Arcserve® Appliance User Guide

Version 6.5

arcserve®

Arcserve® Appliance

Online Help

Version 6.5

List of Content 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.

© 2018 Arcserve, including its affiliates and subsidiaries. All rights reserved. Any third party trademarks or copyrights are the property of their respective owners.

Contact Arcserve Support

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

Contact Support

With Arcserve Support:

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

Arcserve Appliance Return Policy

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

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

Information needed for the RMA request:

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

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

Contents

Chapter 1: About Arcserve Appliance Documentation 11

Language Support 12

Product Documentation 13

Chapter 2: Introducing the Arcserve Appliance 14

Introduction 15

Arcserve Unified Data Protection 16

Arcserve Unified Data Protection Agent for Linux 17

Arcserve Replication and High Availability (Arcserve RHA) 18

Arcserve Backup 19

Safety Precautions 20

What is Included in the Box 21

What is Included in the Box of Appliance 8000 Series 22

What is Included in the Box of Appliance 9000 Series 23

What is Not Included in the Box 24

Available Models 25

Models 7100-7300v 26

Models 7400-7600v 28

Models 8100-8400 30

Models 9012 - 9504DR 32

Controls and Indicators 34

Front Panel 7100-7300v 35

Front Panel 7400-7600v 37

Front Panel 8100-8200 39

Front Panel 8300-8400 41

Front Panel 9012-9048 43

Front Panel 9072 DR - 9504 DR 45

Rear Panel 7100-7300v 46

Rear Panel 7400-7600v 48

Rear Panel 8100-8200 50

Rear Panel 8300-8400 52

Rear Panel 9012-9048 54

Rear Panel 9072DR-9504DR 56

Ports Used by the Appliance 58

Arcserve UDP 59
Components installed on Microsoft Windows 60
Components installed on Linux 65
Node protected by UDP Linux remotely 67
Arcserve Backup 68
Appliance for Linux Support 69
How to Add Ports to CentOS 6.6 x64 Firewall 70
Chapter 3: Installing the Arcserve Appliance 72
How to Install Arcserve Backup r17.5 SP1 73
How to Install 8100-8200 Series Appliance 75
How to Install 8300-8400 Series Appliance 76
How to Install 9012-9048 Series Appliance 77
How to Install 9072-9504DR Series Appliance 78
Chapter 4: Upgrading Arcserve UDP on the Appliance 79
How to Apply a License After Upgrading Arcserve Software 80
Upgrade Sequence on the Arcserve Appliance 81
Upgrade the Arcserve Appliance Used as Arcserve UDP Console and RPS 82
Upgrade the Arcserve Appliance Used as Arcserve UDP RPS 83
Upgrade Steps When Two or More Arcserve Appliances are Used in the Environment 84
Upgrade the Arcserve UDP Linux Agent on the Arcserve Appliance 85
Upgrade the Arcserve Backup on the Arcserve Appliance 86
Upgrade Sequence for UDP Console, RPS, and Agent 87
Chapter 5: Configuring the Arcserve Appliance 88
How to Configure Network Settings for Arcserve Appliance 89
How to Set up the Arcserve Appliance 94
Configure Arcserve Appliance as Gateway 103
Chapter 6: Working with Arcserve Appliance 104
Activate Arcserve Product on the Appliance 105
Create a Plan Using Arcserve Appliance Wizard 106
Add Nodes to a Plan 107
Add Nodes by Hostname/IP Address 108
Add Nodes by Active Directory 110
Add vCenter/ESX Nodes 112
Add Hyper-V Nodes 114
Create a Backup Plan for Linux Nodes 116
Create a Backup Plan to a Tape Device 117

