: Make sure all applications are closed before starting the upgrade process.



Verify Updated BIOS

Use one of the following methods:

- [Verify the updated BIOS using System Logs](#)
- [Verify the updated BIOS from iDRAC Web Interface or BIOS](#)

Upgrade iDRAC Firmware for Arcserve Appliance X Series

This section describes how to do the following:

Viewing iDRAC Firmware Version

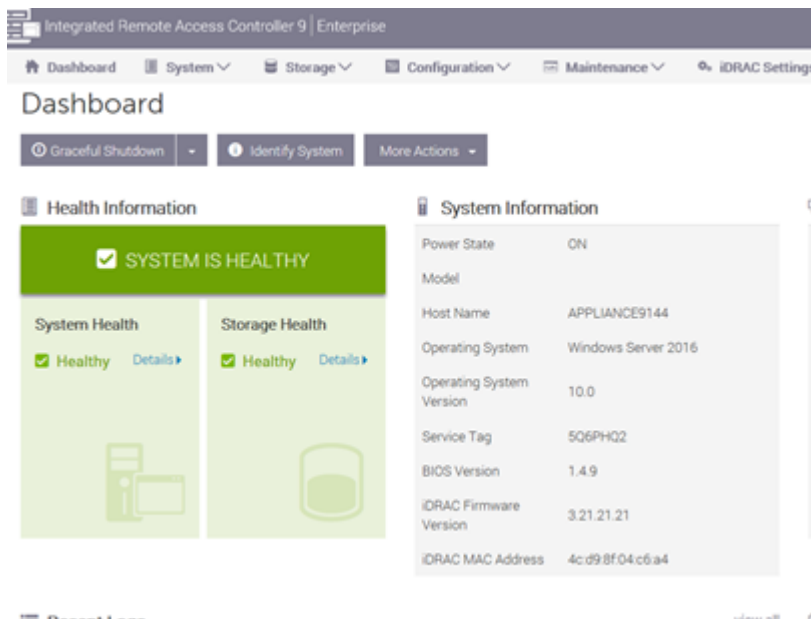
Use one of the following methods to view the iDRAC firmware version:

- [Method 1: View iDRAC firmware version from iDRAC Web Interface](#)
- [Method 2: View iDRAC firmware version from BIOS Arcserve Appliance X Series](#)

Method 1: View iDRAC firmware version from iDRAC Web Interface

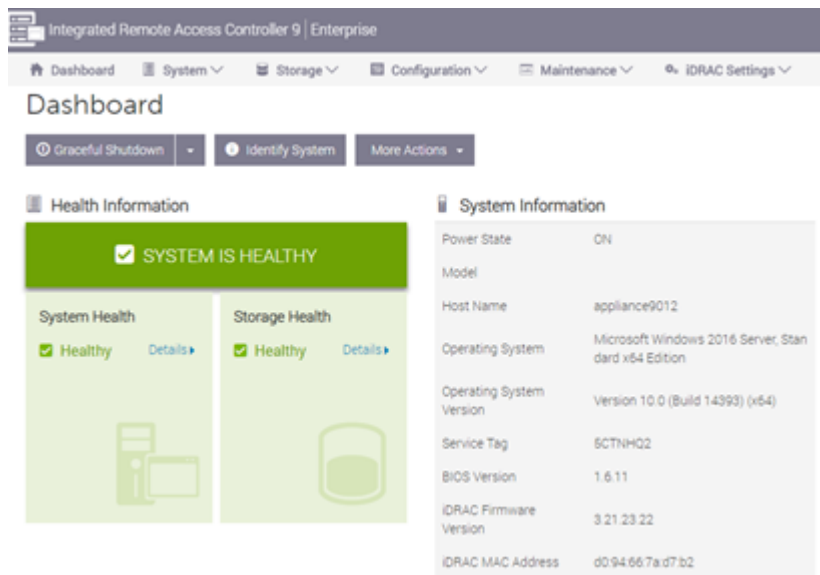
Follow these steps:

1. Navigate to the iDRAC web interface.
2. To log in, enter the following:
 - **Username:** root
 - **Password:** ARCADMIN



The iDRAC dashboard displays the system information, which contains iDRAC

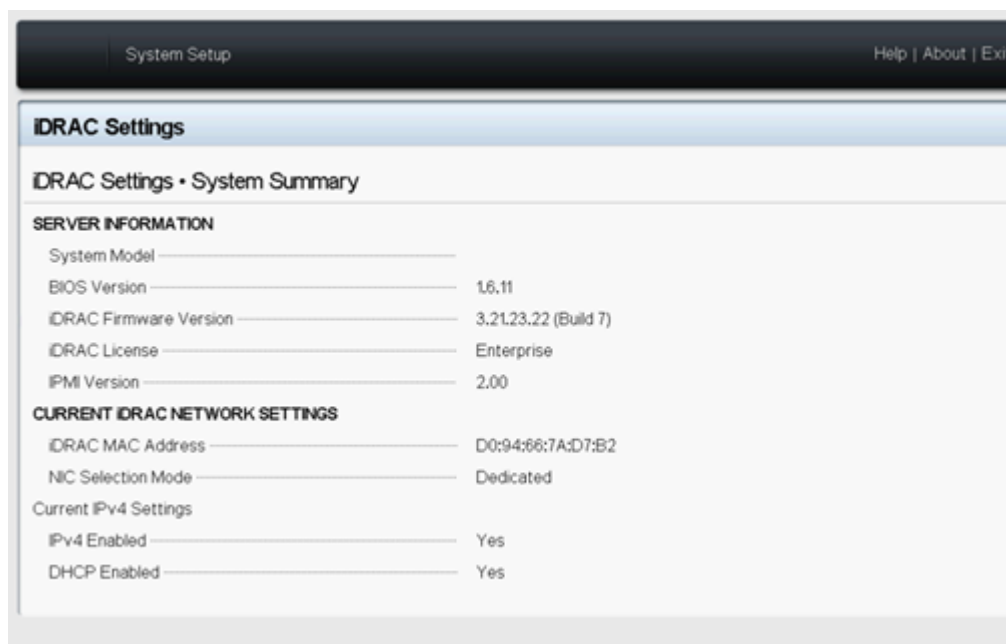
firmware version.



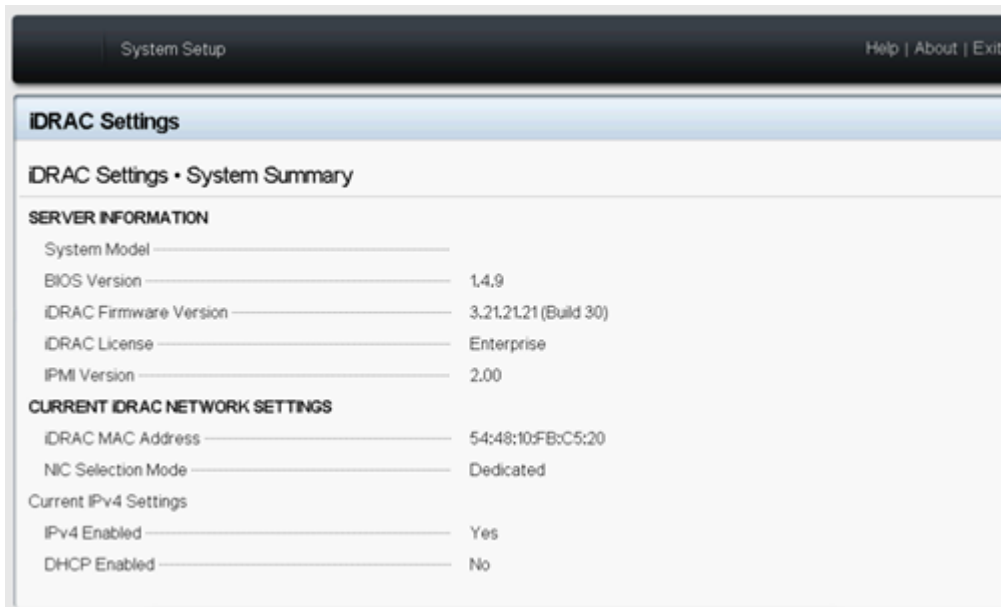
Method 2: View iDRAC firmware version from BIOS Arcserve Appliance X series

Follow these steps:

1. When the system starts, press **F11** to enter Setup.
2. To view the iDRAC Version, navigate to **System Setup > iDRAC Settings** or **System BIOS**.



