Appliance User Guide

Arcserve Unified Data Protection

Version 10.0

arcserve®

Appliance User Guide

Arcserve Unified Data Protection

Version 10.0

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

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 10000 Series 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
Model 10024BU-10576DR 17
Models 9012 - 9504DR 19
Model X Series 21
Controls and Indicators 23
Front Panel 10048DR-10576DR 23
.Drive Carriers LED 24
Control Panel 25
Information LED 25
Front Panel 9012-9048 26
Front Panel 9072DR - 9504DR 27
Front Panel X Series 28
Rear Panel 10048DR-10576DR 28
Power Supply Indicators 29
Rear Panel 9012-9048 29
Rear Panel 9072DR-9504DR 31
Rear Panel X Series 32
Ports Used by the Appliance 33

Arcserve UDP 34
Components installed on Microsoft Windows 35
Components installed on Linux 40
Node protected by UDP Linux remotely 42
Arcserve Backup 43
Appliance for Linux Support 44
Chapter 3: Upgrading Arcserve UDP on the Appliance 45
How to Apply a License After Upgrading Arcserve Software 46
Upgrade Sequence on Arcserve Appliance 47
Upgrade the Arcserve Appliance Used as Arcserve UDP Console and RPS 48
Upgrade the Arcserve Appliance Used as Arcserve UDP RPS 49
Upgrade Steps When Two or More Arcserve Appliance Are Used in the Environment 50
Upgrade the Arcserve UDP Linux Agent on the Arcserve Appliance 51
Upgrade the Arcserve Backup on the Arcserve Appliance 52
Upgrade Sequence for UDP Console, RPS, and Agent 53
Chapter 4: Configuring the Arcserve Appliance 54
How to Configure Network Settings for Arcserve Appliance 55
How to Set Up the Arcserve Appliance 59
Configure Arcserve Appliance as Gateway 68
Chapter 5: Working with Arcserve Appliance 69
Activate Arcserve Product on the Appliance 70
Create a Plan Using Arcserve Appliance Wizard 71
Add Nodes to a Plan 72
Add Nodes by Hostname/IP Address 73
Add Nodes by Active Directory 75
Add vCenter/ESX Nodes 77
Add Hyper-V Nodes 79
Create a Backup Plan for Linux Nodes 81
Create a Backup Plan to a Tape Device 82
Create an On-Appliance Virtual Standby Plan 83
Create Plan to Backup the Linux Backup Server 84
Setting-up to Perform Linux Instant VM Job to Local Appliance Hyper-V 87
Migrate Arcserve UDP Console Using ConsoleMigration.exe 88
Perform Migration between Arcserve Appliances 90
Solution 91
Modify the Input Source of Pre-installed Linux Backup Server 94

Chapter 6: Monitoring the Appliance Server Remotely 97

Working with Integrated Dell Remote Access Controller (iDRAC) 98

Monitor and Manage Integrated Dell Remote Access Controller (iDRAC) 99

Find the IP address of Integrated Dell Remote Access Controller for 9000 Series (iDRAC) 101

Find the IP address of Integrated Dell Remote Access Controller for X Series (iDRAC) 102

Configure DHCP or Static IP address of iDRAC 104

Working with Baseboard Management Controller (BMC) 108

Monitor and Manage Baseboard Management Controller (BMC) 108

How to Find the IP address of BMC 110

Find the IP address using BIOS 110

Find the IP address in POST screen 110

Configure the DHCP or Static IP Address of BMC 111

Configuring UEFI BIOS 111

Configuring the IP Address of BMC 112

Configure the DHCP IP Address using the DHCP Server 112

Configure the Static IP Address using BIOS 112

Connecting to BMC using BIOS 114

Chapter 7: Restoring or Repairing the Arcserve Appliance 117

Debug Factory Reset 118

Installing the Arcserve Appliance 120

How to Install Arcserve Backup 19.0 121

How to Install 10024BU-10048BU Series Appliance 128

How to Install 10048DR-10576DR Series Appliance 129

How to Install 9012-9048 Series Appliance 129

How to Install 9072-9504DR Series Appliance 129

How to Install X Series Appliance 129

Apply Arcserve UDP Factory Reset in 10024BU-10576DR Series Appliance 129

Factory Reset from BIOS 130

Factory Reset from Arcserve UDP Console 132

Apply Arcserve UDP Factory Reset Using Boot Option in 9012-9504DR Series Appliance 134

Apply Arcserve UDP Factory Reset Using Boot Option in X Series Appliance 136

Clear Configuration and Apply Appliance Factory Reset 139

Remove and Replace a Hard Drive 141

Perform Bare Metal Recovery (BMR) without Preserving Data in 9012-9504DR Series Appliance 143

Perform Bare Metal Recovery (BMR) and Preserving Data in 9012-9504DR Series Appliance 157

Chapter 9: Performing Appliance Capacity Expansion 164
Working with Expansion Kit in Arcserve Appliance 10024BU-10576DR Models 164
Working with SSD Flash Expansion Kit in Arcserve Appliance 10024BU-10576DR Models 168
Working with Arcserve Appliance Expansion Kit - X Series Models 171
Working with SSD Flash Expansion Kit in Arcserve X Series Appliance 173
Working with Expansion Kit in Arcserve Appliance 9072-9504 DR Models 180
Working with SSD Flash Expansion Kit in Arcserve Appliance 9072-9504 DR Models 185
Chapter 10: Working with Network Configuration 190
Understanding the Network Configuration Details 191
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
Upgrading Firmware for Arcserve Appliance 10000 Series 206
Viewing Firmware Version 206
Download the Firmware Upgraded Package 207
Upgrade Firmware 208
How to Upgrade BMC firmware 208
How to Upgrade BIOS firmware 211
Verify Updated Firmware 215
Chapter 11: Upgrading Firmware for Arcserve Appliance 9000 Series 216
Upgrade BIOS Firmware for Arcserve Appliance 9000 Series 216
Viewing Firmware Version 216
Method 1: View BIOS firmware version from iDRAC Web Interface 218
Method 2: View BIOS firmware version from BIOS Arcserve Appliance 9000 series 218
Download the Updated Package for BIOS 219
Upgrade BIOS 219
Verify Updated Firmware 220
Verify Updated BIOS using System Logs 221
Verify Updated BIOS from iDRAC Web Interface or BIOS 222

Upgrade iDRAC Firmware for Arcserve Appliance 9000 Series 222
Viewing iDRAC Firmware Version 222
View iDRAC Firmware Version from iDRAC Web Interface 222
Method 2: View iDRAC Firmware Version from BIOS Arcserve Appliance 9000 series 223
How to Change the iDRAC Password 224
Download the Updated Package for iDRAC 225
Upgrade iDRAC 225
Verify Updated iDRAC 226
Verify Updated iDRAC using System Logs 226
Verify Updated iDRAC from iDRAC Web Interface or BIOS 227
Upgrade Firmware for Arcserve Appliance X Series 228
Upgrade BIOS Firmware for Arcserve Appliance X Series 228
Viewing BIOS Firmware Version 228
Method 1: View BIOS firmware version from iDRAC Web Interface 228
Method 2: View BIOS firmware version from BIOS Arcserve Appliance X series 229
Download the Updated Package for BIOS 230
Upgrade BIOS 230
Verify Updated BIOS 231
Upgrade iDRAC Firmware for Arcserve Appliance X Series 231
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 12: Troubleshooting 235
Linux Backup Server Fails to Connect from the Console 236
Backing Up Arcserve Appliance from Another Appliance Reports Duplicated Nodes 237
Linux Backup Server Cannot Communicate with Any Node in the Network 238
Linux Backup Server Cannot Get the Network DNS Suffix 240
Default Time Zone on the Appliance 241
Licenses Error even when the licenses are available 242
Chapter 13: Applying Best Practices 243
Best Practices for Network Configuration 244
Best Practices for Windows Defender with PowerShell cmdlets 247
Configure Preinstalled Linux Backup Server to External Network 247

Best Practice for Creating Deduplication Datastore across Volumes 248
Chapter 14: Acknowledgements 251
PuTTY 252

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 23

Ports Used by the Appliance 33

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:

- 10000 Series
- 9000 Series
- X Series

What is Included in the Box of Appliance 10000 Series

The following items are included in the 10048DR-10576DR Accessory box:

- Quick Start Guide, Arcserve Appliance READ ME FIRST SHEET
- Arcserve QR Leaflet (with QR code to guides)
- 1x Arcserve 10K Server Hardware Installation Guide
- 2x Power cord (c13 to nema 5-15p). A pair of power cords will be added to the box of the destination country for the order, in addition to the default US power cord.
- 1x rail kit / bracket set
- 1x 3.5 HDD screws bag
- 1x 2.5 HDD screws bag
- CABLE, FLEXBOOT,CAT6,NETWORK,3FT,BLUE CABLE, FLEXBOOT,CAT6,NETWORK,7FT,BLACK

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
  - 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:

- Model 10024BU - 10576DR
- Models 9012 - 9504 DR
- Model X Series

Model 10024BU-10576DR

Arcserve Appliance Models 10024BU - 10576DR

Arcserve Appliance 10K Series Specifications							
Appliance Model	**10048DR**	**10072D-R**	**10144D-R**	**10192D-R**	**10288D-R**	**10384DR**	**10576D-R**
Effective capacity (TB)1	48	72	144	192	288	384	576
Usable Capacity	16 TB	24 TB	48 TB	64 TB	96 TB	128 TB	192 TB
Maximum usable capacity using expansion kit	40 TB	40 TB	80 TB	80 TB	160 TB	160 TB	NA
Form Factor	2U						
Base RAM (DDR5 5600)	128 GB (4x32 GB)	256 GB (8x32 GB)					384 GB (12X32 GB)
Max RAM	512 GB						
SAS 12G HDD Enterprise Grade 7.2k	6x4 TB	8x4 TB	8x8 TB	10x8 TB	8x16 TB	10x16 TB	14X16 TB
NVMe M.2	2x480 GB (RAID 1) for OS and UDP						
SSD	2x 3.2 TB for Hash (RAID 1)						
CPU	Dual Intel ® Xeon® Silver 4510T 12C 2 G						
RAID Controller	Broadcom 3916 with CacheVault write cache protection						
HDD RAID	RAID6						

Con-figuration							
Drive Bays	14xHDD, 2xSSD						
Optional RAM Expan-sion Kits	✓	✓	✓	✓	✓	✓	✓
DIMM Slots	16						
NIC	Total 4 Ports. 2x 10GbE on-board. 2x 10 GbE Base-T via Broadcom BCM57416						
Available PCIe slots	3 (Low Profile)						
Remote Hardware Man-agement	IPMI(Advance License)						
Power Sup-plies	2x 1600W Redundant Titanium Level (96%) hot-swap replacement						
HDD Kit (optional)	8x4 TB(24 TB) RAM Upgrade recom-mended	6x4 TB (16 TB)	6x8 TB (32 TB)	4x8 TB (16 TB)	6x16 TB (64 TB)	4x16 TB(32 TB) RAM Upgrade recom-mended	X
RAM Expan-sion Kit (Optional)	Each kit of 128 GB (4x32) can be ordered in multiples. Max 3 Kits		Each kit of 128 GB (4x32) can be ordered in multiples. Max 2 Kits.				128 GB (4x32) Max 1 kit.
Broadcom Aero HBA 9500-8e PCIe Gen4	Optional						
Broadcom BCM57416 dual-port 10Gbps Base-T Adapter	Optional						
Intel X710 Std LP Dual port 10G SFP+	Optional						
Broadcom BCM57414	Optional						

Std LP Dual port 25G SFP28	
QLogic 2692 Dual Port 16Gb Fibre Channel HBA	Optional
Weight	Gross Weight: 62 lbs (28.12 kg) Net Weight: 41.5 lbs (18.82 kg)
Packaging Dimensions	658 x 274 x 998mm (25.9" x 10.8" x 39.3")
In-Rack Dimensions	437 x 89 x 705mm (17.2" x 3.5" x 27.75")

Note: Effective capacity considers global source deduplication and equals 3x the usable capacity. Actual backup capacity may vary depending on data types, backup type, schedule, and other factors.

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	1			2							

Processors									
RAID Card	PERC H730P Low Profile, adaptor, 2 GB NV Cache	PERC H730P, MiniCard, 2 GB NV Cache							
RAID Con-figuration	RAID-5	RAID-6							
Drive Bays	4	16							
Expansion Kit	NA	11	10	8	6	4	6	4	NA
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							Broad-com 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 Sup-	Dual, Hot-	Dual, Hot-Plug, Redundant Power Supply (1+1), 750 W							

plies	Plug, Redund-ant Power Supply (1+1), 550 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 Capa-city 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				
Continuous Availability with Automated Failover	Arcserve Continuous Availability optional				
Compute Node					
CPU	Dual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)				
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)				

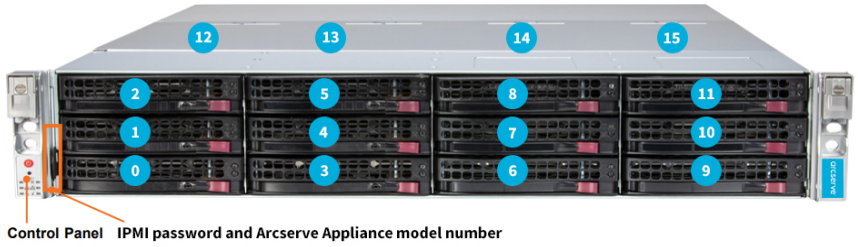
Controls and Indicators

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 10024BU-10048BU
- Front Panel 10048DR-10576DR
- Front Panel 9012-9048
- Front Panel 9072DR-9504DR
- Front Panel X Series
- Rear Panel 10024BU-10048BU
- Rear Panel 10048DR-10576DR
- Rear Panel 9012-9048
- Rear Panel 9072DR-9504DR
- Rear Panel X Series
- Top View 10024BU-10048BU

Front Panel 10048DR-10576DR

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



Control / Indicator	Description
0 - 5	SAS 3.5" HDDs. For more information, see Drive Carriers LED.
6 - 11	SAS 3.5" HDDs. For more information, see Drive Carriers LED.
12-13	SAS 3.5" HDDs. For more information, see Drive Carriers LED.
14-15	SAS 2.5" SSDs. For more information, see Drive Carriers

	LED.
Control Panel	Contains the power button, reset button and LED indicators. For more information, see Control Panel.
IPMI password and Arcserve appliance model number	Contains the IPMI password and Arcserve appliance model number.

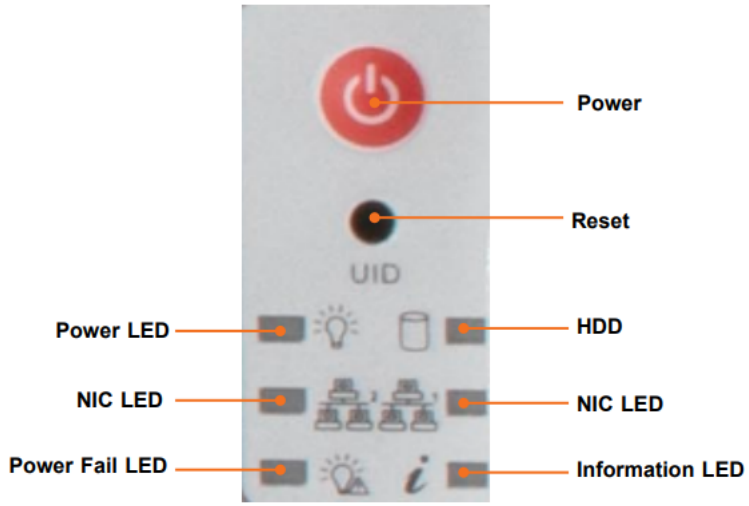
.Drive Carriers LED

Each drive carrier has two LED indicators: activity and status indicators. For RAID configurations using a controller, the meaning of the status indicator is described in the table below:

	Color	Blinking Pattern	Behavior for Device
Activity LED	Blue	Solid On	Idle SAS/NVMe drive installed
	Blue	Blinking	I/O activity
	Off		Idle SATA drive installed
Status LED	Red	Solid On	Failure of drive with RSTe support
	Red	Blinking at 1 Hz	Rebuild drive with RSTe support
	Red	Blinking with two blinks and one stop at 1 Hz	Hot spare for drive with RSTe support
	Red	Blinking with two blinks and one stop at 1 Hz	Power on for drive with RSTe support
	Red	Blinking at 4 Hz	Identify drive with RSTe sup-

			port
	Green	Solid On	Safe to remove NVMe drive
	Amber	Blinking at 1 Hz	Do not remove NVMe drive

Control Panel



Control / Indicator	Description
Power button	The main power switch applies or removes primary power from the power supply to the server but maintains standby power.
Reset Button	Reboots the system.
Power LED	Indicates power is being supplied to the system power supply units. This LED is illuminated when the system is operating normally.
HDD	Indicates activity on the storage drives when flashing.
NIC LEDs	Indicates network activity on LANs when flashing.
Power Fail LED	Indicates a power supply module has failed.
Information LED	Alerts operator to several states. For more information, see Information LED.

Information LED

The following table describes the Information LED status:

Color, Status	Description
Red, continuously	An overheat condition has occurred.
Red, blinking at 1 Hz	Fan failure, check for an inoperative fan.
Red, blinking at 0.25 Hz	Power failure, check for a non-operational power supply.
Blue, solid	UID has been activated locally to locate the server in a rack environment.
Blue, blinking	UID has been activated using the BMC to locate the server in a rack environment.

Front Panel 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	Contains the system health and system ID, status LED, and the iDRAC Quick Sync 2 (wireless) indicator. **NOTE:** The iDRAC Quick Sync 2 indicator is available only on certain configurations. • **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 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

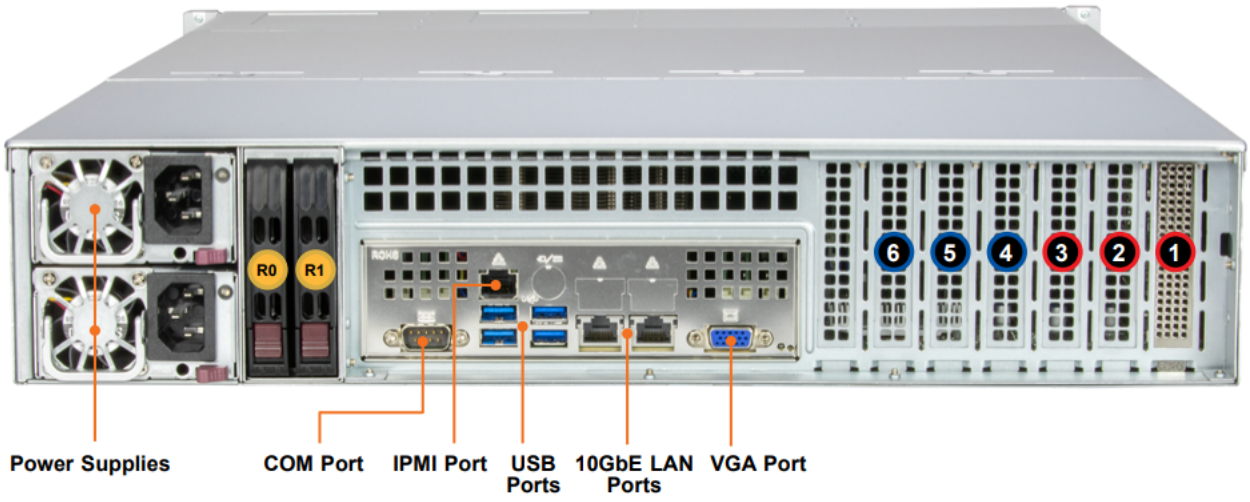
			supported on your system. For more information, see link.
3	Right control panel	NA	Contains the power button, VGA port, iDRAC Direct micro USB port and two USB 2.0 ports.
4	Information tag	NA	The Information Tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC 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 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 10048DR-10576DR

The rear panel of the Arcserve Appliance contains Expansion card slots, power supply modules, Unit identifier LED, LAN ports, USB ports, VGA ports, BMC LAN port, and COM port. The following table describes these items:



Control / Indicator	Description
R0, R1	Non-usable
1	Hardware RAID controller
2	Cache vault for Hardware RAID controller

3	10 GbE Base-T
4	Expansion slot for optional cards (Low Profile)
5	Expansion slot for optional cards (Low Profile)
6	Expansion slot for optional cards (Low Profile)
Power Supplies	Dual redundant 1600 W power supplies. For more information, see Power Supply Indicators.
COM Port	Serial port (RS-232)
IPMI Port	Dedicated IPMI LAN port
USB ports	Four USB 3.0 ports
VGA Port	One video port
LAN Ports	Two RJ45 10 GbE LAN ports

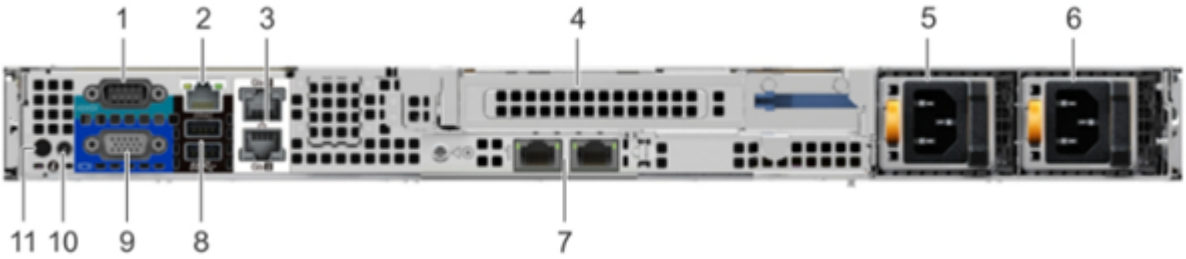
Note: You can find the series number on the rear panel of the server near the VGA port and on the IPMI interface.

Power Supply Indicators

Power Supply Conditions	Green LED	Amber LED
No AC power to the power supply	OFF	OFF
Power supply critical events causing a shut-down/failure/ OCP/OVP/Fan Fail/OTP/UVP	OFF	Amber LED
Power supply warning events where the power supply continues to operate: high temperature, over voltage, under voltage, etc	OFF	1 Hz Blink Amber
AC power present and only 12 VSB ON (PS OFF)	1 Hz Blink Green	OFF
Output ON and OK	Green	OFF
AC cord unplugged and in redundant mode	OFF	Amber

Rear Panel 9012-9048

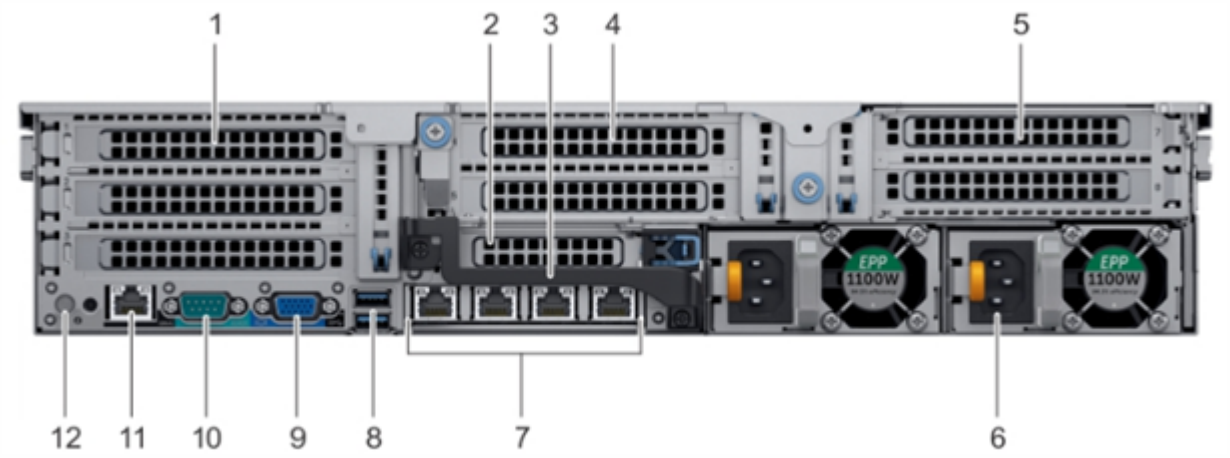
The rear panel of the Arcserve Appliance contains the power supplies, cable connections, and ports for the appliance. The following table describes these items:



Number	Control / Indicator	Icon	Description
1	Serial port		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 (PSU)		For more information about the PSU configurations, 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		Press the system ID button: • To locate a particular system within a rack. • To turn the system ID on or off. To reset iDRAC, press and hold the button for 15 seconds. **Notes:** • 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 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 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	sqlsrvr.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

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

				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	tffpd	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	CASTapeEngine	Tapeng.exe	Arcserve Tape Engine
6503	TCP	CASJobEngine	Jobengine.exe	Arcserve Job Engine
6504	TCP	CASDBEngine	DBEng.exe	Arcserve Database Engine
7854	TCP	CASportmapper	Catirpc.exe	Arcserve PortMapper
41523	TCP	CASDiscovery	casdscsvc.exe	Arcserve Discovery Service
41524	UDP	CASDiscovery	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: Upgrading Arcserve UDP on the Appliance

This section contains the following topics:

How to Apply a License After Upgrading Arcserve Software 46

Upgrade Sequence on Arcserve Appliance 47

Upgrade Sequence for UDP Console, RPS, and Agent 53

How to Apply a License After Upgrading Arcserve Software

After upgrading Arcserve UDP to 10.0 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 10.0 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 v9.1 to Arcserve UDP 10.0 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

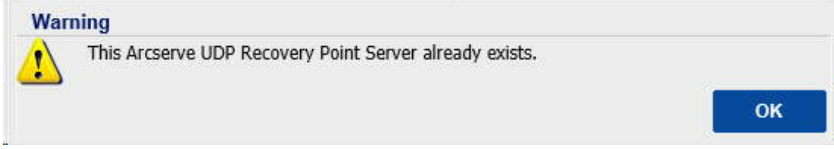
Upgrade this Arcserve Appliance, then follow up the upgrade sequence described to upgrade the environment.

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 4: Configuring the Arcserve Appliance

This section contains the following topics:

How to Configure Network Settings for Arcserve Appliance 55

How to Set Up the Arcserve Appliance 59

Configure Arcserve Appliance as Gateway 68

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

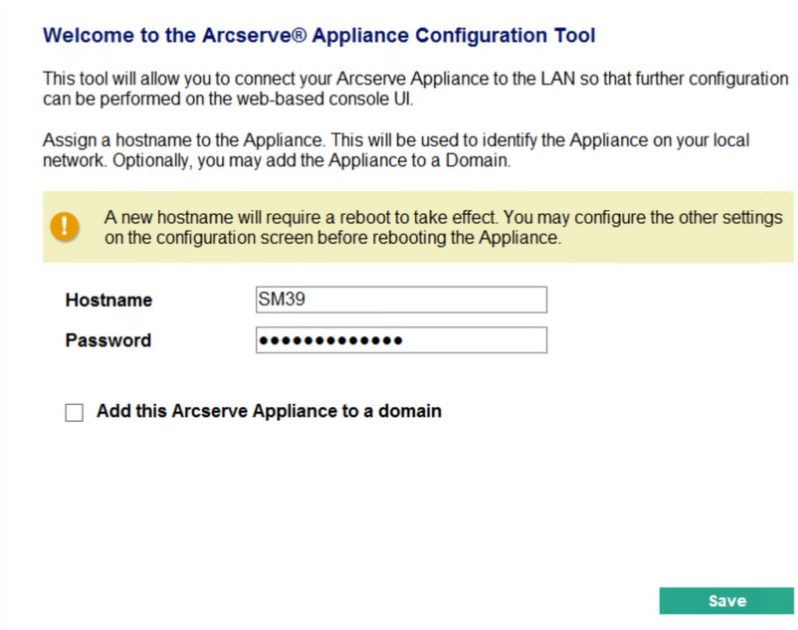
   Enter a host name for the appliance. Assigning a name helps identify the appliance on your network.

   Password

   Specifies the Administrator password.

   Add this Arcserve Appliance to a domain

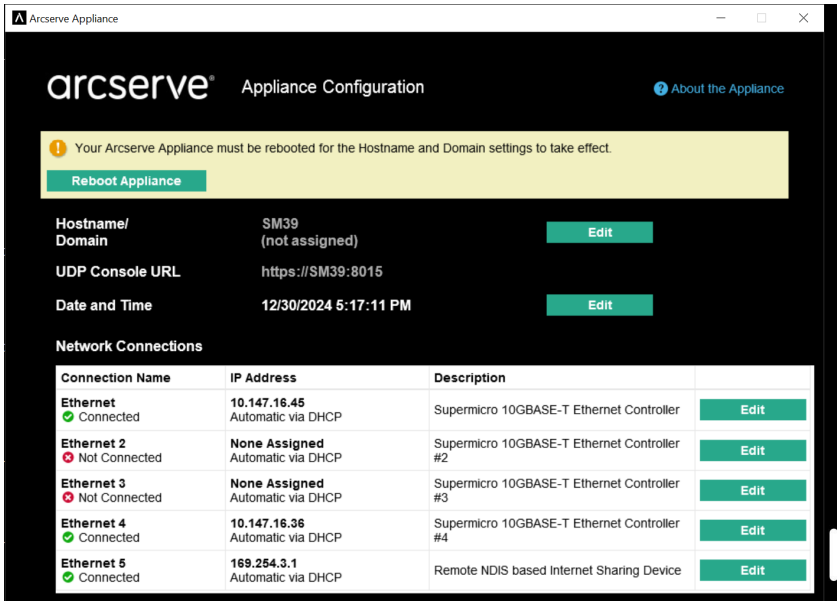
   Select the check-box to make your appliance a member of a domain in your network. Specify the values in Domain, Username, and Password fields that are displayed when the option is selected.



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*.

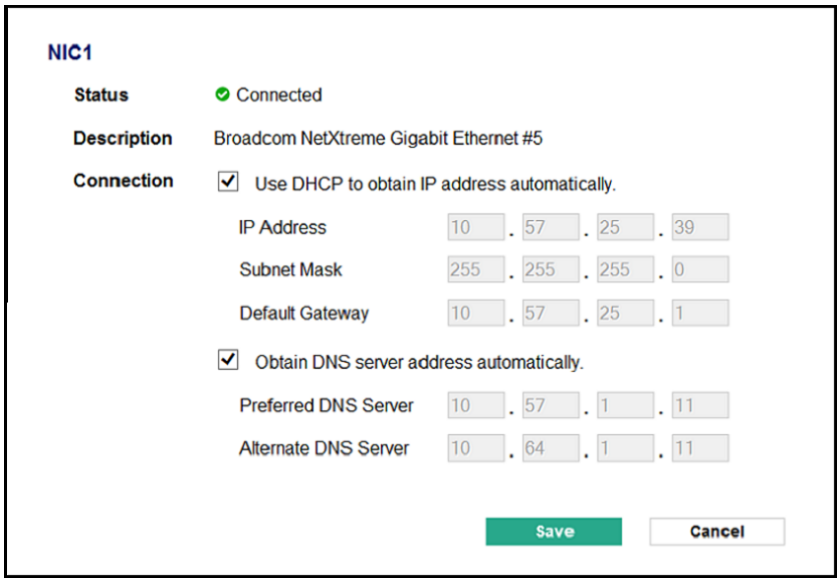
4. Click **Save**.

   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.



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

   The **Network Connection** dialog opens.



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.

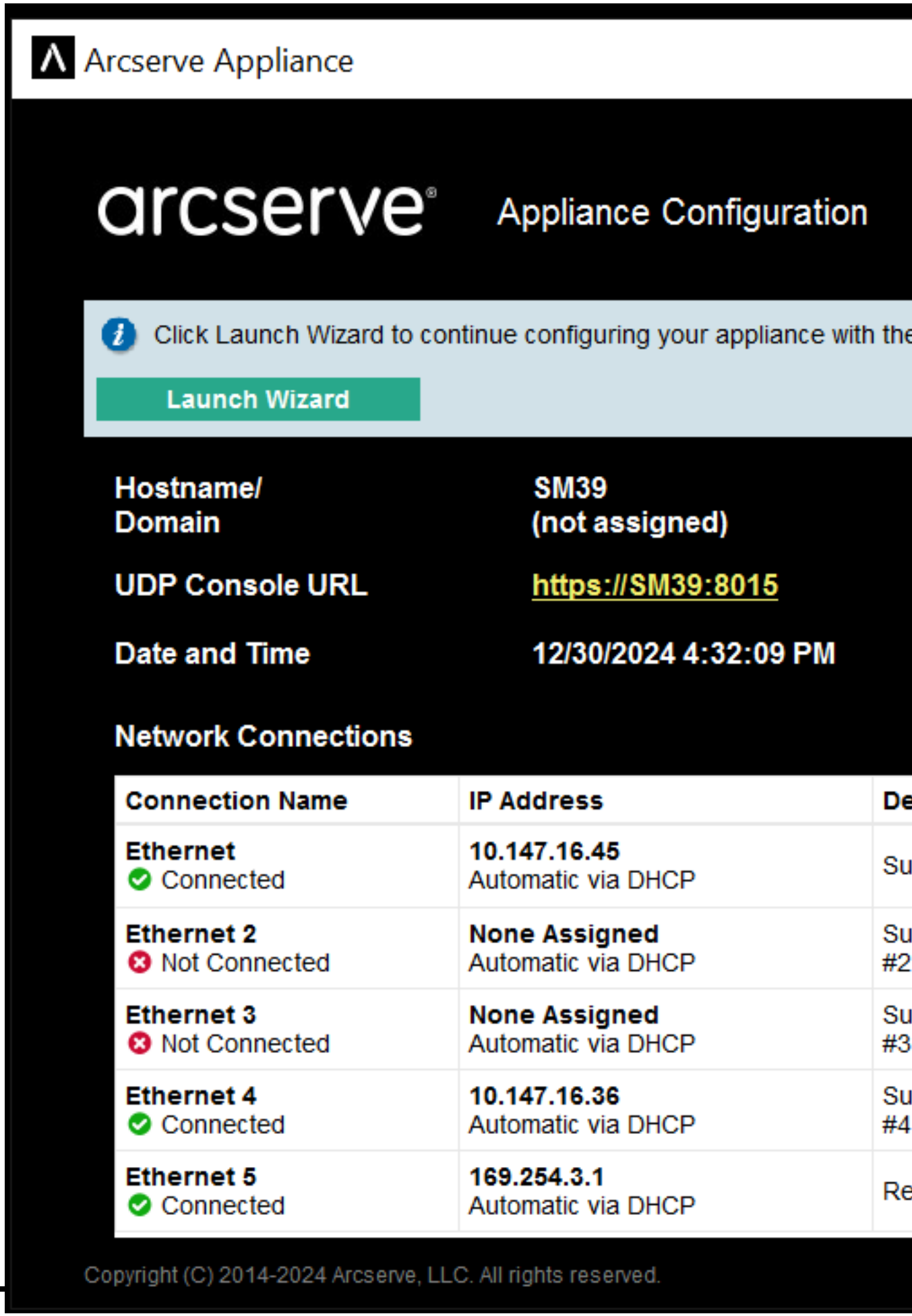
7. To apply the changes, click **Reboot Appliance** to restart the appliance.

   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
arcserve
Appliance Configuration
Click Launch Wizard to continue configuring your appliance with the
Launch Wizard
Hostname/
Domain
SM39
(not assigned)
UDP Console URL
https://SM39:8015
Date and Time
12/30/2024 4:32:09 PM
Network Connections
Connection Name
IP Address
De
Ethernet
Connected
10.147.16.45
Automatic via DHCP
Su
Ethernet 2
Not Connected
None Assigned
Automatic via DHCP
Su
#2
Ethernet 3
Not Connected
None Assigned
Automatic via DHCP
Su
#3
Ethernet 4
Connected
10.147.16.36
Automatic via DHCP
Su
#4
Ethernet 5
Connected
169.254.3.1
Automatic via DHCP
Re
Copyright (C) 2014-2024 Arcserve, LLC. All rights reserved.

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.

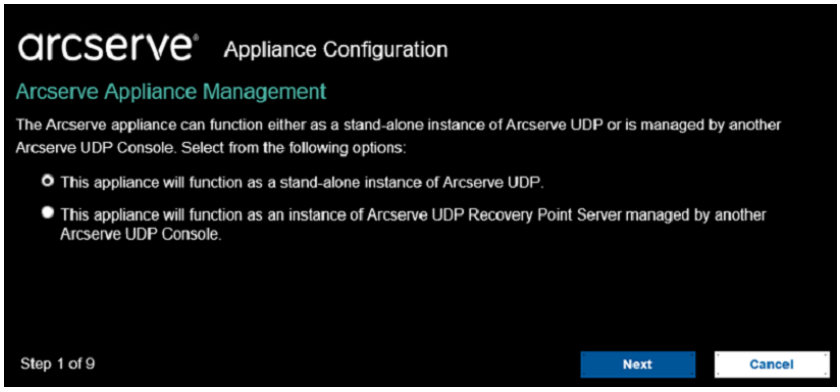
All the steps on the Arcserve Appliance Configuration wizard are optional, you can skip by clicking **Cancel** and directly open the UDP console and create plans.

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

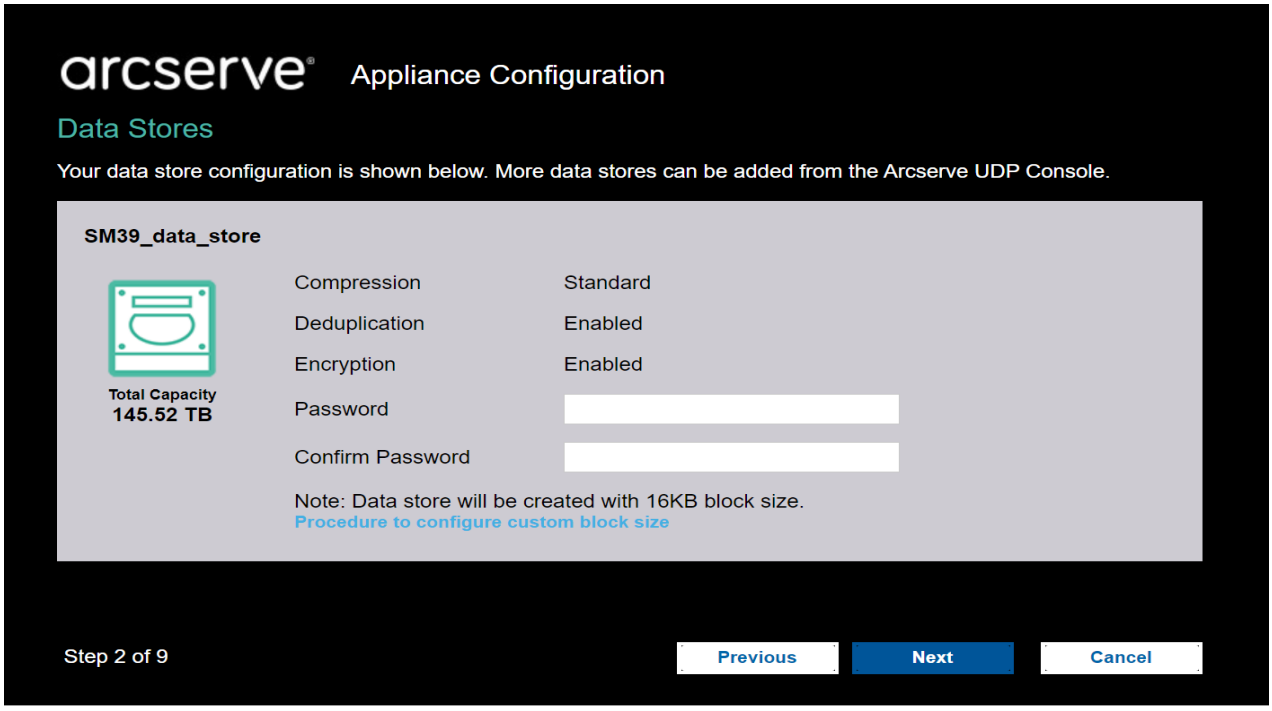
  b. Open the **ApplianceDefaultSetting.properties** file, and then edit *deduplicationBlockSize*.

- 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**.



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.

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.

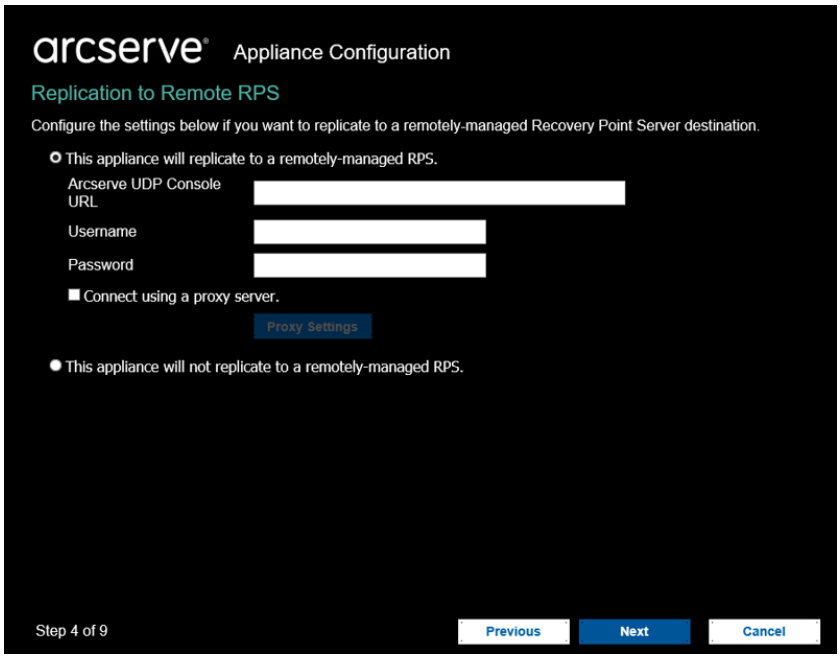
Username and Password

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.



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.

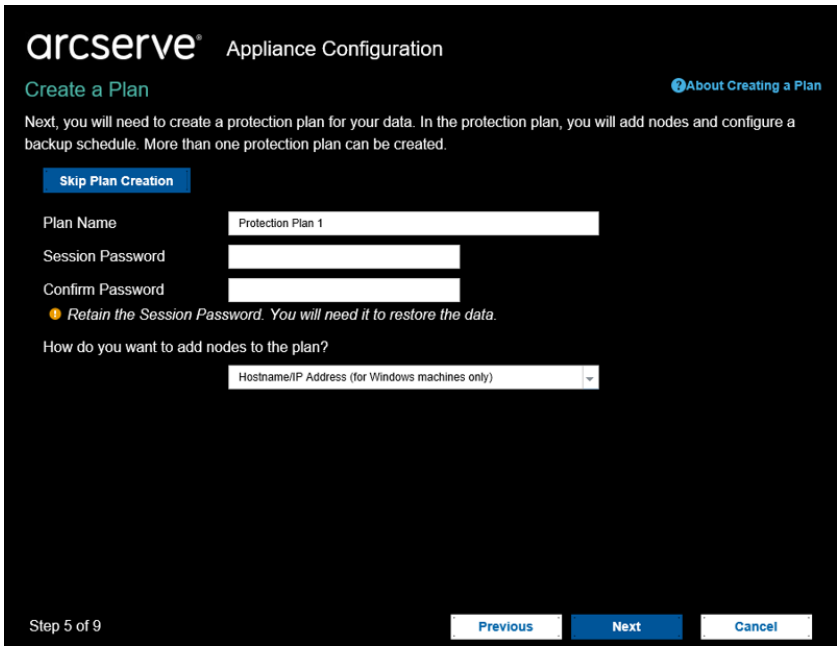
- Importing from a vCenter/ESX Server

  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.