Create an On-Appliance Virtual Standby Plan 118
Create Plan to Backup the Linux Backup Server 119
Setting-up to Perform Linux Instant VM Job to Local Appliance Hyper-V 124
Migrate Arcserve UDP Console Using ConsoleMigration.exe 125
Migrate Pre-installed Linux Backup Server to CentOS 7.4 127
Perform Migration between Arcserve Appliances 129
Solution 1 130
Solution 2 135
Modify the Input Source of Pre-installed Linux Backup Server 138
Chapter 7: Monitoring the Appliance Server Remotely 142
Working with IPMI 143
How to Change IPMI Password 144
How to Upgrade IPMI Firmware 147
Working with Integrated Dell Remote Access Controller (iDRAC) 148
Restoring or Repairing the Arcserve Appliance 150
Apply Arcserve UDP Factory Reset Using Boot Option in 7000-8000 Series Appliance 151
Apply Arcserve UDP Factory Reset Using Boot Option in 9012-9504DR Series Appliance 154
Clear Configuration and Apply Appliance Factory Reset 157
How to Replace Factory Reset Image Using Set Appliance Image Utility 160
Remove and Replace a Hard Drive 163
How to Perform Bare Metal Recovery (BMR) without Preserving Data 166
How to Perform Bare Metal Recovery (BMR) and Preserving Data 179
Chapter 9: Performing Appliance Capacity Expansion 188
Working with Expansion Kit in Arcserve Appliance 9012-9504 DR Models 189
Connecting Appliance Expansion Shelf to the Appliance Server 195
Appliance Infield Expansion for all the Available Models 196
What is included in the box 205
How to Connect the Appliance Expansion Shelf to the Appliance Server 208
How to Modify Arcserve UDP Data store 216
Adding a Data Path on Expansion Shelf to Arcserve UDP Data Store 217
Migrating Hash Destination to the new SSD 218
Checking the Overall Capacity of Data Store from Arcserve UDP Console 219
Resuming all the plans from Arcserve UDP Console 220
Chapter 10: Working with Network Configuration 222
Understanding the Network Configuration Details 223
How to Configure the NIC Teaming Process 228

How to Disable DHCP Server 230
How to Configure IP Address for the preinstalled Linux Backup Server 231
How to Enable Round Robin on the DNS Server to Balance Load 233
Chapter 11: Understanding Safety Precautions 234
General Safety Precautions 235
Electrical Safety Precautions 237
FCC Compliance 238
Electrostatic Discharge (ESD) Precautions 239
Chapter 12: Troubleshooting 240
Linux Backup Server Fails to Connect from the Console 241
Backing Up Arcserve Appliance from Another Appliance Reports Duplicated Nodes 242
Linux Backup Server Cannot Communicate with Any Node in the Network 244
Linux Backup Server Cannot Get the Network DNS Suffix 246
Default Time Zone on the Appliance 247
Licenses Error even when the licenses are available 248
Arcserve UDP Console Shows Error while adding Remote Console in Replicate to a Remotely Managed RPS Task 249
Unable to Perform VSB Task Using Another Appliance as Monitor 251
IVM Job Fails to Create Linux IVM to ESXi Server with HBBU Session on Appliance Data Store 253
Chapter 13: Applying Best Practices 254
Best Practices for Network Configuration 255
Best Practices for Windows Defender with PowerShell cmdlets 258
Chapter 14: Acknowledgements 259
PuTTY 260

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 12

Product Documentation 13

Language Support

Documentation is available in English as well as multiple local languages.

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 in the following languages:

- English
- Chinese (Simplified)
- Chinese (Traditional)
- French
- German
- Italian
- Japanese
- Portuguese (Brazil)
- Spanish

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 15
Safety Precautions 20
What is Included in the Box 21
What is Not Included in the Box 24
Available Models 25
Controls and Indicators 34
Ports Used by the Appliance 58

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.

The 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 Replication and High Availability (RHA)

Arcserve Appliance is defined with Hardware Warranty. Please visit arcserve.com/arcserve-appliance-warranty for detailed information about this 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 data stores 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-BackupSv*. 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 Replication and High Availability (Arcserve RHA)

Arcserve RHA 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 RHA 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.

For more information about how to install and configure Arcserve RHA, see online documents.

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 is installed at "C:\Program Files (x86)\Arcserve" on your computer after you run InstallASBU.bat. 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 r17.5 documentation.

Arcserve Backup Server uses the following default login information:

- Username -- caroot
- Password -- Arcserve

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

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

- 8000 Series
- 9000 Series

What is Included in the Box of Appliance 8000 Series

The following items are contained in the box:

- Arcserve Appliance (serial number label is located on rear of appliance)
- Power cable: 1
- Network Cables: 1 red, 1 blue (3-feet long each)
- IPMI port cable: 1 (7-feet long)
- Rail/Rack Mounting Kit that contains the following:
  - 2 quick-install outer rails
  - 2 inner rail extensions
  - 3 rail adapters (standard rail mounting only)
  - Other associated hardware as required
- Arcserve faceplate
- Microsoft Client Access License

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 Included in the Box of Appliance 9000 Series

Arcserve Appliance 9000 series contains two boxes: R440 and R740. Below list provides included items in both the boxes.