The page displays the firmware version.



Download the Updated Package for iDRAC

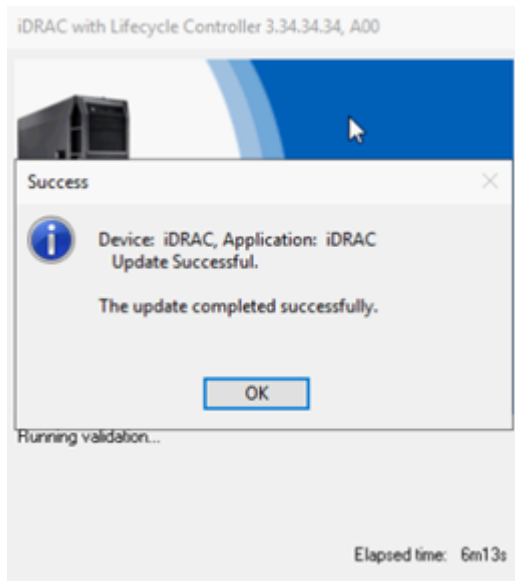
You can download the latest iDRAC firmware package of specific Arcserve Appliance X Series model from the [Dell](#) website or contact Arcserve support.

Upgrade iDRAC

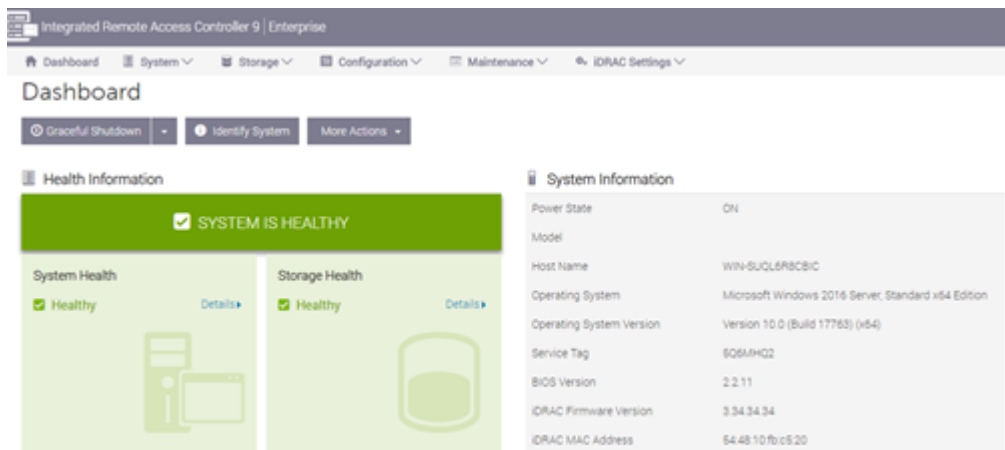
Follow these steps:

1. Copy the upgrade package to local disk of Arcserve Appliance X Series.
2. Start the upgrade package, and then follow the prompts to complete the upgrade.

Note: Make sure all applications are closed before starting the upgrade process.



3. During the upgrade process, iDRAC and virtual console gets disconnected for a few minutes. Log into iDRAC and restart the virtual console. The upgrade completes now.



Verify Updated iDRAC

Use one of the following methods:

- [Verify the updated iDRAC using System Logs](#)
- [Verify the updated iDRAC from iDRAC Web Interface or BIOS](#)

Chapter 13: Troubleshooting

This section contains the following topics:

Linux Backup Server Fails to Connect from the Console	237
Backing Up Arcserve Appliance from Another Appliance Reports Duplicated Nodes	238
Linux Backup Server Cannot Communicate with Any Node in the Network	239
Linux Backup Server Cannot Get the Network DNS Suffix	241
Default Time Zone on the Appliance	242
Licenses Error even when the licenses are available	243

Linux Backup Server Fails to Connect from the Console

Symptom

When I try to connect my Linux Backup Server from the Arcserve UDP Console, connection is unsuccessful and I see a red mark.

Solution

When a Linux Backup Server fails to connect from the console, you can troubleshoot the connection to determine the problem.

To troubleshoot the connectivity issue

1. Launch the Hyper-V Manager, connect the Linux Backup Server virtual machine and login.
2. Run the following command:

```
service network restart
```
3. Verify that the IP address assigned to the Linux Backup Server is 192.168.10.2. To verify, run the following command:

```
ifconfig
```
4. If the IP address is 192.168.10.2, navigate to the Arcserve UDP Console and update the Linux Backup Server node that you are trying to connect.
5. If the IP address is not 192.168.10.2, follow the instructions in the Troubleshoot from DHCP Microsoft Management Console (MMC) section.

Troubleshoot from DHCP Microsoft Management Console (MMC)

Important! Ensure that the DHCP Server service is running appropriately on the appliance.

1. Launch DHCP MMC from the Server Manager, Tools, DHCP.
2. Expand the Linux Server node, IPV4, Scope and ensure that the scope with the name 192.168.10.0 exists under it.
3. Expand the Address Leases and delete the presence of any other lease record.
4. Log into the Linux Backup Server and run the following command:

```
service network restart
```
5. Navigate to the Arcserve UDP Console and update the Linux Backup Server node that you are trying to connect.

The Linux Backup Server now connects from the Console.

Backing Up Arcserve Appliance from Another Appliance Reports Duplicated Nodes

Symptom

When I back up Appliance B from Appliance A, I see the following warning message in the activity log:

"The following nodes are duplicated: Appliance_B, Appliance_A. As a result, they have the same agent identifier and may cause unexpected results. This duplicate node problem can be caused if the node was added using a different node name (such as the DNS name or IP address), or if some machines were set up by cloning from one to another."

Case 1: Appliance B is added as an RPS to the Appliance A UDP Console.

For example: From Appliance B, you can configure the appliance using the UDP wizard and select "This appliance will function as an instance of Arcserve UDP Recovery Point Server managed by another Arcserve UDP console."

Solution

1. Stop the datastore in the Appliance B node from the RPS pane of the UDP console.
2. Log into Appliance B and delete the registry key of the Node ID that is located under [HKEY_LOCAL_MACHINE\SOFTWARE\CA\ARCserve Unified Data Protection\Engine].
3. Restart the Arcserve UDP Agent Web Service from the Appliance B node.
4. Restart the Arcserve UDP RPS datastore Service from the Appliance B node.
5. From the UDP console, go to the Nodes, All Nodes pane and update the Appliance B node.
6. Go to the Recovery Point Server pane and update the Appliance B node.
7. Import the existing datastore to the Appliance B RPS by setting it with the original backup destination.

Case 2: Appliance B is added only as an agent node to the Appliance A UDP Console.