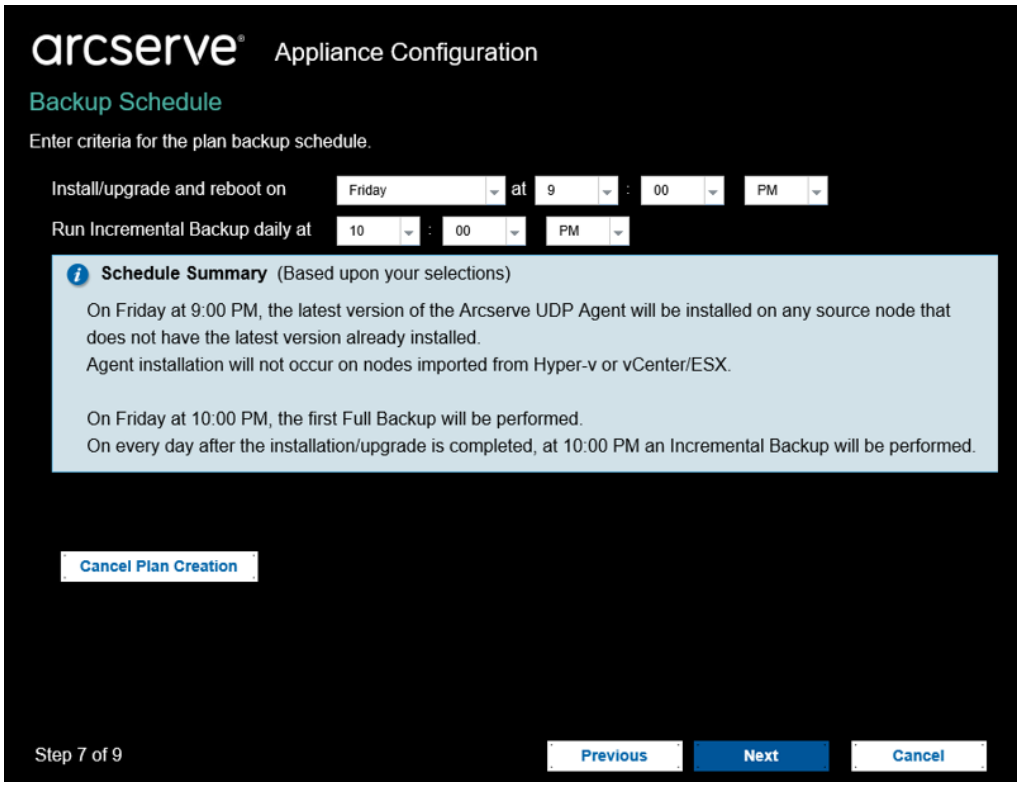
10. After the nodes are added to your plan, click **Next**.

    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**.



12. Click **Next**.

    The Plan Confirmation dialog opens.

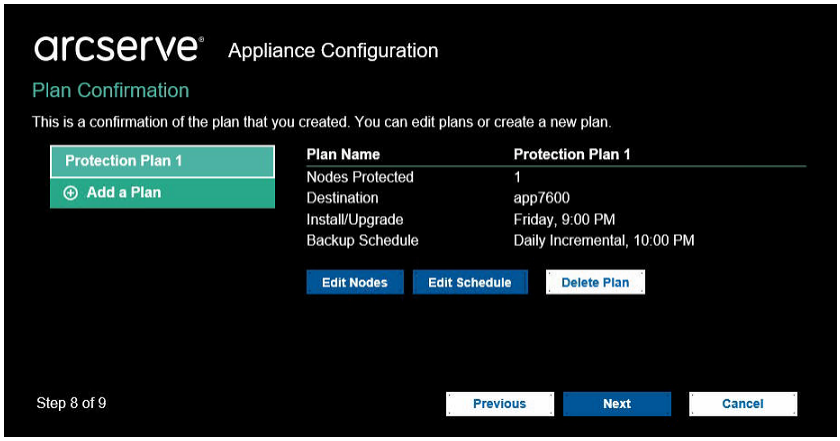
13. On the Plan Confirmation dialog, review the details of your plan. If necessary, you can edit the nodes or the schedule by clicking Edit Nodes or Edit Schedule, or you can add or delete a plan.

    Edit Nodes

    Modifies the source nodes you want to protect.

    Edit Schedule

    Modifies the backup schedule.

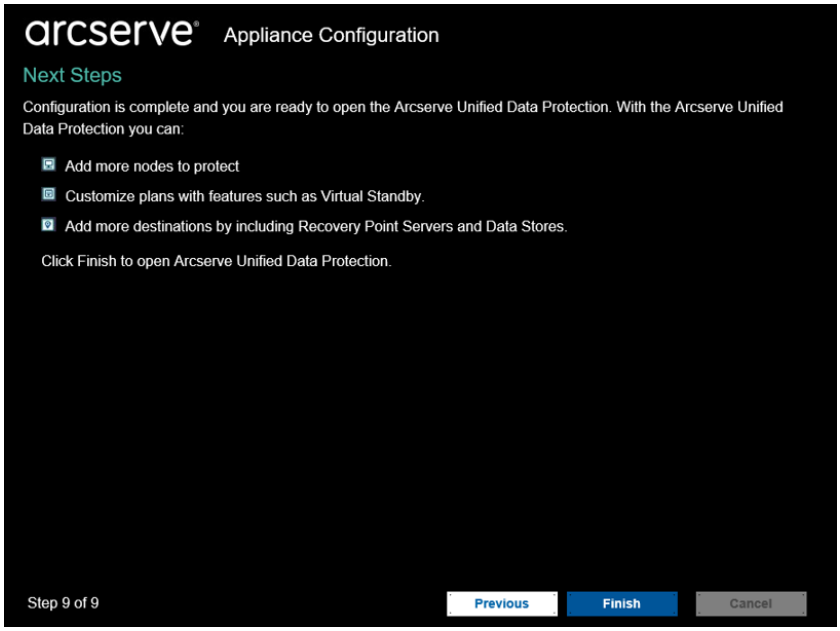


14. After verifying the plans, click **Next**.

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.



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 5: 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 70
Create a Plan Using Arcserve Appliance Wizard 71
Add Nodes to a Plan 72
Create a Backup Plan for Linux Nodes 81
Create a Backup Plan to a Tape Device 82
Create an On-Appliance Virtual Standby Plan 83
Create Plan to Backup the Linux Backup Server 84
Setting-up to Perform Linux Instant VM Job to Local Appliance Hyper-V 87
Migrate Arcserve UDP Console Using ConsoleMigration.exe 88
Perform Migration between Arcserve Appliances 90
Modify the Input Source of Pre-installed Linux Backup Server 94

Activate Arcserve Product on the Appliance

For activating Arcserve product on the Appliance, see Arcserve Product Licensing Online Help.

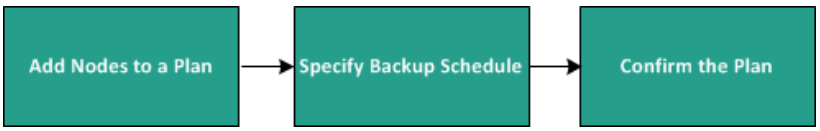
Create a Plan Using Arcserve Appliance Wizard

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

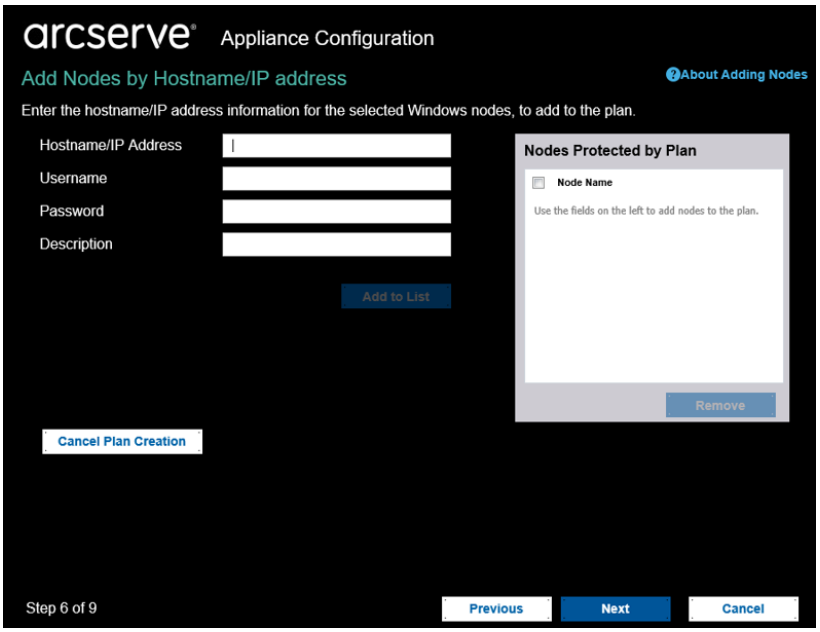
  (Add Hyper-V Nodes)

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:



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

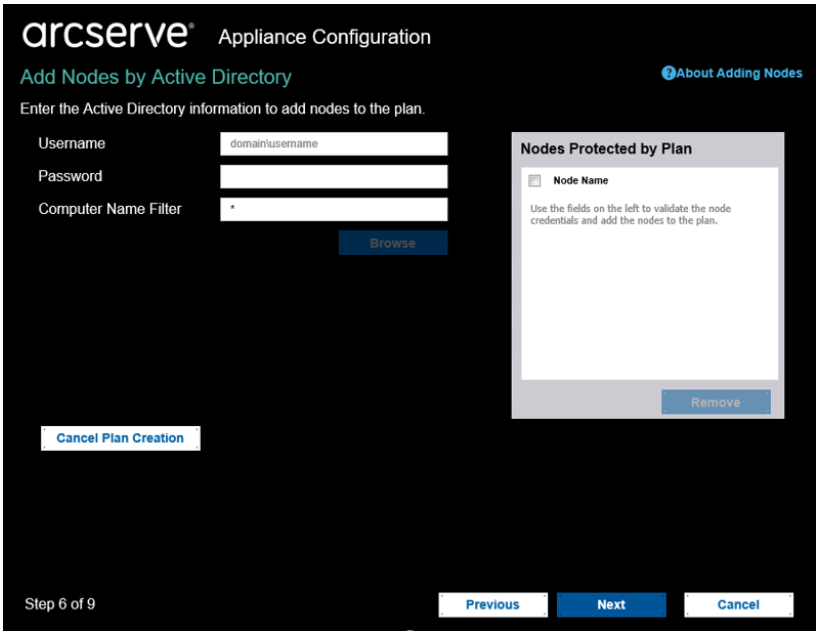
   Specifies the user password.

   Computer Name Filter

   Specifies the filter to discover node names.

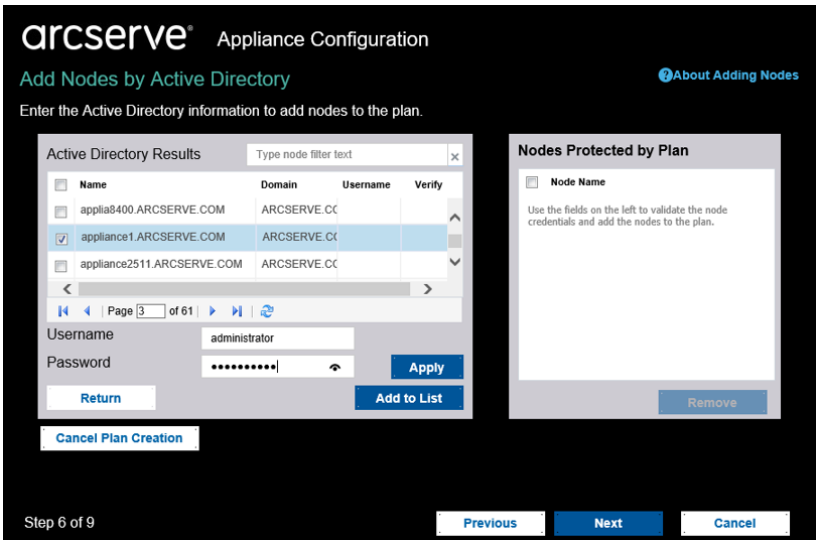
   Cancel Plan Creation

   Cancels the plan that you just created.



2. Click **Browse**.

   The discovered nodes are displayed.



To add nodes, select the nodes and verify.

3. 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.

4. Click **Add to List**.

   The selected node is 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 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

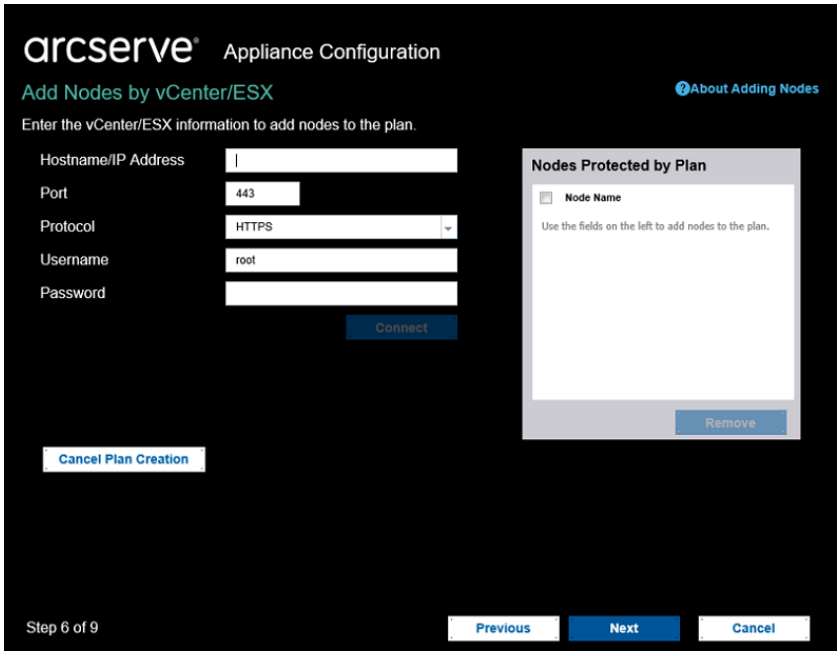
   Specifies a user name of the Server.

   Password

   Specifies the user password.

   Cancel Plan Creation

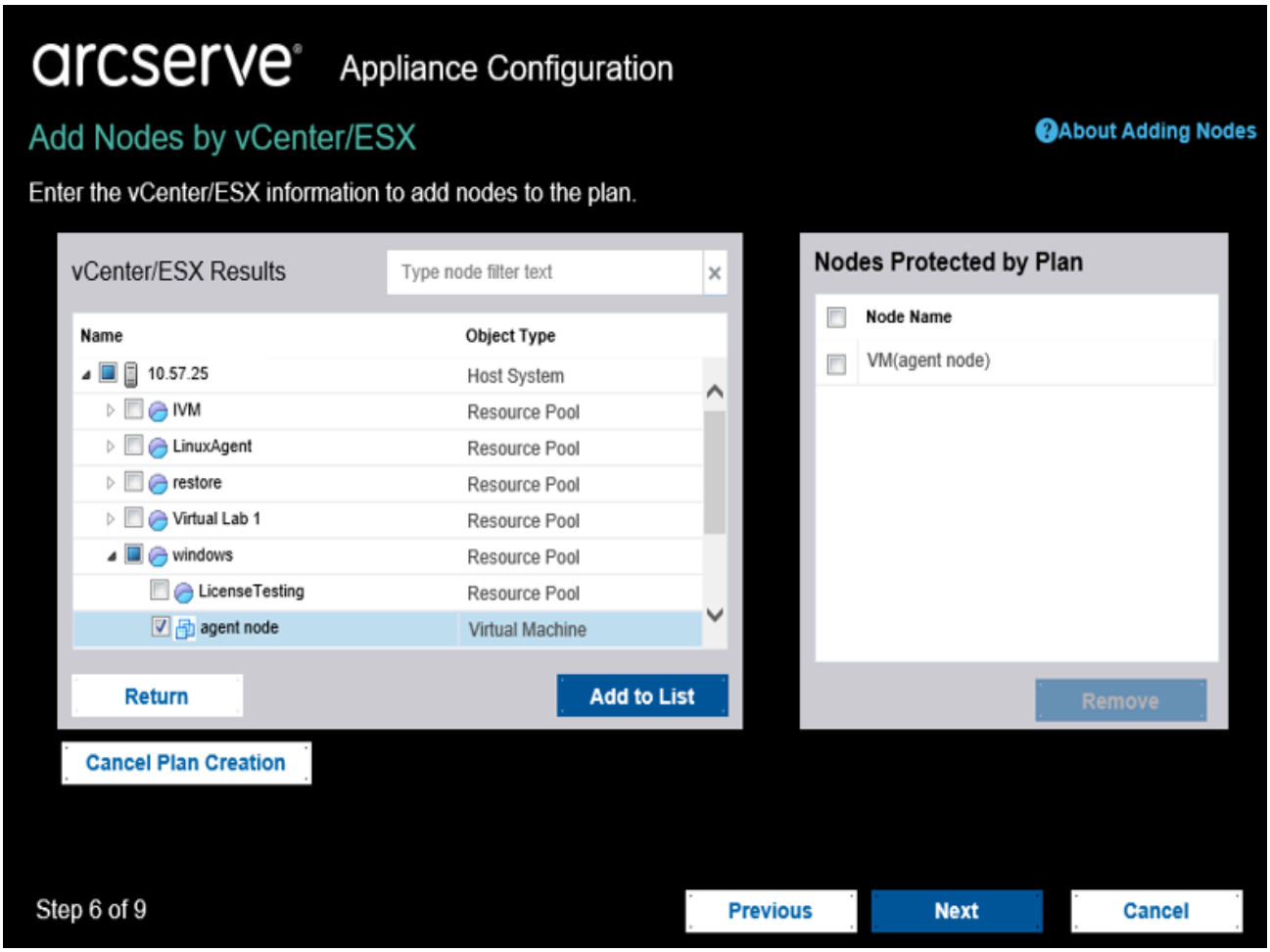
   Cancels the plan that you just created.



2. Click **Connect**.

The discovered hostnames are displayed.

3. Expand a hostname to see the nodes.



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**.

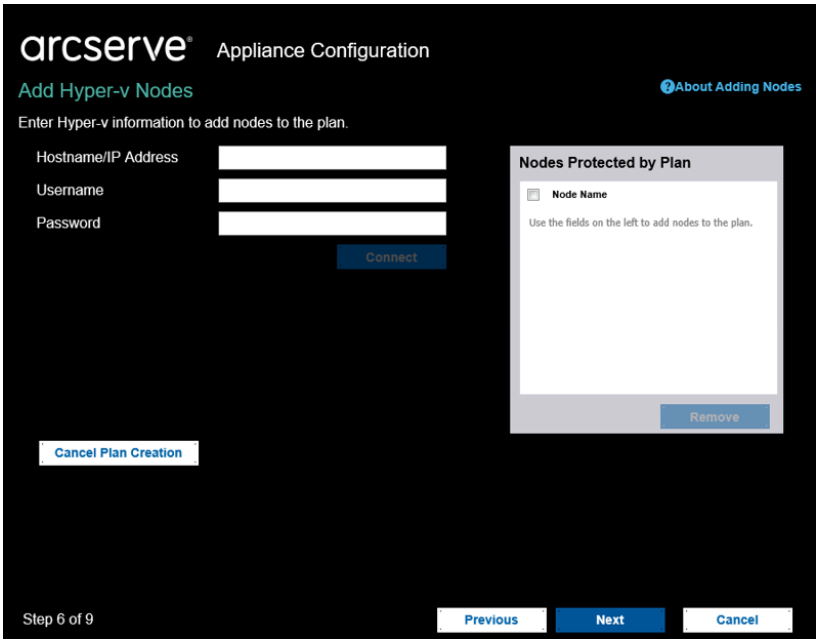
The nodes are added to the plan.

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.



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

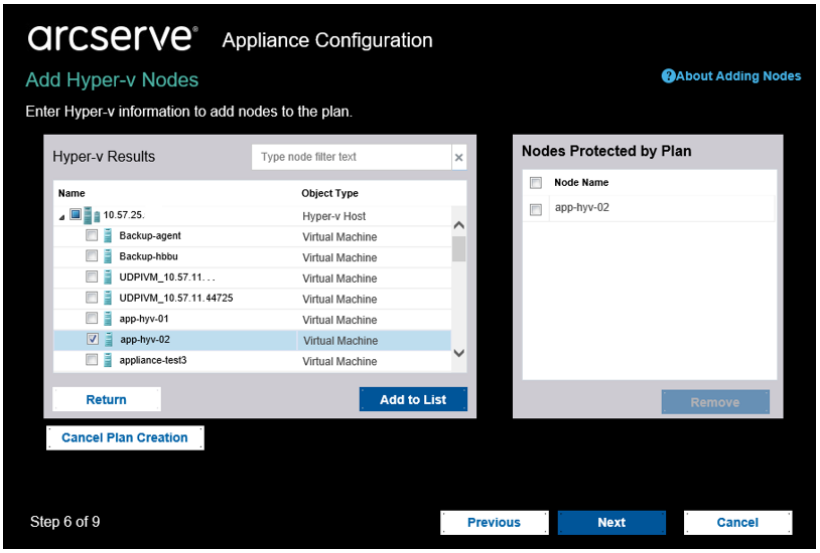
Specifies the password of user name.

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 des-tination 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.

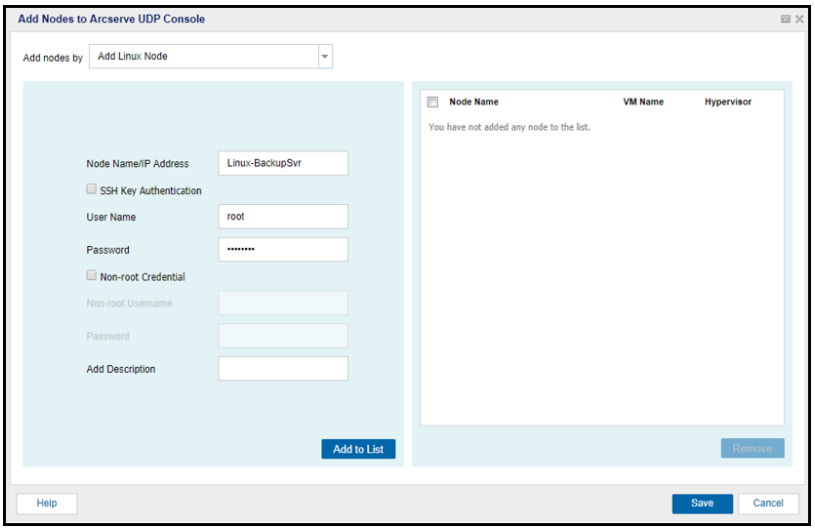
Create Plan to Backup the Linux Backup Server

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

Follow these steps:

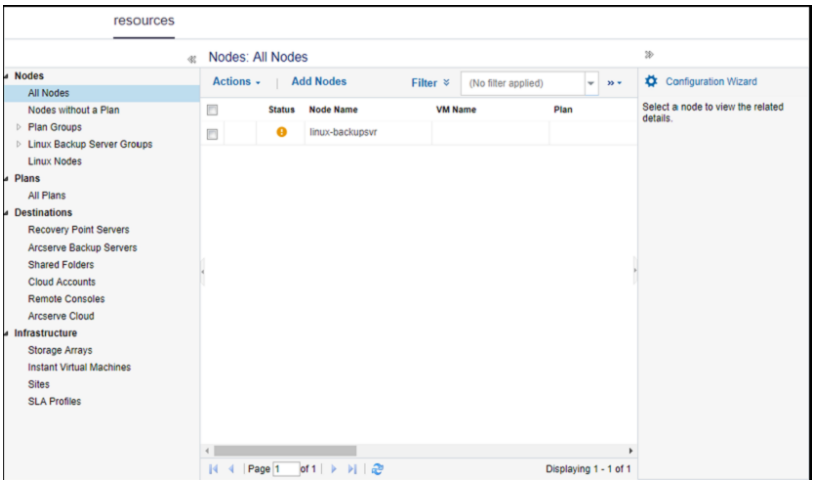
1. From Arcserve UDP Console, click the **resources** tab.
2. Click **All Nodes** in the right pane.
3. From the center pane, click **Add Nodes**.

   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**.



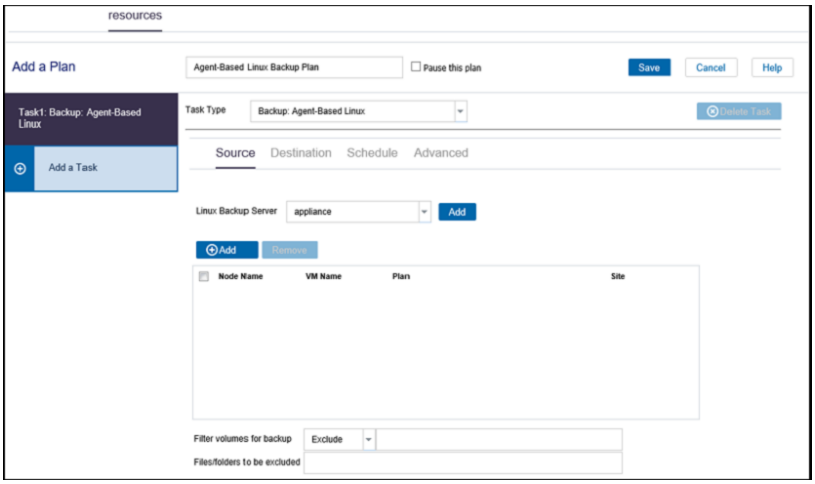
6. Click **Save**.

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

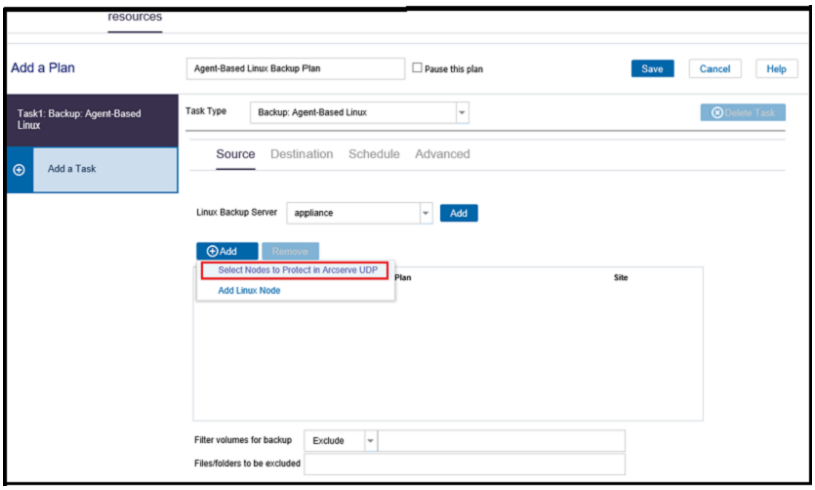


7. Navigate to **All Plans** and create an Agent-based Linux plan.

The **Source** tab appears.

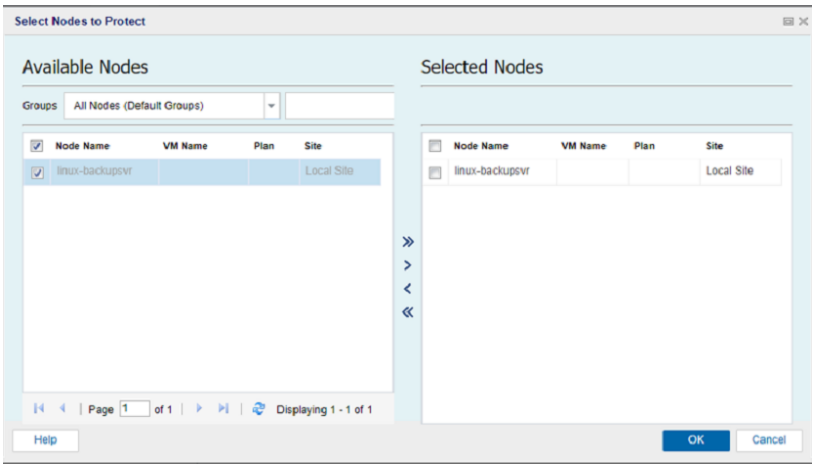


8. From the **Add** drop-down list, select *Select Nodes to Protect in Arcserve UDP*.



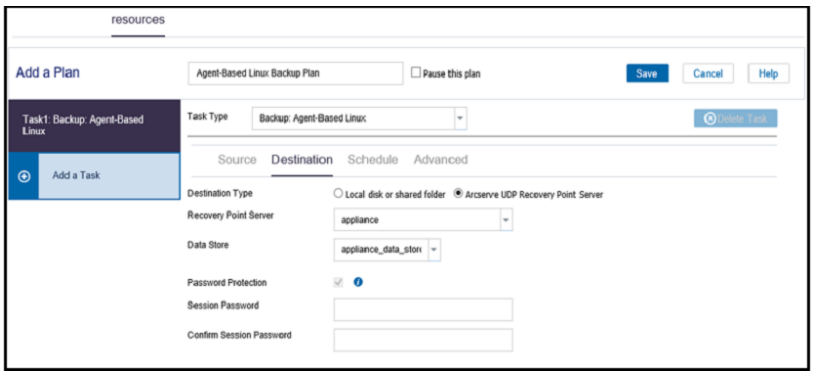
The **Select Nodes to Protect** dialog opens.

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

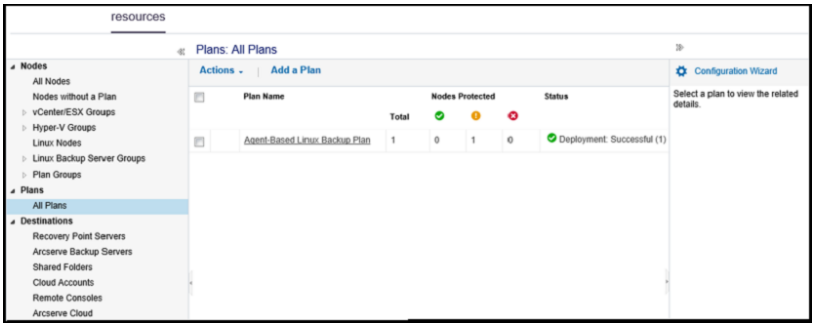


The **Destination** tab appears.

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



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



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. Turn off the Linux Backup Server and add an external switch to the Linux Backup Server.
4. Turn on the Linux Backup Server and add profile to network settings under the new ethernet connection to get an IP address.

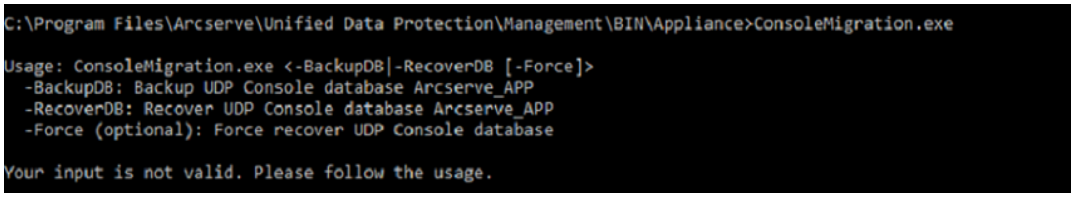
   Note: The Linux Backup Server is rebooted during the process if the IP address is not assigned.
5. To perform Linux instant VM job to local Hyper-V, select the newly added virtual network switch created.

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

Migrate Arcserve UDP Console Using ConsoleMigration.exe

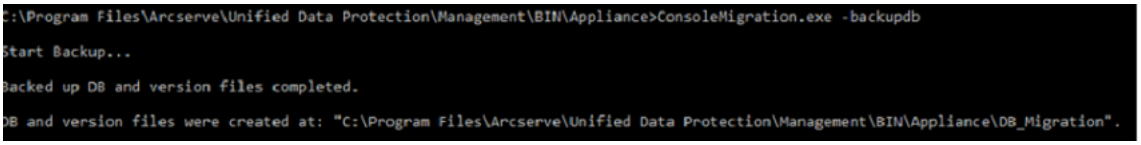
On the Arcserve Appliance, you can migrate the Arcserve UDP Console to another Appliance using *ConsoleMigration.exe*. From Arcserve UDP v6.5 Update 2 onwards, you can migrate the Arcserve UDP Console between any two Arcserve UDP consoles, even when not belonging to Appliance.

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



To complete the migration process, follow these steps:

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

   The *DB_Migration* folder is created successfully.

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

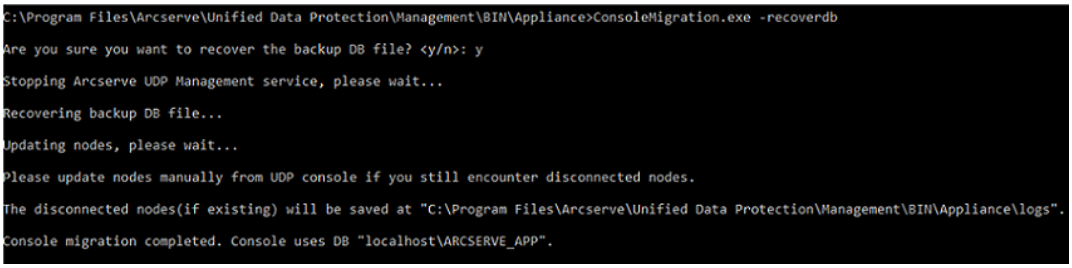
   <UDP_Home> *Management**BIN**Appliance*\

3. If the new Arcserve UDP Console is Arcserve Appliance then change hostname 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.



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 the solution for user to perform migration from existing Arcserve Appliance to another fresh Arcserve Appliance.

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

- Ensure that you can connect to both Appliance one and Appliance two.
- Capacity of the Appliance two should have enough memory to hold all the data on the Appliance one.
- In the Arcserve Appliance one, 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, follow the solution given below.

- Solution

Solution

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:

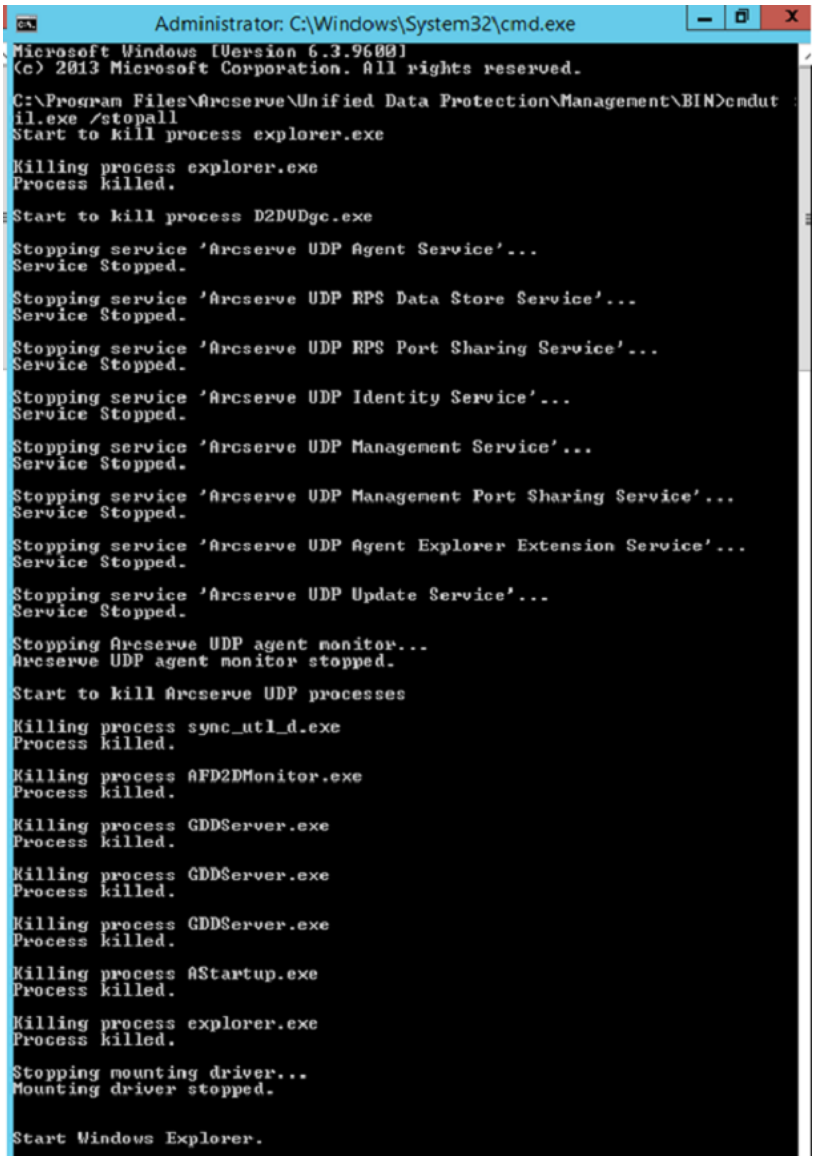
- On Arcserve Appliance one, ensure that no job runs.
- You have migrated the Arcserve UDP Console from Arcserve Appliance one to two.

  Note: For more information about how to migrate the Arcserve UDP Console from Appliance one to two, refer How to Migrate Arcserve UDP Console Using ConsoleMigration.exe.

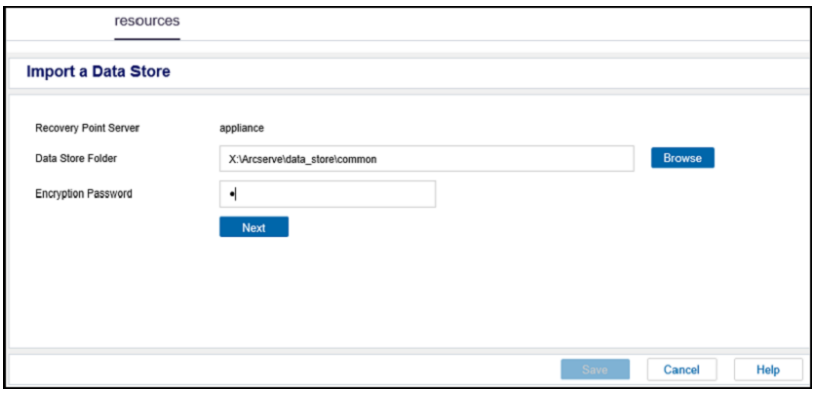
Follow these steps:

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

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



2. Copy all the data on disk X and Y from Arcserve Appliance one to two manually.
3. On Appliance two, start all Arcserve UDP services and then import the data-stores copied from Appliance one.



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

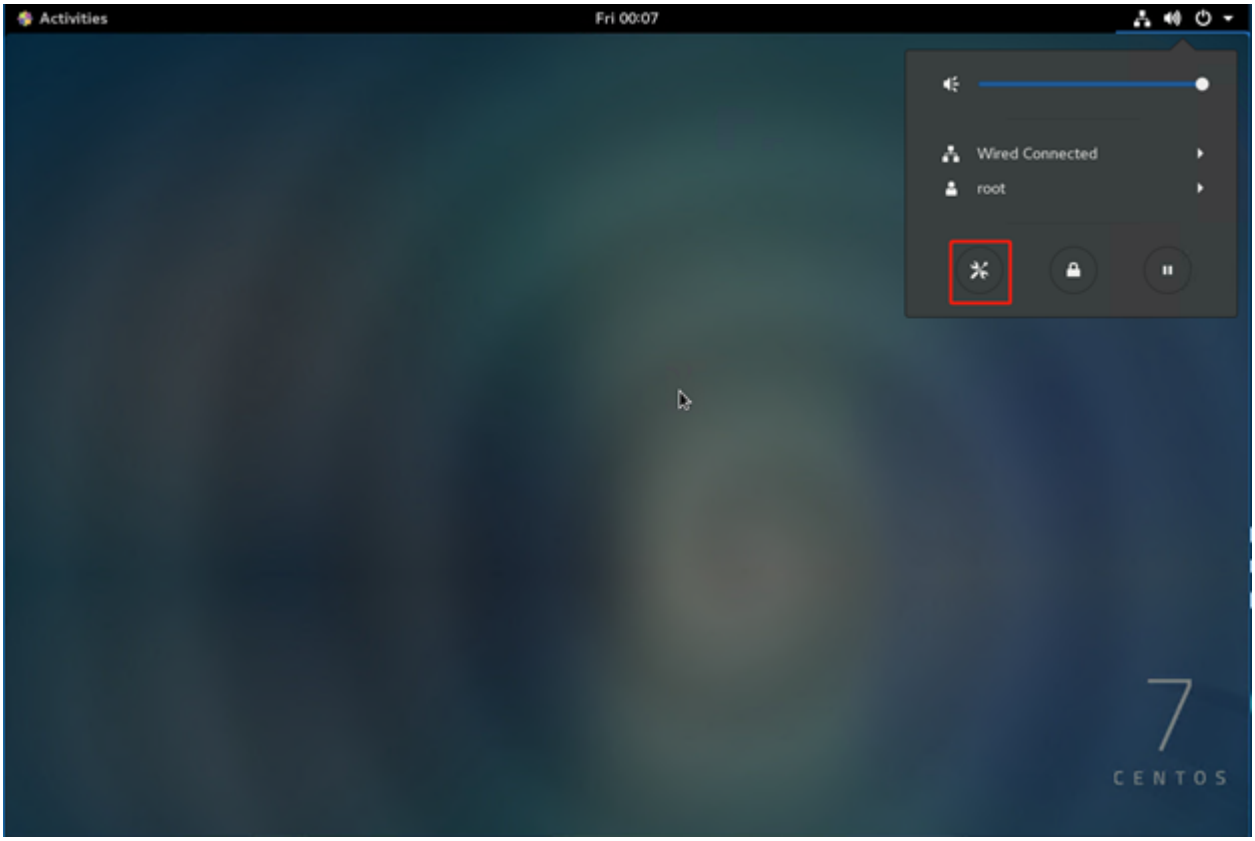
You have migrated the existing Arcserve Appliance to another fresh Arcserve Appliance successfully.

Modify the Input Source of Pre-installed Linux Backup Server

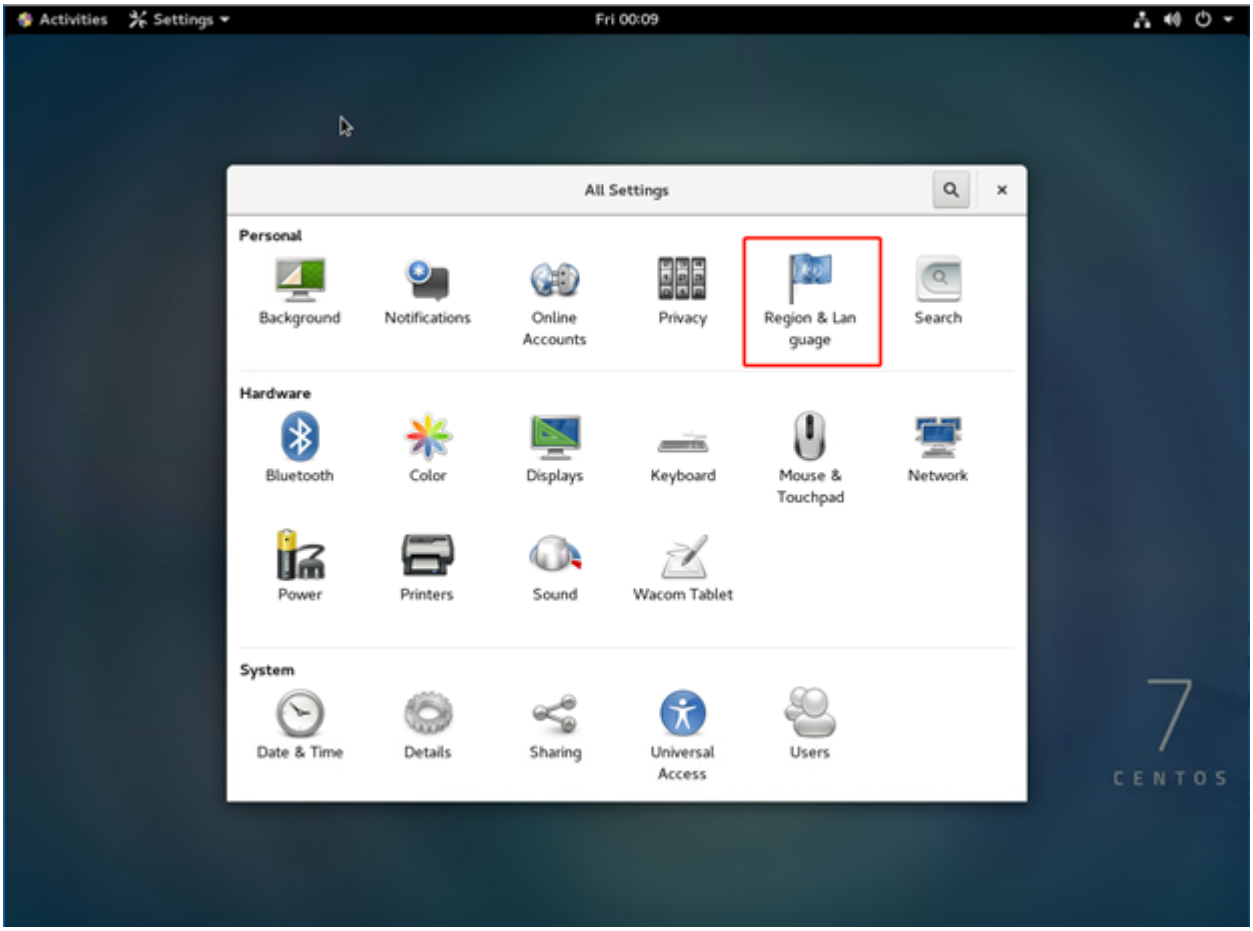
You can change the Keyboard of pre-installed Linux Backup Server.