The following items are included in the in R440 Accessory box:

- BEZEL, DELL 1U, CUS 14G BEZEL ASSEMBLY, LCD, AR, (380-7406)
- QUICK START GUIDE, ARCSERVE, READ ME FIRST SHEET UDP 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 R740 Accessory box with a Rack Rail kit:

- BEZEL, DELL 2U, CUS 14G BEZEL ASSEMBLY, LCD, AR, (380-7405)
- QUICK START GUIDE, ARCSERVE, READ ME FIRST SHEET UDP 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 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 7000 series, 8000 series and 9000 series are available in a variety of different models designed to meet your specific needs:

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

Models 7100-7300v

Arcserve Appliance Models 7100 - 7300v

Arcserve Appliance 7000 Series Specifications					
Appliance Model	**7100**	**7200**	**7200V**	**7300**	**7300V**
Backup Storage Capacity					
Raw Storage capacity*	3 TB	6 TB	6 TB	9 TB	9 TB
Usable backup capacity**	2.8 TB	5.8 TB	5.8 TB	8.8 TB	8.8 TB
Protected (source data) capacity***	Up to 8 TB	Up to 17 TB	Up to 17 TB	Up to 26 TB	Up to 26 TB
Standard Features					
Unified management console, global deduplication, block level infinite incremental backups, compression, encryption, WAN optimized replication, advanced virtualization support, agentless backup, remote virtual standby, tape support, application consistent backups, granular restore, unified reporting and dashboard.					
On-Appliance Virtual Standby	N/A	N/A	Up to 3 VMs	N/A	Up to 3 VMs
Warranty and Technical Specifications					
Full System Depot Warranty	3 Years				
Physical Dimensions (H x W x D in Inches)	1.7" x 17.2" x 25.6" (1U - 19" Rack Mount rails provided)				
Remote management and network interface ports	1 x IPMI & 2 x 1 GbE (RJ45)				
Hard Disk type and RAID configuration	4 x 1 TB SAS (RAID 5)	4 x 2 TB SAS (RAID 5)	4 x 2 TB SAS (RAID 5)	4 x 3 TB SAS (RAID 5)	4 x 3 TB SAS (RAID 5)
External Tape Backup Connectivity (SAS, SATA, FC)	1 x PASS				
Total system RAM	16 GB	16 GB	32 GB	32 GB	48 GB
SSD drive (For deduplication hash tables)	120 GB SSD	120 GB SSD	120 GB SSD	240 GB SSD	240 GB SSD
Maximum weight (lbs)	41 lbs				
Power Supplies (Single or redundant)	1 x 600 W				
Power consumption	93/116/143	122/164/143	125/167/145	125/167/145	129/188/152

(Watts @ idle/-load/startup)					
AC voltage & frequency range	100 - 240 V				
Ampere rating	7.5 Amp Max				
*1 TB = 1,000,000,000,000 bytes. ** On "V" models, space available for backup is reduced by the size of virtual standby VMs. ***Estimated capacity assuming a typical 3:1 deduplication and compression ratio. Actual backup capacity may vary significantly, based upon data type, backup type, schedule, and more.					

Models 7400-7600v

Arcserve Appliance Models 7400 - 7600v

Arcserve Appliance 7000 Series Specifications						
Appliance Model	**7400**	**7400V**	**7500**	**7500V**	**7600**	**7600V**
Backup Storage Capacity						
Raw Storage capacity*	16 TB	16 TB	20 TB	20 TB	30 TB	30 TB
Usable backup capacity**	15.8 TB	15.8 TB	19.8 TB	19.8 TB	29.8 TB	29.8 TB
Protected (source data) capacity***	Up to 46 TB	Up to 46 TB	Up to 58 TB	Up to 58 TB	Up to 90 TB	Up to 90 TB
Standard Features						
Unified management console, global deduplication, block level infinite incremental backups, compression, encryption, WAN optimized replication, advanced virtualization support, agentless backup, remote virtual standby, tape support, application consistent backups, granular restore, unified reporting and dashboard.						
On-Appliance Virtual Standby	N/A	Up to 6 VMs	N/A	Up to 9 VMs	N/A	Up to 12 VMs
Warranty and Technical Specifications						
Full System Depot Warranty	3 Years					
Physical Dimensions (H x W x D in Inches)	3.5" x 17.2" x 25.6" (2U - 19" Rack Mount rails provided)					
Remote management and network interface ports	1 x IPMI & 2 x 1 GbE (RJ45) and 4 x 1GbE (RJ45). Optional 2 x 10Gb					
Hard Disk type and RAID configuration	10 x 2 TB SAS (RAID 6)	10 x 2 TB SAS (RAID 6)	12 x 2 TB SAS (RAID 6)	12 x 2 TB SAS (RAID 6)	12 x 3 TB SAS (RAID 6)	12 x 3 TB SAS (RAID 6)
External Tape Backup Connectivity (SAS, SATA, FC)	1 x PASS					