For example, a plan protects Appliance B through an agent-based backup task on the Appliance A UDP console.

1. Log into Appliance B and delete the registry key of the Node ID that is located under [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve Unified Data

Protection\Engine].

2. Restart the Arcserve UDP Agent service from Appliance B.
3. From the UDP console, go to the Nodes, All Nodes pane and update the node from Appliance B.

Linux Backup Server Cannot Communicate with Any Node in the Network

Symptom

Linux Backup Server cannot communicate with any node in the network.

Solution

If the Appliance windows server cannot communicate with any node in the network, the Linux Backup Server cannot also communicate with any node.

Follow these steps:

1. Verify if the node is accessible from Appliance windows server.
2. Navigate to the following location to verify if network adapter LinuxBkpSvr exist as shown below:

Control Panel>Network and Internet>Network Connections

3. If LinuxBkpSvr is unavailable, navigate to the following location and verify if flag file adapterNameChanged.flag exists:

C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance

If existing, remove the adapterNameChanged.flag file.

4. Verify if all available network interfaces and LinuxBkpSvr are added to NAT as shown below.

If all network interfaces and LinuxBkpSvr are already listed, verify if different physical network interfaces are connected with different sub network. This action resolves the communication problem of Linux Backup Server.

If all the network interfaces and *LinuxBkpSvr* are listed, continue with next step.

5. Delete the file *dhcpcdone.flag* from the following location:

C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance

6. Using Command Line, enter folder *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance* and run *resetdhcp.ps1* as shown below.

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

When the script runs successfully, the communication issue for the Linux Backup Server is resolved.

Linux Backup Server Cannot Get the Network DNS Suffix

When you set the static IP address to the appliance Server, the Linux Backup Server cannot get the network DNS suffix properly after restarting the network service. This issue leads to communication problems between the Linux backup Server and the UDP console. You then cannot use this Linux backup Server to protect the Linux node due to the communication problems.

Symptom

The status of the Linux Backup Server remains in a disconnected state on the UDP console. The **Update Node** cannot update the Linux Backup Server successfully and the yellow warning icon will not change to green. This occurs when the static IP address is set to the appliance Server that will then cause the Linux Backup Server to not get the network DNS suffix properly.

Solution

To resolve this issue, you can update the file/etc/resolv.conf directly in the Linux machine to add the correct DNS suffix.

Default Time Zone on the Appliance

Symptom

The default time zone is *(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi* no matter what region you select when you first power on the appliance.

Solution

Navigate to **Arcserve Backup Appliance Wizard**, click **Edit** and set **Date and Time** to change the time zone.

Licenses Error even when the licenses are available

For more information on license related errors in the Appliance even when the licenses are available, refer the [link](#).

Chapter 14: Applying Best Practices

The section contains the following topics:

Best Practices for Network Configuration	245
Best Practices for Windows Defender with PowerShell cmdlets	248
Configure Preinstalled Linux Backup Server to External Network	248
Best Practices for replacing Factory Reset Image When Secured by Sophos	249
Best Practice for Creating Deduplication Datastore across Volumes	257

Best Practices for Network Configuration

- If multiple network interfaces are connected in the production environment, ensure that each network adapter is connected to different sub network.
- If Linux node is not available in the production environment to protect, we recommend to stop the VM Linux-BackupSvr, and DHCP Server service on the Appliance.

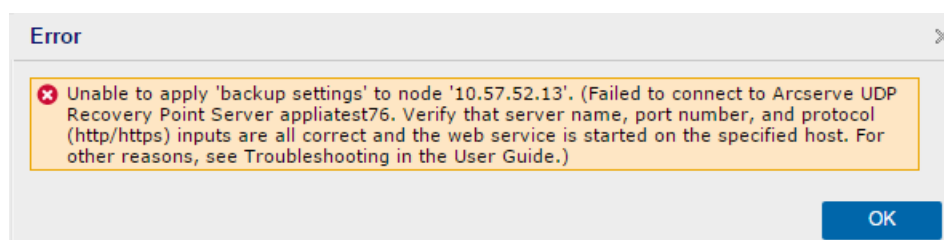
For more information, refer [How to Disable DHCP Server](#).

- When both the Appliance and the Agent node are online on the same sub network, a connection problem occurs between the Appliance and an Agent node if there are multiple network interfaces connected to the same sub network in the Appliance.

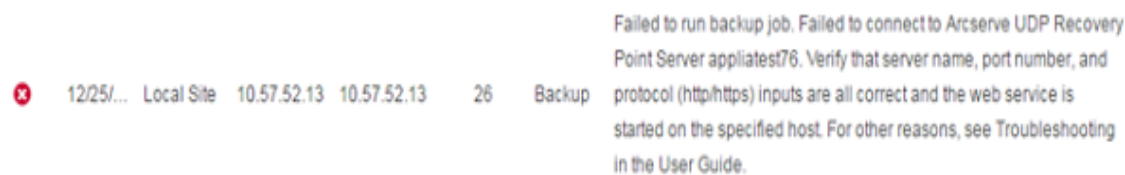
Symptom

If both the Appliance and Agent nodes are online on the same sub network, the following symptoms may occur:

- ♦ On the Arcserve UDP Console, when you deploy the plan to Agent node, the following error message is displayed:



- ♦ Backup job of the Agent node fails as below:



- ♦ Ping the Agent node from the Appliance and verify whether the Agent node is connected or not as follows:

```
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
```

- ♦ Ping Appliance host name from the Agent node and the Appliance is NOT connected as follows:

```
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),
```

Solution

To resolve the connection problem between the Appliance and Agent node, perform one of the following steps:

- ♦ If Linux node is not available in the production environment, stop the DHCP Server service on the Appliance and verify whether the problem is resolved or not.

For more information, refer [How to Disable DHCP Server](#).

- ♦ On the Appliance and Agent node, follow these steps:

Steps to be followed on Appliance:

1. Run *ipconfig /all* from DOS Command Prompt to get the available IPv4 address on the Appliance:
2. Run *Route Print* from DOS Command Prompt to get the IPv4 Route Table, record the order list for all the available IPv4 address on the Appliance as below:

IPv4 Route Table					
=====					
Active Routes:					
Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	10.57.52.1	10.57.52.46	10
	0.0.0.0	0.0.0.0	10.57.52.1	10.57.52.35	10
	0.0.0.0	0.0.0.0	10.57.52.1	10.57.52.45	10
	0.0.0.0	0.0.0.0	10.57.52.1	10.57.52.47	10
10.57.52.0		255.255.255.0	On-link	10.57.52.46	266
10.57.52.0		255.255.255.0	On-link	10.57.52.35	266
10.57.52.0		255.255.255.0	On-link	10.57.52.45	266

Steps to be followed on Agent node:

1. From the DOS Command Prompt, try to ping each available IPv4 address of Appliance one by one according to the order above to get the first IPv4 of the Appliance connected on the Agent node as follows:

```
C:\Users\Administrator>ping 10.57.52.46  
Pinging 10.57.52.46 with 32 bytes of data:  
Reply from 10.57.52.46: bytes=32 time<1ms TTL=128  
Reply from 10.57.52.46: bytes=32 time<1ms TTL=128  
Reply from 10.57.52.46: bytes=32 time<1ms TTL=128  
Reply from 10.57.52.46: bytes=32 time<1ms TTL=128
```

2. Modify the file `C:\Windows\System32\drivers\etc\hosts` to add a record for the pair *the_IPv4_got_above Appliance_hostname* and save the file.