Follow these steps:

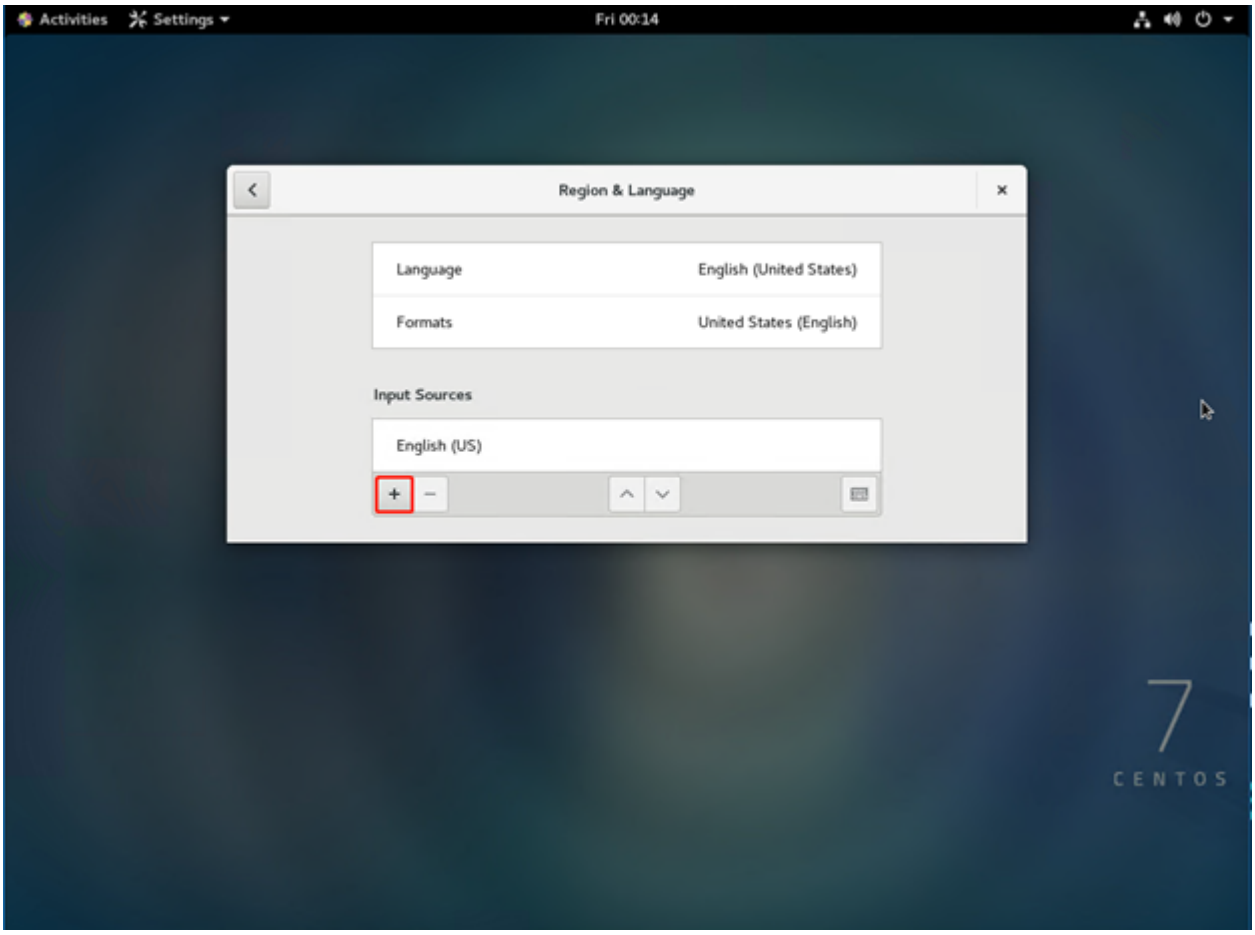
1. Log into Arcserve Appliance as administrator.
2. Click **Settings**.



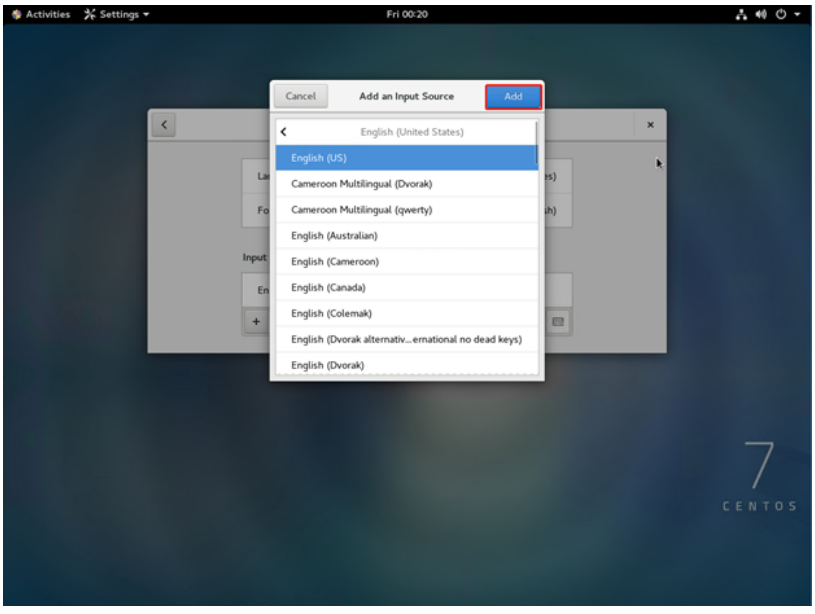
3. Click **Region & Language**.



4. Click **+** to select a new input source.



5. Select the language and keyboard layout.



6. Click **Add**.

   Input source is successfully added.

Chapter 6: 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)

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.

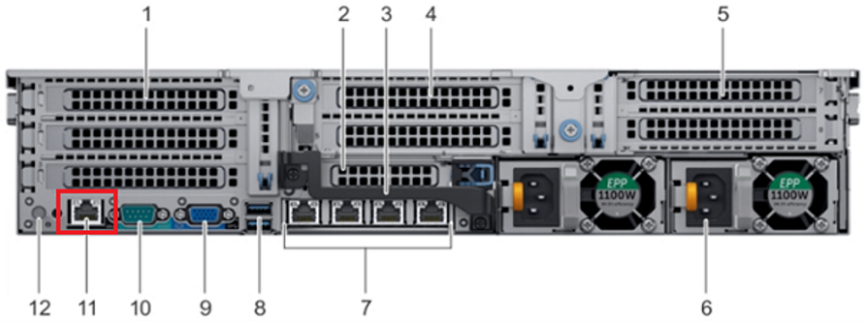
Find the IP address of Integrated Dell Remote Access Controller for 9000 Series (iDRAC)

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 real panel and iDRAC9 dedicated network port of Arcserve Appliance 9012-9504DR series models, see Real panel of 9012-9048, Real Panel 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

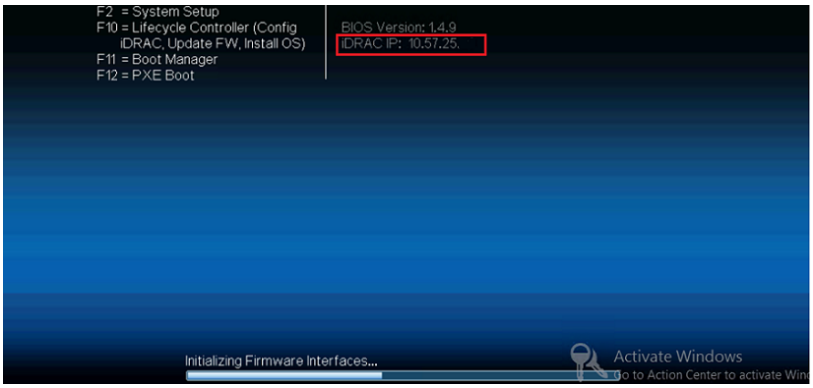


iDRAC9 dedicated network port on
rear panel of Arcserve Appliance 9072DR-9504DR series models

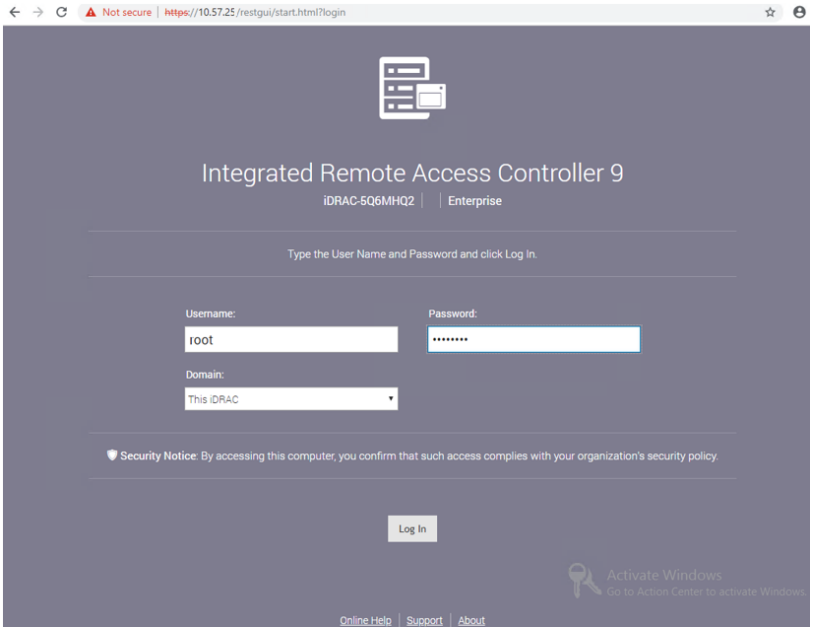
You can find the IP address of iDRAC from appliance.

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)

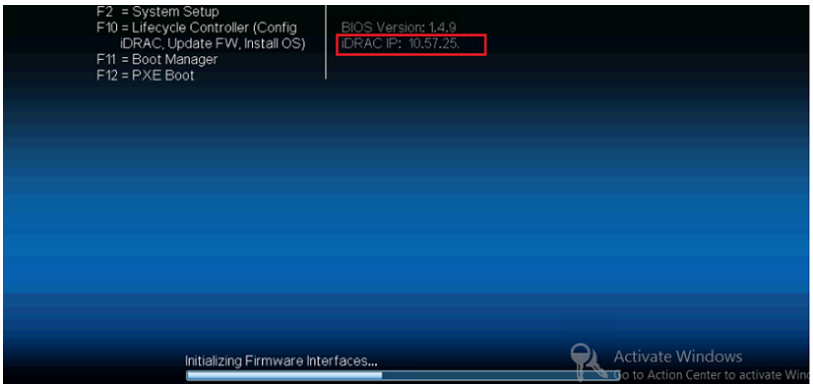
Arcserve Appliance X series model is configured to use DHCP for iDRAC by default. To access iDRAC, ensure that you connect the ethernet cable to the iDRAC9 dedicated network port. For information about real panel and iDRAC9 dedicated network port of Arcserve Appliance X Series model, see Real panel of X Series.

View Rear Panel of X Series

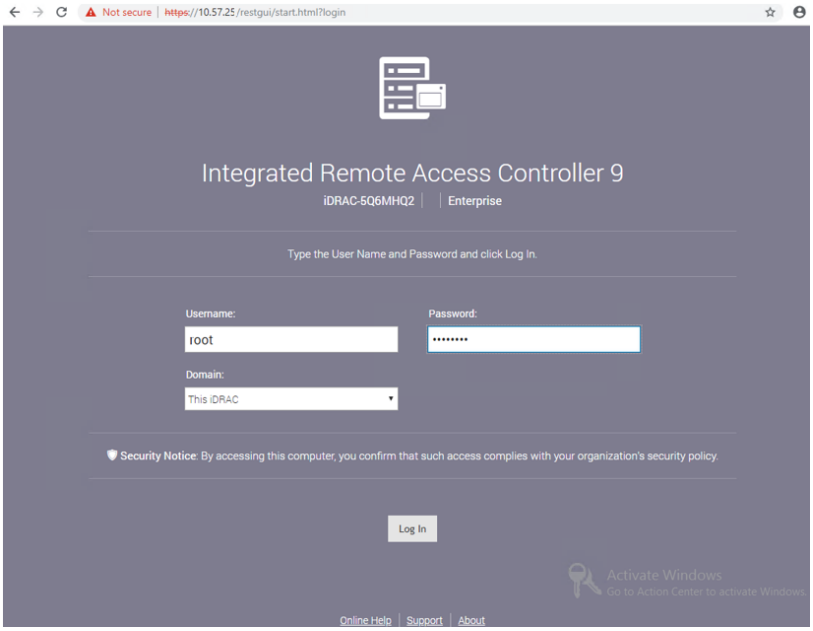
You can find the IP address of iDRAC from appliance.

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>*.



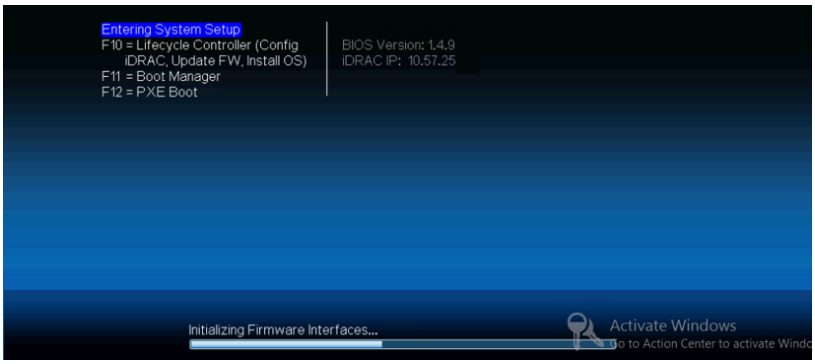
iDRAC login page is displayed.

Configure DHCP or Static IP address of iDRAC

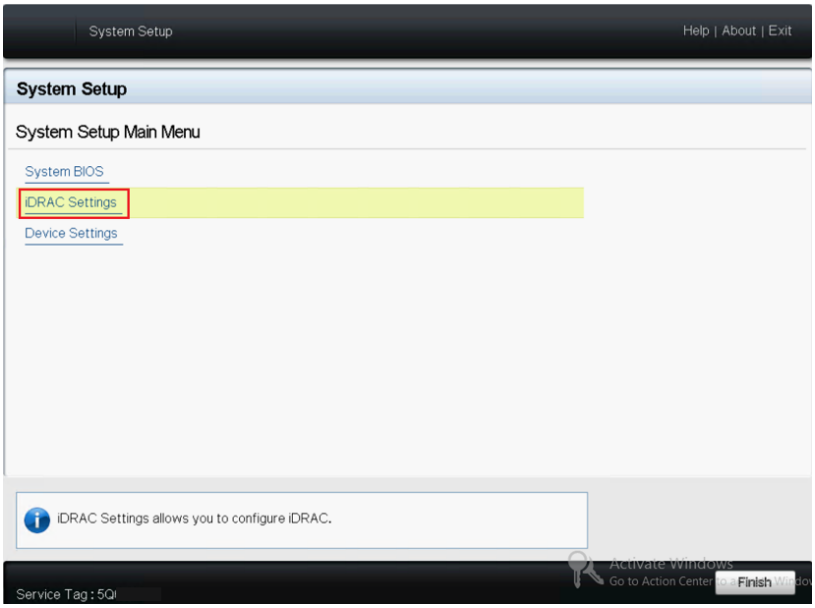
You can set DHCP network mode for iDRAC.

Follow these steps:

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

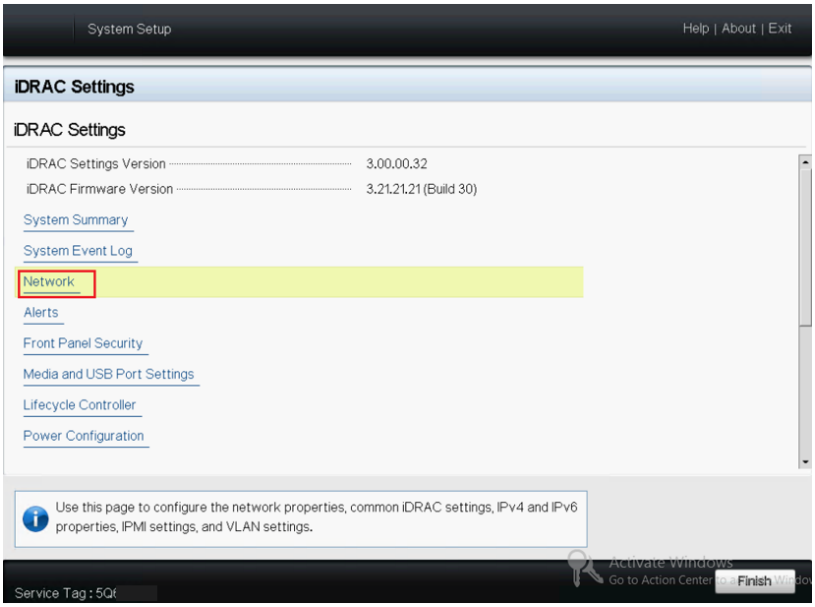


2. From the System Setup Main Menu screen, click i**DRAC Settings**.

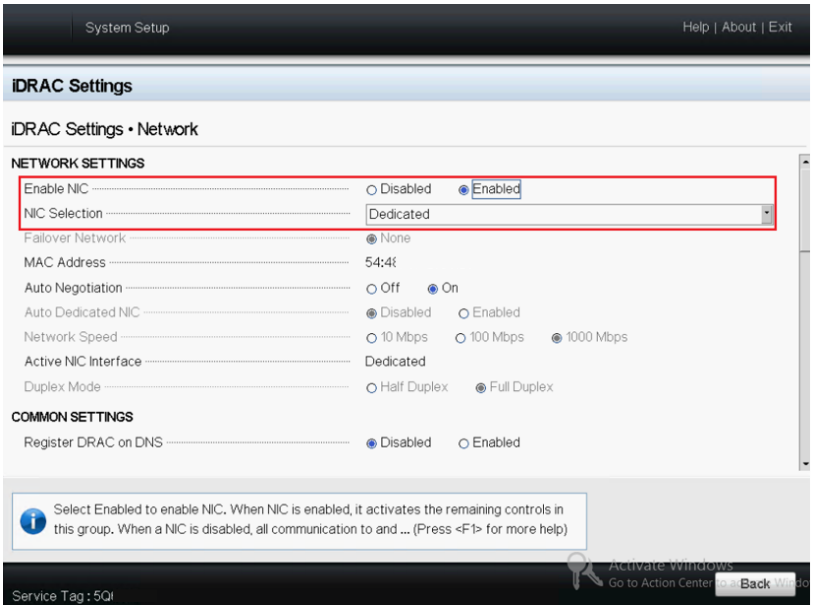


3. From the options of iDRAC Settings, click **Network**.

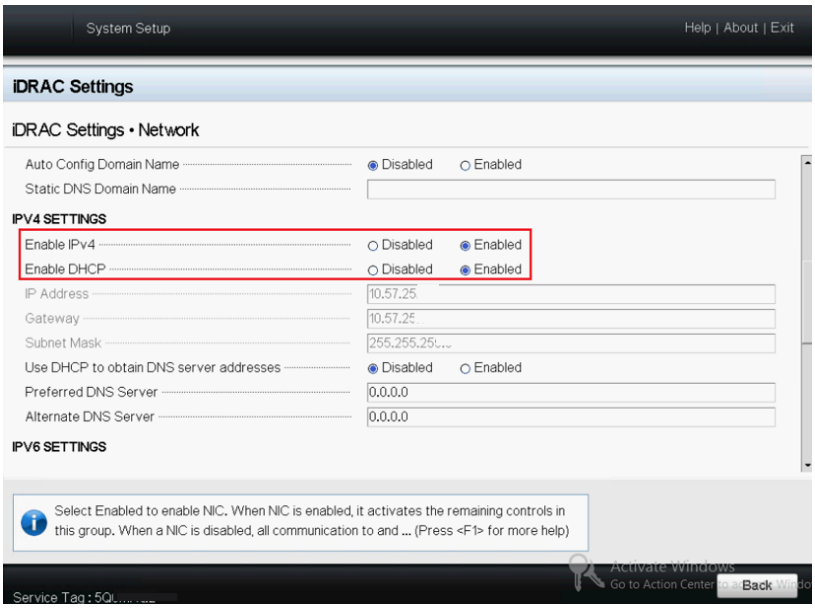
The Network Settings fields are displayed.



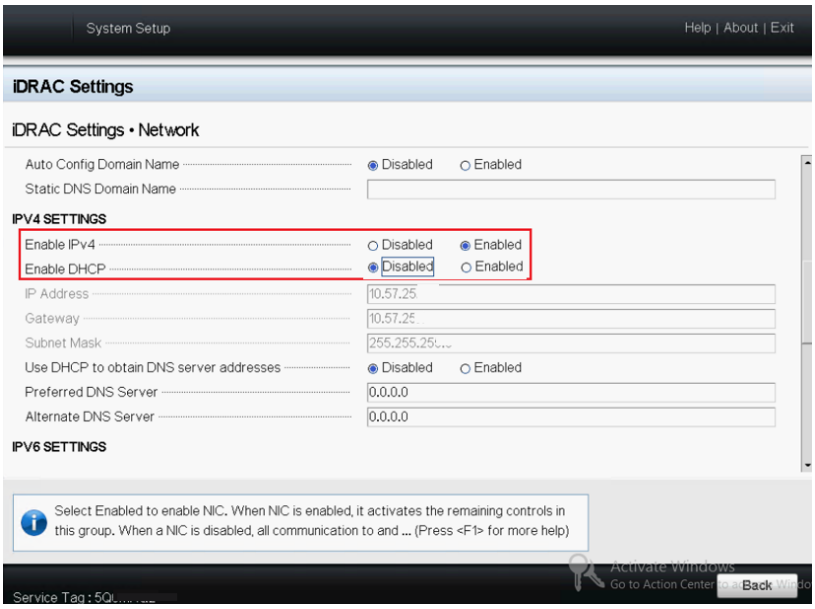
4. Select **Enabled** for **Enable NIC setting**, and select **Dedicated** for **NIC Selection** to use the dedicated network interface.



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

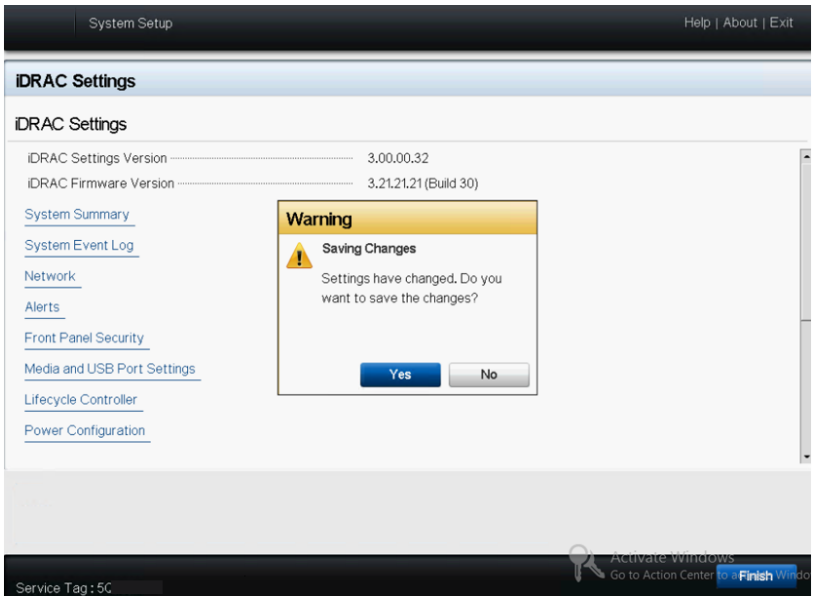


Note: If you want to set Static IP for iDRAC dedicated network, set **Enable IPv4** as **Enabled** and **Enable DHCP** as **Disabled**. Set IP Address, Gateway, and Subnet Mask according to the network configuration.

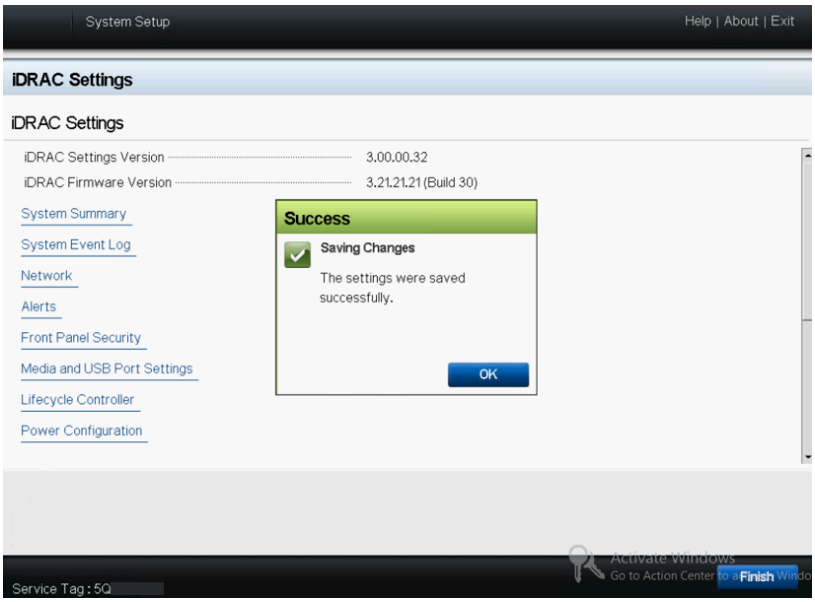


6. Click **Back**, click **Finish**, and then click **Yes** on the **Warning** dialog.

   The network information is saved.

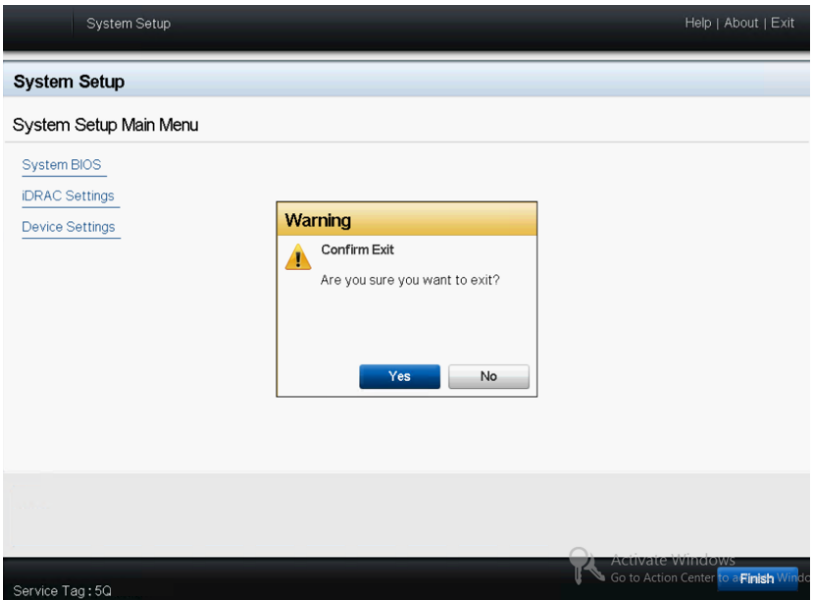


7. From the **Success** dialog, Click **OK**.



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.

Working with Baseboard Management Controller (BMC)

This section contains the following topics:

Monitor and Manage Baseboard Management Controller (BMC)

Arcserve Appliance 10024BU-10576DR series models are installed with Baseboard Management Controller (BMC). BMC lets the server administrators improve the overall availability of Arcserve Appliance.

BMC provides alerts to administrators about server issues, allows to perform remote server management, and reduces the need for physical access to the server. It also provides remote access to multiple users from different locations for system maintenance and management.

To monitor the system status, manage system information and launch remote console, you must log into the Intelligent Platform Management Interface (IPMI).

Follow these steps:

1. Open a web browser and enter the BMC IP address in the following format:

   https://BMC-IP-address.

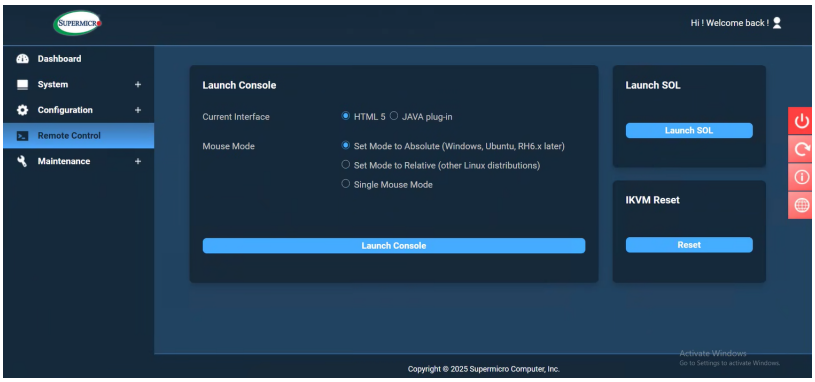
   The login screen appears.

2. Type the login credentials as follows:
   - **Username:** ADMIN

     Note: The username must be in caps.
   - **Password:** Type the BMC password

     Note: You can find the BMC unique password in the pull-out tag on the front panel of the server. The BMC password is listed in the bottom row just below the BMC/IPMI MAC Address.

3. Click **Login**.
4. Navigate to **Remote Console** and then click **Launch Console**.



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

You can also monitor the BMC 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

How to Find the IP address of BMC

Arcserve Appliance 10024BU-10576DR series models are configured to use DHCP for BMC by default. To access BMC, ensure that you connect the ethernet cable to the BMC dedicated network port. For information about real panel and BMC dedicated network port of Arcserve Appliance 10024BU-10576DR series models, see Rear Panel 10024BU-10048BU, and Rear Panel 10048DR-10576DR.

You can find the IP address of BMC in the following ways:

Find the IP address using BIOS

This section provides instructions on how to find the IP address using BIOS.

Follow these steps:

1. Power-On the Appliance server.
2. During the system boot up, click the **Del** key to invoke BIOS menu.
3. Navigate to **Server Management** tab and then select **BMC Network Configuration.**

   The *BMC Network Configuration* screen appears.

   You can view the IP address on the *IPV4 Station IP address* parameter. You can also change the DHCP issued IP address to the desired static IP address. For more information, see Configure BMC IP address using BIOS.

Find the IP address in POST screen

This section provides instructions on how to find the IP address in POST screen.

Follow these steps:

1. Power-On the Appliance server.
2. Initiate the system boot up.

   The POST screen appears.

   You can find the IP address on the lower-right corner of the POST screen.

Configure the DHCP or Static IP Address of BMC

This section provides information about how to configure UEFI BIOS and the IP address of BMC.

Configuring UEFI BIOS

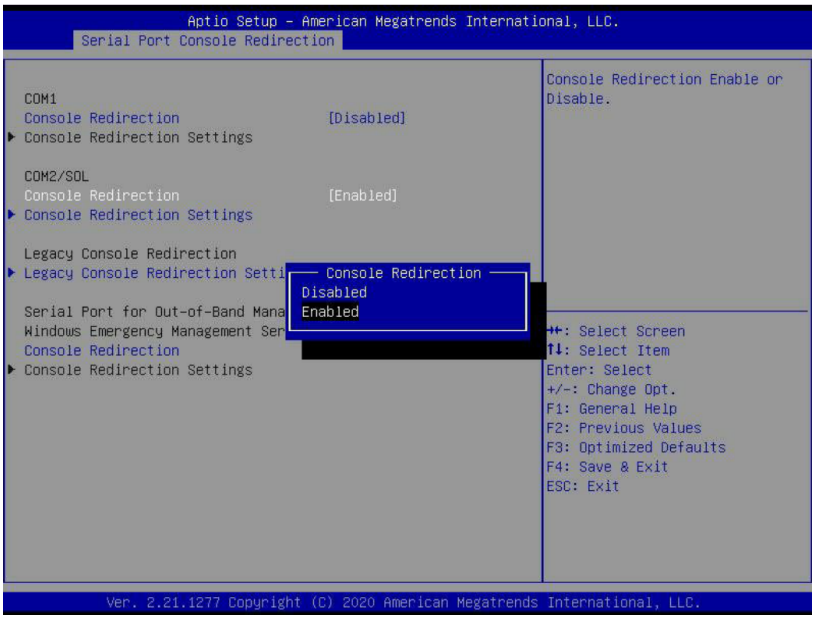
This section provides information about how to configure UEFI BIOS.

Note: Before configuring BMC, you must configure BIOS on the monitor directly connected to the Arcserve appliance server. You can perform this process within the BIOS of the BMC only.

Follow these steps:

1. Power-On the Arcserve Appliance Server.
2. During the system bootup, click the **Del** key to enter the BIOS.

   Note: To navigate through the BIOS, use the arrow keys. To select, press the **Enter** key, and to return to the previous screen, press the **Esc** key.
3. Select the **Advanced** tab from the BIOS setup menu.
4. Select **Serial Port Console Redirection** and press the **Enter** key.
5. Navigate to **Console Redirection** under COM2/SOL, press the **Enter** key and select **Enabled**.



6. Press the **F4** key to save and exit.

The BIOS is configured successfully.

Configuring the IP Address of BMC

This section contains the following topics:

Configure the DHCP IP Address using the DHCP Server

This section provides instructions on how to configure the DHCP IP Address using the DHCP server

Follow these steps:

1. On the Appliance server, find the pull-out ID tag with MAC address bar-code.
2. Use the MAC address value to set a known registered DHCP IP address with the DHCP server.

You can view the IP Address from POST screen or BIOS. For more information, see How to Find IP Address of BMC.

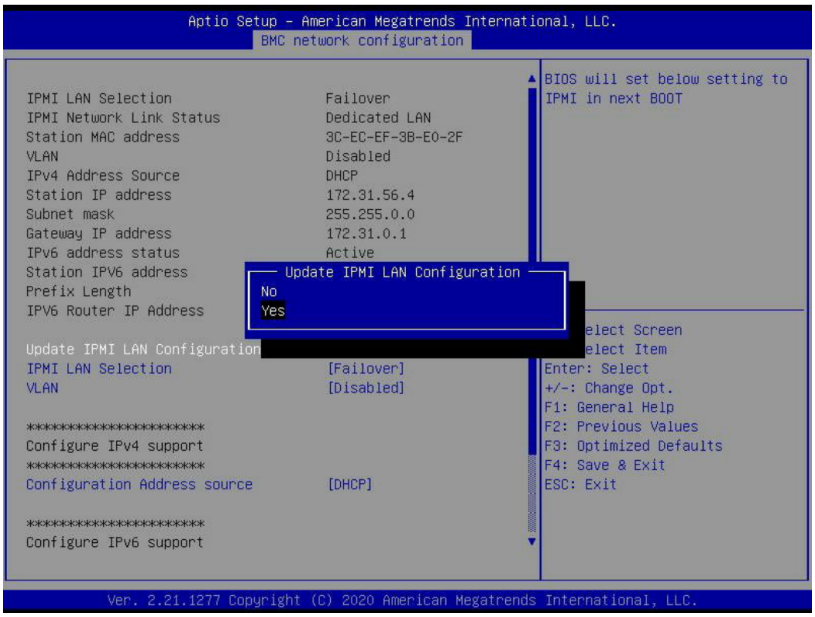
Configure the Static IP Address using BIOS

This section provides instructions on how to configure the Static IP Address using BIOS.

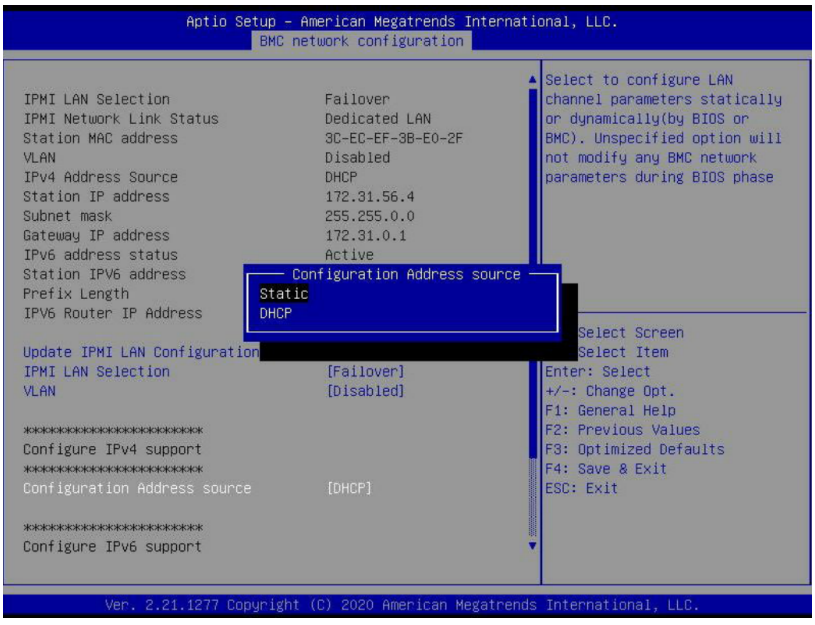
Follow these steps:

1. Power-On the Arcserve Appliance Server.
2. During the system bootup, click the **Del** key to enter the BIOS.
3. Navigate to the **Server Management** tab > **BMC Network Configuration**, and then press the **Enter** key.

The *BMC Network Configuration* screen appears.

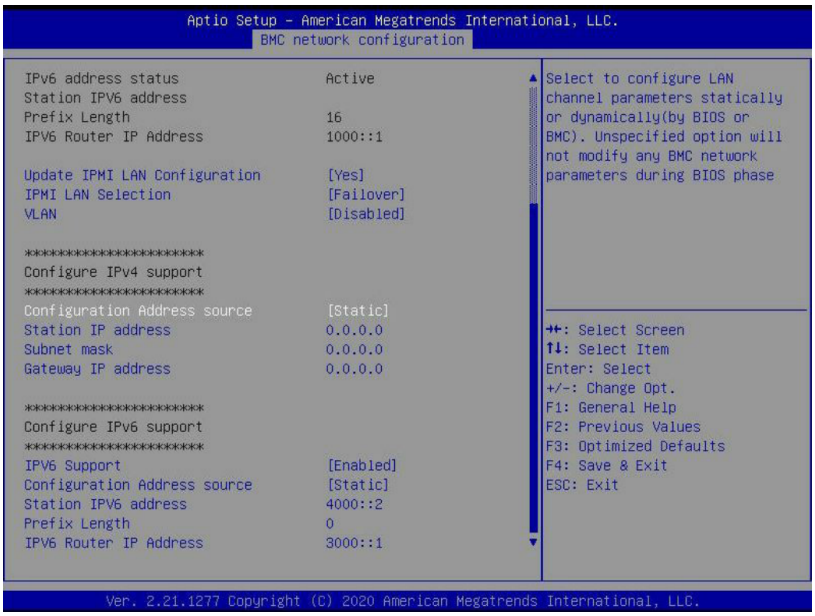


4. Select **Update IPMI LAN Configuration**, press the **Enter** key, and then select **Yes**.
5. Select **Configuration Address source**, press the **Enter** key, and then select **Static**.



After the Configuration Address source is set to Static, you can update the values 0.0.0.0 in the fields of the Static IP Address, Subnet Mask, and Gateway IP Address.

6. Enter the desired values for the Static IP Address, Subnet Mask, and Gateway IP Address, and then press the **Enter** key.



7. Press the **F4** key to save and exit.

The BMC Static IP Address is configured successfully.

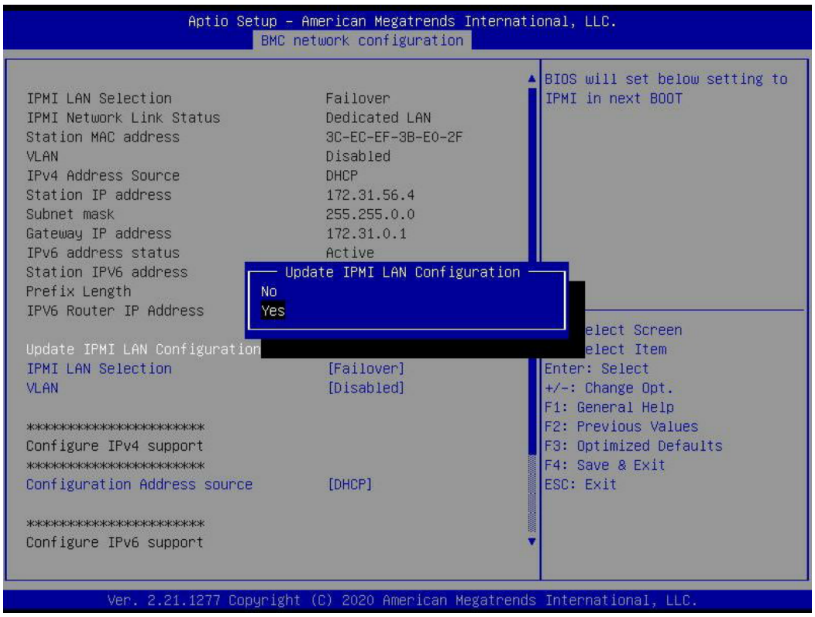
Connecting to BMC using BIOS

To connect to BMC and invoke BIOS menu on your device, connect one end of an Ethernet cable to the laptop or device's Ethernet port. Then plug the other end of the cable into the server's IPMI or SHARED port. Now the BMC and the device is connected to the same network connection.

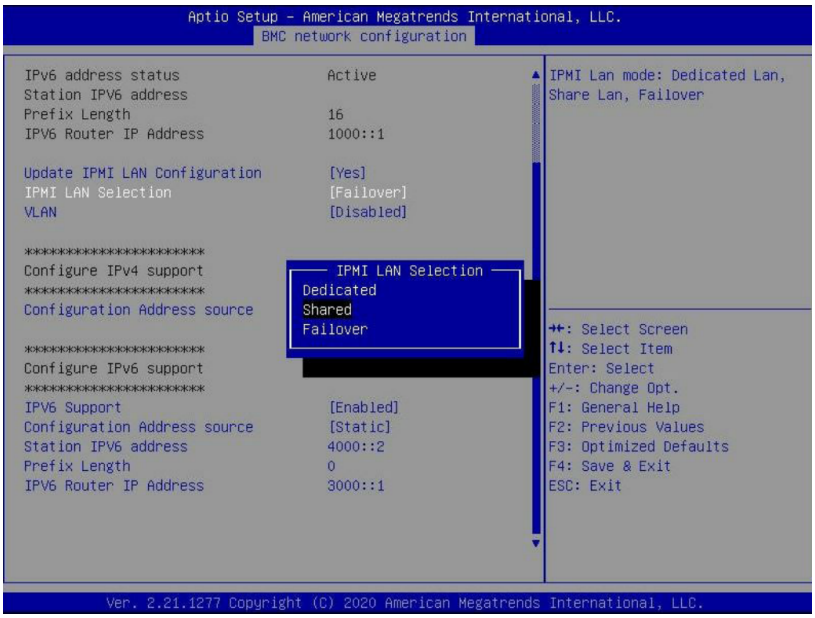
Follow these steps:

1. Power-On the Arcserve Appliance Server.
2. During the system bootup, click the **Del** key to enter the BIOS.
3. Navigate to the **Server Management** tab > **BMC Network Configuration**, and then press the **Enter** key.