Best Practices for Windows Defender with PowerShell cmdlets

You can get the Defender cmdlets by using the following commands:

- *PS C:\> (Get-MpPreference).ExclusionPath*
Gets exclusion path of Defender.
- *PS C:\> (Get-MpPreference).ExclusionProcess*
Gets exclusion processes of Defender.
- *PS C:\> Add-MpPreference -ExclusionPath "full_path_of_the_folder_or_file"*
Excludes a folder or file to the exclusion list.
- *PS C:\> Add-MpPreference -ExclusionProcess "full_path_of_executable_programs"*
Excludes files opened by the processes.
- *PS C:\> Remove-MpPreference -ExclusionPath "full_path_of_the_folder"*
Removes a folder from the exclusion list.

Configure Preinstalled Linux Backup Server to External Network

Follow these steps:

1. Disable DHCP server. For more information, see [How to Disable DHCP Server](#).
2. To set Linux Backup Server network to external network, follow these steps:
 - a. Open the **Hyper-V** manager.
 - b. Create a new external virtual network switch.
 - c. Change the Linux Backup Server VM network adapter setting to use the newly created external virtual network switch.
 - d. Check network setting of Linux Backup Server, ensure it has got IP address and DNS through the external virtual network switch.
 - e. Remove the original Linux Backup server from UDP Console.
 - f. Add the Linux Backup Server to UDP Console again with the following information:

- **Hostname:** Linux-BackupSvr
- **Port:** 8014

Best Practices for replacing Factory Reset Image When Secured by Sophos

After Sophos has been activated and running on Arcserve Appliance, by default you cannot replace factory reset image using the Set Appliance Image Utility. Otherwise, the execution of SetImage.exe will fail as shown in the illustration below.

```
PS C:\Program Files\Arcserve\Unified Data Protection\Management\bin\Appliance> .\SetImage.exe -applianceimage X:\appliance.wim
Start to check appliance image, this may need about 30 minutes, please wait...
Mounting the old appliance image, please wait...
Unmounting the old appliance image, please wait...
Failed to unmount the appliance image, please contact Arcserve Technical Support for assistance.
```

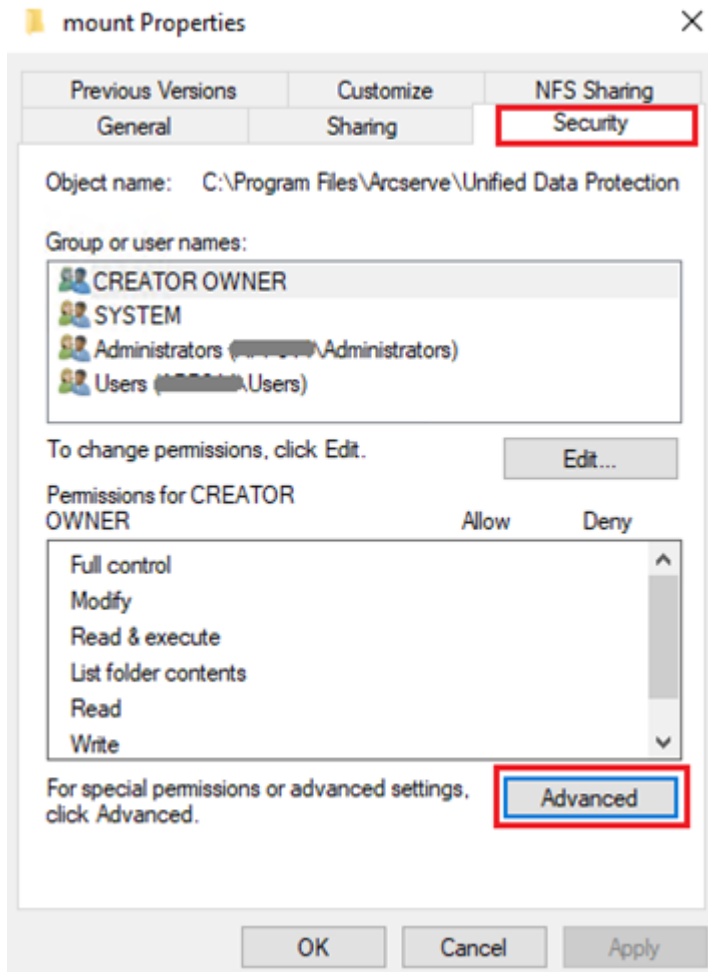
Before running the SetImage.exe command to replace factory reset image when Sophos is running on Arcserve Appliance, verify if the image has already been mounted.

As given in the illustration, the following prompt appears: *A subdirectory or file C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\mount already exists.*

```
PS C:\Program Files\Arcserve\Unified Data Protection\Management\bin\Appliance> .\SetImage.exe -applianceimage X:\appliance.wim
Start to check appliance image, this may need about 30 minutes, please wait...
Mounting the old appliance image, please wait...
A subdirectory or file C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\mount already exists.
Failed to mount the old appliance image. Please run this tool again.
If mounting fails again, please contact Arcserve Technical Support for assistance.
```

To unmount the image, follow these steps:

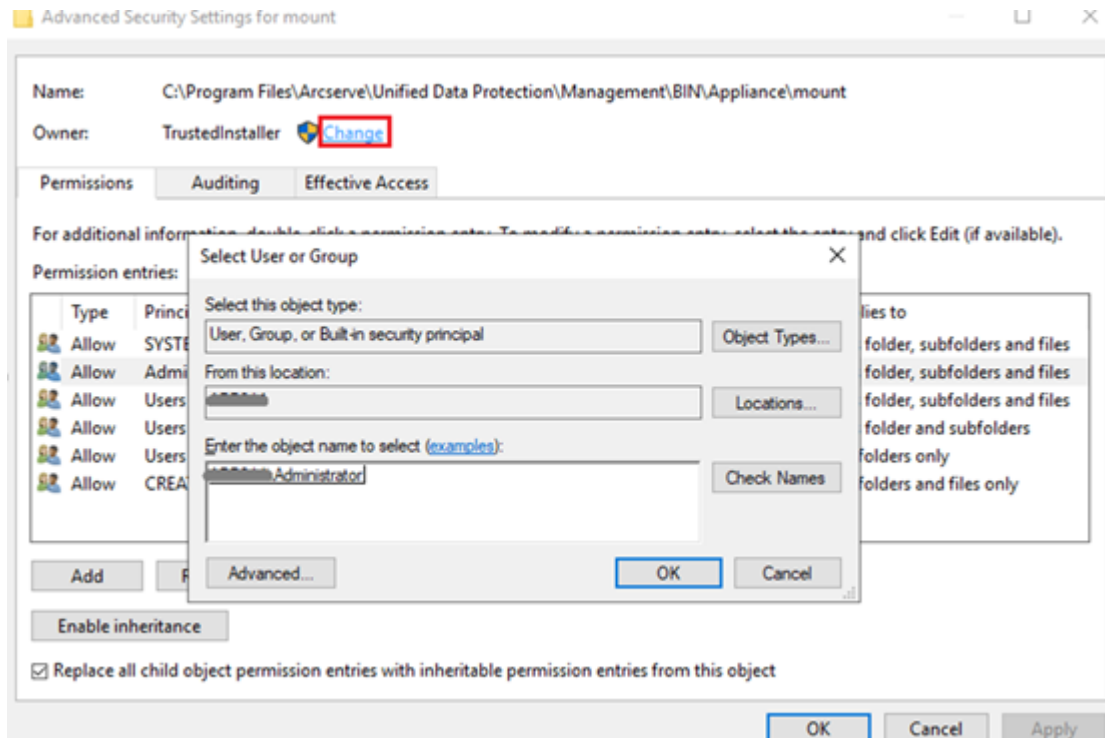
1. To locate the folder, open Windows Explorer, and go to C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\mount. Right-click the folder, and then click Properties > Security tab > Advanced.