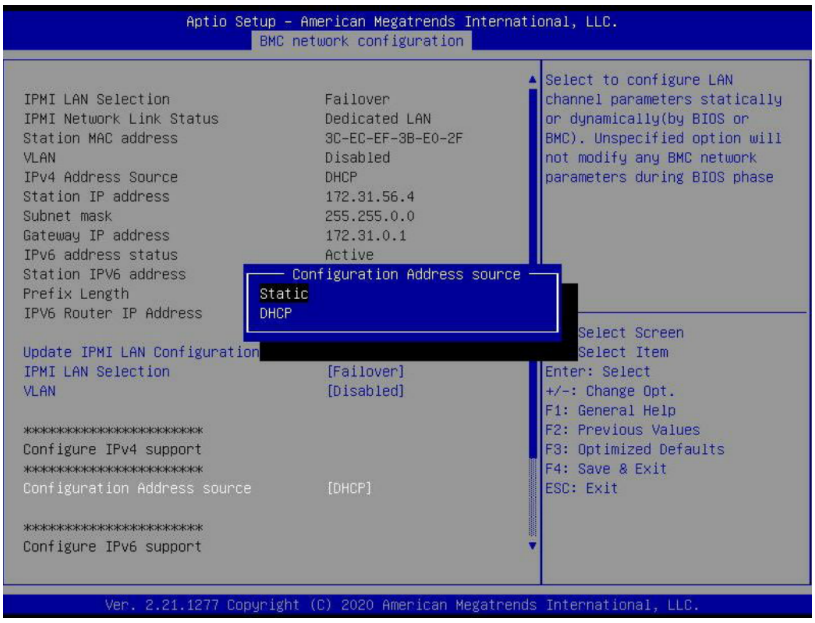
   The *BMC Network Configuration* screen appears.
4. Select **Update IPMI LAN Configuration**, press the **Enter** key, and then select **Yes**.



5. Select **IPMI LAN Selection**, press the **Enter** key, and then select **Shared**.

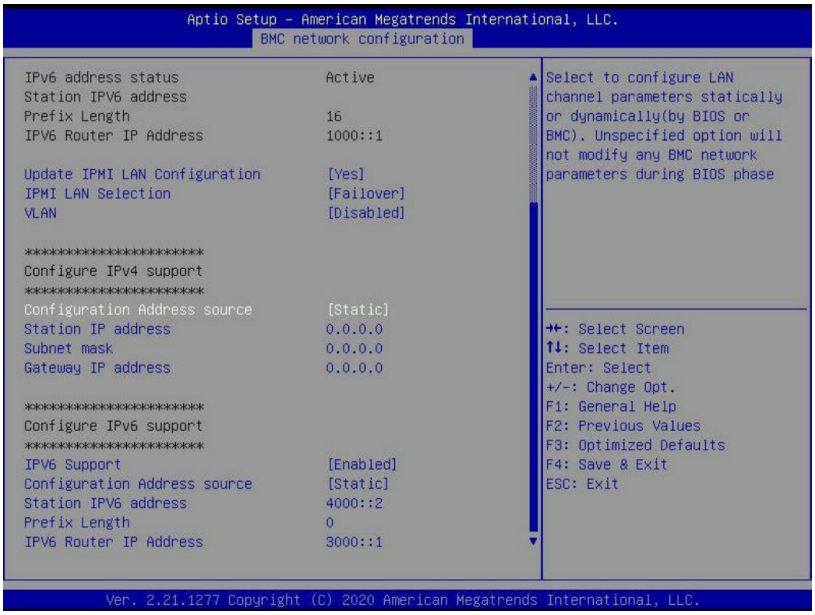


6. Select **Configuration Address source**, press the **Enter** key, and then select **Static**.



After the Configuration Address source is set to Static, you can update the values 0.0.0.0 in the fields of the Static IP Address, Subnet Mask, and Gateway IP Address.

7. Enter the desired values for the Static IP Address, Subnet Mask, and Gateway IP Address and then press the **Enter** key.



8. Press the **F4** key to save and exit.

The device is connected to BMC successfully.

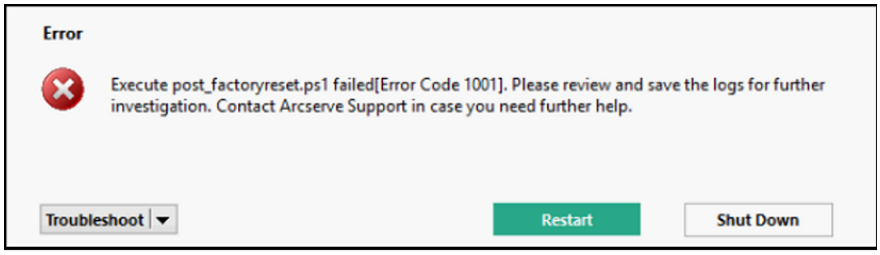
Chapter 7: Restoring or Repairing the Arcserve Appliance

This section contains the following topics:

Debug Factory Reset 118

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

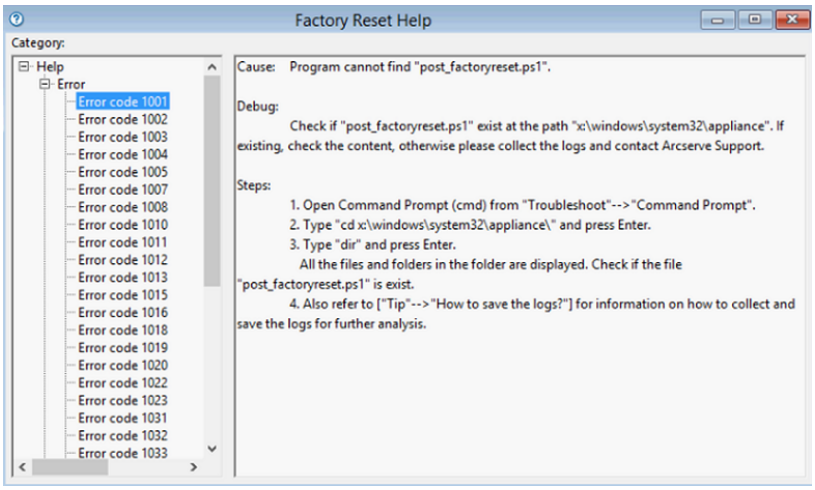
   This option lets you restart Factory Reset when the issue is esolved.

   Help

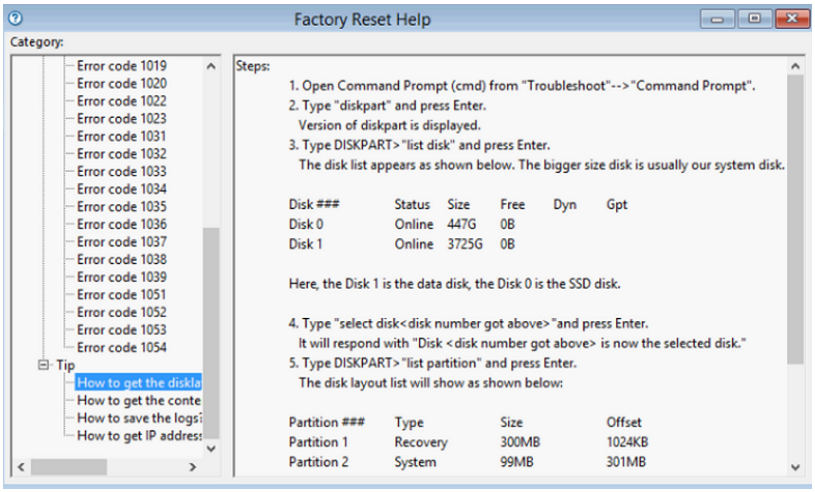
   The Help Dictionary dialog box provides information about the cause, basic analysis, and solutions for the error. Follow the steps to resolve the issue. Some tips about common operations are also displayed. For example, how to get the disk layout, how to get the content of factory reset property file,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

Installing the Arcserve Appliance

This section contains the following topics:

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.

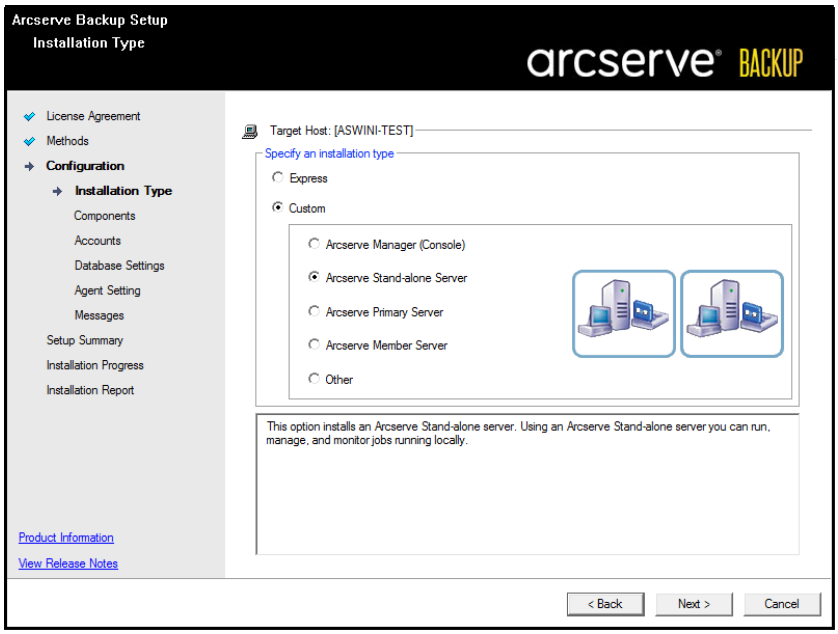
   Note: The setup program for cluster machines does not support remote installation of the Arcserve Backup base product or the Arcserve Backup agents. This remote install limitation for the Arcserve Backup agents (for example, the Agent for Microsoft SQL Server and the Agent for Microsoft Exchange Server) 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 Installation/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.

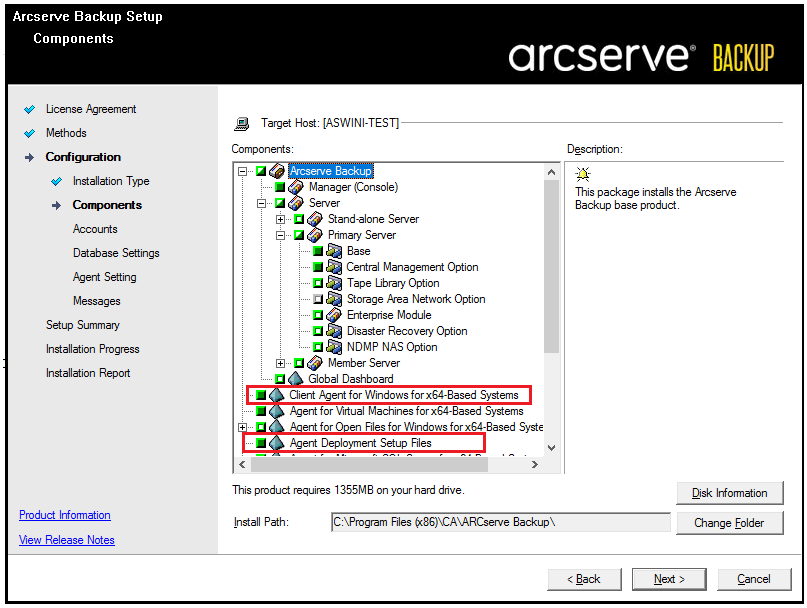
Be aware of the following considerations:

- 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:

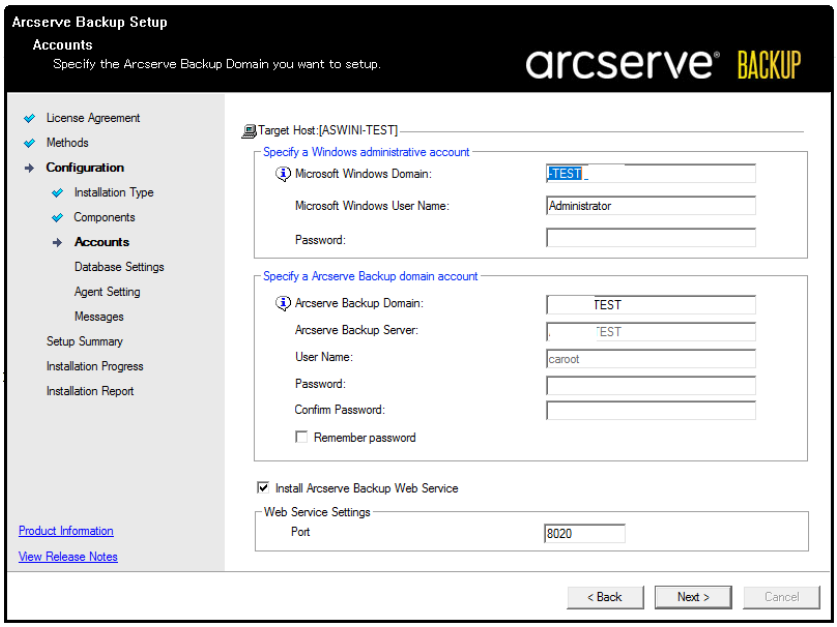


Accounts dialog

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.



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.
2. In the command prompt type the following command:

   Bconfig –c

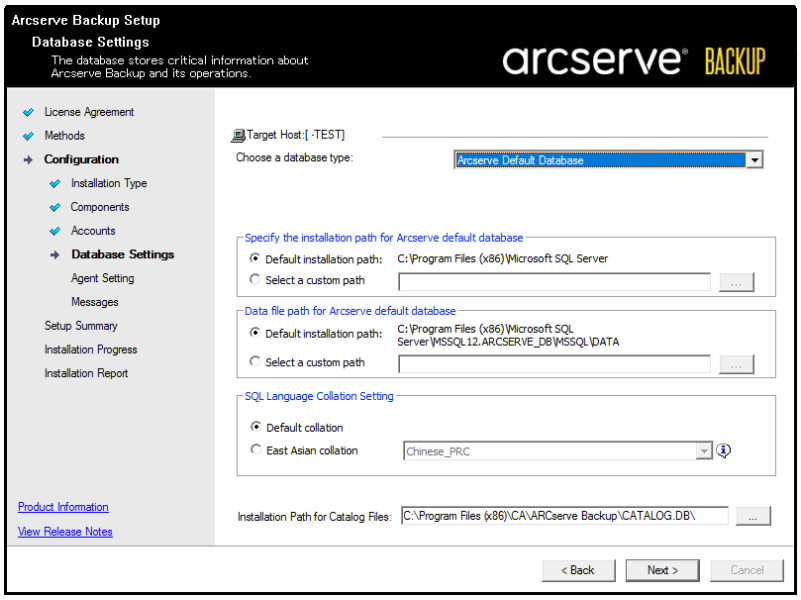
   <Arcserve Backup> Accounts dialog opens.
3. Configure or update the web service.

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.

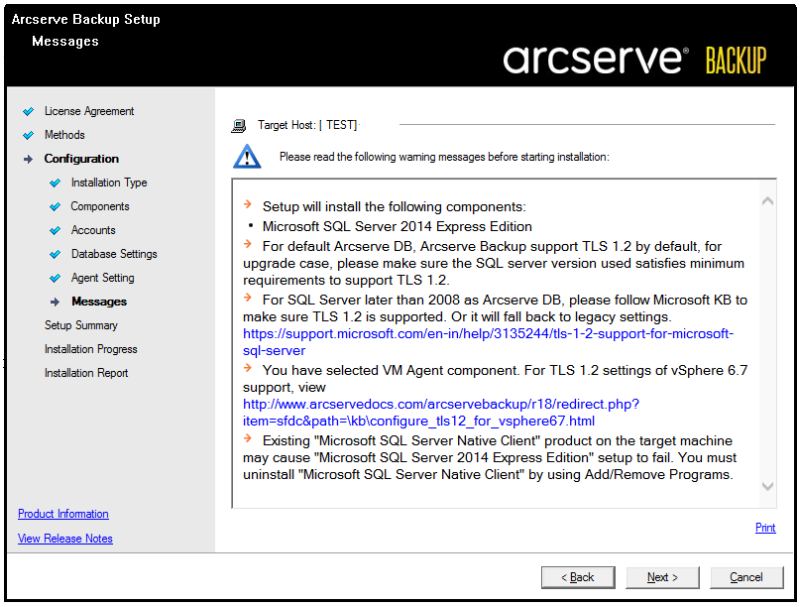
Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that Arcserve Backup can search and sort the data. To do this, click East Asian collation and then select a language from the drop-down list.



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:



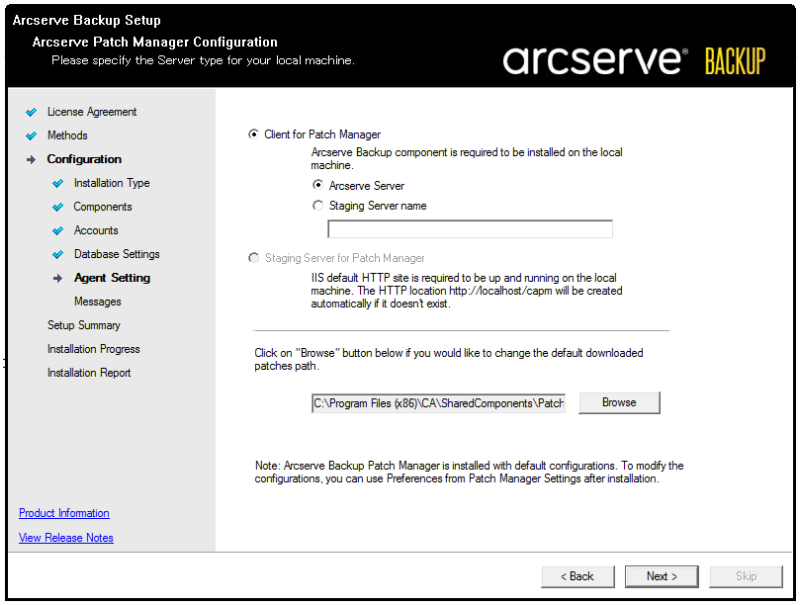
Setup Summary dialog

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 10024BU-10048BU 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 10024BU-10048BU.

How to Install 10048DR-10576DR 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 10048DR-10576DR.

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.

Apply Arcserve UDP Factory Reset in 10024BU-10576DR Series Appliance

This section provides information about how to perform factory reset in 10000 series appliance.

Using the UDP Factory Reset option, you can return your Arcserve Appliance 10000 series to clean and non-configured status.

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

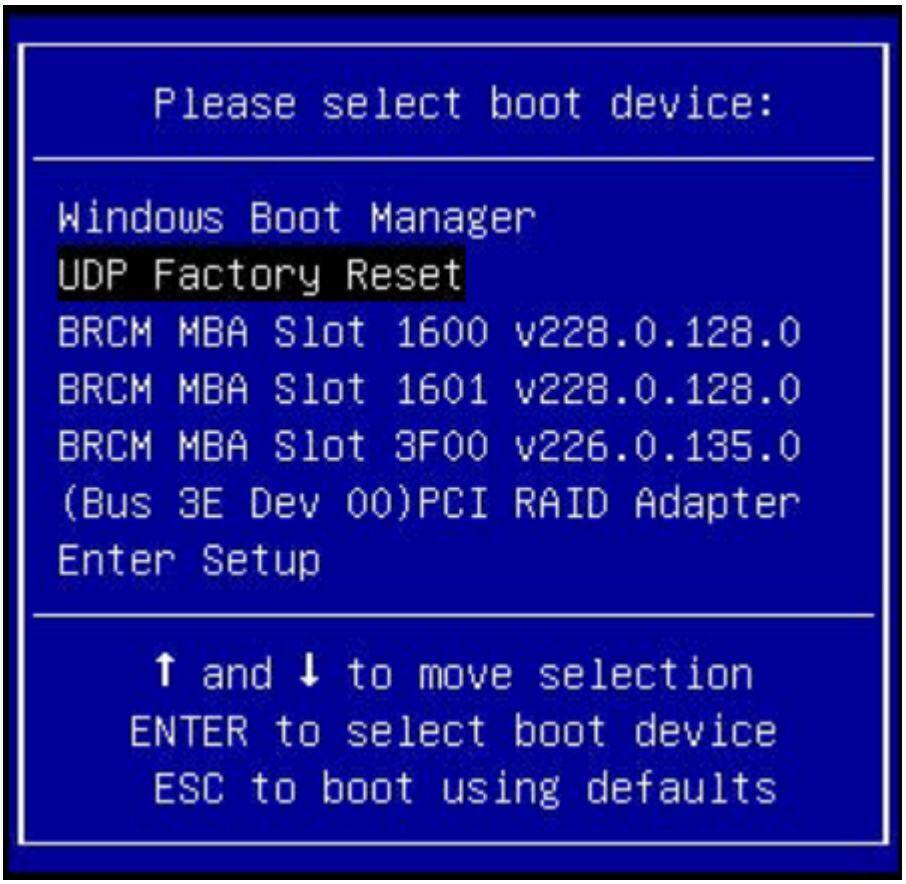
Use one of the following two ways to perform factory reset for 10000 series appliance:

Factory Reset from BIOS

This section provides information about how to perform UDP factory reset from BIOS.

Follow these steps:

1. Power-On the Arcserve Appliance.
2. Press **F11** key on keyboard to invoke Boot Menu.
3. Select the **UDP Factory Reset** boot option.



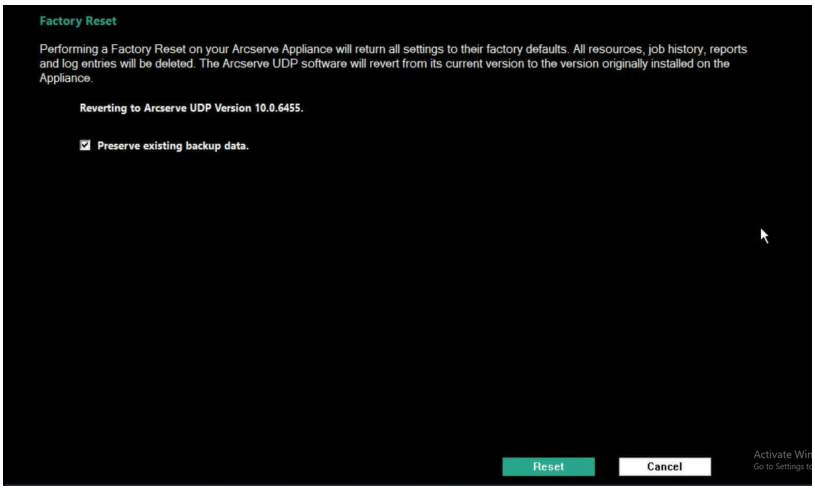
The Factory Reset wizard appears.

4. Click **Reset**.

Notes:

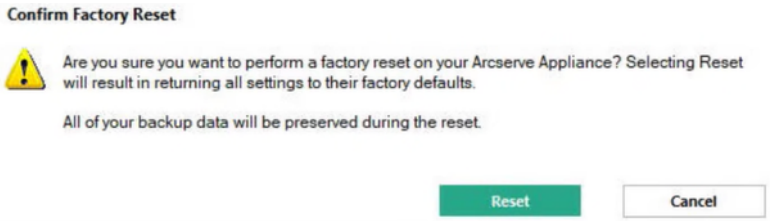
- The **Preserve existing backup data** checkbox is selected by default. All the backup data is preserved during the reset. Only C:\ volume in the original operating system is rebuilt.

- If you uncheck the **Preserve existing backup data** checkbox, all the backup data is deleted during the reset. The data on the respective volumes of C:\, X:\, and Y:\ in the original operating system is rebuilt.

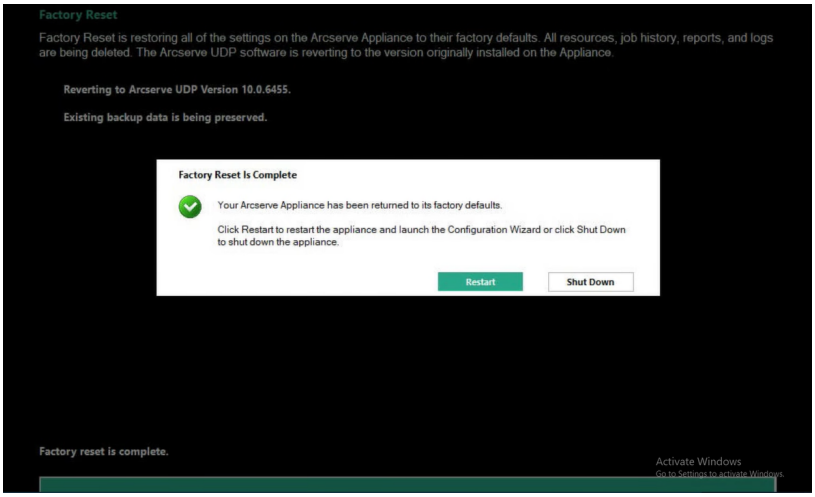


A confirmation dialog appears.

5. To perform factory reset, click **Reset**.



6. After the factory reset is completed, you can perform one of the following actions:
   - To reboot the appliance, click **Restart**.
   - To close the appliance, click **Shut Down**.



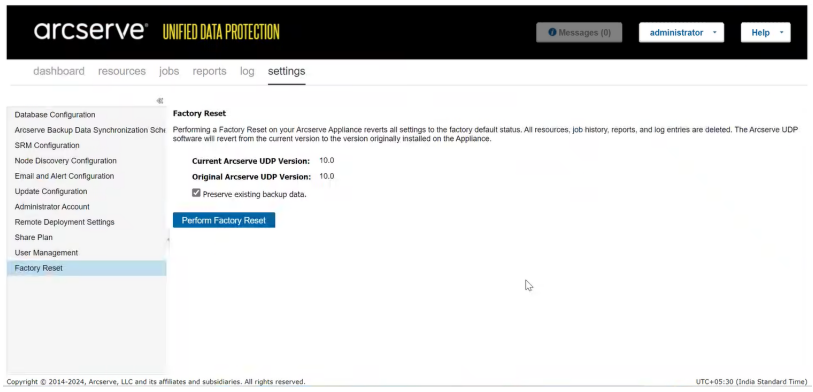
The factory reset from BIOS for 10000 series appliance is successfully completed.

Factory Reset from Arcserve UDP Console

This section provides information about how to perform factory reset from Arcserve UDP console.

Follow these steps:

1. Log into the Arcserve UDP Console.
2. Navigate to **settings** > **Factory Reset**.



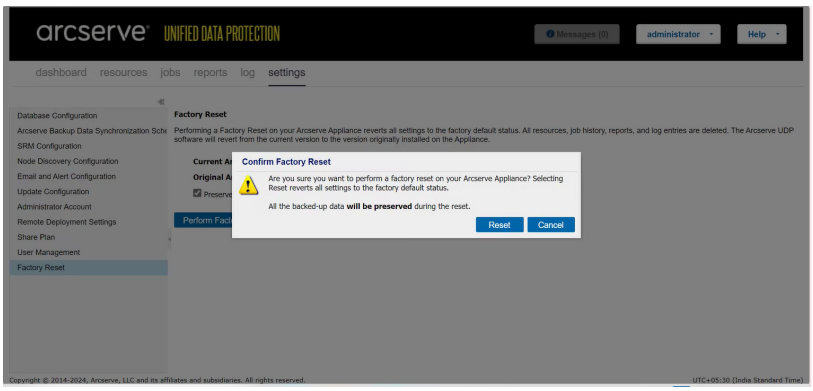
3. On the *Factory Reset* screen, click **Perform Factory Reset**.

Notes:

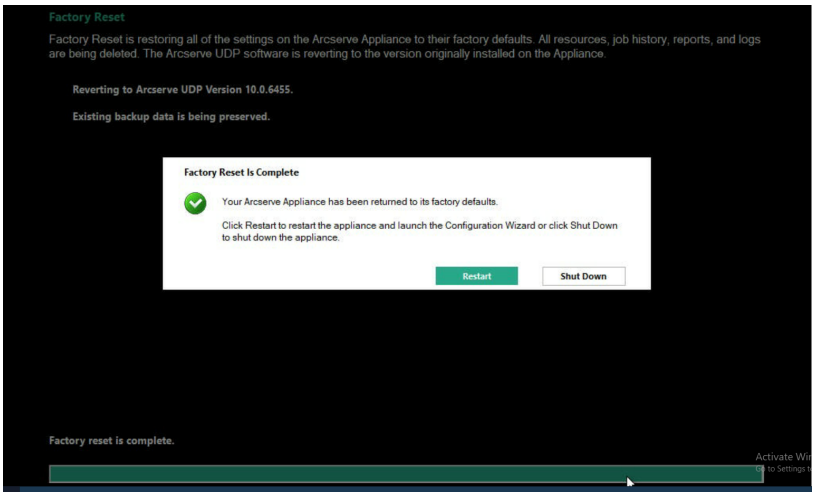
- The **Preserve existing backup data** check box is selected by default. All the backup data is preserved during the reset. Only C:\ volume in the original operating system is rebuilt.
- If you clear the **Preserve existing backup data** checkbox, all the backup data is deleted during the reset. All the data on the respective volumes of C:\, X:\, and Y:\ in the original operating system is rebuilt.

A confirmation dialog appears.

4. To perform factory reset, click **Reset**.



5. After the factory reset is completed, you can perform one of the following actions:
   - To reboot the appliance, click **Restart** .
   - To close the appliance, click **Shut Down** .



The factory reset from Arcserve UDP Console for 10000 appliance is successfully completed.

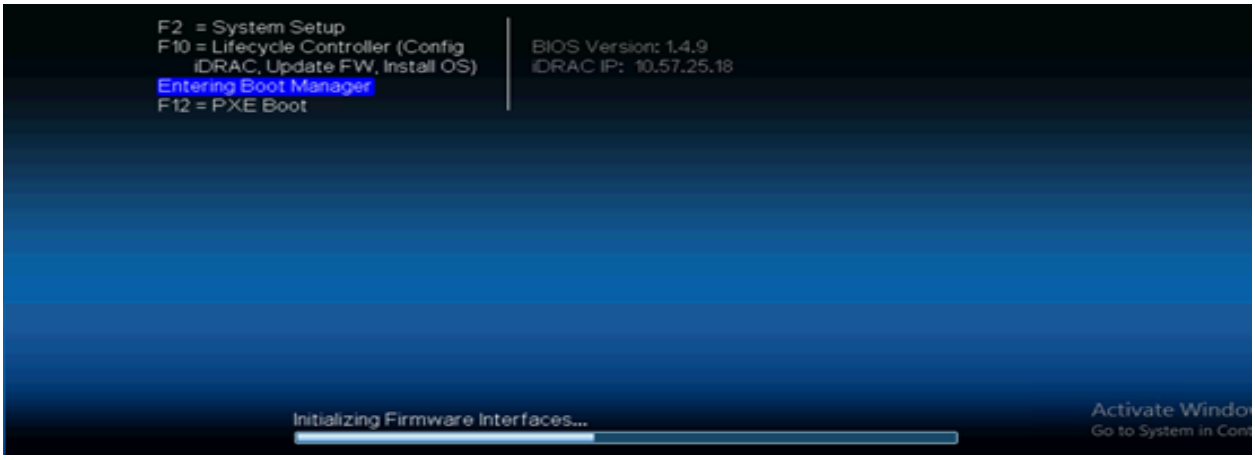
Apply Arcserve UDP Factory Reset Using Boot Option in 9012-9504DR Series Appliance

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.

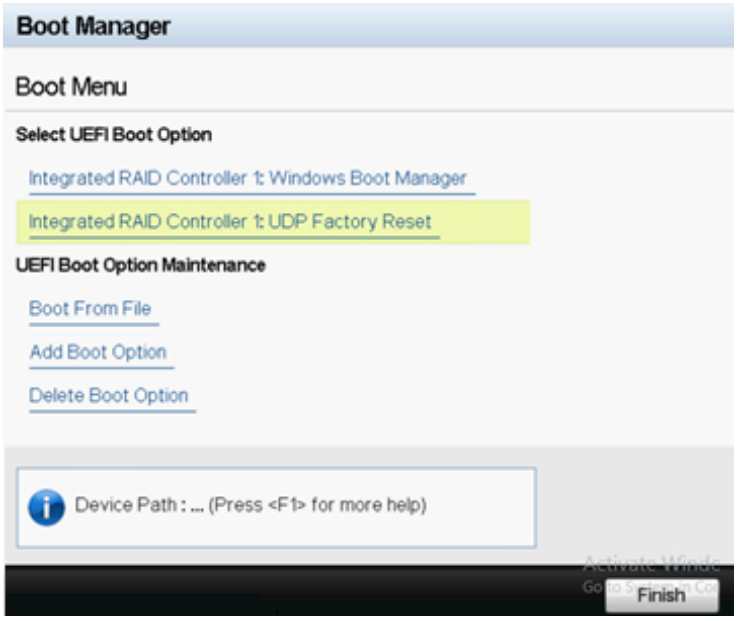
Note: You can also select the Preserve the backup data option while running UDP factory reset.

Follow these steps:

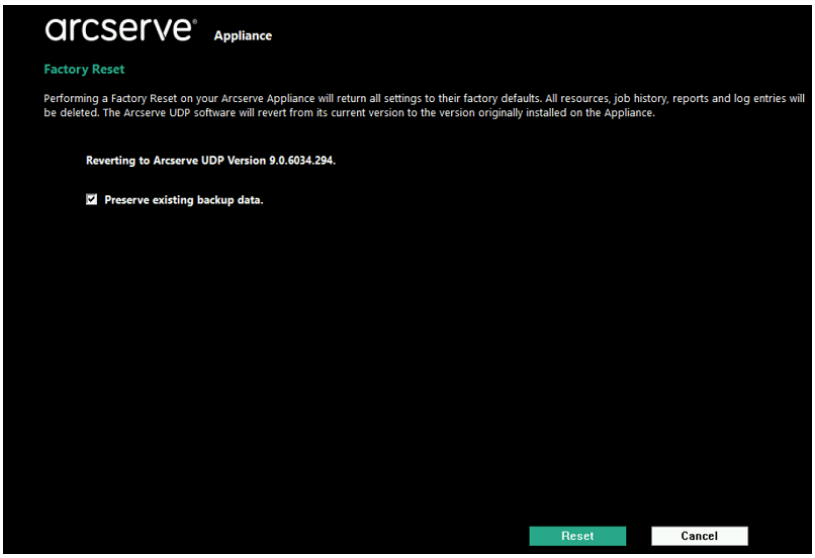
1. Press F11 on the keyboard to invoke Boot Menu.



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



A page about factory reset is displayed.

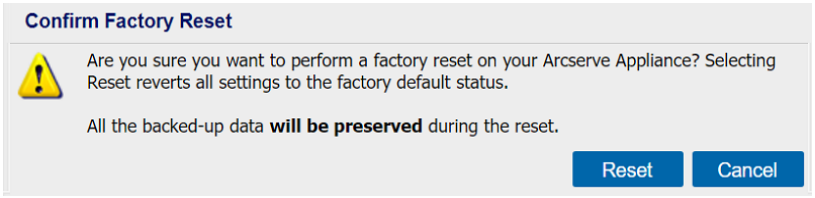


Notes:

- 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**.

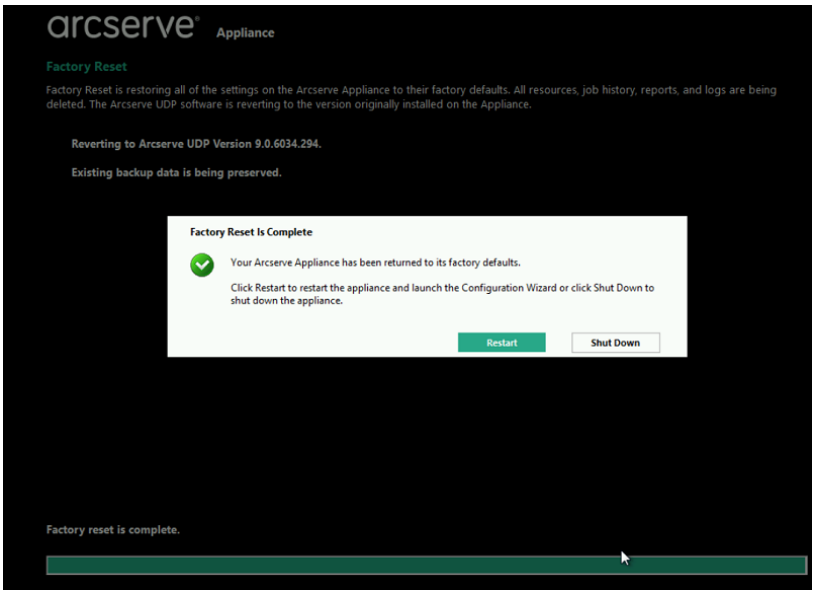
A confirmation dialog appears.



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

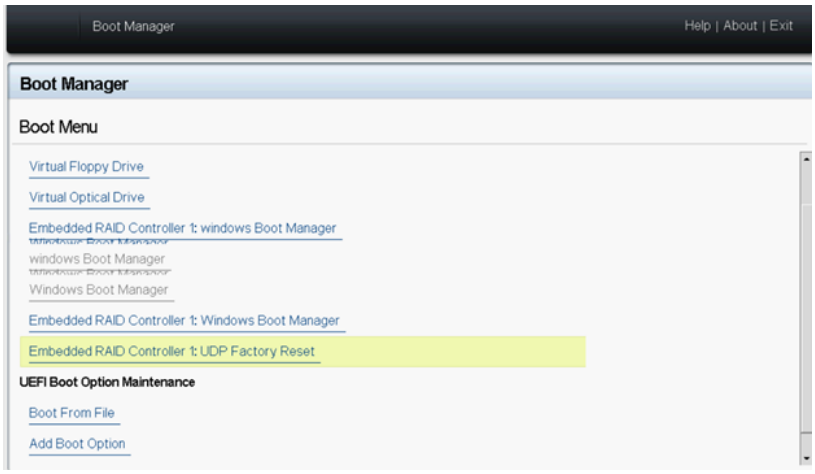
You can apply UDP factory reset from the Boot Menu of the Arcserve Appliance X series. Using UDP factory reset, you can return your Arcserve Appliance X series to clean and non-configured status.

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

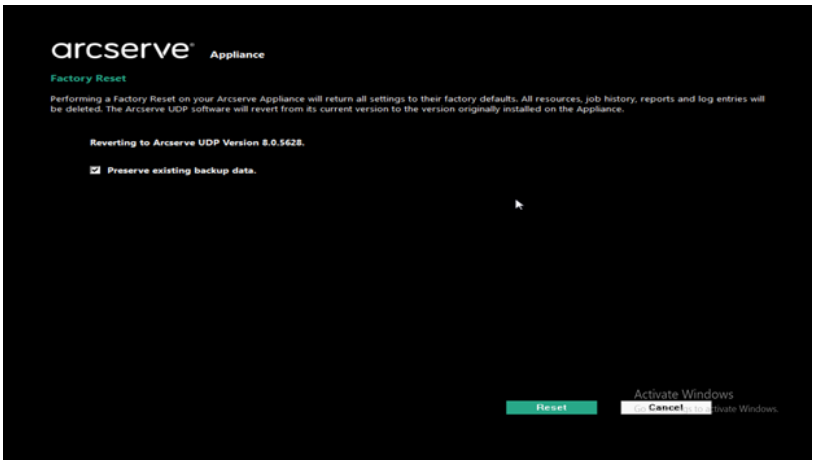
Follow these steps:

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.

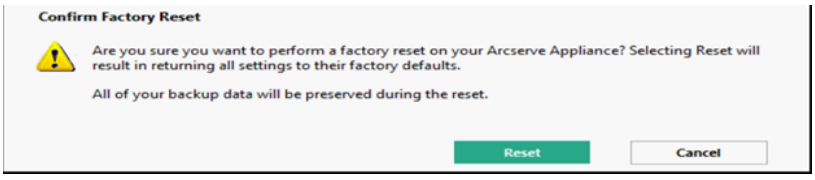


Notes:

- 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**.

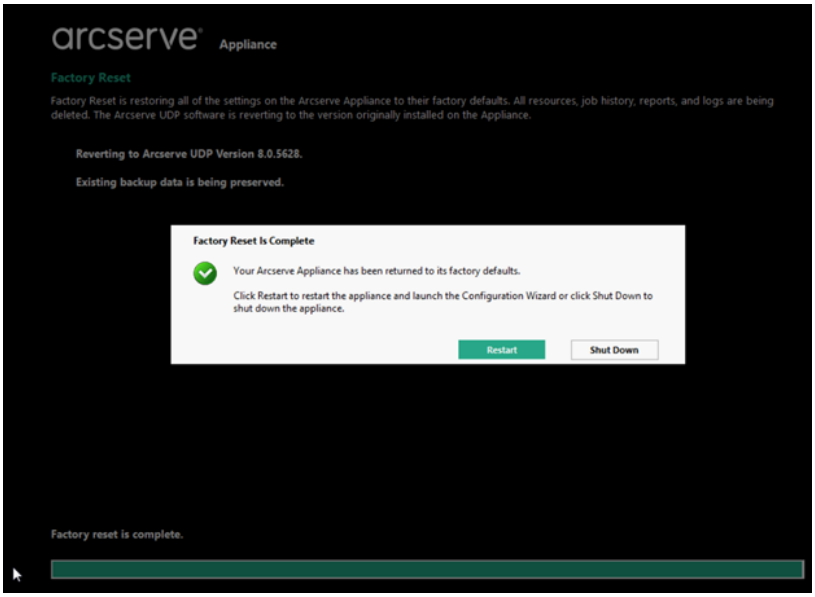
A confirmation dialog appears.



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.

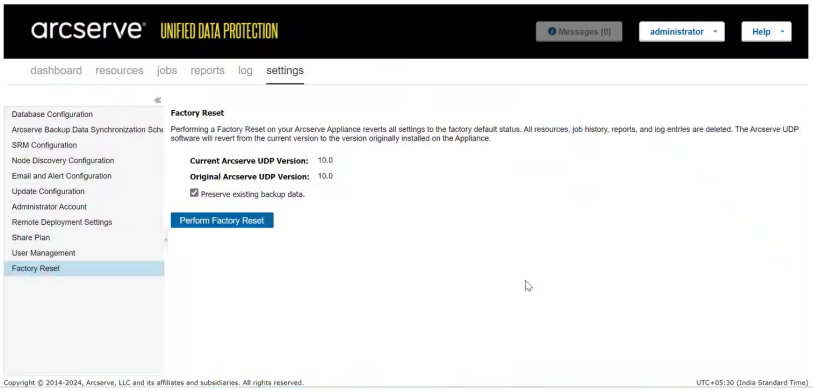


Clear Configuration and Apply Appliance Factory Reset

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.



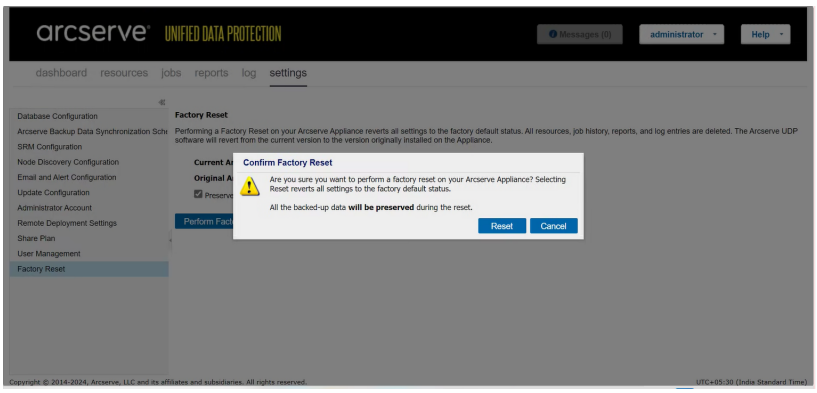
   All the backed up data is preserved by default.

   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.

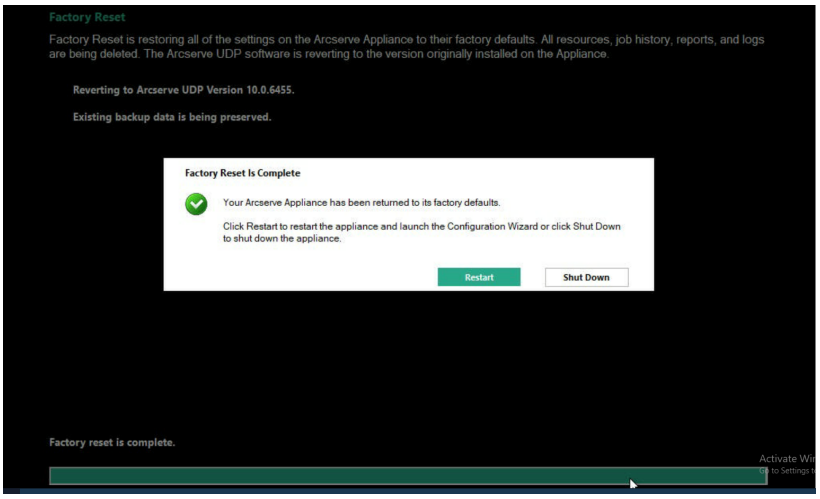


3. From the confirmation dialog, click **Reset** to launch the factory reset.

   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.



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.

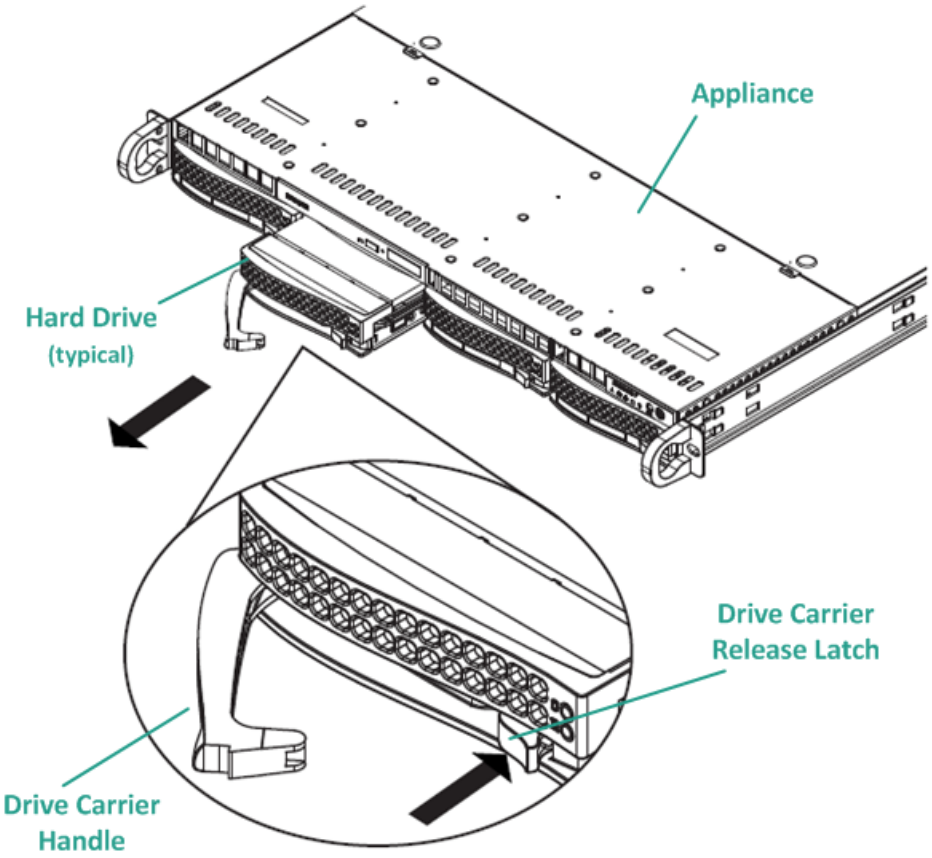
The Arcserve Appliance contains four hard drive carriers which are labeled 0, 1, 2 and 3 from left to right. If you replace more than one hard drive at a time, you should label the replacement hard drives so that you know which drive is placed into each drive carrier. You should also label the hard drives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

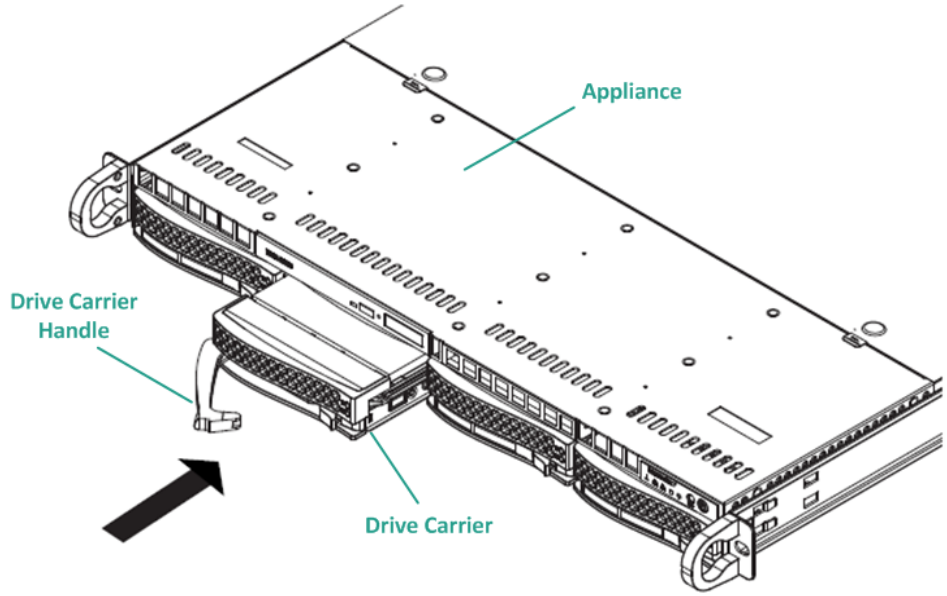
1. To gain access to the drive holders, you first need to remove the faceplate:
    a. Unlock the faceplate lock.
    b. Press the release knob to retract the faceplate pins.
    c. Carefully remove the faceplate (using two hands).
2. Press the release latch on the drive carrier. This extends the drive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

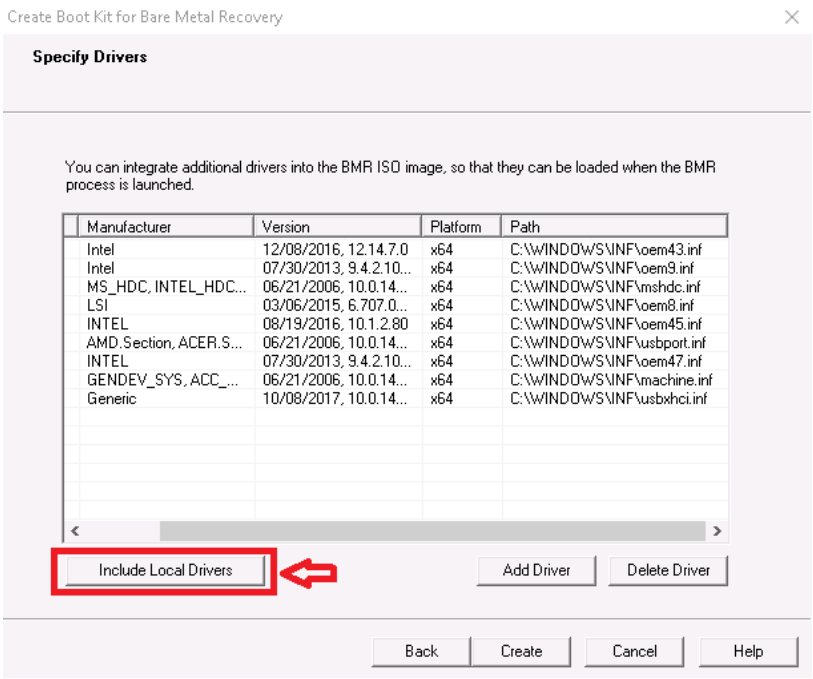
Perform Bare Metal Recovery (BMR) without Preserving Data in 9012-9504DR Series Appliance

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.

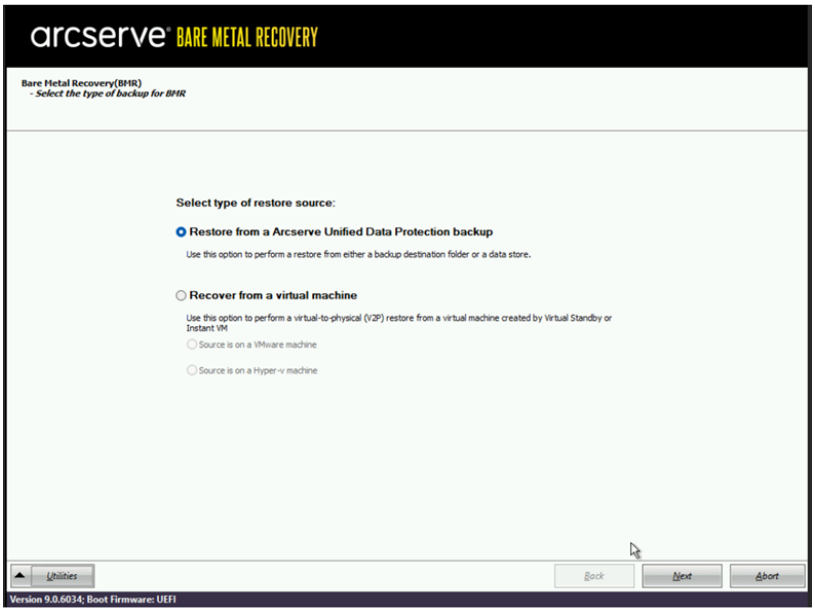


2. Boot the Arcserve Appliance using BMR ISO image or USB Stick.

   The **Arcserve bare metal recovery** setup appears.

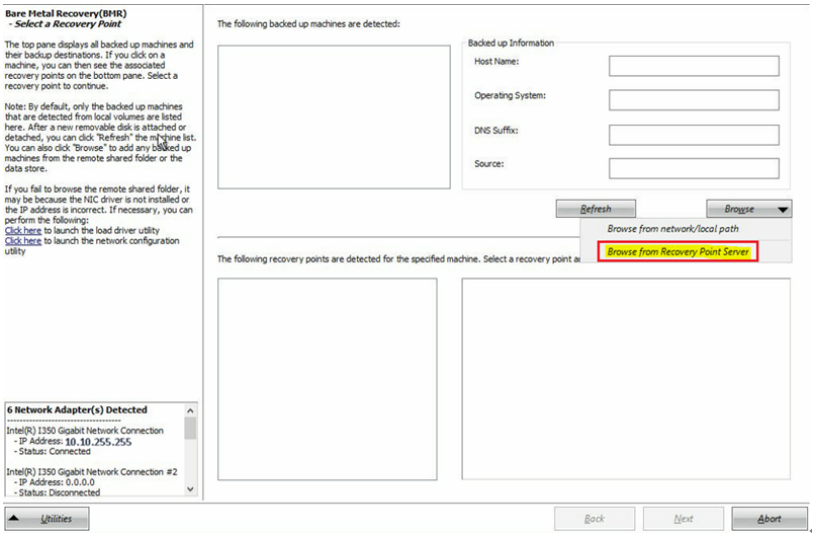
3. Select the required language and click **Next**.

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



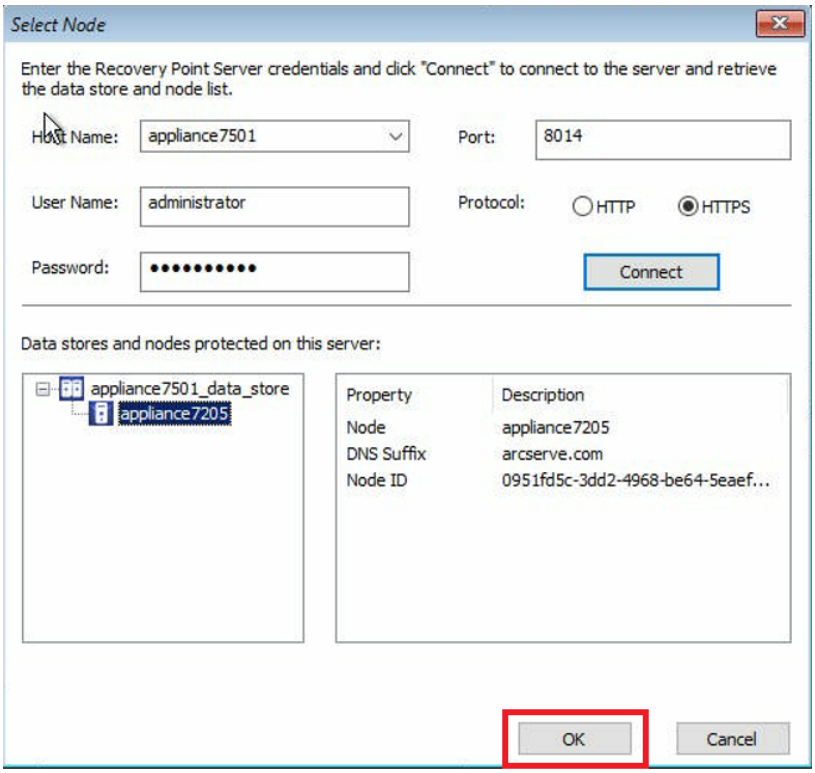
The **Select a Recovery Point wizard** window appears.

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



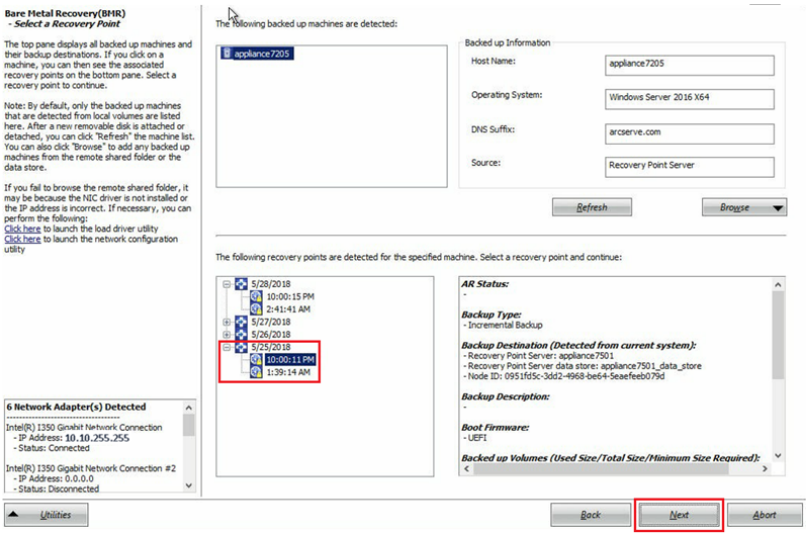
The **Select Node** window appears.

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**.



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

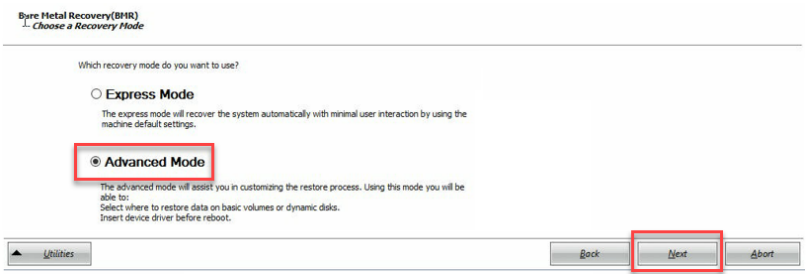
9. Select the recovery point to restore and click **Next**.



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

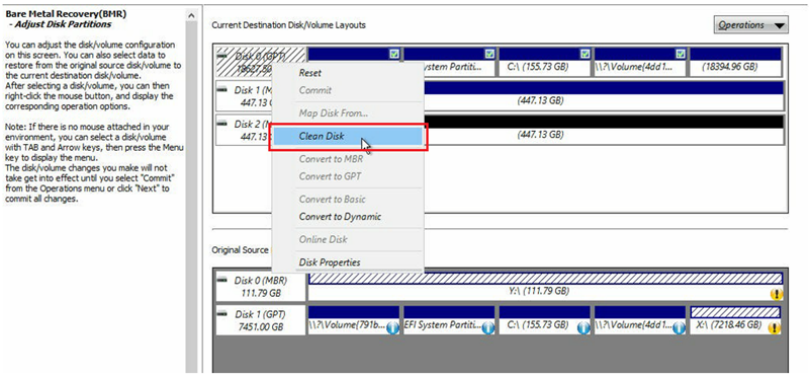
The **Bare Metal Recovery(BMR)- Choose a Recovery Mode** dialog appears.

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

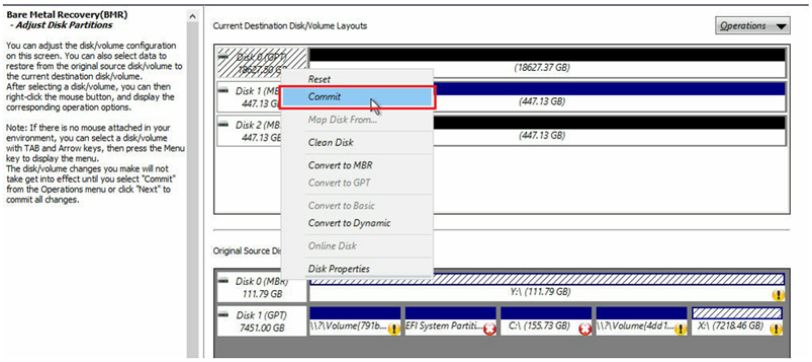


The **Bare Metal Recovery(BMR)- Adjust Disk Partitions** dialog appears.

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

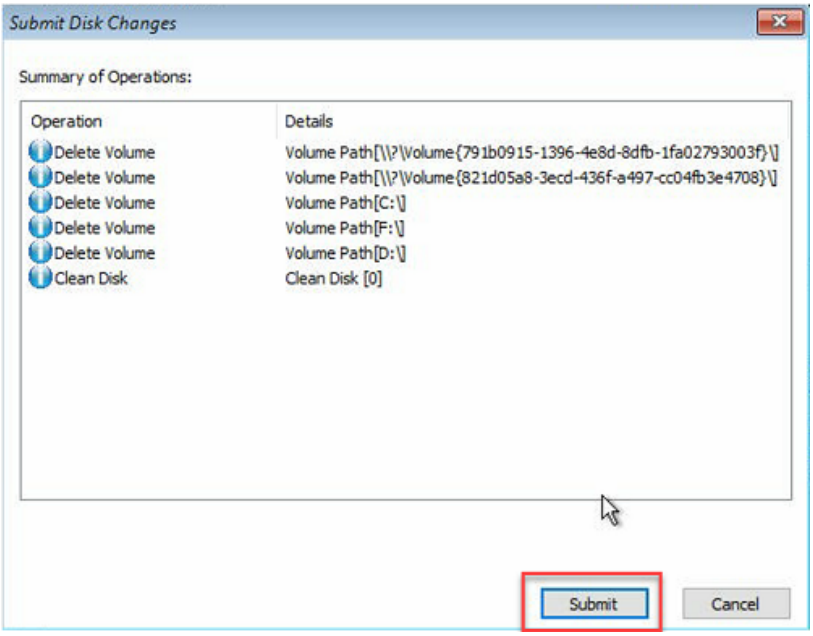


13. After cleaning the disk, right click on the same disk and click **Commit**.

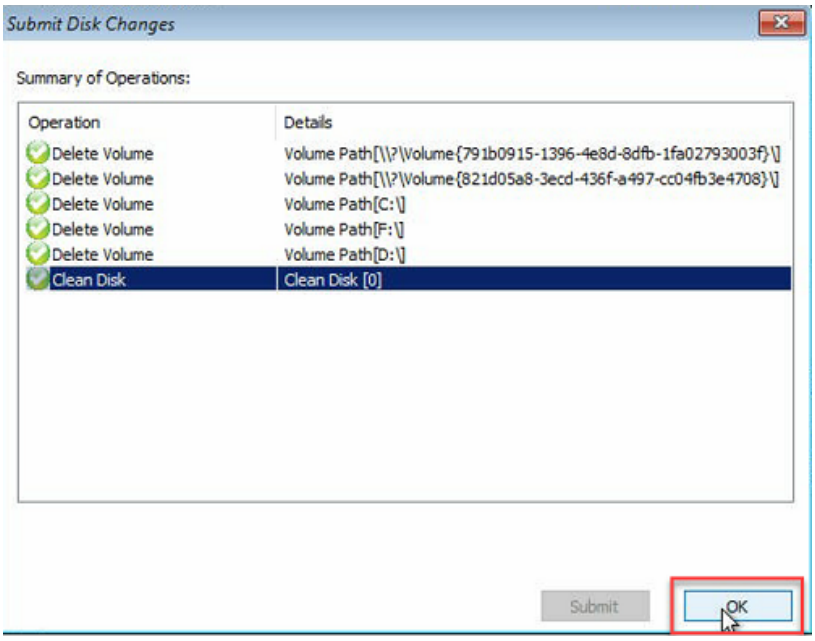


The **Submit Disk Changes** window appears.

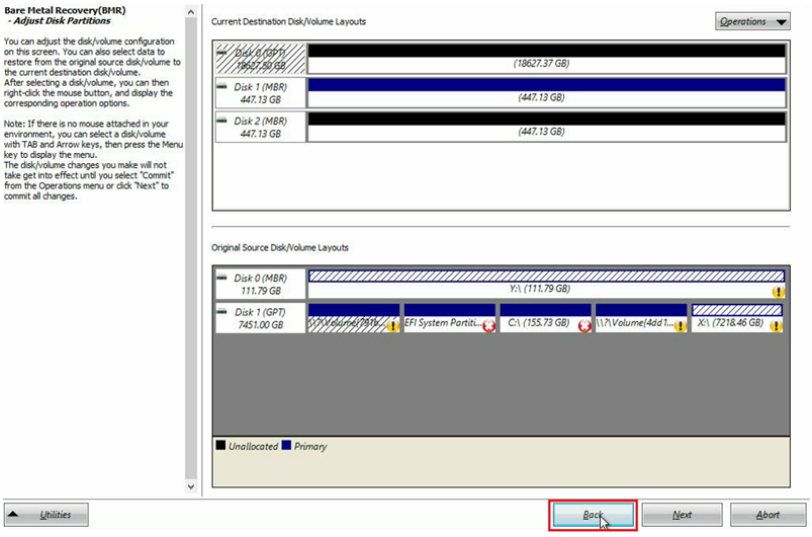
14. Click **Submit**.



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

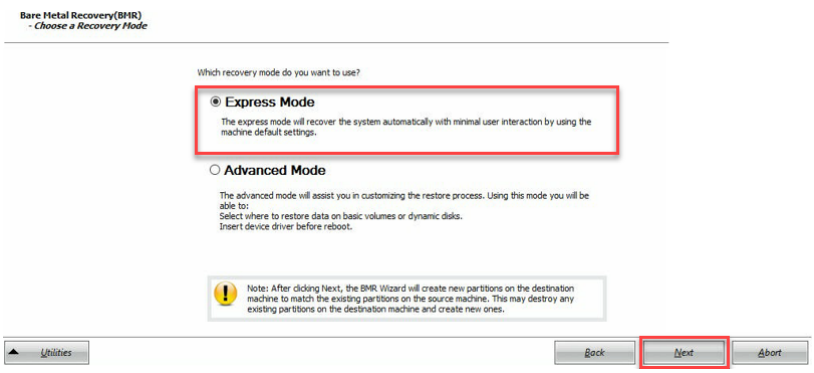


16. From the **Bare Metal Recovery(BMR)- Adjust Disk Partitions** dialog, click **Back**.



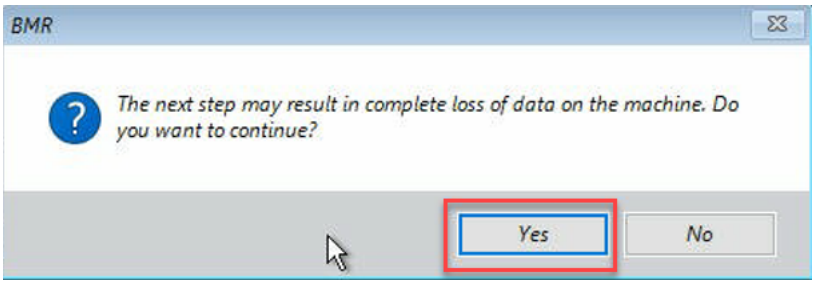
The **Bare Metal Recovery(BMR)- Choose a Recovery Mode** dialog appears.

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



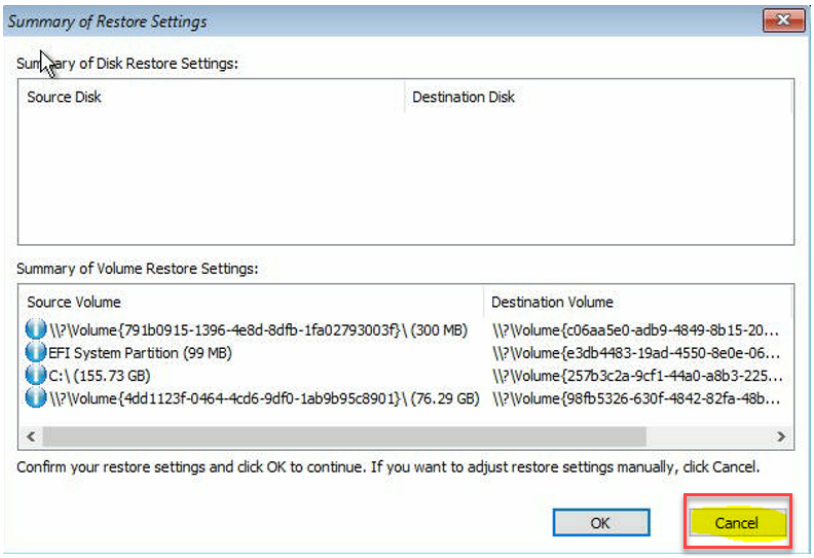
The **BMR** dialog appears.

18. Click **Yes**.



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

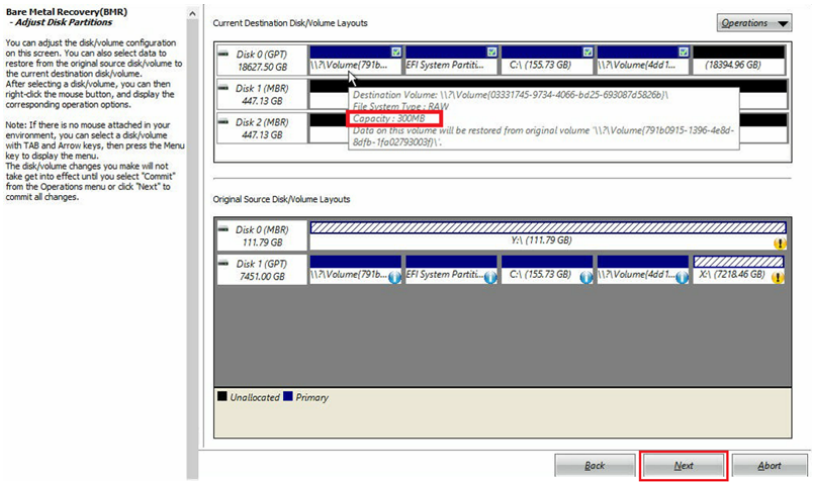
19. Click **Cancel**.



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

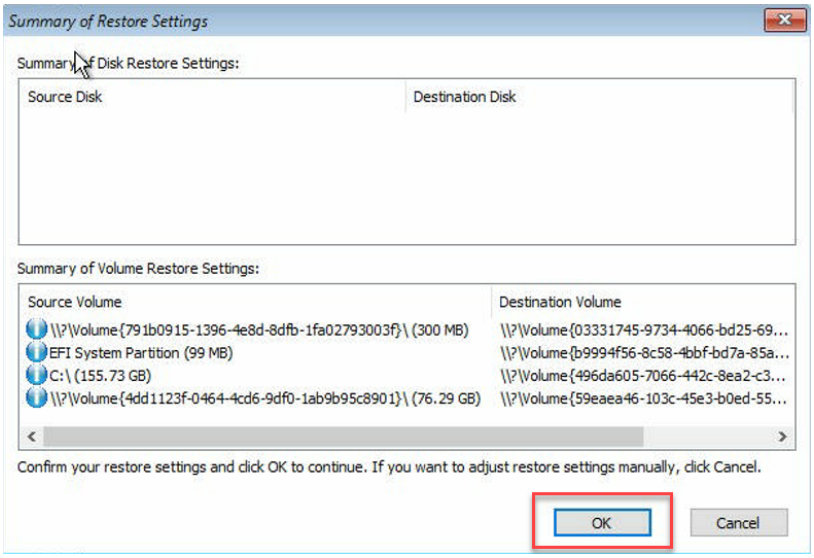
20. Compare and verify if the capacity of the first four partitions available in the **Current Destination Disk/Volume Layouts** tab matches with the largest GPT disk available in the **Original Source Disk/Volume Layouts** tab and click **Next**.

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



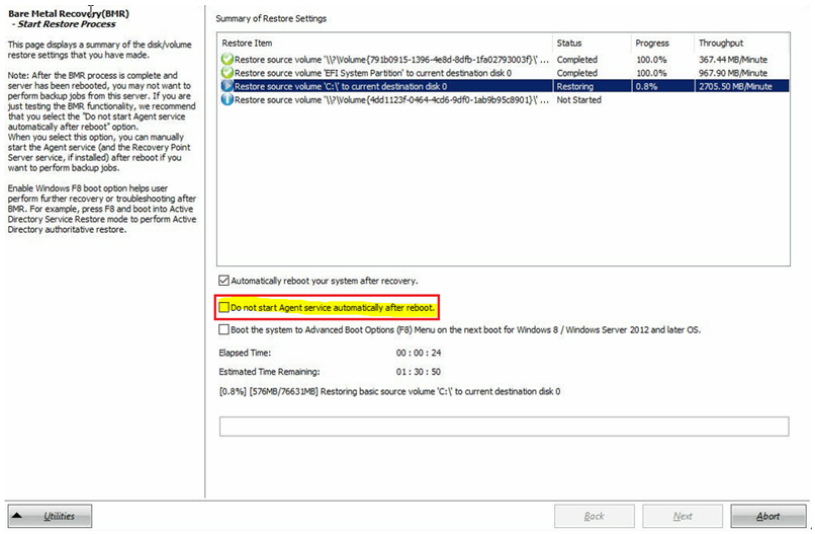
The **Summary of Restore Settings** dialog appears.

21. Click **OK**.



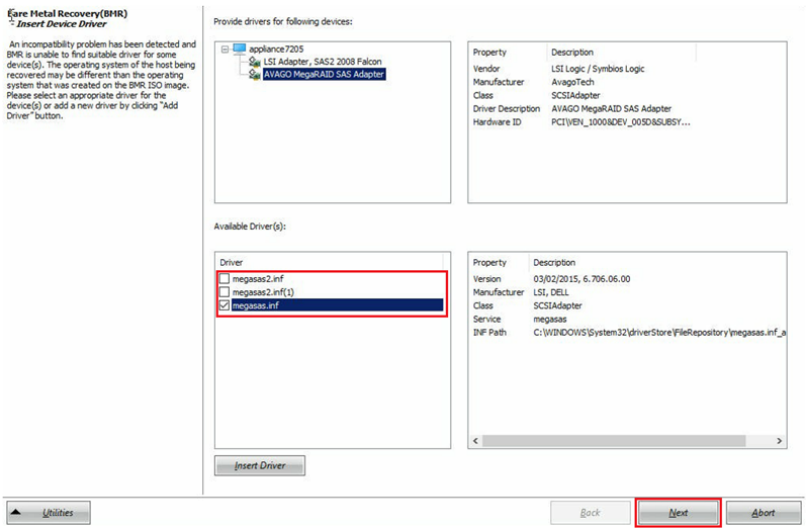
The **Bare Metal Recovery(BMR)- Start Recovery Process** dialog appears.

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

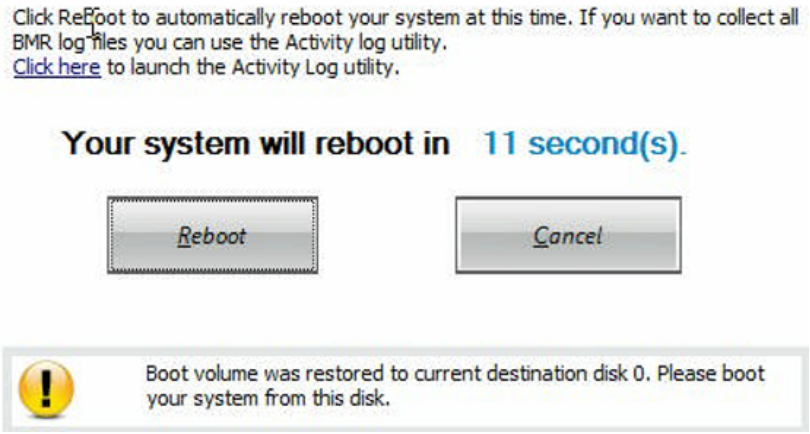


The **Bare Metal Recovery(BMR)- Insert Device Driver** dialog appears.

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



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



The BMR process is completed successfully.

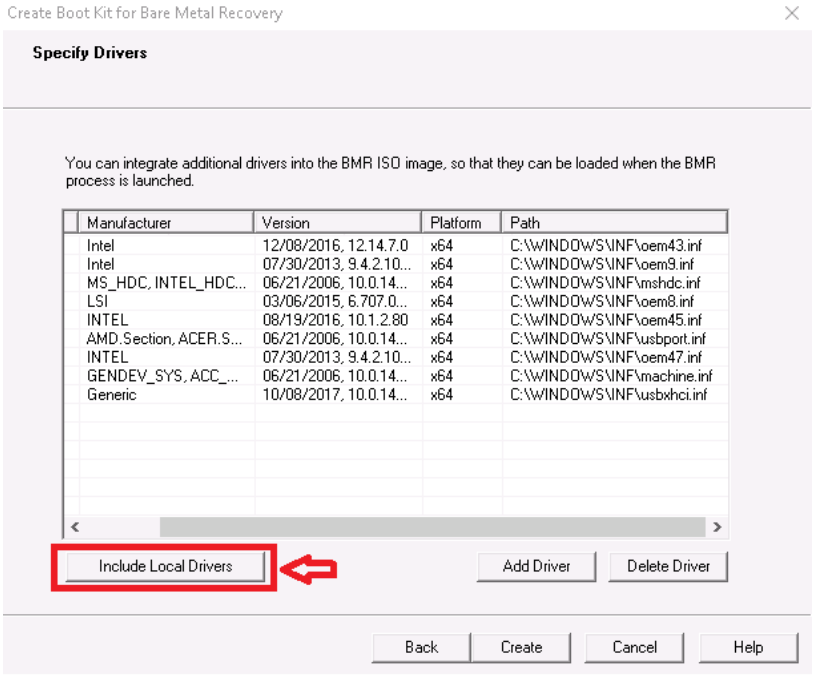
Perform Bare Metal Recovery (BMR) and Preserving Data in 9012-9504DR Series Appliance

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.

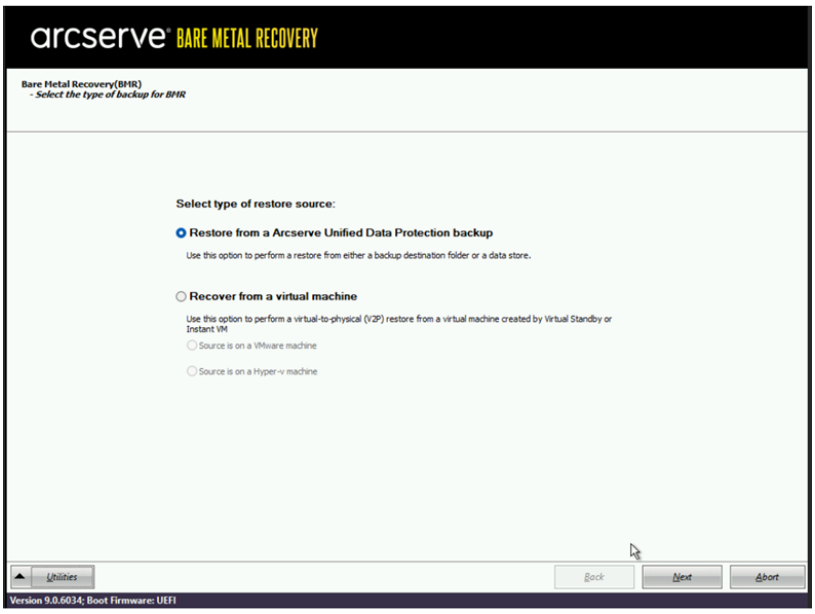


2. Boot the Arcserve Appliance using BMR ISO image or USB Stick.

   The **Arcserve bare metal recovery** setup appears.

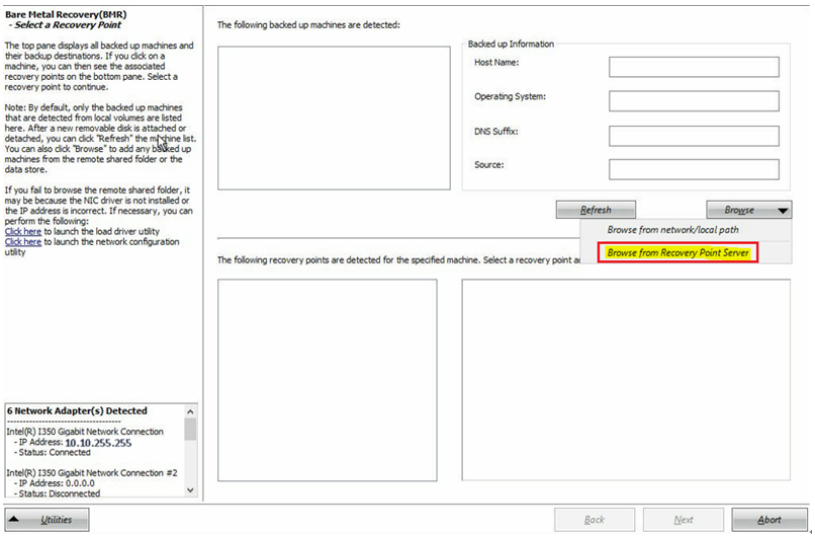
3. Select the required language and click **Next**.

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



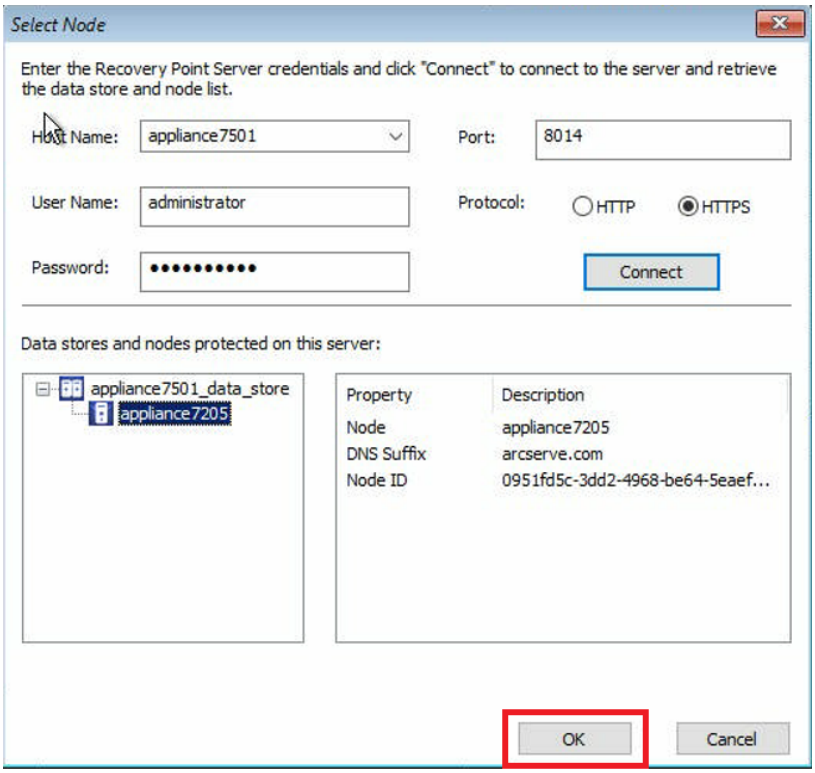
The **Select a Recovery Point wizard** window appears.

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



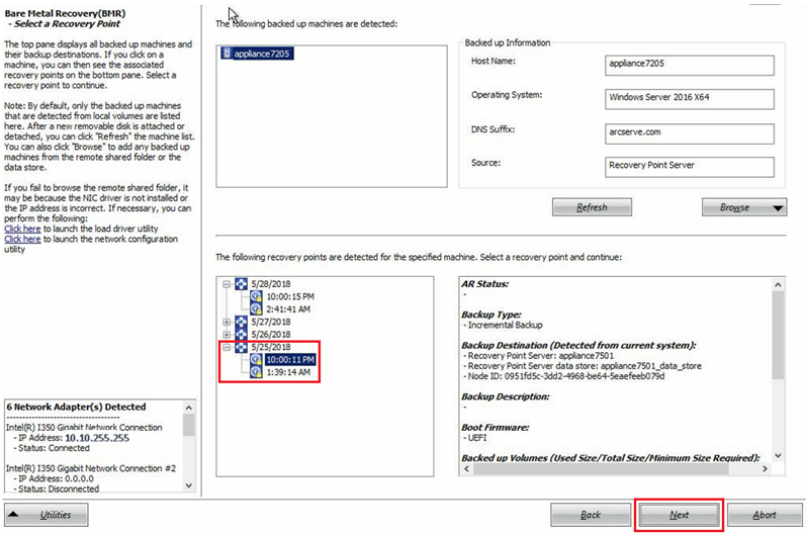
The **Select Node** window appears.

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**.



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

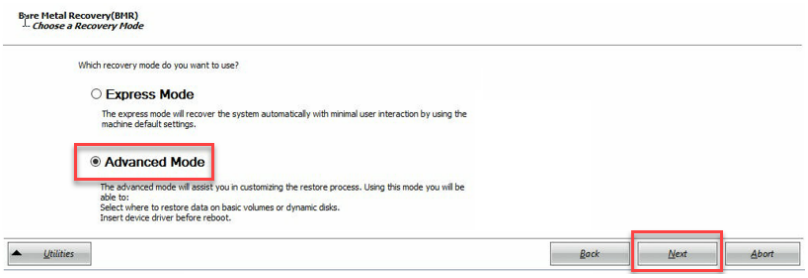
9. Select the recovery point to restore and click **Next**.



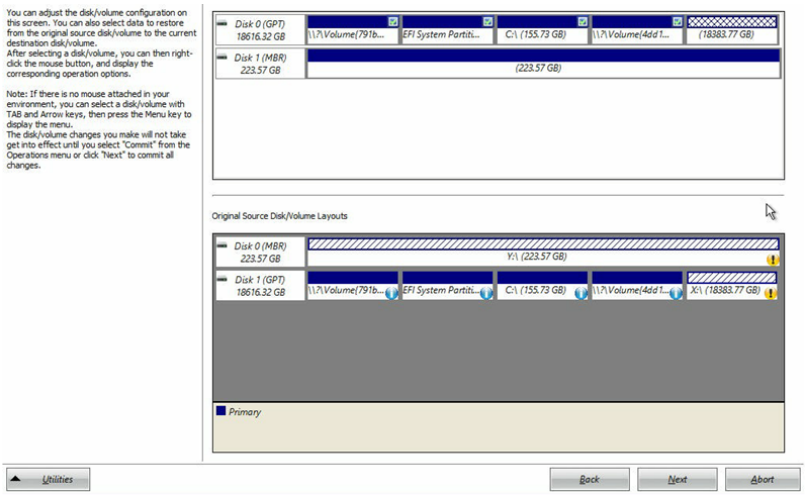
10. (Optional) Enter the session password if prompted, and click **OK**.