2. To change the owner of the mount folder to a local administrator, click the **Change** link.

In the Advanced Security Settings page, to take control of the subfolders inside of the folder and replace the subfolders permissions with the settings from the parent folder, select the check boxes for the following options:

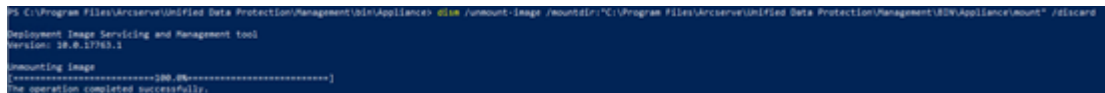
- ♦ Replace ownership on subcontainers and object
- ♦ Replace all child object permission entries with inheritable permission entries from this object



Apply all the changes. For mount folder, subfolders, and files, make sure the owner is changed to a local administrator.

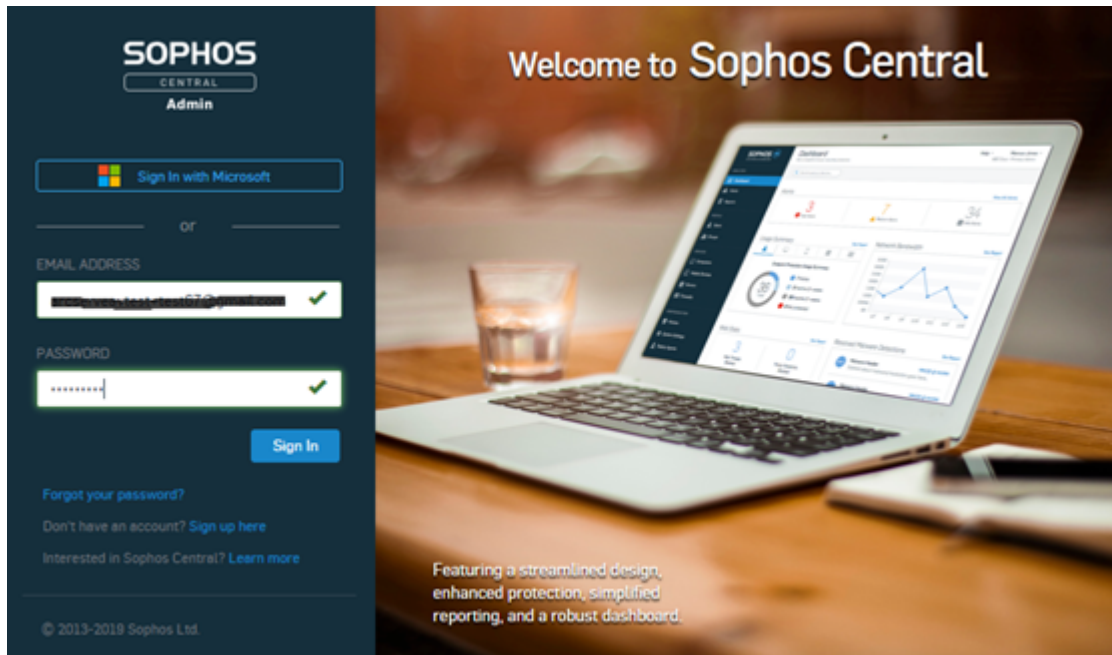
3. To unmount the image, execute the following command using command prompt:

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

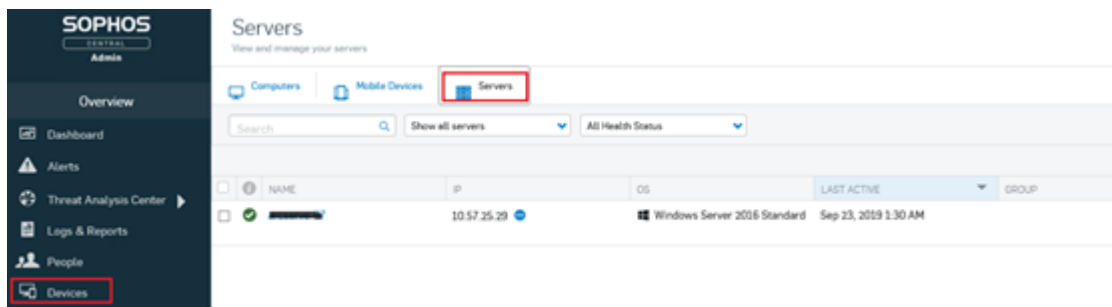


To run SetImage.exe command to replace factory reset image when Sophos runs on Arcserve Appliance, follow these steps:

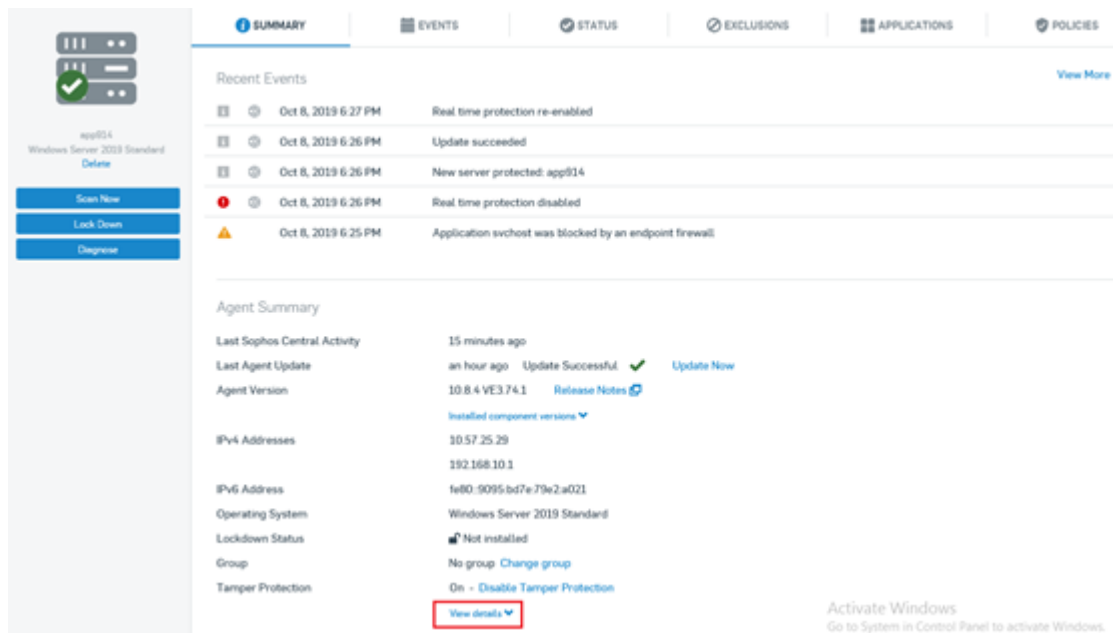
1. Log into the Arcserve Appliance system as an administrator. Use your email address and password to access the Sophos Central Admin page <https://cloud.sophos.com/manage/>.



2. Navigate to Devices > Servers, and then click the server name of your Arcserve Appliance.



3. On the SUMMARY tab, for the Tamper Protection field, click **View details**.



- For Show Password, select the check box. Make a note of the password that displays in the text field.