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

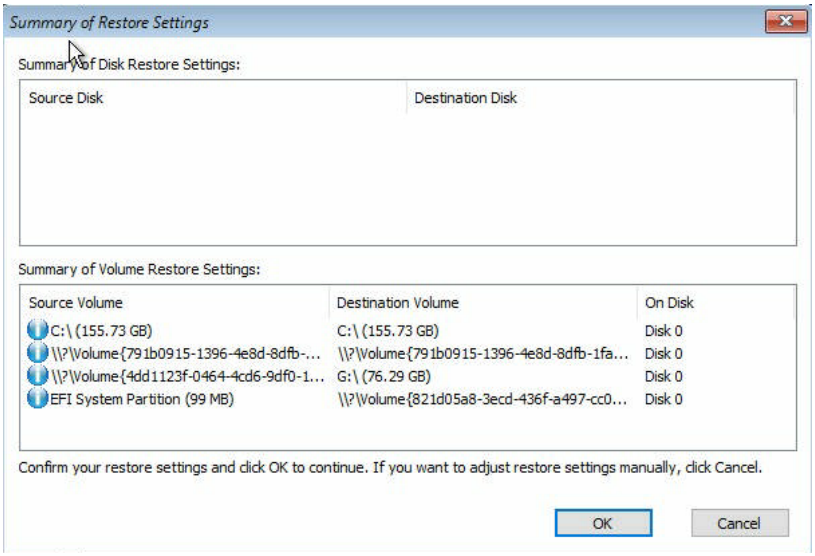
11. Select **Advanced Mode** and click **Next**.



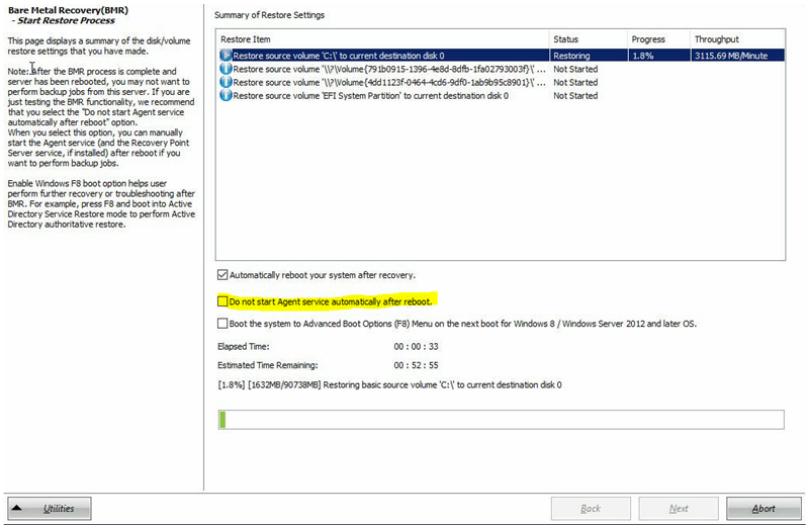
12. On the **Bare Metal Recovery(BMR)- Adjust Disk Partitions** dialog, click **Next**.



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.



The BMR process is completed successfully.

Chapter 9: Performing Appliance Capacity Expansion

This section contains the following topics:

Working with Expansion Kit in Arcserve Appliance 10024BU-10576DR Models 164
Working with SSD Flash Expansion Kit in Arcserve Appliance 10024BU-10576DR Models 168
Working with Arcserve Appliance Expansion Kit - X Series Models 171
Working with SSD Flash Expansion Kit in Arcserve X Series Appliance 173
Working with Expansion Kit in Arcserve Appliance 9072-9504 DR Models 180
Working with SSD Flash Expansion Kit in Arcserve Appliance 9072-9504 DR Models 185

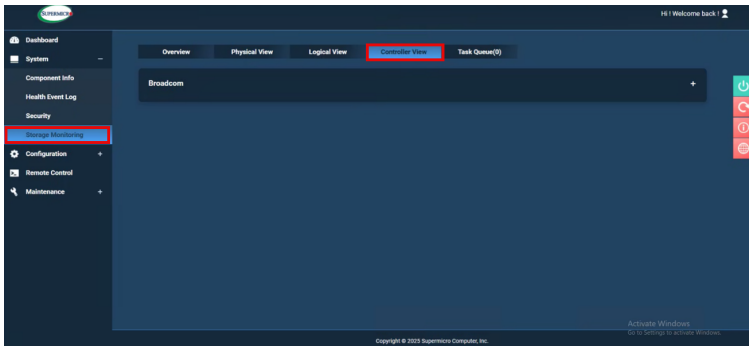
Working with Expansion Kit in Arcserve Appliance 10024BU-10576DR Models

Arcserve Expansion Kit lets you expand the data capacity in Arcserve Appliance 10024BU-10576DR models.

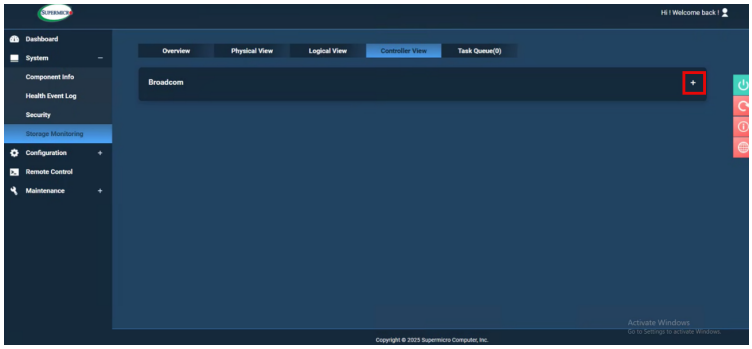
Follow these steps:

1. To insert HDDs in the empty disk slots, perform the following steps:
   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.

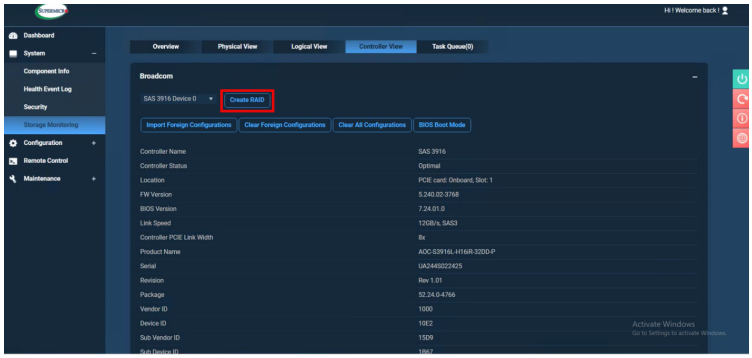
2. To create and configure Raid-6 from IPMI web interface, perform the following steps:
   a. Log into the IPMI console.
   b. Navigate to **System** > **Storage Monitoring** > **Controller view**.



c. On the Controller View tab, click the **plus sign (+)** to expand the **Broadcom**.



d. On the Broadcom screen, click **Create RIAD**.

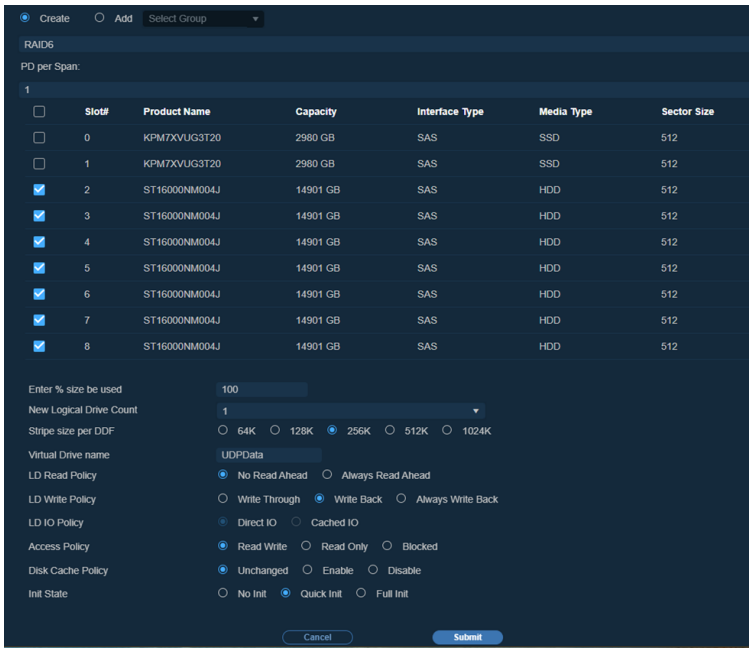


e. On the Create page, select all the HDD slots, and then specify the following:

- **RAID**: From the RAID level drop-down, select RAID6
- **PD per Span**: 1
- **Enter % size be used**: Enter the value as **100**
- **New Logical Drive Count**: Enter the value as **1**
- **Stripe size per DDF**: Select the **256K** option
- **Virtual Drive name**: Enter the desired name for the virtual drive
- **LD Read Policy**: Select **No Read Ahead** option

- **LD Read Policy**: Select **Write Back** option
- **LD IO Policy**: By default, **Direct IO** option is selected.
- **Access Policy**: Select **Read White** option.
- **Disk Cache Policy**: Select **Unchanged** option
- **Init State**: Select **Quick Init** option

f. Click **Submit**.



g. In the search box on the taskbar, type **Computer Management**, and then press the Enter key.

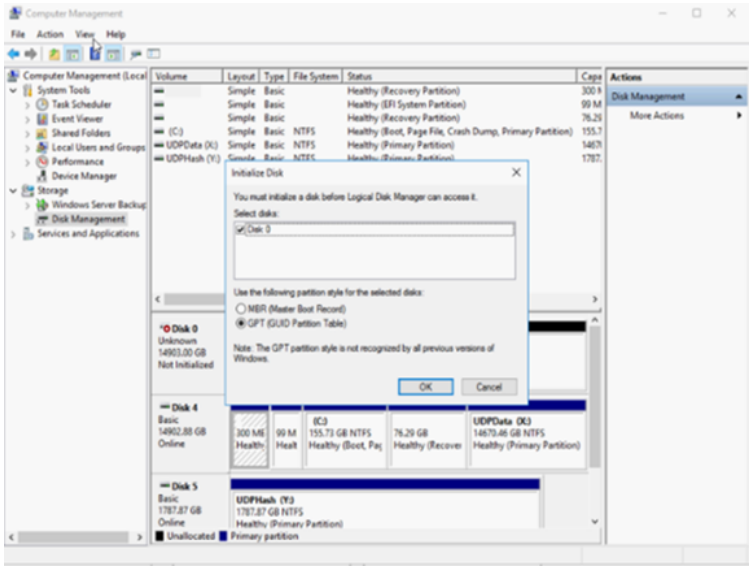
   The Computer Management window opens.

h. Navigate to **Storage** > **Disk Management**.

i. Double-click the new virtual disk that you have added.

   The Initialize Disk window appears.

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



k. On 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

3. To expand the datastore, perform the following steps:

a. Navigate to the drive that you have added, and then create a folder.

b. From the Arcserve Appliance desktop, launch the **Arcserve Appliance** wizard.

Arcserve Appliance Configuration page opens.

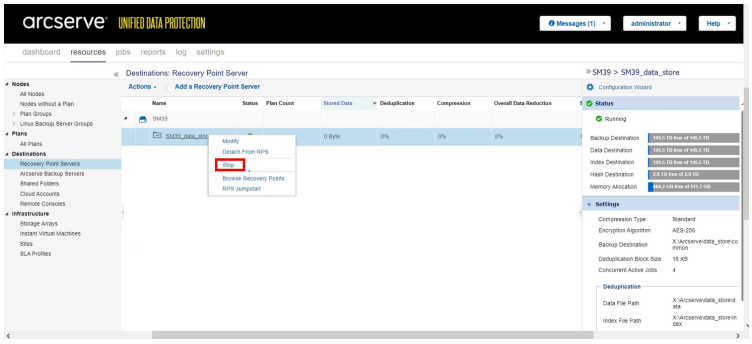
c. Click **Launch UDP Console**.

Arcserve UDP Console login page appears.

d. Log into the UDP Console as Administrator.

e. Navigate to **resources** > **Destinations** > **Recovery Point Servers**.

f. Right-click the datastore, and then select **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 the expanded data path.

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

as_gddmgr.exe –DataPath Display <datastore name>

The new expanded data path is added to the datastore Successfully.

h. In UDP Console, navigate to **resources** > **Destinations** > **Recovery Point Servers**.

i. Right-click the datastore, and then select **Start**.

j. Resume the plans that you have paused before from the UDP Console.

The data capacity of the Arcserve Appliance is successfully expanded.

Working with SSD Flash Expansion Kit in Arcserve Appliance 10024BU-10576DR 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 10024BU-10576DR models.

Follow these steps:

1. To insert SSDs in the empty disk slots, perform the following steps:

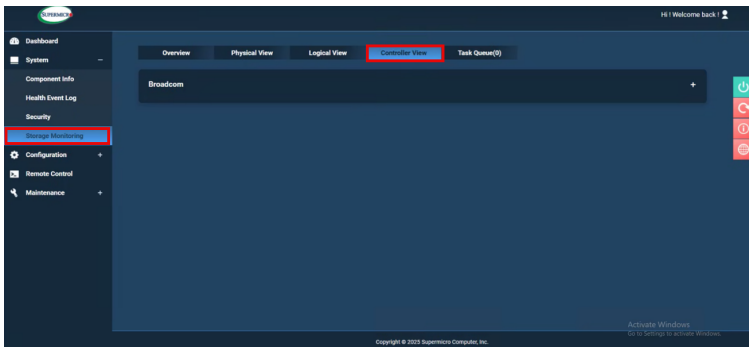
   a. From the Arcserve UDP Console, verify and make sure that no jobs are running on the Appliance Server. In case any jobs are running, pause the corresponding plans.

b. Insert SSDs in the empty disk slot.

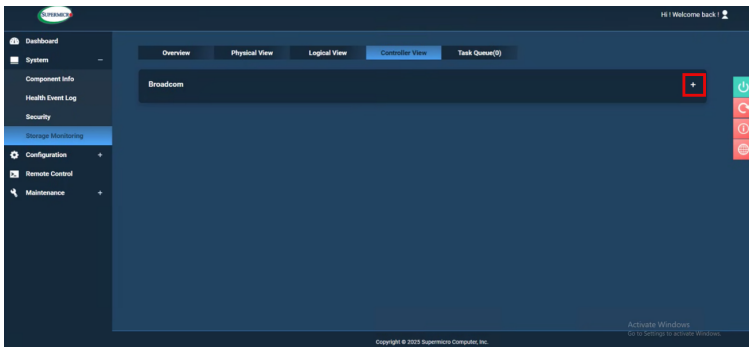
2. To create and configure Raid-5 from IPMI web interface, perform the following steps:

a. Log into the IPMI console.

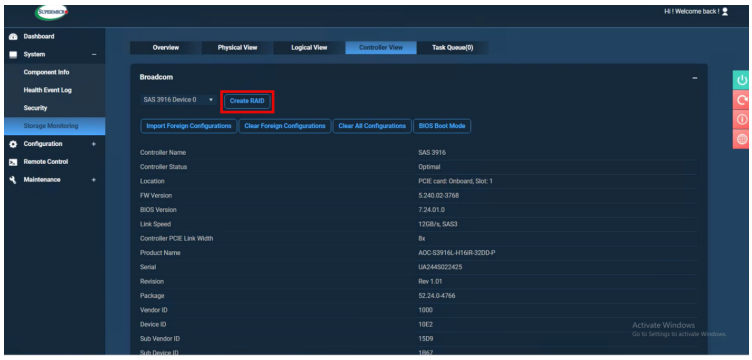
b. Navigate to **System** > **Storage Monitoring** > **Controller view**.



c. On the *Controller View* tab, click the **plus sign (+)** to expand the **Broadcom**.



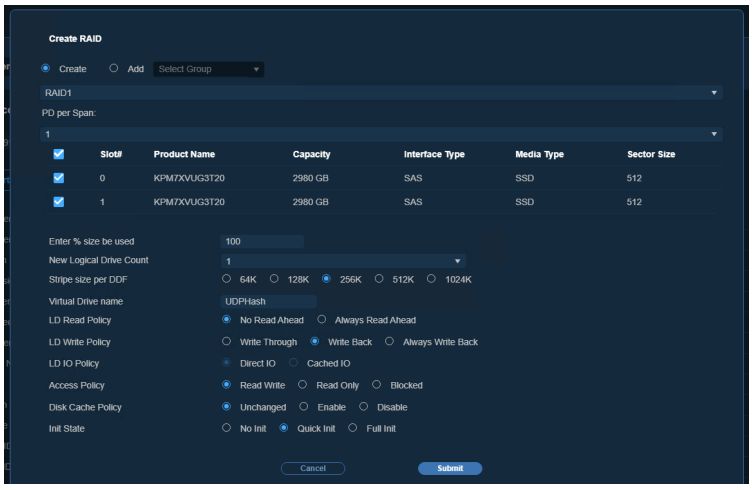
d. On the Broadcom screen, click **Create RIAD**.



e. On the Create page, select all the SSD slots and then do the following:

- **RAID**: From the RAID level drop-down, select RAID1
- **PD per Span**: 1
- **Enter % size be used**: Enter the value as **100**
- **New Logical Drive Count**: Enter the value as **1**
- **Stripe size per DDF**: Select the **256K** option
- **Virtual Drive name**: Enter the desired name for the virtual drive
- **LD Read Policy**: Select **No Read Ahead** option
- **LD Read Policy**: Select **Write Back** option
- **LD IO Policy**: By default, **Direct IO** option is selected.
- **Access Policy**: Select **Read White** option.
- **Disk Cache Policy**: Select **Unchanged** option
- **Init State**: Select **Quick Init** option

f. Click **Submit**.



g. In the search box on the taskbar, type **Computer Management**, and then press the Enter key.

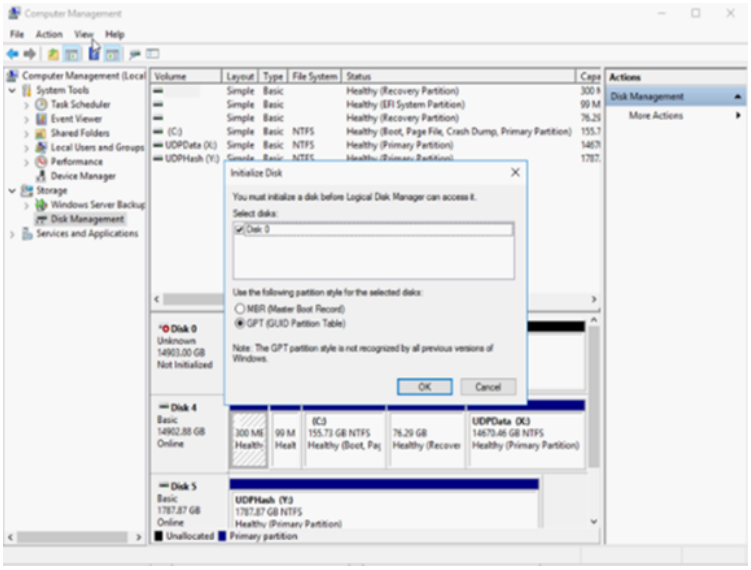
The Computer Management window opens.

h. Navigate to **Storage** > **Disk Management**.

i. Double-click the new virtual disk that you have added.

The Initialize Disk window appears.

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



k. On 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 successfully.

Working with Arcserve Appliance Expansion Kit - X Series Models

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

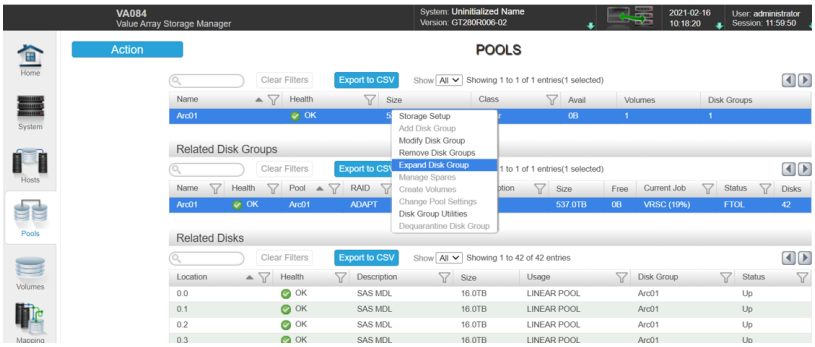
Follow these steps:

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.

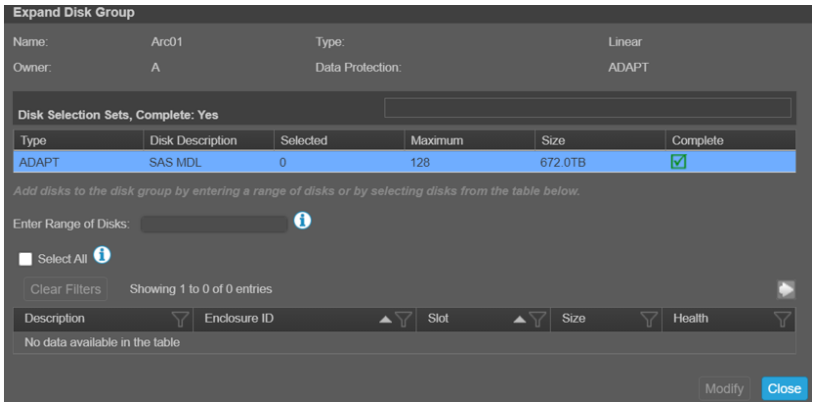
b. Insert the HDDs in the empty disk slots of Storage Unit - ME4084 Value Array. Each kit in the X series Expansion kit consists of 14 x 16TB disks.

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



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

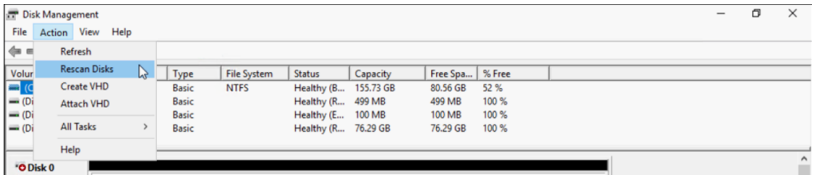
The Expand Disk Group panel opens and displays the disk group information and disk tables.



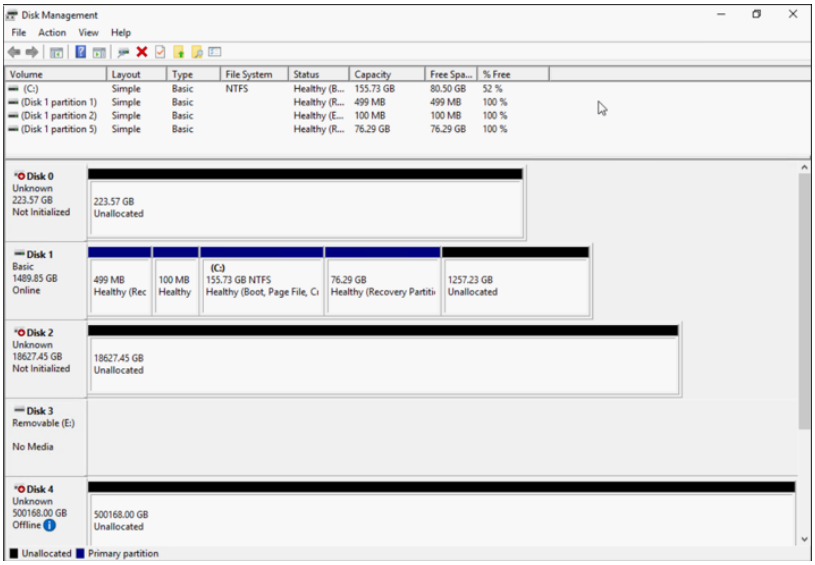
5. To add additional disks to the disk group, enter a range of disks in the **Enter Range of Disks** field or select the disks from the table.
6. Click **Modify**.
7. On the confirmation panel, click **Yes** to start the group expansion, and then click **OK** to close the panel.

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

8. 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:

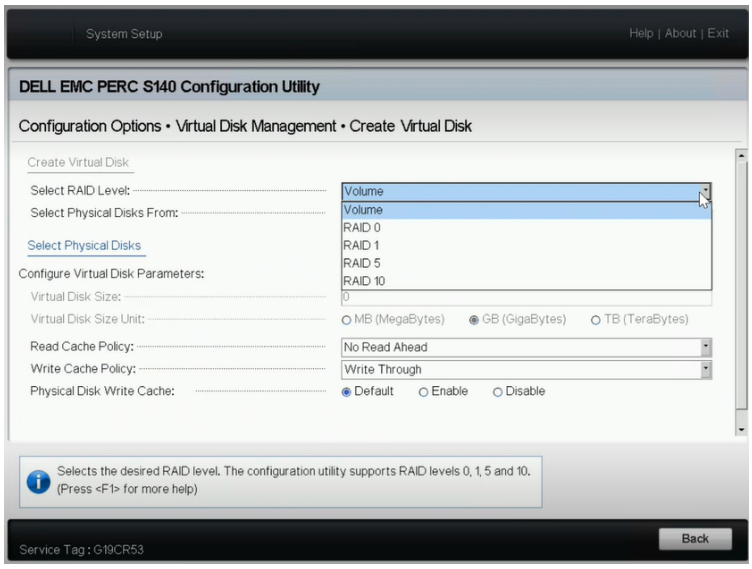
1. Perform the following steps to insert SSDs in the empty disk slots:
   a. From the Arcserve UDP Console, verify and make sure that no jobs are running on the Appliance Server. If in case any jobs are running, pause the corresponding plans.
   b. Insert SSDs in the empty disk slot.

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.

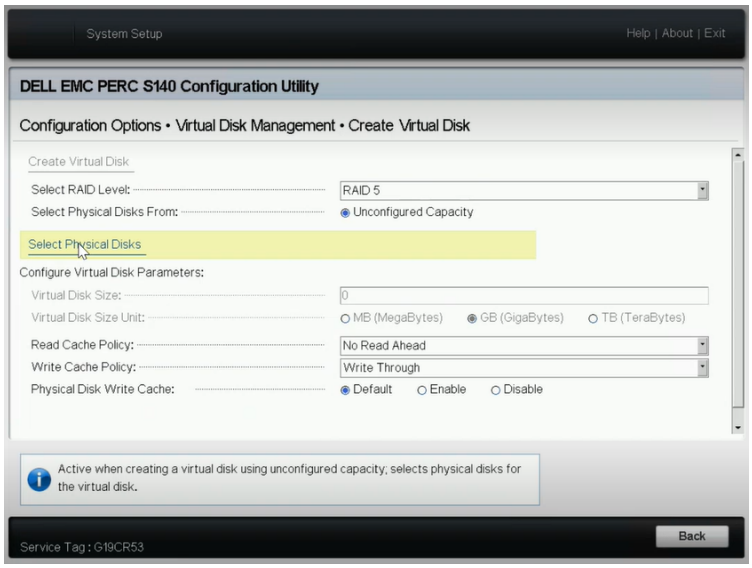
      On the confirmation window, click **Yes** to restart the BIOS Boot Manager.
   c. Click **Power**, and then select **Reset system (warm boot)**.

      The appliance boots and relaunches 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.



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

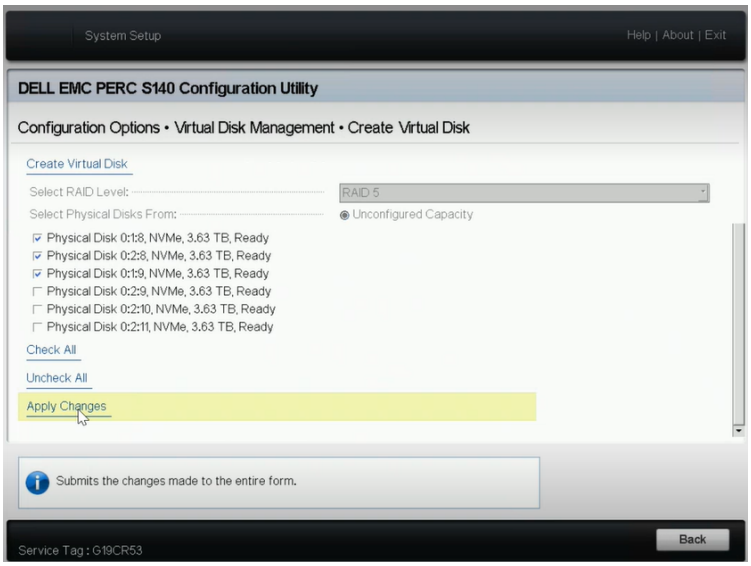


The Select Physical Disk Operation window opens.

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.

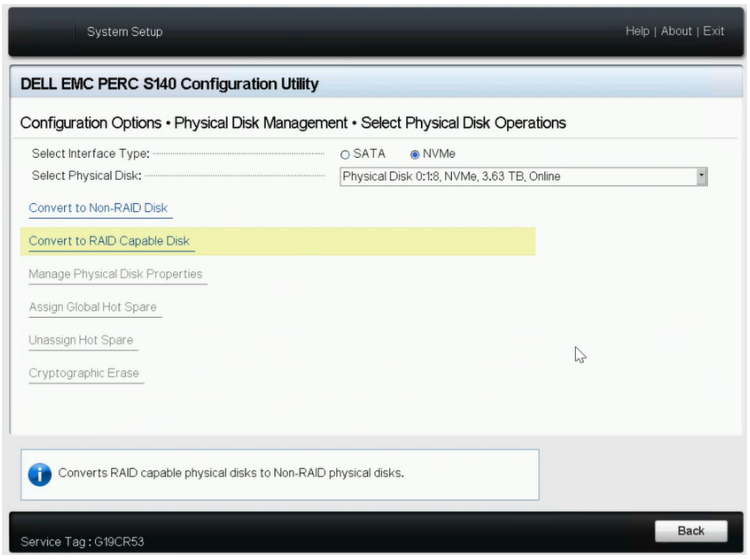
i. After the changes are applied, click the **Create Virtual Disk** option again to complete the process of creating the virtual disk.

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.

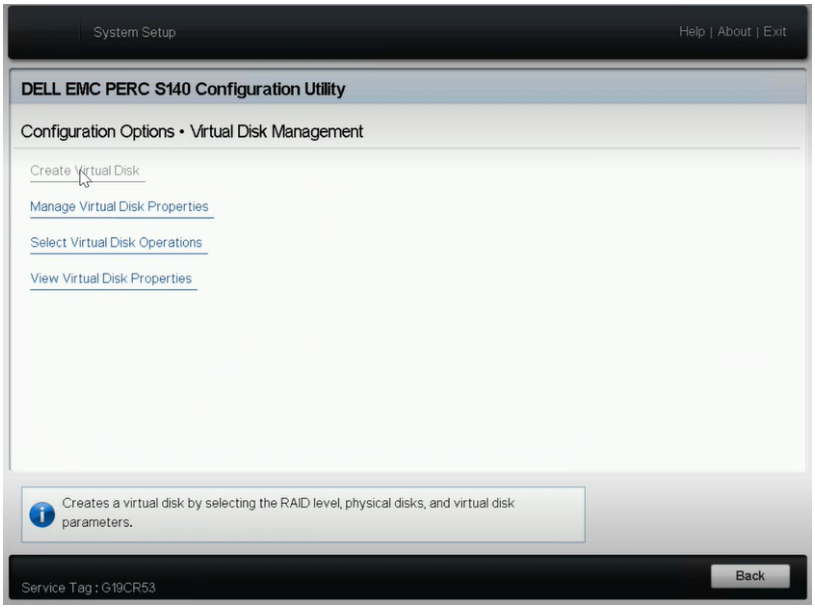


   c. When the following warning message is displayed, do the following:

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

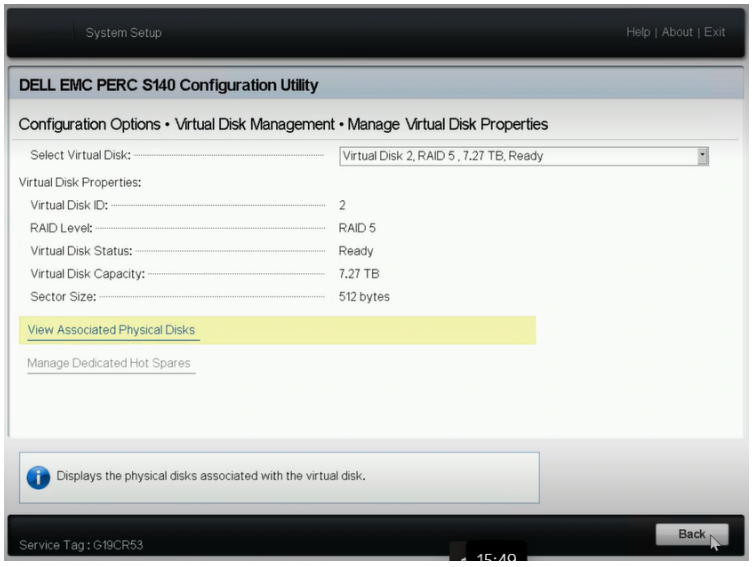
1. Verify that there are no OS-configured RAID arrays, and then click OK.
2. Click OK.

4. Navigate to **Configuration Options** > **Virtual Disk Management**, and then do the following:

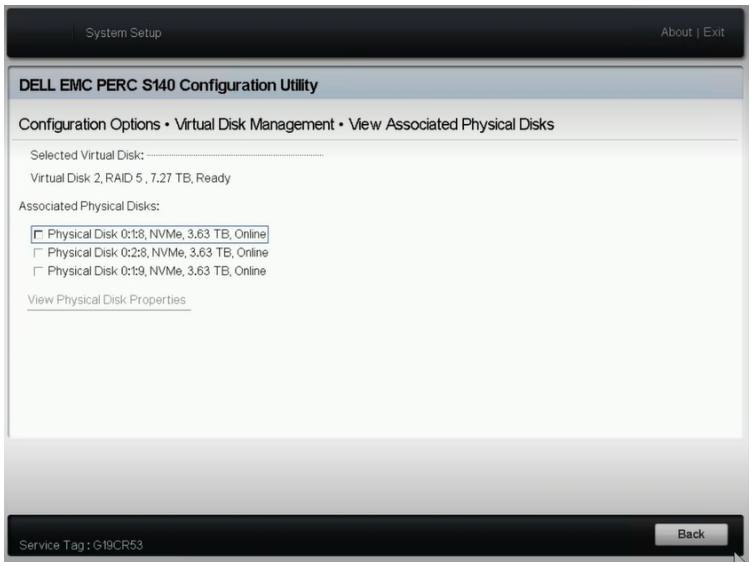


a. To manage your virtual disks, click **Manage Virtual Disk Properties**.

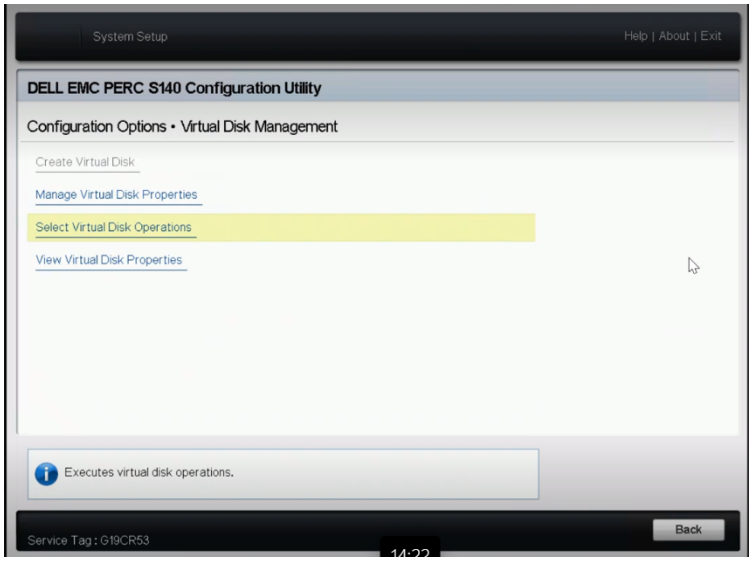
From the Select Virtual Disks drop-down list, select any RAID 5 disk, and then click **View Associated Physical Disks**.



The associated disks are displayed.

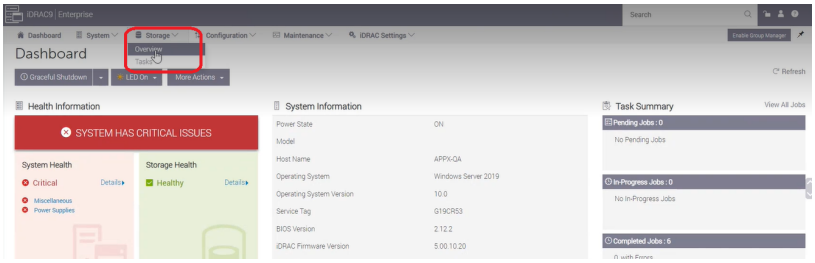


b. To select the virtual disk operations, click **Select Virtual Disk Operations**.

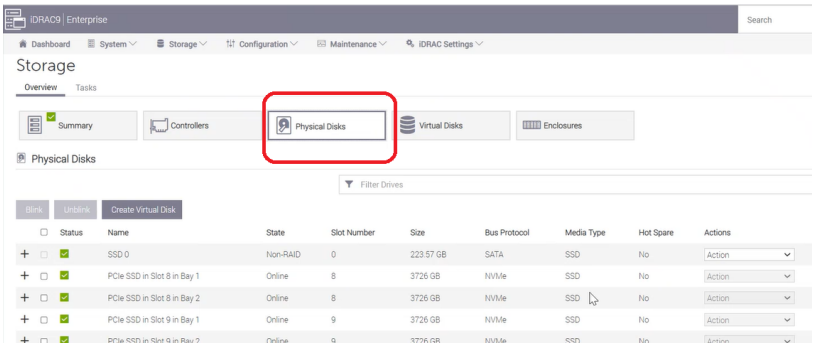


c. To view the virtual disk properties in the Boot Manager, click **View Virtual Disk Properties**.

5. To view the disk information in iDRAC, log into iDRAC, and then click **Storage** > **Overview**.

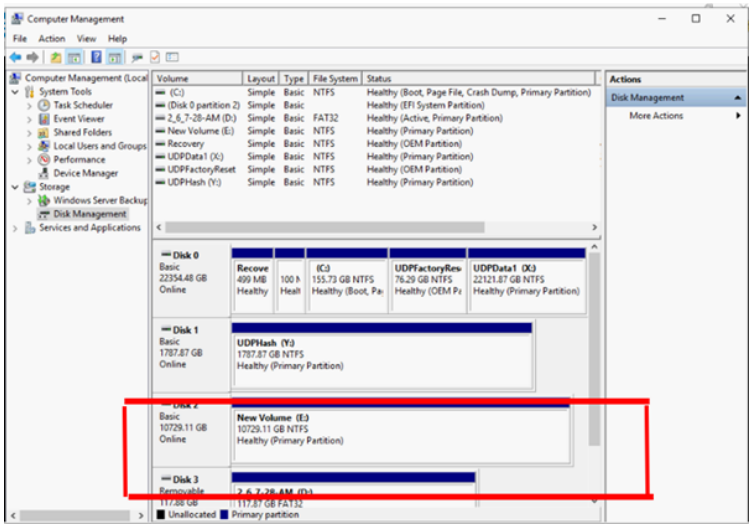


In the Overview section, click **Physical Disks** to view the list of physical disks that you have created.



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



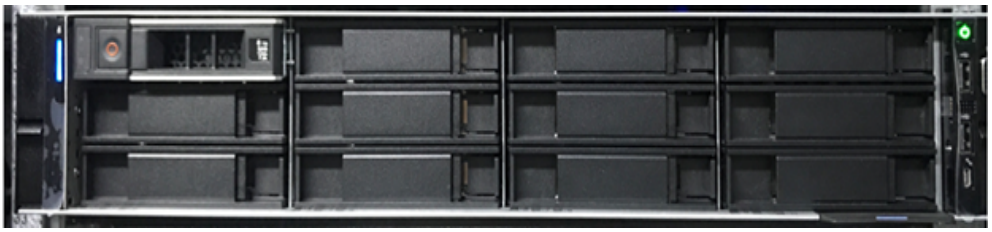
The virtual disk is created.

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.

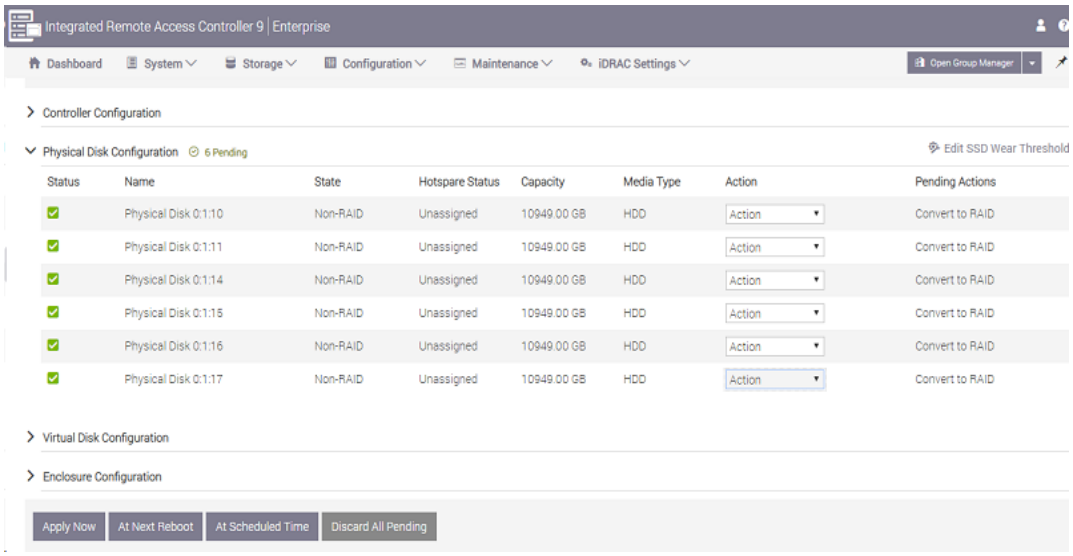
    A dialog appears to display the following warning message:

    RAC0516: Converting physical disk drives to RAID-compatible will over-write 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:

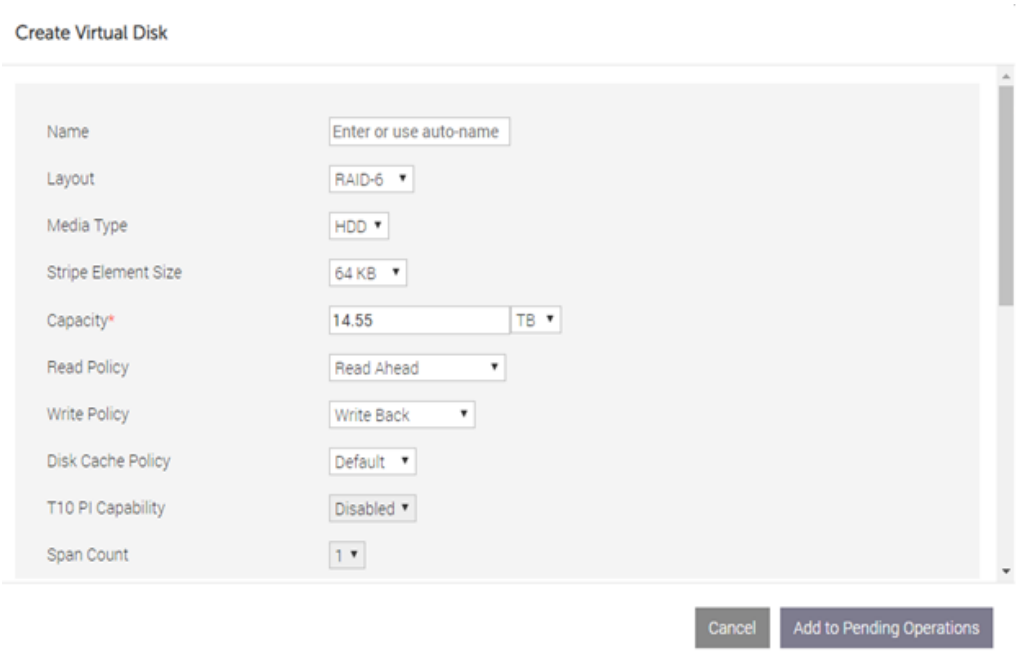
a. Navigate to Configuration, Storage Configuration and Virtual Disk Configuration.

b. Under **Virtual Disk Configuration** section, click **Create Virtual Disk**.

c. Select **RAID-6** as **Layout**.

d. Under **Select Physical Disks** section, select the disks that are converted to RAID.

e. Click **Add to Pending Operations**.



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**.

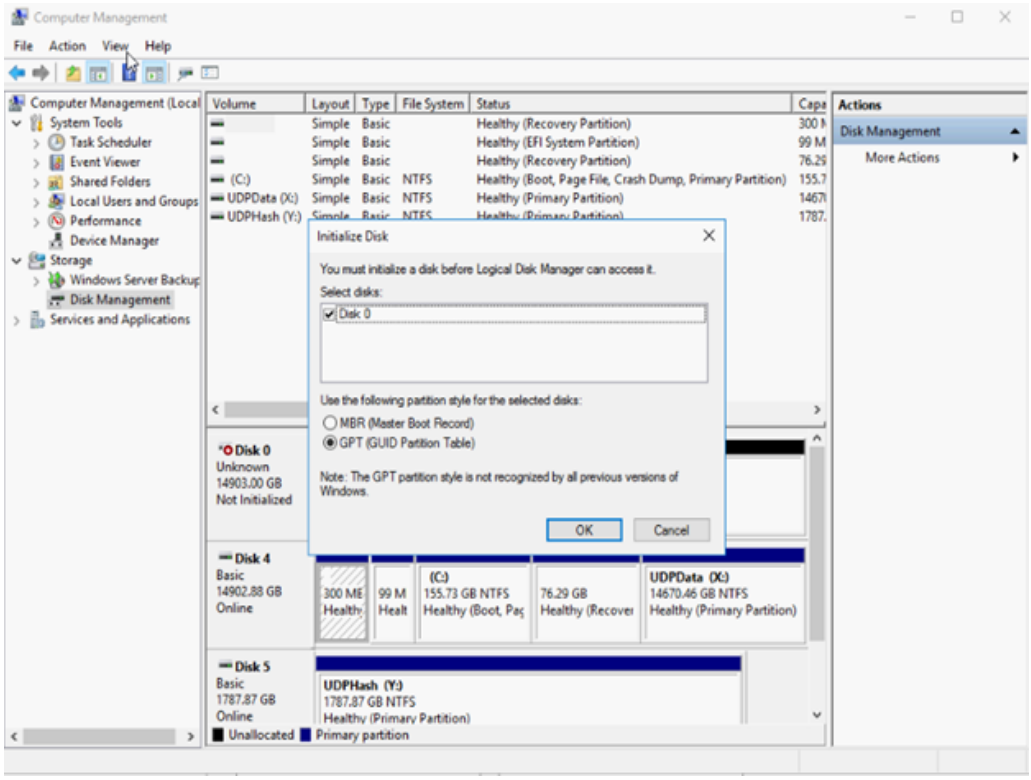
j. Double click the new virtual disk that you added.

The Initialize Disk window appears.

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

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



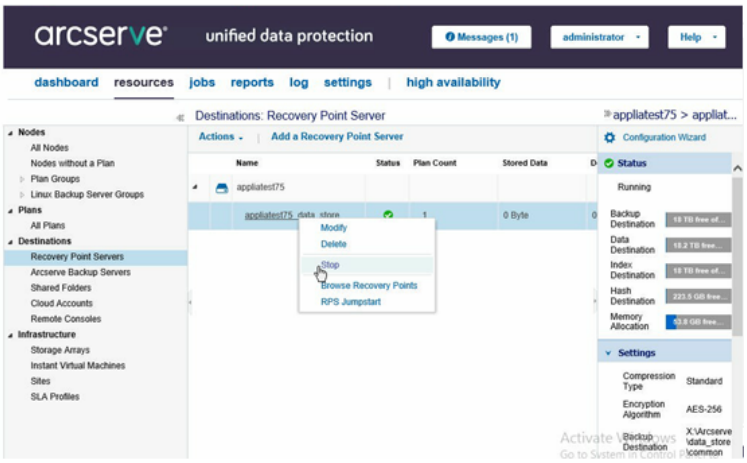
4. Perform the following steps to expand the datastore:
   a. Navigate to the Drive that you added and create a folder.
   b. From the Arcserve Appliance desktop, launch the **Arcserve Appliance** wizard.

   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.

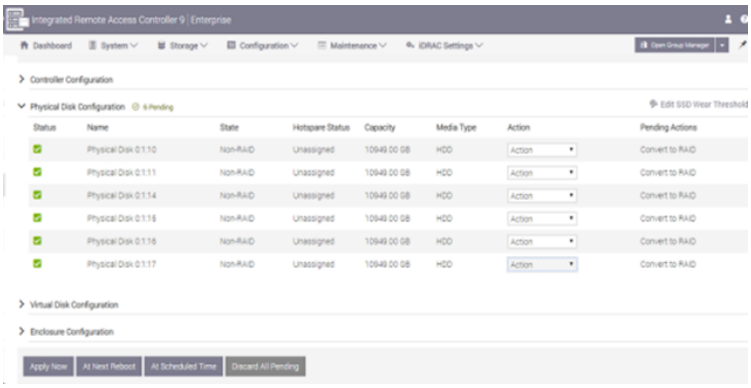
2. Perform the following steps to configure Raid-5 from iDRAC:
   a. Log into iDRAC, and then navigate to **Configuration > Storage Configuration > Physical Disk Configuration**.
   b. Under the Physical Disk Configuration section, from the **Actions** drop-down list of each new SSD DISK, select the **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

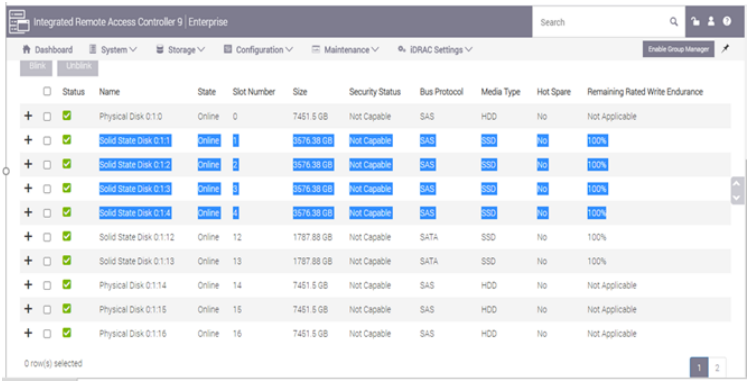
Starts the convert to Raid action at the scheduled time.

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%.



3. Perform the following steps to create virtual disk:

a. Navigate to **Configuration > Storage Configuration > Virtual Disk Configuration**.

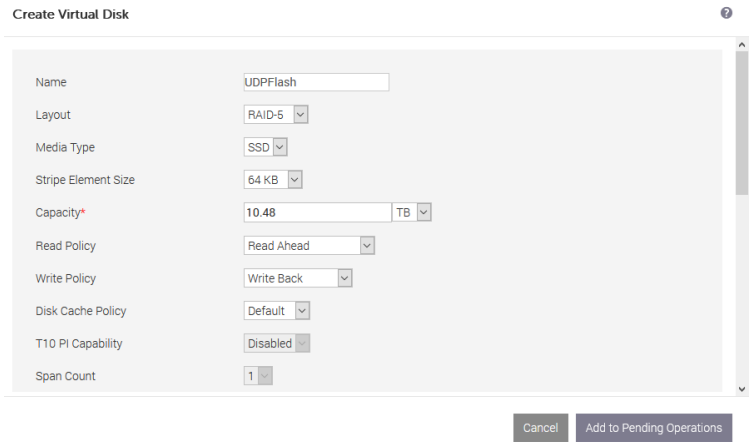
b. Under Virtual Disk Configuration section, click **Create Virtual Disk**.

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.

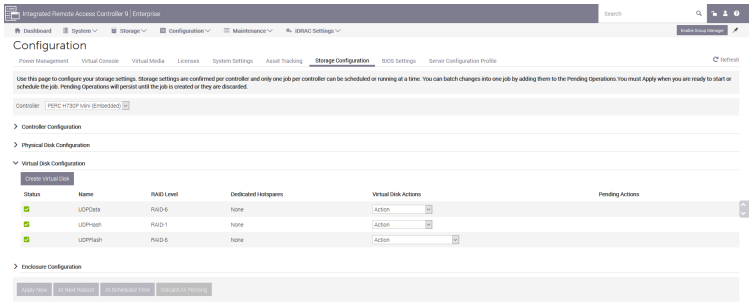
d. Under Select Physical Disks section, scroll down and select all the SSD disks that are converted to RAID.

e. Click **Add to Pending Operations**.



f. Navigate to **Configuration > Storage Configuration**.

g. To create the virtual disk operation immediately, click **Apply Now**.



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**.

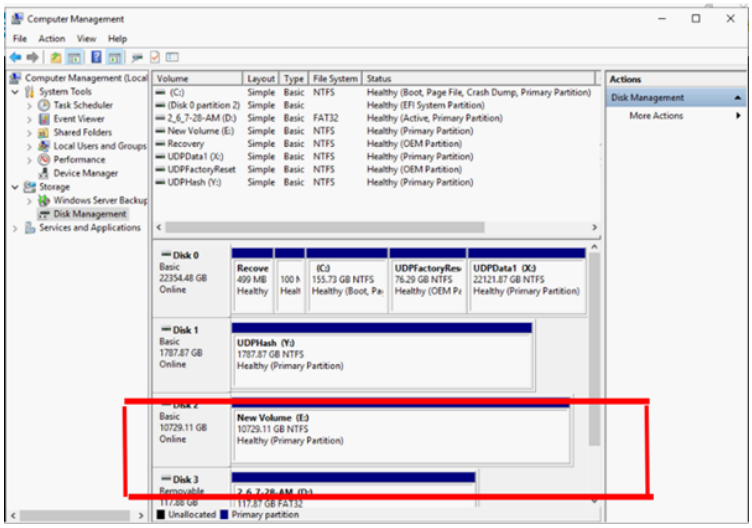
j. Double click the new virtual disk that you added.

   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 191

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

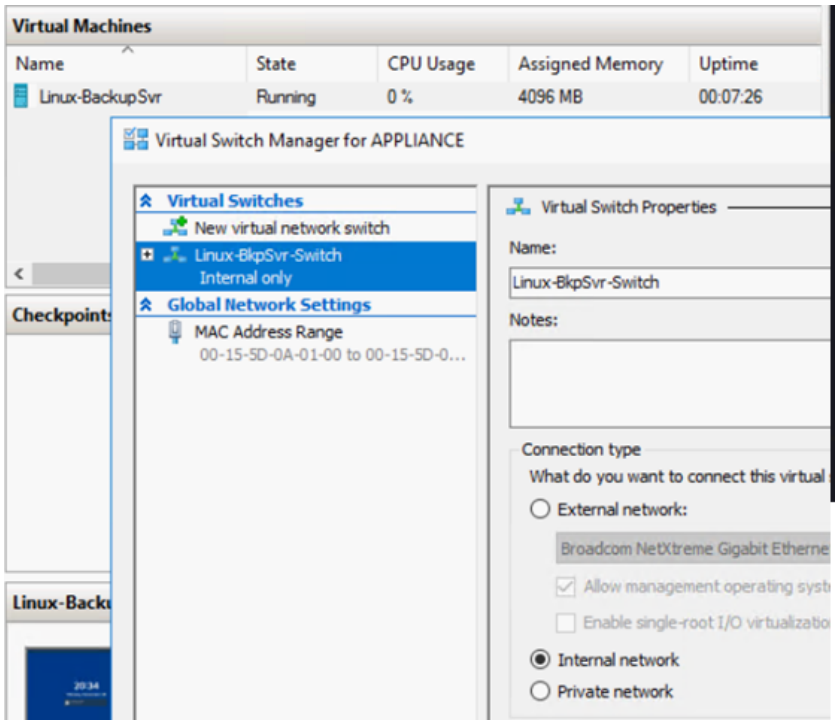
Understanding the Network Configuration Details

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:

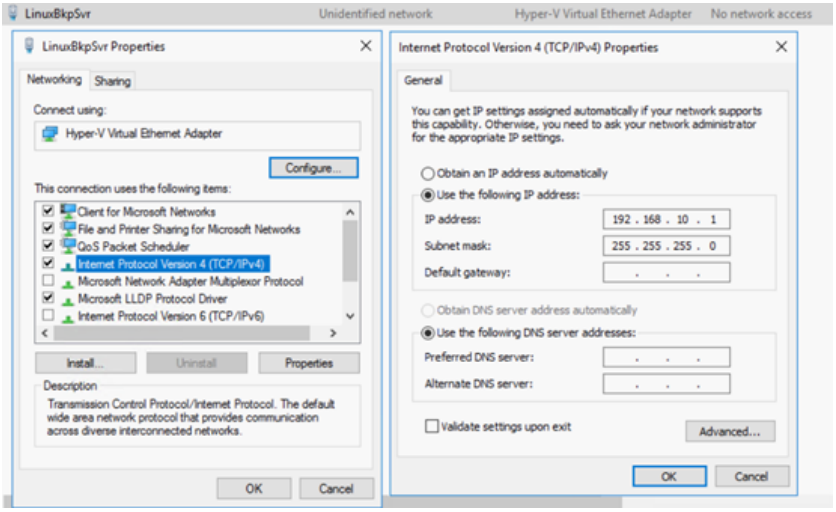
- User does not need to change the host name of the built-in Linux.
- User saves an IP on the network for the Linux Backup Server.
- The Linux Backup Server can connect to any machine on the public network.
- Any machine on the public network can connect to the Linux Backup Server through the special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

Network Configuration Details:

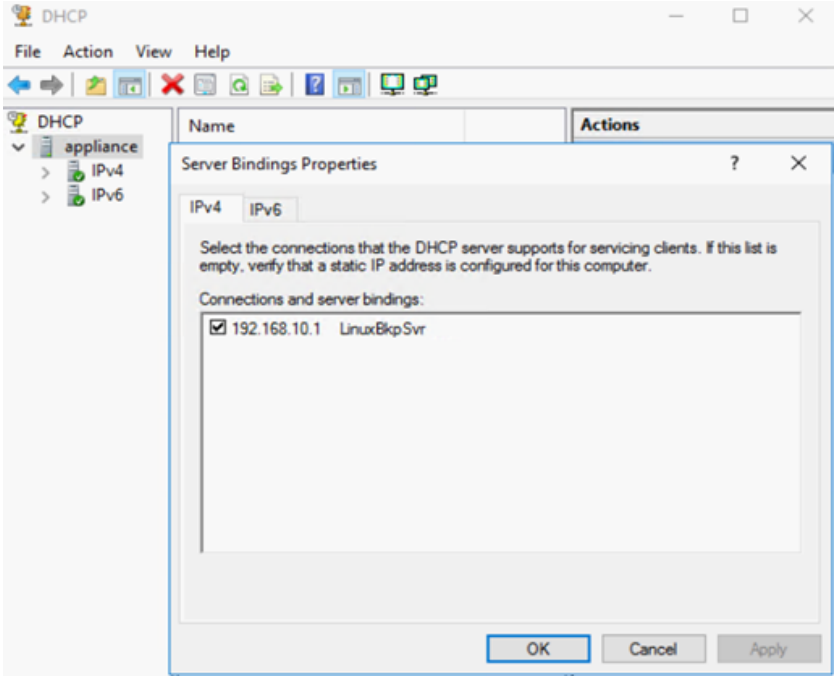
- On the Hyper-V Manager, an internal only virtual switch – *Linux-BkpSvr-Switch* is available that is used only by Linux-BackupSvr.



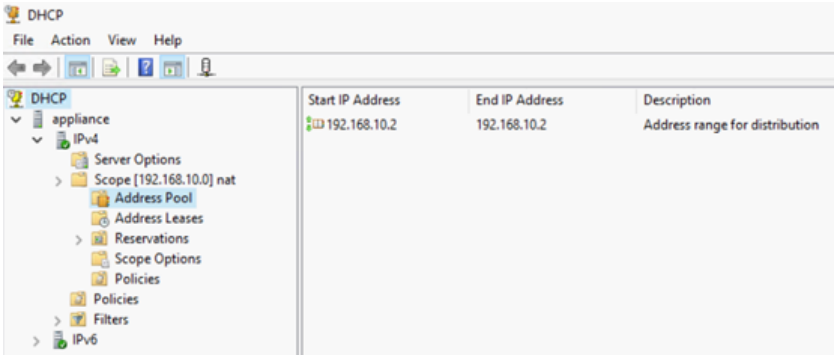
- In the *Control Panel\Network and Internet\Network Connections*, you can see “Hyper-V Virtual Ethernet Adapter” named as “LinuxBkpSvr”. You have configured the IPv4 for this switch as “192.168.10.1” by default as below.



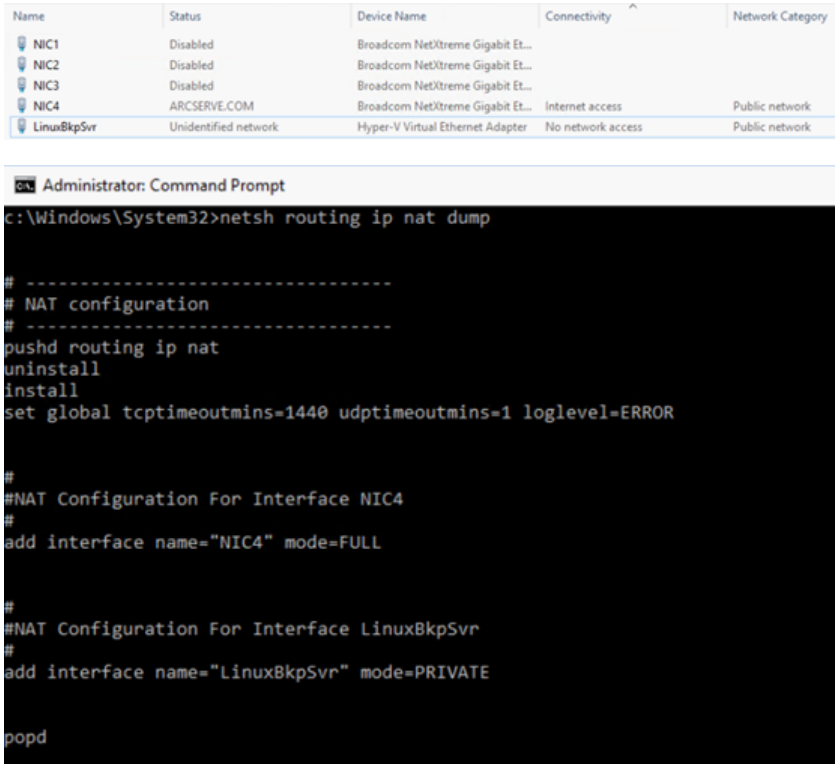
- You have configured DHCP Server on the appliance machine by default. The DHCP Server works only on the Hyper-V virtual adapter.



- 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.

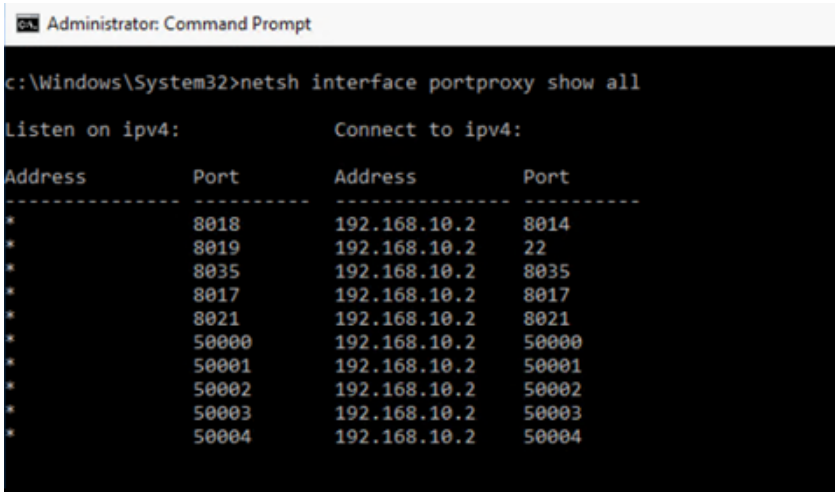


- We have configured NAT on the Appliance machine.



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

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



- 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\dhcpdone.flag* file.
5. Run *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\User_Utilities\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:

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

Using this method, a Resolver always obtains IPAddress1 when sending a query for Altname1 and always obtains IPAddress2 when sending a query for Altname2.

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.

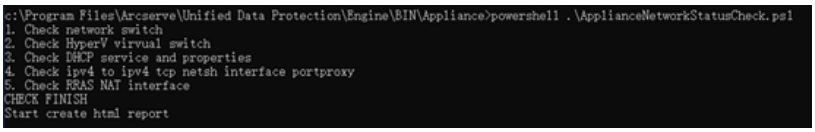
The ApplianceNetworkStatusCheck.ps1 tool is available in Arcserve Appliance Server UDP V7.0 Update1.

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



   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)

  이기기는업무용(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.

Upgrading Firmware for Arcserve Appliance 10000 Series

This section describes how to perform the following:

Viewing Firmware Version

This section provides information about how to view the current firmware version.

Follow these steps:

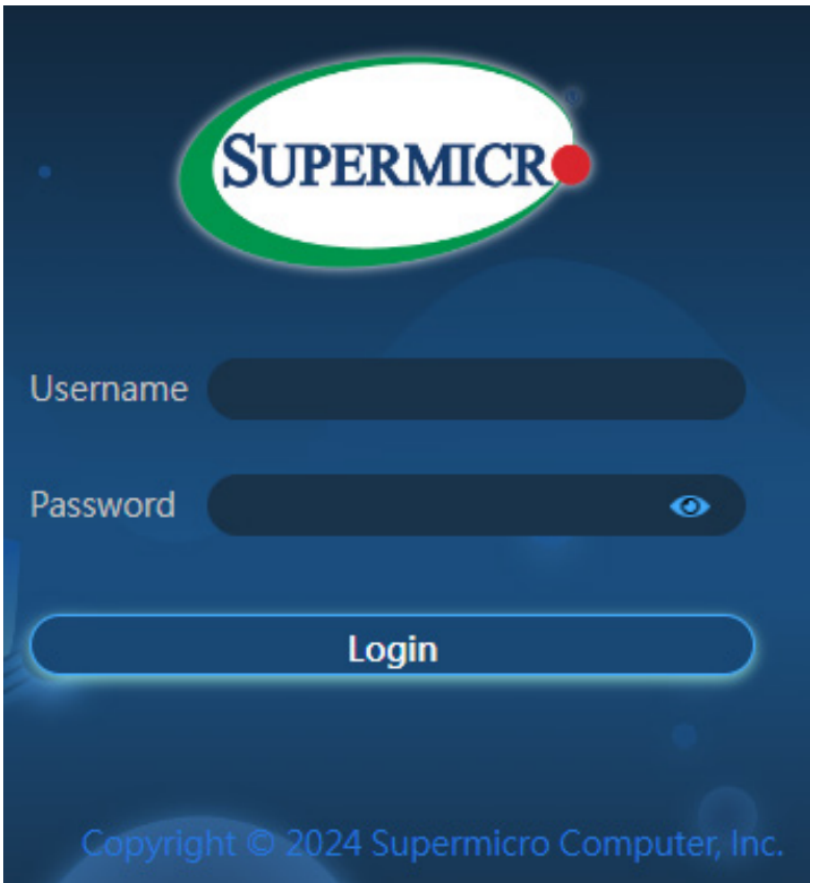
1. Open a web browser and enter the static IP of Intelligent Platform Management Interface (IPMI).

   The login screen appears.

2. Type the login credentials as follows:
   - **Username:** ADMIN.

     Note: The username must be in caps.
   - **Password:** Type the BMC password**.**

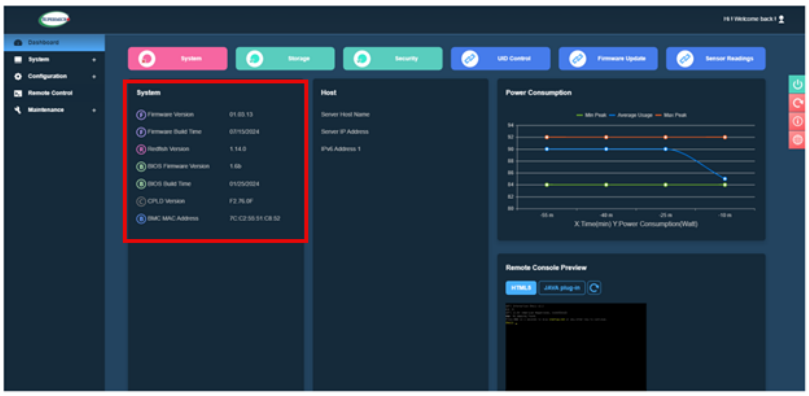
3. Click **Login.**



The IPMI Web Server interface appears.

Note: You can find the BMC/IPMI unique password in the pull-out tag on the front panel of the server. The BMC password is listed in the bottom row just below the BMC/IPMI MAC Address.

The Dashboard screen displays the firmware version under System.



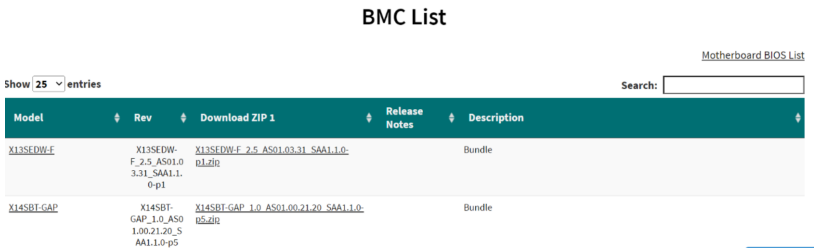
Download the Firmware Upgraded Package

This section provides information about how to download the current firmware version.

Follow these steps:

Note: You can download the latest firmware update package from the Supermico website or contact Supermicro support.

1. Go to the Supermicro website.
2. On the BMC List, search for the motherboard model of Server 1U (X13SEW-F) or 2U (X13DEI-T) to download the firmware update.



3. Click **Download Zip 1** corresponding to the selected motherboard model.

   The *End User License Agreement* page appears.

4. Click **Accept** to initiate the download.

   The firmware update file gets downloaded and saved locally on your system.

   Note: The firmware update file type varies according to the device such as BMS, BIOS, and so on.

The firmware update file is downloaded successfully.

Upgrade Firmware

This section contains the following topics:

How to Upgrade BMC firmware

This section provides information about upgrading the BMC firmware.

Follow these steps:

1. Open a web browser and enter the static IP of Intelligent Platform Management Interface (IPMI).

   The login screen appears.

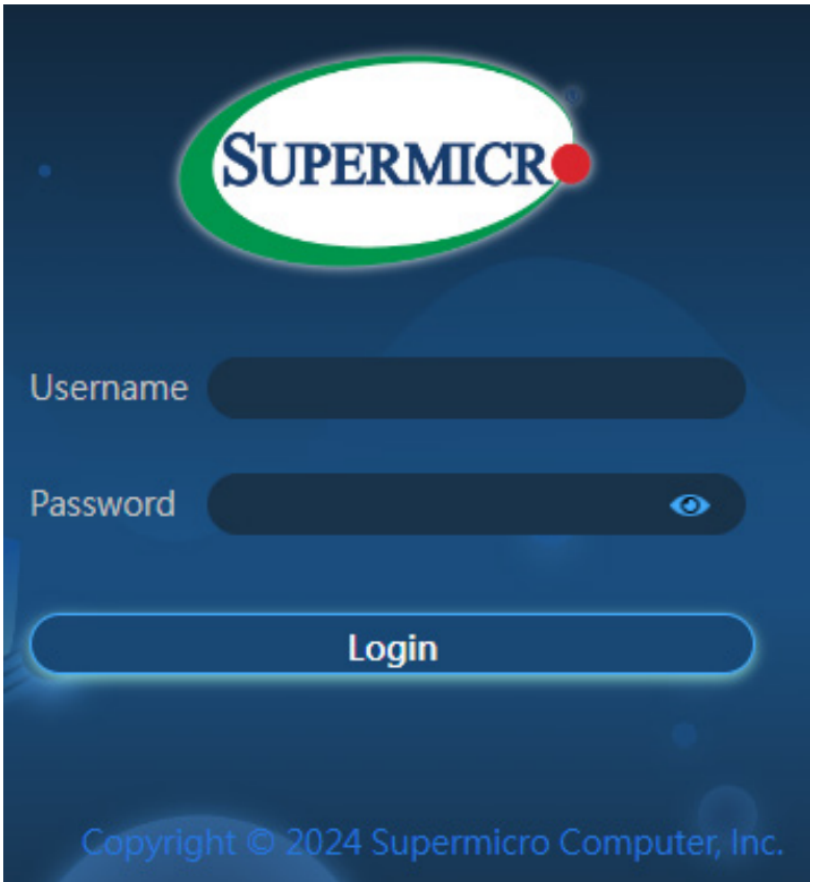
2. Type the login credentials as follows:

   - **Username:** ADMIN.

     Note: The username must be in caps.

   - **Password:** Type the BMC password**.**

3. Click **Login.**



The IPMI Web Server interface appears.

Note: You can find the BMC Unique password in the service tag on the server chassis. The BMC password is listed in the bottom row just below the Intelligent Platform Management Interface (IPMI) MAC Address.

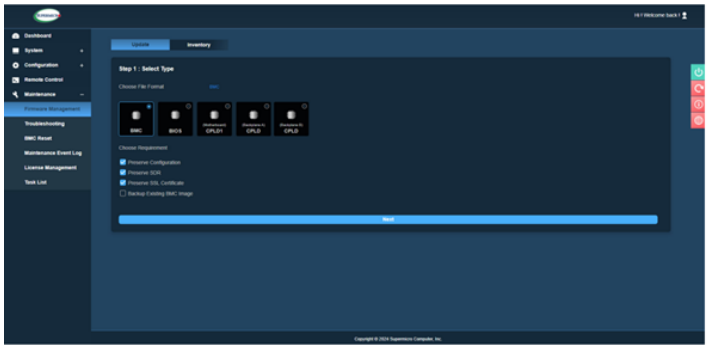
4. Navigate to **Maintenance** -> **Firmware Management**.
5. On the Update screen, do the following:

a. Under *Step 1: Select Type*, select **BMC** as file format.

b. (Optional) Select the following preserve configuration options as required and then click **Next**:.

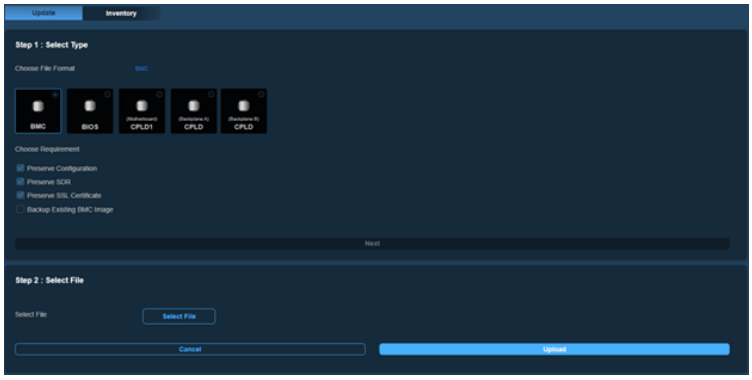
- Preserve Configuration:
- Preserve SDR:
- Preserve SSL certificate:
- Backup existing BMC image:

  To backup the existing BMC image, select the **Backup Existing BMC Image** check box. In case of failed integrity at any time, you can use the Backup image for auto-recovery. You can also manually recover BMC from the Inventory page.

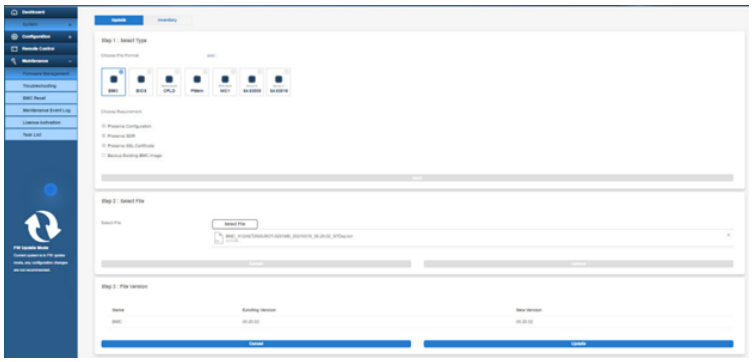


c. Under *Step 2: Select File*, click **Select File**, browse the locally saved firmware update file, and then click **Upload**.

Note: If you click **Upload** without including a BMC image, the following message gets displayed: *Please select an image file. Click here to return.*

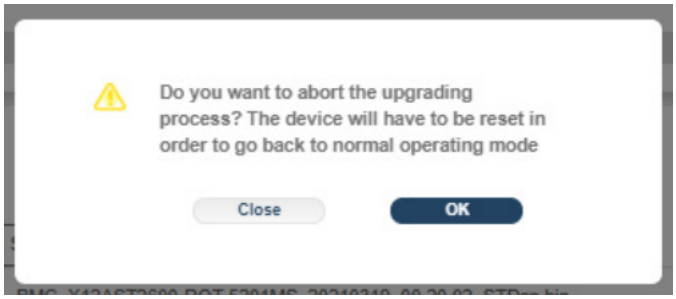


d. Under *Step 3: File Version*, review the existing and new firmware versions, and then click **Update**.



Notes:

- For most firmware updates, you must shut down the motherboard as per the system prompt. After shutting down the motherboard, you can proceed with the update.
- If you cancel the firmware BMC updating process, an alert appears asking if you want to abort the upgrade. If you click **OK**, the BMC resets and displays the message: *BMC is restarting*. After confirmation, do not remove the power source until BMC is back online to prevent data loss.



- After completing the firmware update, you might experience a long time in refreshing the web browser. Tthe rebooting message may display for a minute or two when logging in.

The firmware upgrade for BMC is upgraded successfully .

How to Upgrade BIOS firmware

To upgrade BIOS firmware, follow these steps:

1. Open a web browser and enter the static IP of Intelligent Platform Management Interface (IPMI).

   The login screen appears.

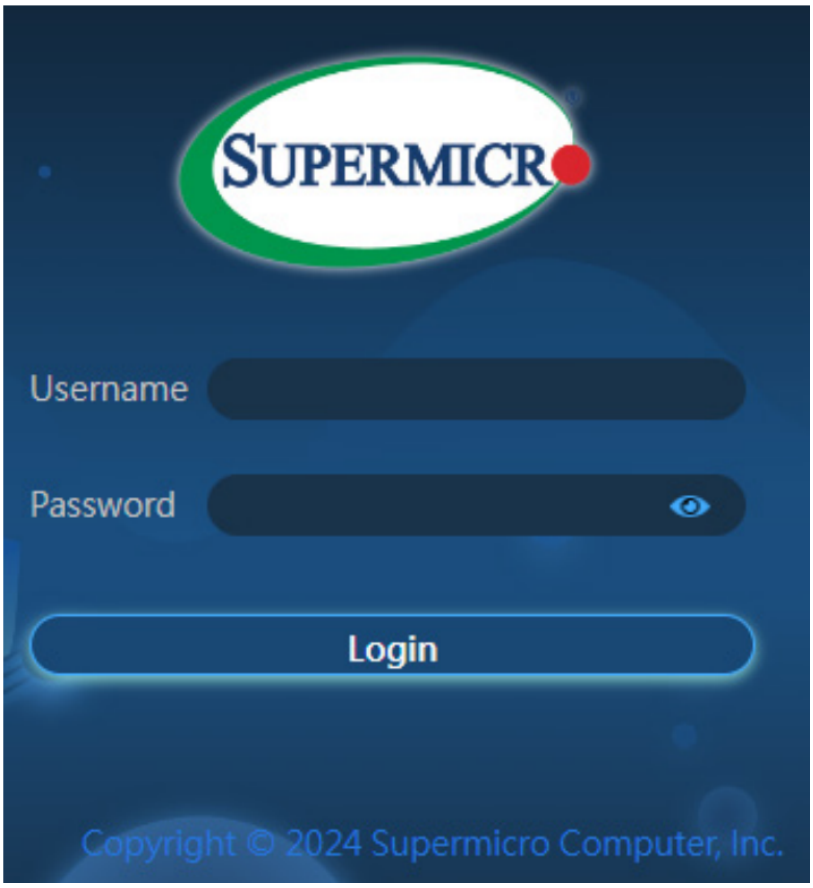
2. Type the login credentials as follows:

- **Username:** ADMIN.

  Note: The username must be in caps.

- **Password:** Type the BMC password**.**

5. Click **Login.**



The IPMI Web Server interface appears.

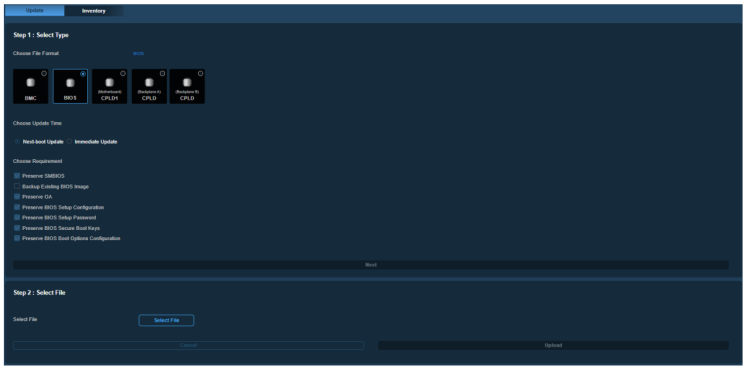
Note: You can find the BMC Unique password in the service tag on the server chassis. The BMC password is listed in the bottom row just below the Intelligent Platform Management Interface (IPMI) MAC Address.

6. Navigate to **Maintenance** -> **Firmware Management**.

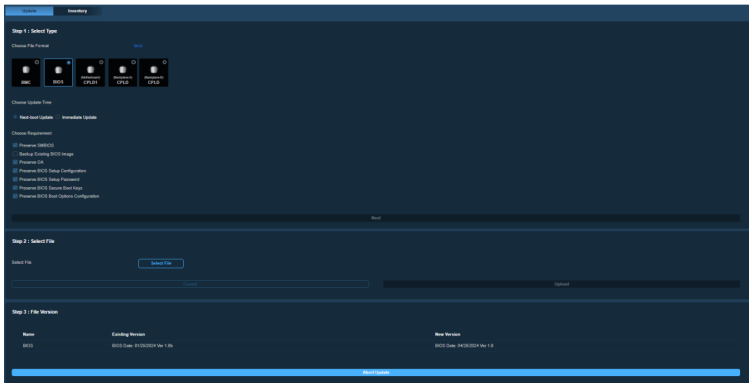
7. On the Update screen, do the following:
   a. Under the *Step 1: Select Type*, select **BIOS** as file format.
   b. (Optional) Select the following preserve configuration options as required, and then click **Next**.
      - Preserve SMBIOS
      - Preserve OA
      - Preserve SMBIOS
      - Preserve BIOS Setup Configuration
      - Preserve BIOS Setup Password
      - Preserve BIOS Setup Secure Boot Keys
      - Preserve BIOS Setup Options Configuration
      - Backup Existing BIOS Image: To backup the existing BIOS image, select the **Backup Existing BIOS Image** check box. In case of failed integrity at any time, you can use the Backup image for auto-recovery. You can also manually recover BIOS from the Inventory Page.
   c. Select one of the following:
      - **Next-boot Update:**The BIOS firmware update is scheduled after the system reboots.

        Note: If you want to cancel the scheduled Next-boot Update, use the delete option on the Task List page.
      - **Immediate Update:**The BIOS firmware update starts immediately.
   d. Under the *Step 2: Select File*, click **Select File**, browse the locally saved firmware update file and then click **Upload**.

      Note: If you click **Upload** without including a BIOS image, the following message gets displayed: *Please select an image file. Click here to return*.

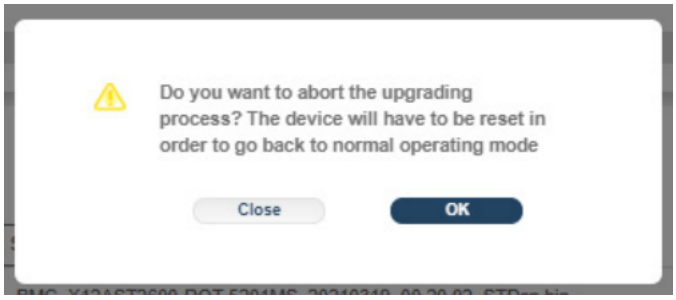


e. Under the *Step 3: File Version*, review the existing firmware version and new firmware version and then click **Update**.



Notes:

- For most firmware updates, you must shut down the motherboard as per the system prompt. After shutting down the motherboard, you can proceed with the update.
- If you cancel the firmware BIOS updating process, an alert appears asking if you want to abort the upgrade. If you click **OK**, the BIOS resets and displays the message: *BIOS is restarting*. After confirmation, do not remove the power source until BIOS is back online to prevent data loss.



- After completing the firmware update, you might experience a long time in refreshing the web browser. Tthe rebooting message may display for a minute or two when logging in.

The firmware upgrade for BIOS is successfully upgraded.

Verify Updated Firmware

This section provides information about how to verify firmware update progress.

Follow these steps:

1. Log into the IPMI website.
2. Navigate to **Maintenance** -> **Task List**.

   The Task List screen appears with the maintenance operation running on the system.

3. Review the log and verify the status and progress of the firmware update.

   The Task List screen provides the following details of the firmware update job:

   - **Health Status:** Provides the health status of current tasks.
   - **Task Name:** Displays the name of the task.
   - **State:** Displays the current state values (Running, Completed, or Failed).
   - **Progress:** Provides the progress of current running task(s).

   Note: Administrators can cancel the pending BMC and BIOS firmware update. To cancel, click the **Abort pending Task** option under Task List.

Chapter 11: 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 222

Upgrade BIOS Firmware for Arcserve Appliance 9000 Series

This section describes how to do the following:

Viewing Firmware Version

This section provides information about how to view the current firmware version.

Follow these steps:

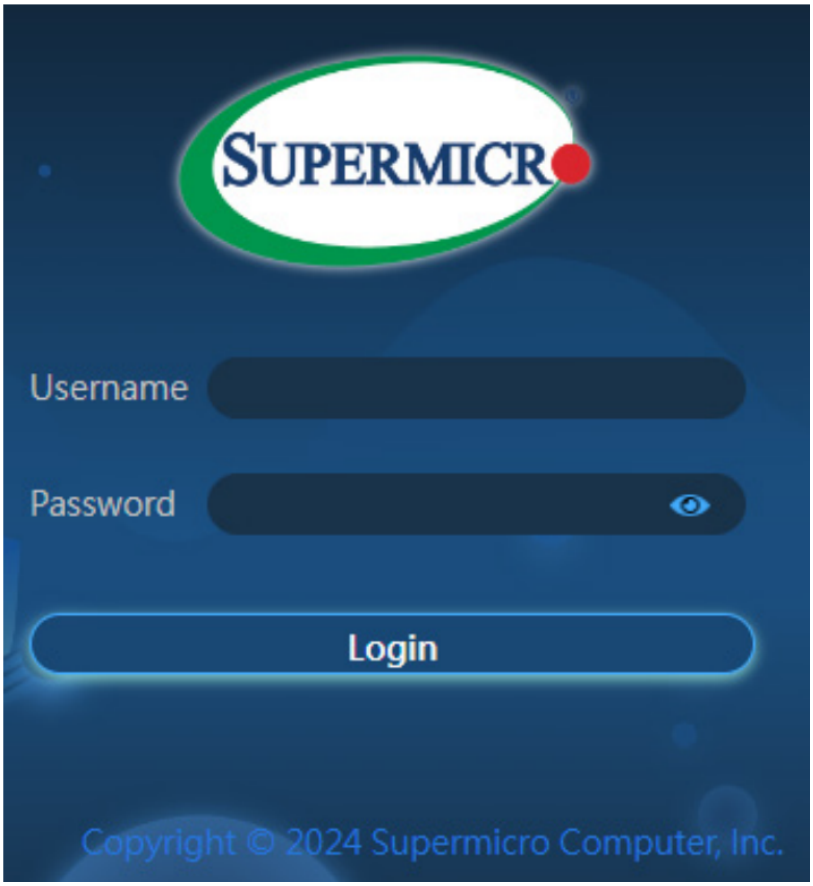
1. Open a web browser and enter the static IP of Intelligent Platform Management Interface (IPMI).