Tamper Protection

On - [Disable Tamper Protection](#)

[Hide details](#) ^

Tamper Protection Password Details

CURRENT PASSWORD

252555555555

☒ Show Password

[Generate New Password](#)

- Click **Disable Tamper Protection**.

Tamper Protection

On - **Disable Tamper Protection**

[Hide details ^](#)

Tamper Protection Password Details

CURRENT PASSWORD

XXXXXXXXXXXX

☒ Show Password

[Generate New Password](#)

Tamper Protection is turned off.

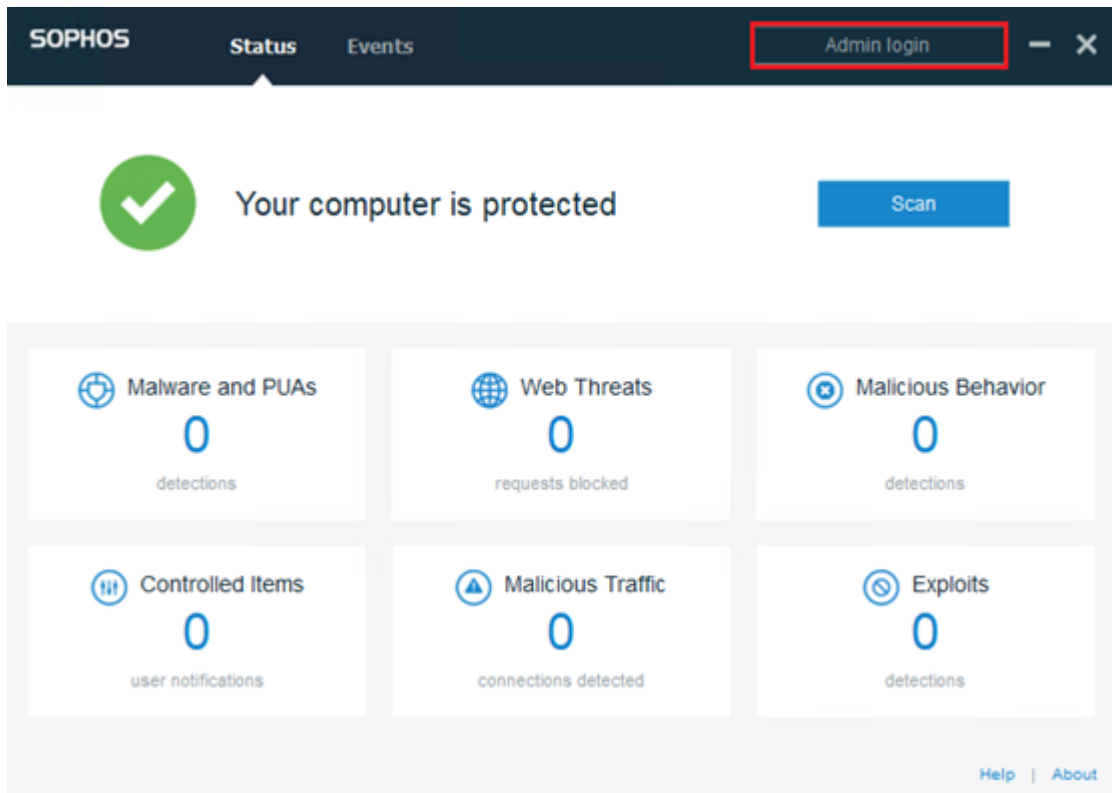
Tamper Protection

Off - [Enable Tamper Protection](#)

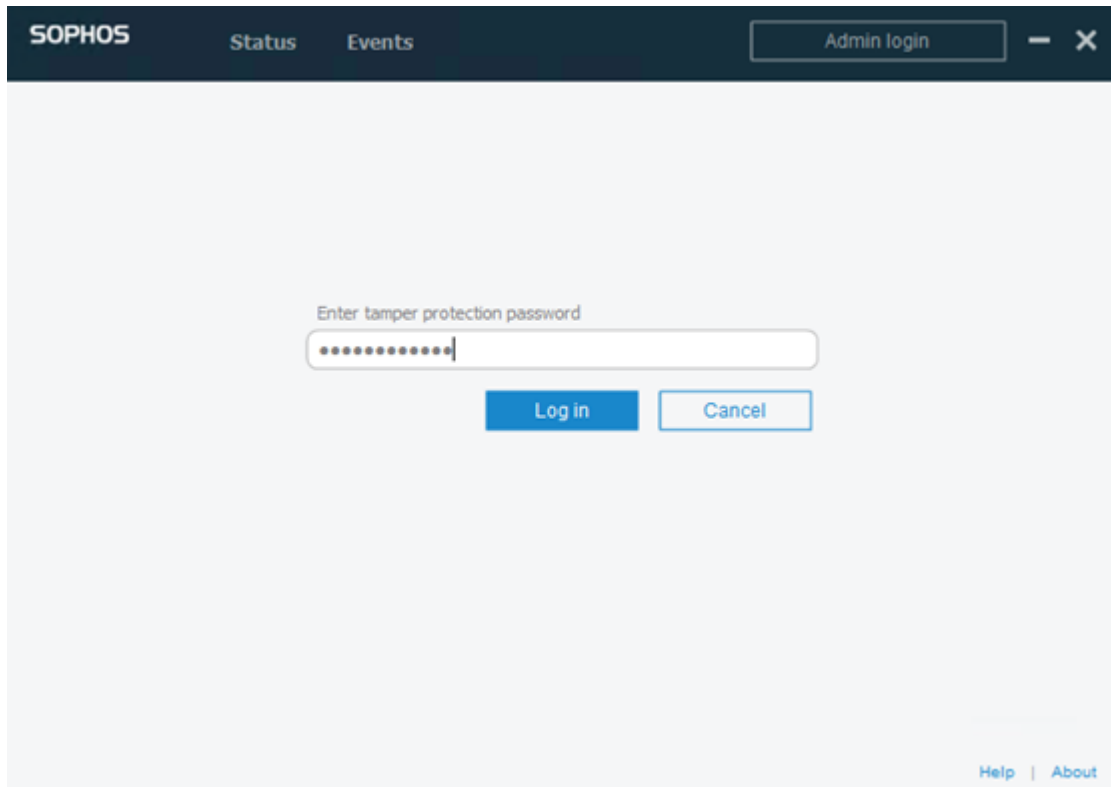
⚠️ Sophos recommends that you enable tamper protection.

Tamper protection ensures that users with local administrator rights can't uninstall Sophos Central Endpoint software or change settings.