   The login screen appears.

2. Type the login credentials as follows:
   - **Username:** ADMIN.

     Note: The username must be in caps.
   - **Password:** Type the BMC password**.**

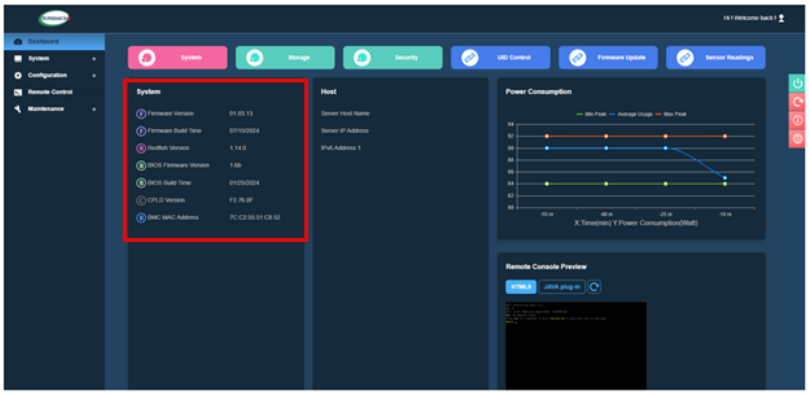
3. Click **Login.**



The IPMI Web Server interface appears.

Note: You can find the BMC/IPMI unique password in the pull-out tag on the front panel of the server. The BMC password is listed in the bottom row just below the BMC/IPMI MAC Address.

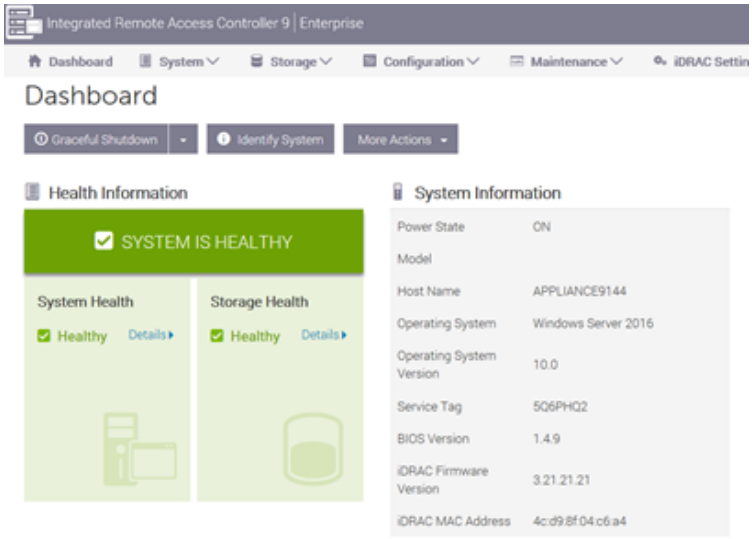
The Dashboard screen displays the firmware version under System.



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

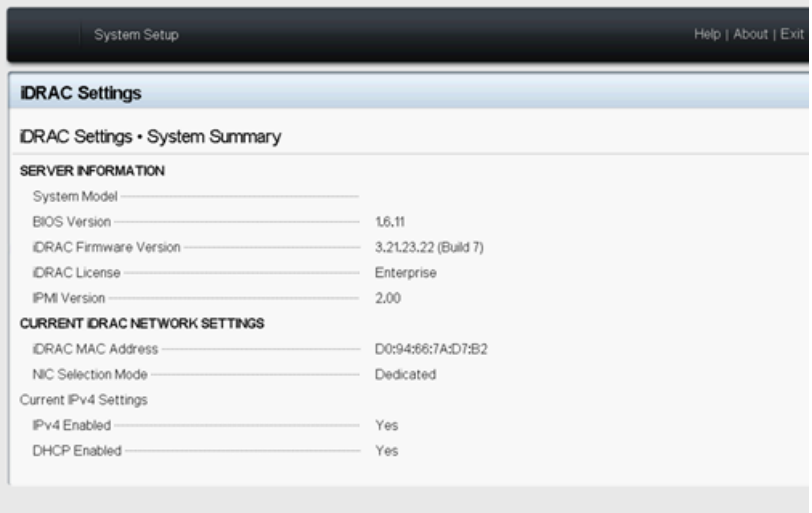


The iDRAC Dashboard page displays the System information, which contains the BIOS firmware version.

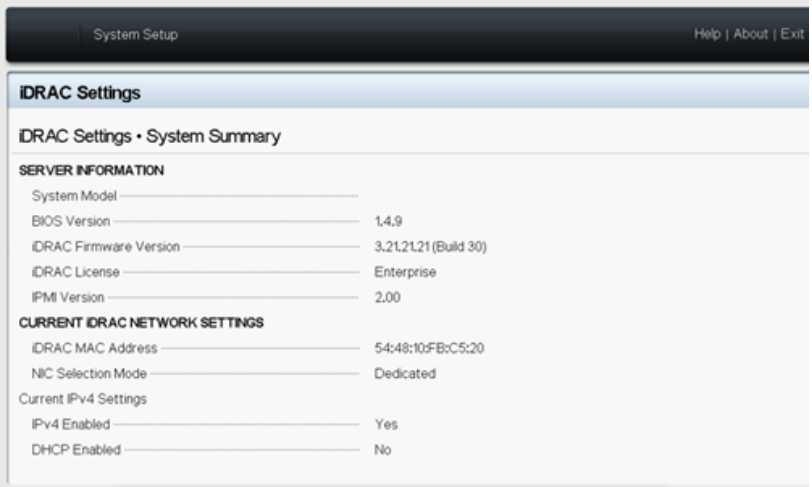
Method 2: View BIOS firmware version from BIOS Arcserve Appliance 9000 series

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.



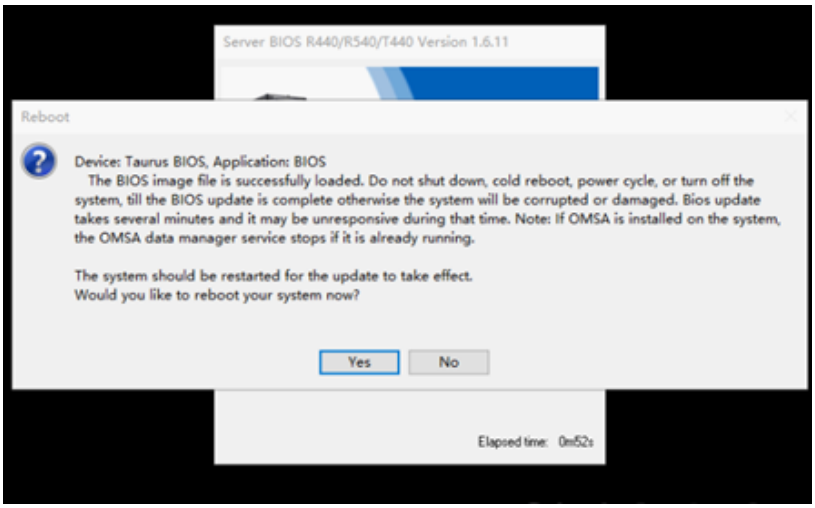
Download the Updated Package for BIOS

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 Firmware

This section provides information about how to verify firmware update progress.

Follow these steps:

1. Log into the IPMI website.
2. Navigate to **Maintenance** -> **Task List**.

The Task List screen appears with the maintenance operation running on the system.

3. Review the log and verify the status and progress of the firmware update.

The Task List screen provides the following details of the firmware update job:

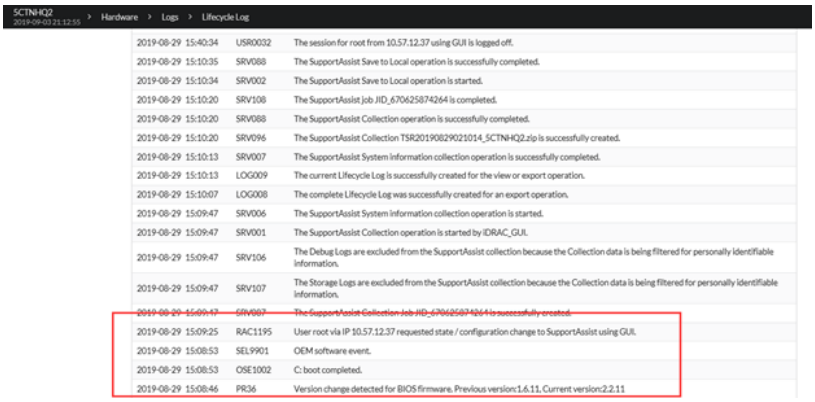
- **Health Status:** Provides the health status of current tasks.
- **Task Name:** Displays the name of the task.
- **State:** Displays the current state values (Running, Completed, or Failed).
- **Progress:** Provides the progress of current running task(s).

Note: Administrators can cancel the pending BMC and BIOS firmware update. To cancel, click the **Abort pending Task** option under Task List.

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.



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

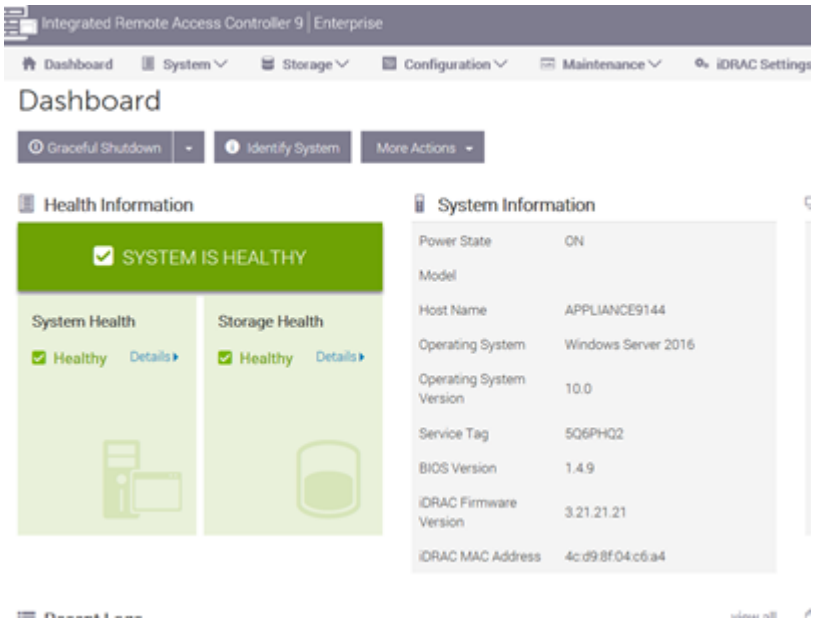
Use one of the following methods to view the iDRAC firmware version:

- 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.

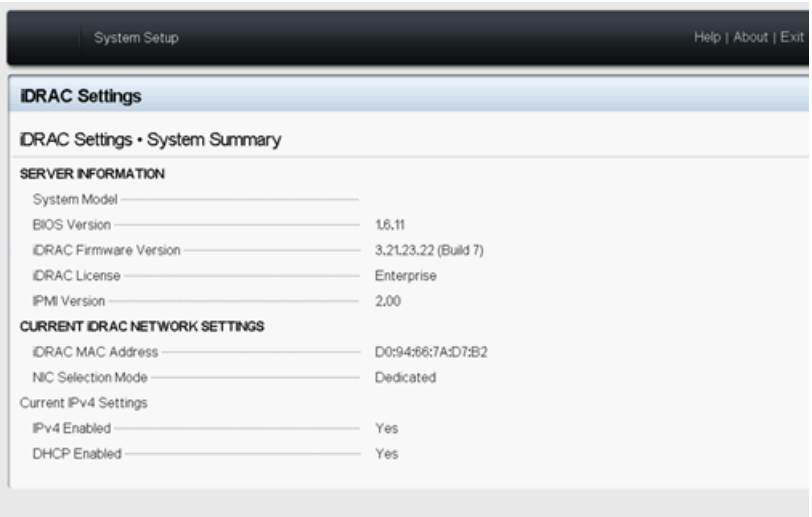


The iDRAC dashboard displays the system information, which contains iDRAC firmware version.

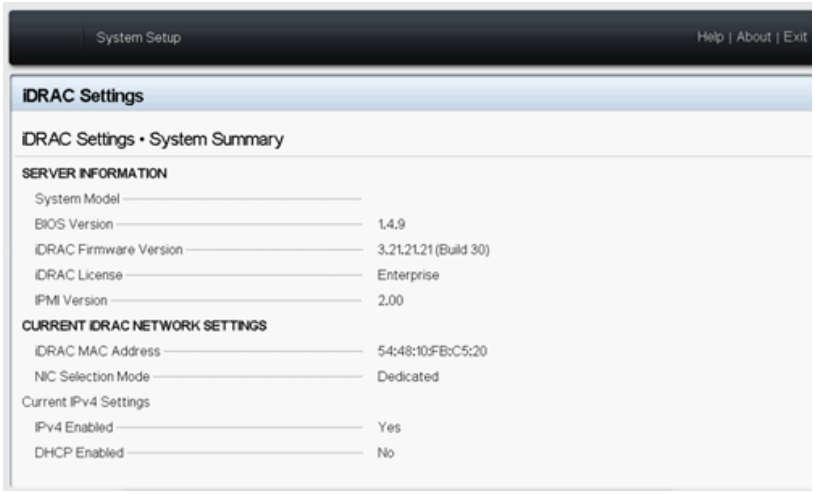
Method 2: View iDRAC Firmware Version from BIOS Arcserve Appliance 9000 series

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.

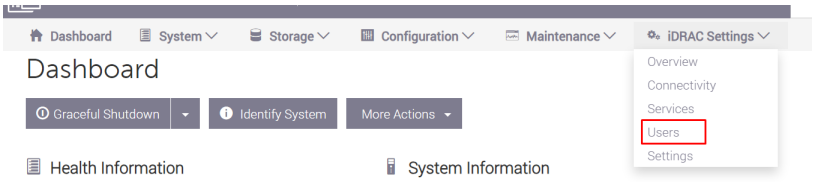


How to Change the iDRAC Password

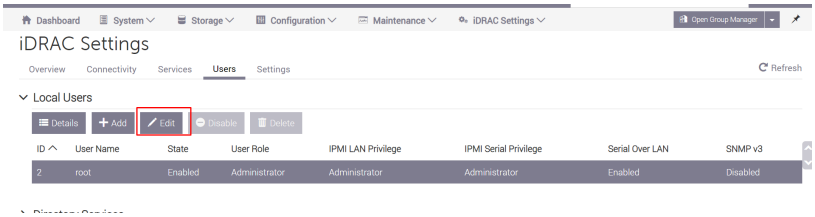
This section provides information about how to change the iDRAC password.

Follow these steps:

1. Log into iDRAC with the current password.
2. Go to **iDRAC Settings**, and then select **Users**.



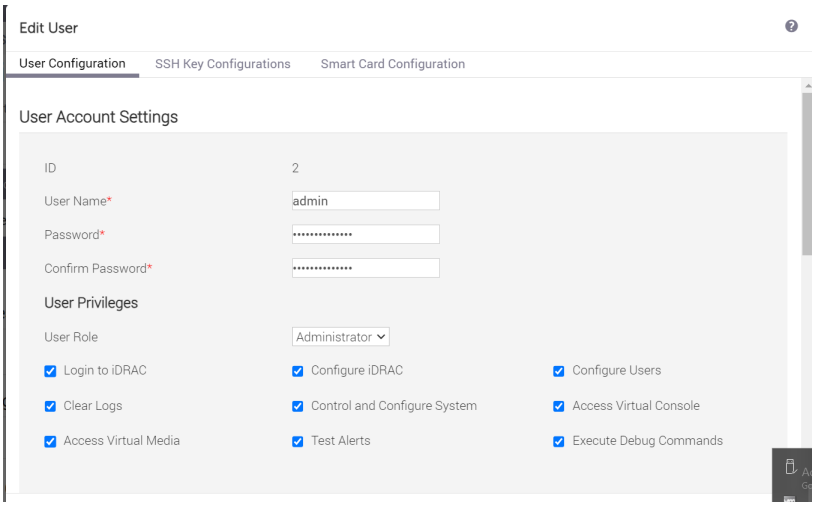
3. On the iDRAC Settings page, click the **Local Users** drop-down, and then click the **Edit** button.



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 iDRAC password is changed successfully.

Download the Updated Package for iDRAC

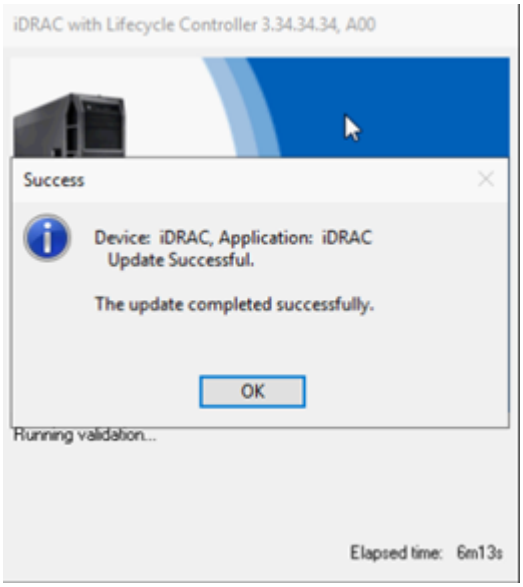
You can download the latest iDRAC firmware package of specific Arcserve Appliance 9000 Series model from the Dell website or contact Arcserve support.

Upgrade iDRAC

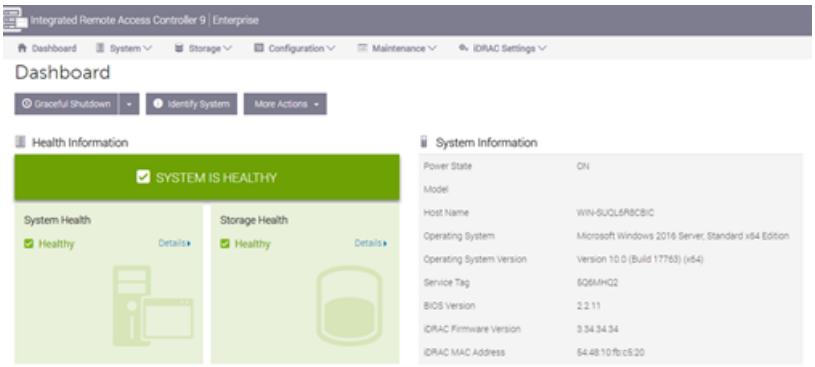
Follow these steps:

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:

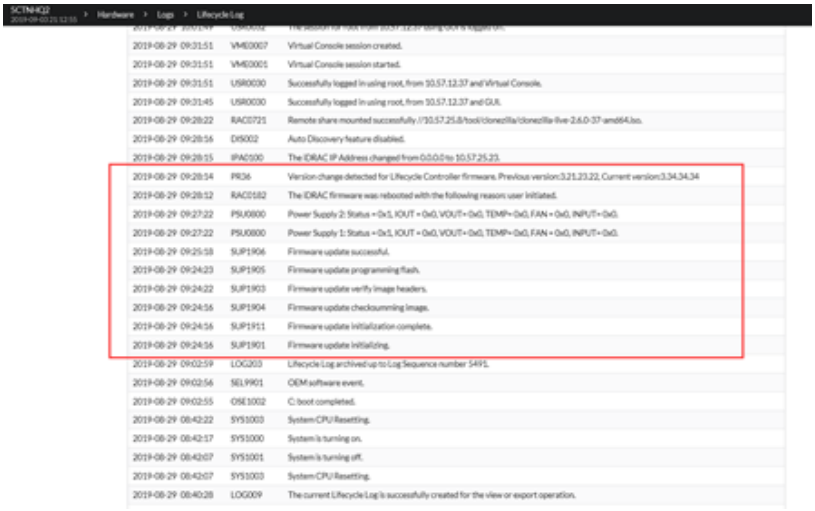
- Verify the updated iDRAC using System Logs
- Verify the updated iDRAC from iDRAC Web Interface or BIOS

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.



2019-08-29 09:31:51	VME0007	Virtual Console session created.
2019-08-29 09:31:51	VME0001	Virtual Console session started.
2019-08-29 09:31:51	USR0030	Successfully logged in using root, from 10.57.12.37 and Virtual Console.
2019-08-29 09:31:45	USR0030	Successfully logged in using root, from 10.57.12.37 and GUI.
2019-08-29 09:28:22	RAC0721	Remote share mounted successfully //10.57.25.8/tool/clonezilla/clonezilla-live-2.6.0-37-amd64.iso.
2019-08-29 09:28:16	DIS002	Auto Discovery feature disabled.
2019-08-29 09:28:15	IPAC500	The iDRAC IP Address changed from 0.0.0.0 to 10.57.25.23.
2019-08-29 09:28:14	PR36	Version change detected for Lifecycle Controller firmware. Previous version:3.21.23.22, Current version:3.34.34.34
2019-08-29 09:28:12	RAC0182	The iDRAC firmware was rebooted with the following reason: user initiated.
2019-08-29 09:27:22	PSU0800	Power Supply 2: Status = 0x1, IOUT = 0x0, VOUT= 0x0, TEMP= 0x0, FAN = 0x0, INPUT= 0x0.
2019-08-29 09:27:22	PSU0800	Power Supply 1: Status = 0x1, IOUT = 0x0, VOUT= 0x0, TEMP= 0x0, FAN = 0x0, INPUT= 0x0.
2019-08-29 09:25:18	SUP1906	Firmware update successful.
2019-08-29 09:24:23	SUP1905	Firmware update programming flash.
2019-08-29 09:24:22	SUP1903	Firmware update verify image headers.
2019-08-29 09:24:16	SUP1904	Firmware update checksumming image.
2019-08-29 09:24:16	SUP1911	Firmware update initialization complete.
2019-08-29 09:24:16	SUP1901	Firmware update initializing.
2019-08-29 09:02:59	LOG203	Lifecycle Log archived up to Log Sequence number 5491.
2019-08-29 09:02:56	SEL9901	OEM software event.
2019-08-29 09:02:55	OSE1002	C: boot completed.
2019-08-29 08:42:22	SYS1003	System CPU Resetting.
2019-08-29 08:42:17	SYS1000	System is turning on.
2019-08-29 08:42:07	SYS1001	System is turning off.
2019-08-29 08:42:07	SYS1003	System CPU Resetting.
2019-08-29 08:40:28	LOG009	The current Lifecycle Log is successfully created for the view or export operation.

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

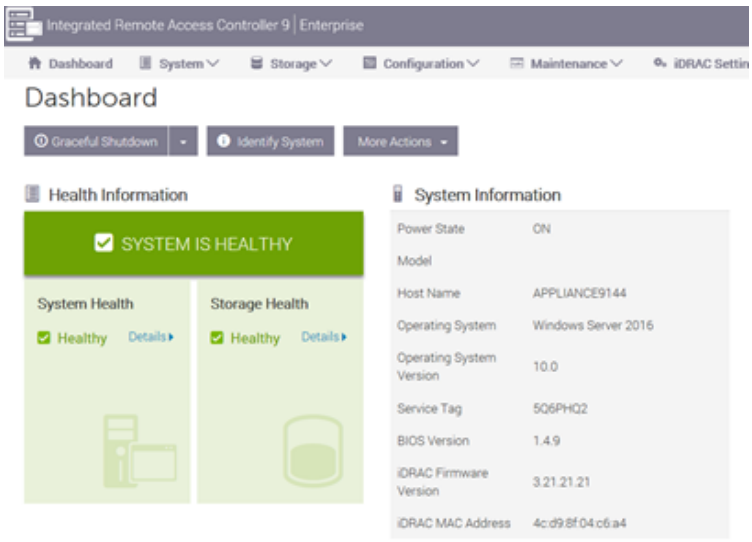
Use one of the following methods to view the BIOS firmware version:

- 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

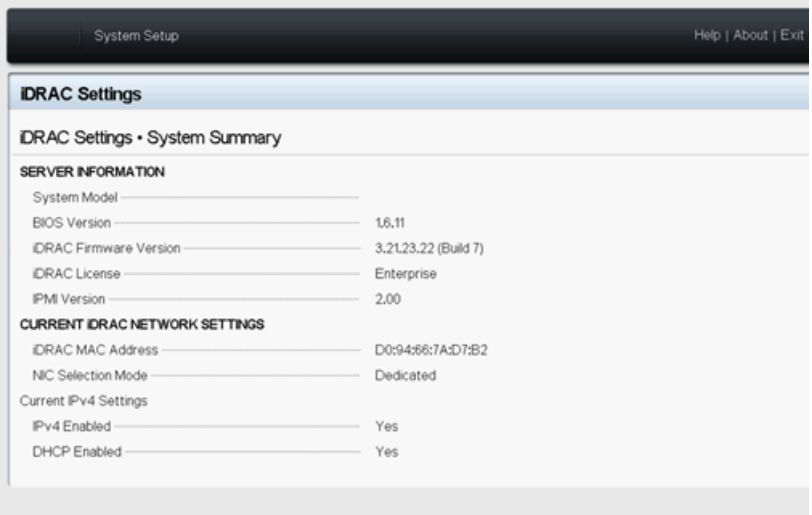


The iDRAC Dashboard page displays the System information, which contains the BIOS firmware version.

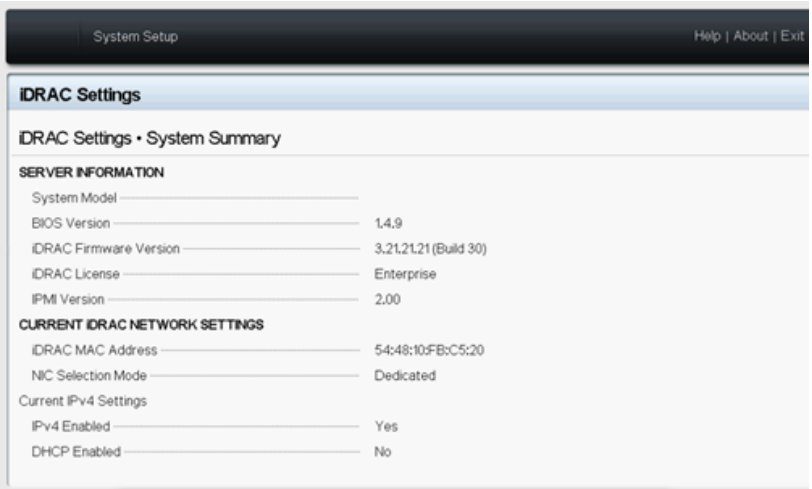
Method 2: View BIOS firmware version from BIOS Arcserve Appliance X series

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.



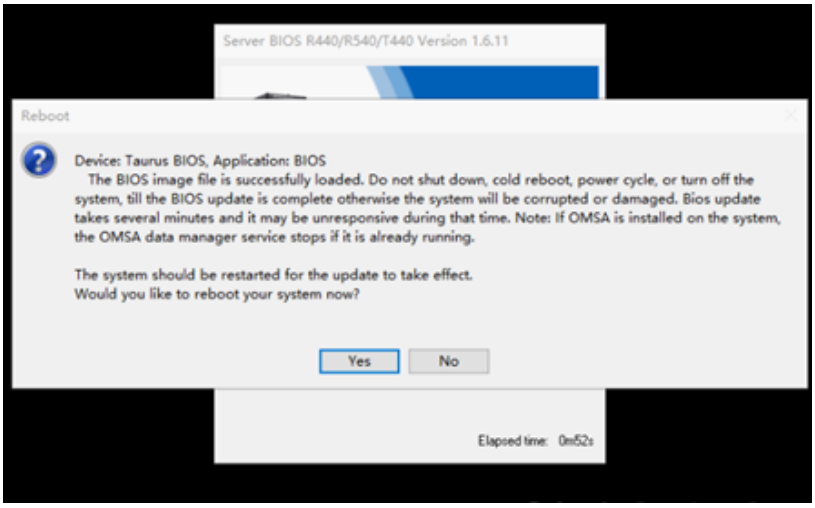
Download the Updated Package for BIOS

You can download the latest BIOS firmware package of specific Arcserve Appliance X Series model from the Dell website or contact Arcserve support.

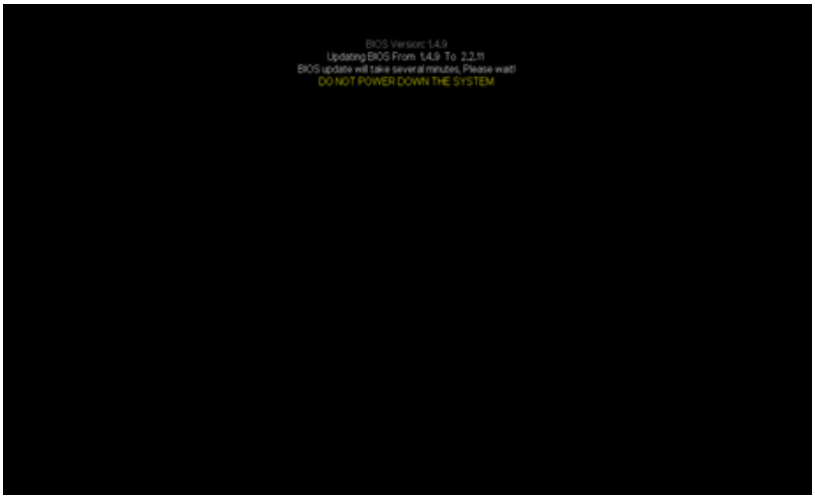
Upgrade BIOS

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

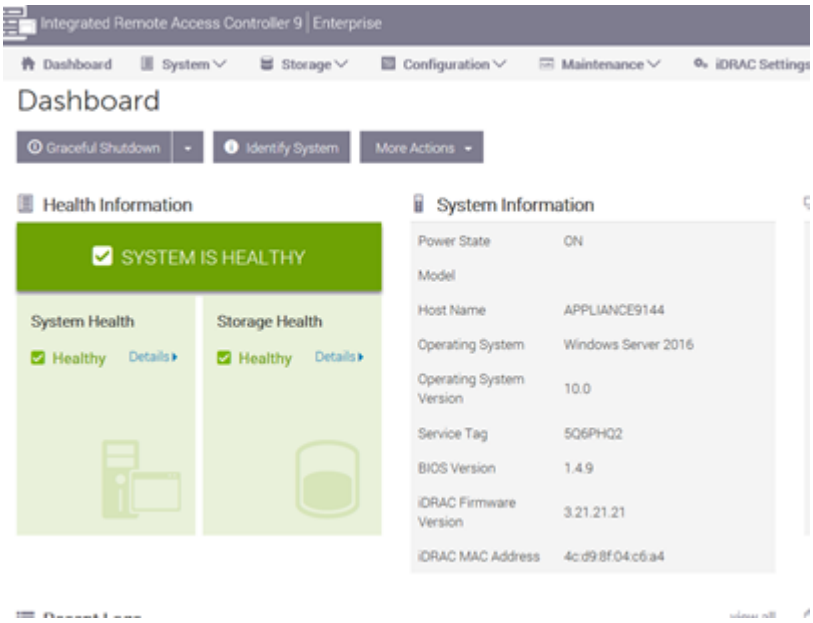
Use one of the following methods to view the iDRAC firmware version:

- Method 1: View iDRAC firmware version from iDRAC Web Interface
- Method 2: View iDRAC firmware version from BIOS Arcserve Appliance X Series

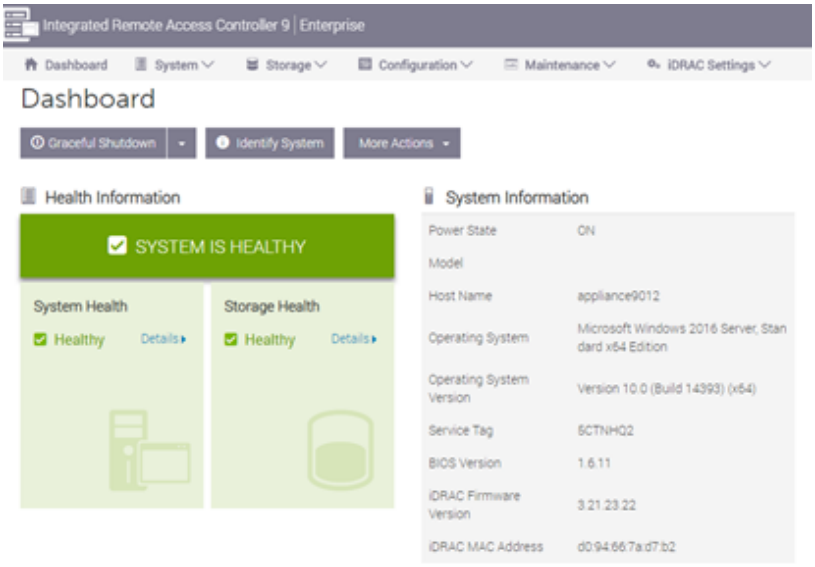
Method 1: View iDRAC firmware version from iDRAC Web Interface

Follow these steps:

1. Navigate to the iDRAC web interface.
2. To log in, enter the following:
   - **Username:** root
   - **Password:** ARCADMIN



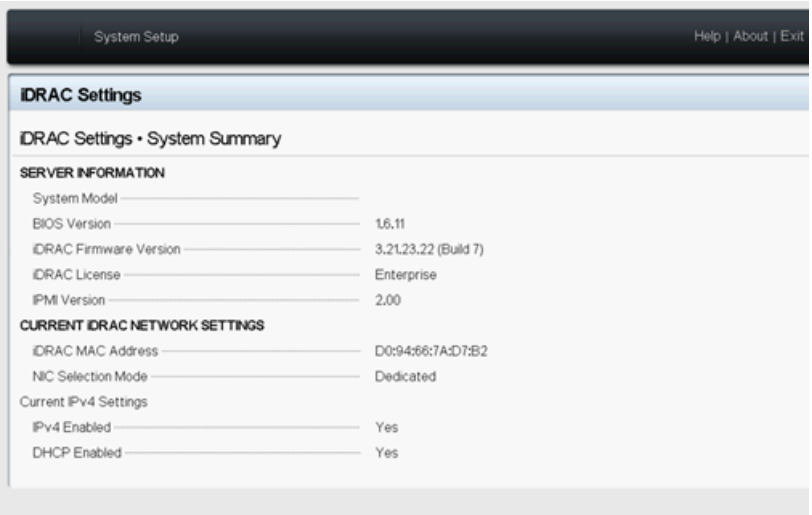
The iDRAC dashboard displays the system information, which contains iDRAC firmware version.



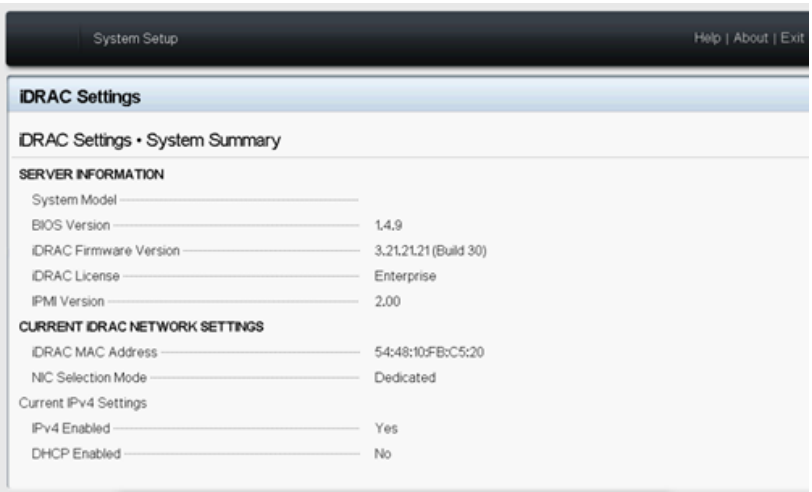
Method 2: View iDRAC firmware version from BIOS Arcserve Appliance X series

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

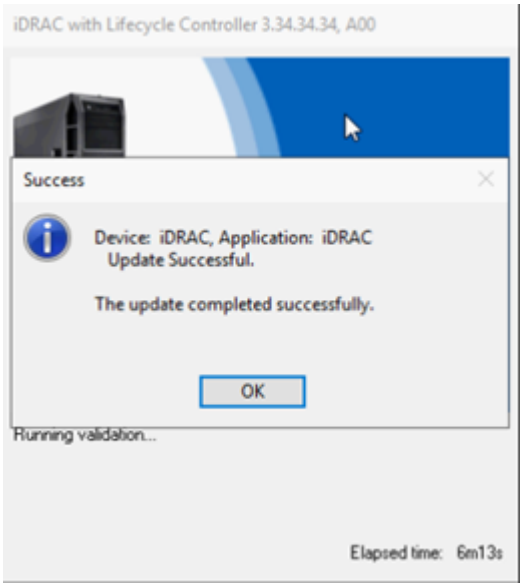
You can download the latest iDRAC firmware package of specific Arcserve Appliance X Series model from the Dell website or contact Arcserve support.

Upgrade iDRAC

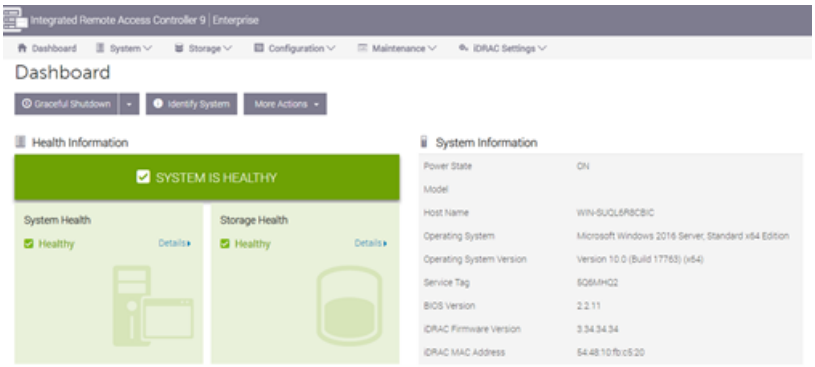
Follow these steps:

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 12: Troubleshooting

This section contains the following topics:

Linux Backup Server Fails to Connect from the Console 236

Backing Up Arcserve Appliance from Another Appliance Reports Duplicated Nodes 237

Linux Backup Server Cannot Communicate with Any Node in the Network 238

Linux Backup Server Cannot Get the Network DNS Suffix 240

Default Time Zone on the Appliance 241

Licenses Error even when the licenses are available 242

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 *dhcpdone.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 Pro-
tection\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 13: Applying Best Practices

The section contains the following topics:

Best Practices for Network Configuration 244

Best Practices for Windows Defender with PowerShell cmdlets 247

Configure Preinstalled Linux Backup Server to External Network 247

Best Practice for Creating Deduplication Datastore across Volumes 248

Best Practices for Network Configuration

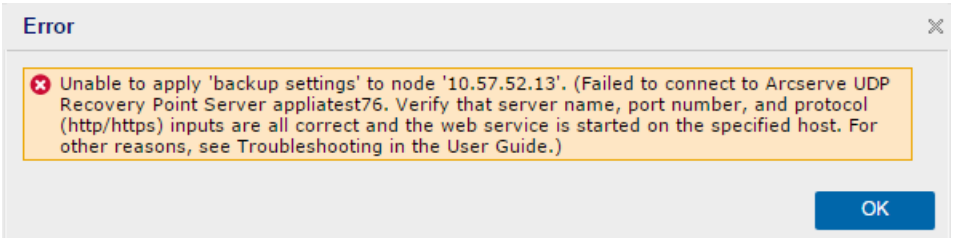
- If multiple network interfaces are connected in the production environment, ensure that each network adapter is connected to different sub network.
- If Linux node is not available in the production environment to protect, we recommend to stop the VM Linux-BackupSvr, and DHCP Server service on the 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.

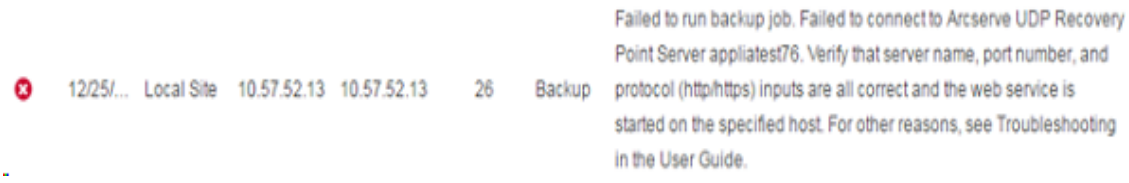
  Symptom

  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 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:

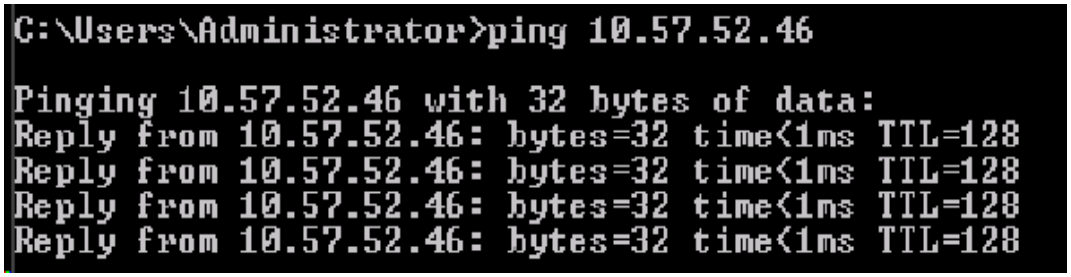
  Steps to be followed on Appliance:

  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:



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 Practice for Creating Deduplication Datastore across Volumes

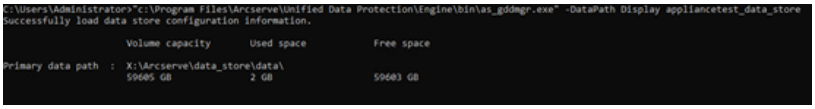
The as_gddmgr.exe, a command line tool, lets you add more data paths across volumes to expand the storage capacity of the existing dedupe datastore.

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:

4. To expand the storage capacity of deduplication datastore, enter the following command:

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

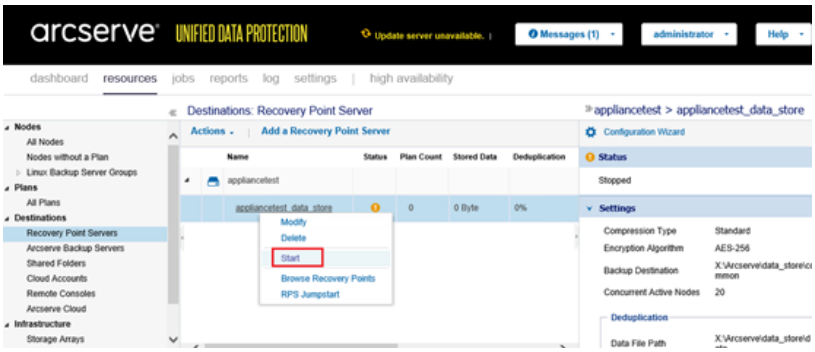
   Note: Make sure the primary path and all expanded paths are not on the same volume.

   The following sample datastore has an expanded data path on W:\volume:

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 14: 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	http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html *PuTTY is copyright 1997-2019 Simon Tatham.* *Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svyatoslav Kuzmich, Nico Williams, Viktor Dukhovni, and CORE SDI S.A.* *Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:* *The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.* *THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,*

	EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN 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.
Copyright Text	http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html *PuTTY is copyright 1997-2019 Simon Tatham.* *Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svyatoslav Kuzmich, Nico Williams, Viktor Dukhovni, and CORE SDI S.A.* *Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:* *The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.* *THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN 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.*
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