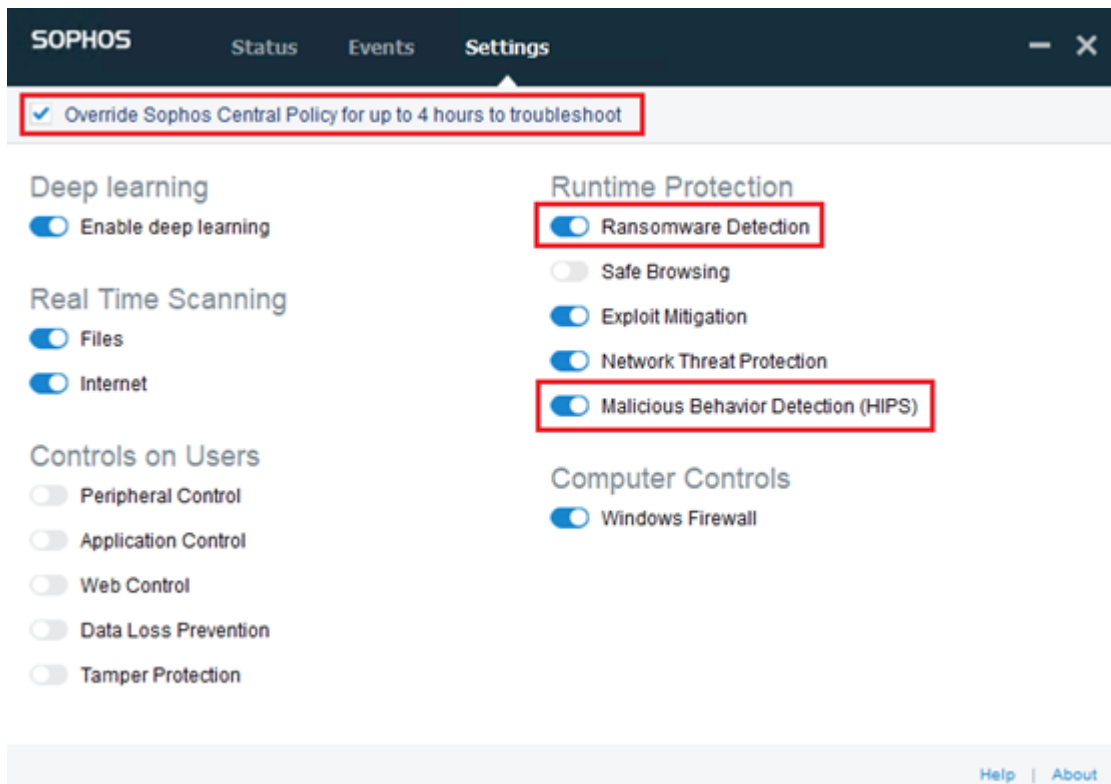
6. Launch Sophos Endpoint, and then click **Admin Login**.



7. Type the Tamper Protection password that was noted in Step 4.



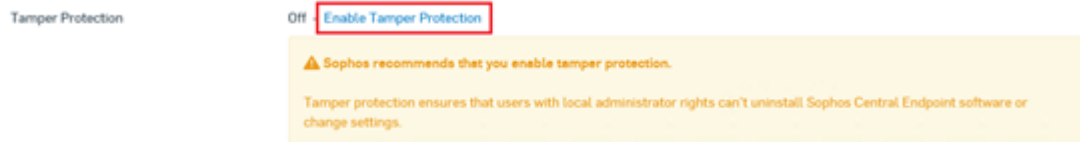
8. On the Settings tab, select the **Override Sophos Central Policy for up to 4 hours to troubleshoot** check box, and disable the **Ransomware Detection** and **Malicious Behavior Detection (HIPS)** options.



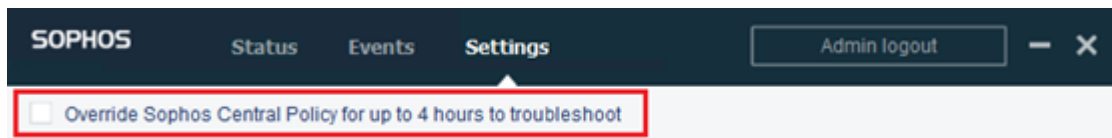
9. To replace factory reset image, run SetImage.exe. SetImage.exe gets executed successfully.

To recover the default configuration of Sophos after the successful execution of SetImage.exe, follow these steps:

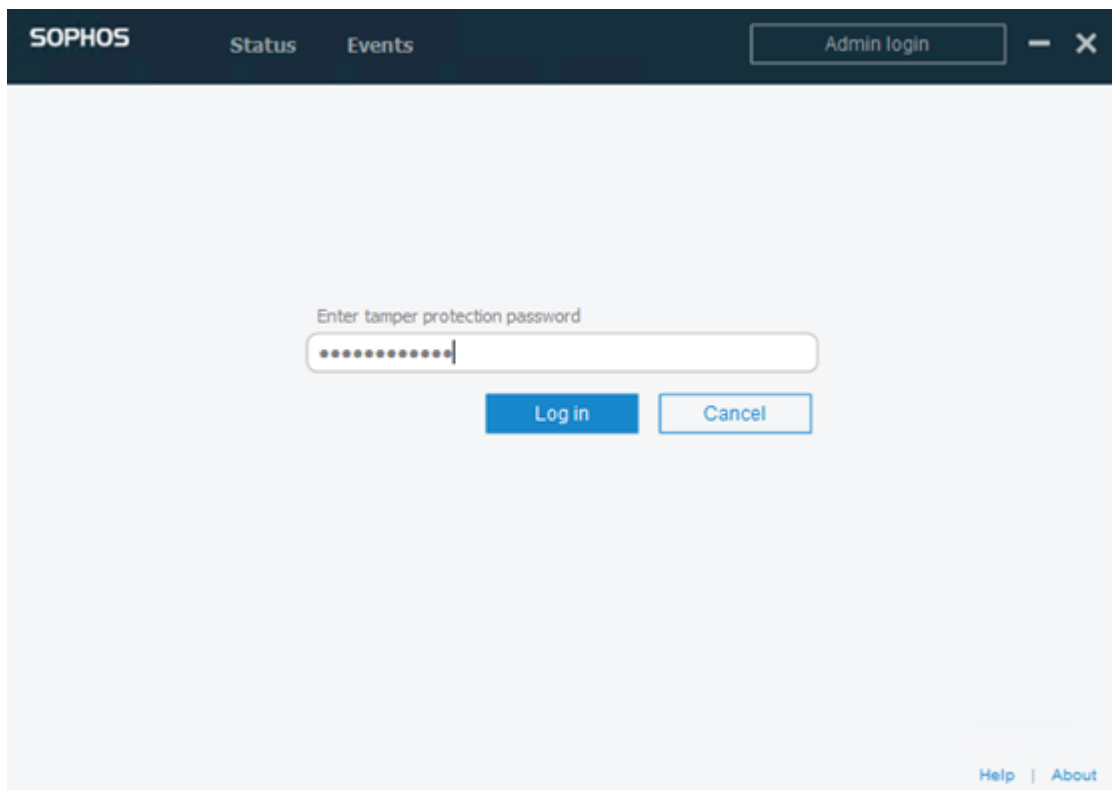
1. To enable Tamper Protection in Sophos Central Admin, click **Enable Tamper Protection**.



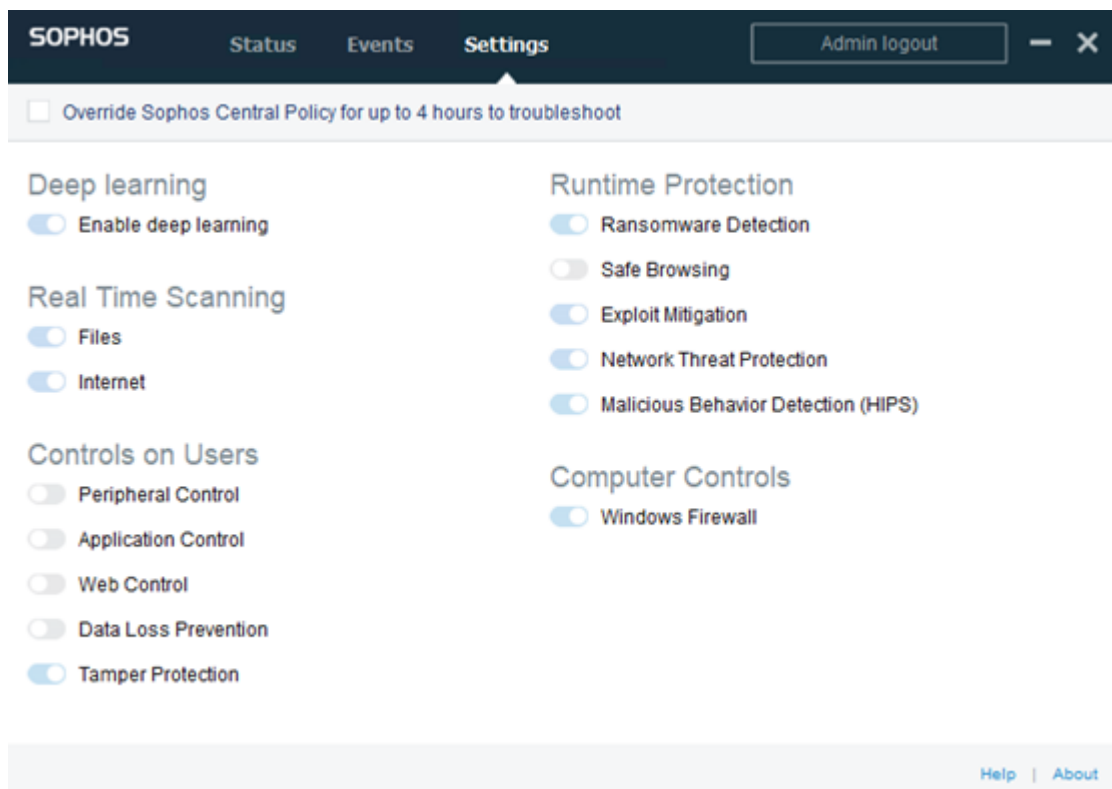
2. Clear the **Override Sophos Central Policy for up to 4 hours to troubleshoot** checkbox.



3. To check the status of the Sophos Settings, wait for a few minutes, and then log into Sophos Endpoint with the tamper protection password.



Now the Sophos Settings have been recovered to the default settings.



Best Practice for Creating Deduplication Datastore across Volumes

The `as_gddmgr.exe`, a command line tool, lets you add more data paths across volumes to expand the storage capacity of the existing dedupe datastore.

To create deduplication datastore across volumes, follow these steps:

1. Log into the Arcserve UDP console user interface, and then create a deduplication datastore without expanded data path. For more information, see [Add a Datastore](#).
2. Stop the datastore. For more information, see [Stop a Datastore](#).
3. Open the command prompt, and then enter the following command to display the current path configuration of datastore:

`as_gddmgr.exe -DataPath Display <datastore name>`

The following sample datastore has one primary data path on X:\volume:

```
C:\Users\Administrator>"c:\Program Files\Arcserve\Unified Data Protection\Engine\bin\as_gddmgr.exe" -DataPath Display appliancestest_data_store
Successfully load data store configuration information.

          Volume capacity    Used space    Free space
Primary data path : X:\Arcserve\data_store\data\
                  59685 GB      2 GB      59683 GB
```

4. To expand the storage capacity of deduplication datastore, enter the following command:

`as_gddmgr.exe -DataPath Add <datastore name> -NewDataPath <new data folder>`

Note: Make sure the primary path and all expanded paths are not on the same volume.

The following sample datastore has an expanded data path on W:\volume:

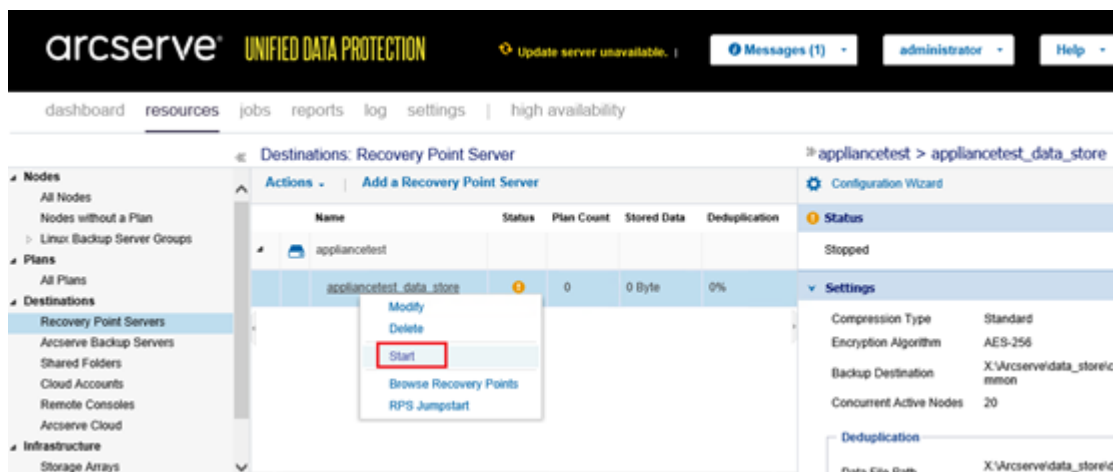
```
C:\Users\Administrator>"C:\Program Files\Arcserve\Unified Data Protection\Engine\bin\as_gddmgr.exe" -DataPath Add appliancestest_data_store -NewDataPath W:\Arcserve\data_store\data1
Successfully load data store configuration information.
Successfully added new expanded data path for the data store.
The data store has 1 expanded data path(s) now!

      Volume capacity   Used space      Free space
-----
Primary data path : X:\Arcserve\data_store\data\
59685 GB              2 GB          59683 GB

Expanded data path: W:\Arcserve\data_store\data1
14678 GB              98 GB          14580 GB

Total                74363 GB          74181 GB
```

5. Repeat step 4 as needed.
6. Return to the Arcserve UDP console user interface and start the datastore. For more information, see [Start a Datastore](#).



Note: We recommend that you import the backed-up datastore on the UDP Appliance with similar disk partitions.

Chapter 15: Acknowledgements

Portions of this product include software developed by third-party software providers. The following section provides information regarding this third-party software.

This section contains the following topic:

[PuTTY](#)

PuTTY

This product includes the "PuTTY" component which entails the following details:

Component Name	PuTTY
Component Vendor	Developed originally by Simon Tatham
Component Version	0.64
Legal Remark	http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html
Project Name	Appliance Rhodium
Component Type	Open Source
Source Code URL	http://the.earth.li/~sgtatham/putty/0.64/
Platform(s) Required	Windows 2012 R2, Windows 2016, Windows 2019
Component URL	http://the.earth.li/~sgtatham/putty/0.64/x86/
Component Version URL	http://the.earth.li/~sgtatham/putty/0.64/x86/
Description	On the appliance machine, we use putty.exe to communicate with the Linux Backup Server to change the system locale and UDP Linux locale.
Features	Appliance
License Text	<p>http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html</p> <p><i>PuTTY is copyright 1997-2019 Simon Tatham.</i></p> <p><i>Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svyatoslav Kuzmich, Nico Williams, Viktor Dukhovni, and CORE SDI S.A.</i></p> <p><i>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:</i></p> <p><i>The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.</i></p> <p><i>THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,</i></p>

	<p>EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.</p>
Copyright Text	<p>http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html</p> <p>PuTTY is copyright 1997-2019 Simon Tatham.</p> <p>Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svyatoslav Kuzmich, Nico Williams, Viktor Dukhovni, and CORE SDI S.A.</p> <p>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:</p> <p>The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.</p> <p>THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.</p>
Intended Usage	On the appliance machine, we use putty.exe to communicate with the Linux Backup Server to change the system locale and UDP Linux locale.
Modifications Required	No