Total system RAM	64 GB	96 GB	64 GB	96 GB	128 GB	192 GB
SSD drive (For dedu-plication hash tables)	240 GB SSD	240 GB SSD	480 GB SSD	480 GB SSD	480 GB SSD	480 GB SSD
Maximum weight (lbs)	52 lbs					
Power Supplies (Single or redundant)	2 x 920 W					
Power con-sumption (Watts @ idle/-load/startup)	208/257/35-8	208/257/35-8	208/257/35-8	208/257/35-8	240/296/36-9	240/296/36-9
AC voltage & fre-quency range	100 - 240 V					
Ampere rating	11 Amp Max					
*1 TB = 1,000,000,000,000 bytes. **On "V" models, space available for backup is reduced by the size of virtual standby VMs. ***Estimated capacity assuming a typical 3:1 deduplication and compression ratio. Actual backup capacity may vary significantly, based upon data type, backup type, schedule, and more.						

Models 8100-8400

Arcserve Appliance Models 8100 - 8400

Arcserve Appliance 8000 Series Specifications				
Appliance Model	**UDP 8100**	**UDP 8200**	**UDP 8300**	**UDP 8400**
Source Backup*	12 TB-18 TB	24T B-36 TB	48 TB-128 TB	96 TB-240 TB
System RAM	32 GB	32 GB	64 GB	128 GB
Max RAM**	64 GB/96 GB/160 GB		96 GB/128 GB/192 GB	160 GB/192 GB/256 GB
SSD drive	120 GB SSD	200 GB SSD	480 GB SSD	1.2 TB SSD
Processor	E5-2609 V4, 8-CORE, 1.7 GHZ	E5-2620 V4, 8-CORE, 2.1 GHZ	E5-2640 V4, 10-CORE, 2.4 GHZ	E5-2650 V4, 12-CORE, 2.2 GHZ
RAID Card	9361-4i		9361-8i	
RAID Con-figuration	RAID-5 with BBU		RAID-6 with BBU	
Drive Bays	4		12	
Drives	3 x 2 TB SAS 12G 4 x 2 TB SAS 12G	3 x 4 TB SAS 12G 4 x 4 TB SAS 12G	6 x 4 TB SAS 12G 7 x 4 TB SAS 12G 8 x 4 TB SAS 12G 9 x 4 TB SAS 12G 10 x 4	6 x 8 TB SAS 12G 7 x 8 TB SAS 12G 8 x 8 TB SAS 12G 9 x 8 TB SAS 12G 10 x 8

			TB SAS 12G 11 x 4 TB SAS 12G 12x 4TB SAS 12G	TB SAS 12G 11 x 8 TB SAS 12G 12 x 8 TB SAS 12G
DIMMs / Max DIMMs	4 x 8 GB DDR4-2400/ 8		4 x 16 GB DDR4-2400/ 8	4 x 32 GB DDR4-2400/ 8
Cards	LSI SAS9200-8E			
Power Supplies	2x hot swap redundant 500 W AC Platinum		Two x 920 W hot swap redundant high-efficiency AC power supply, Platinum Level	

*Estimated capacity assuming a typical 3:1 deduplication & compression ratio. Actual backup capacity may vary significantly, based upon data type, backup type, backup schedule, etc.

**Arcserve Appliances have additional RAM to host Virtual Standby / Instant VM recovery on the appliances. VM memory allocation should be sized based on guest OS workload. Arcserve also provides the option to add additional RAM to the standard appliance configuration based on customer needs.

Models 9012 - 9504DR

Arcserve Appliance Models 9012 - 9504DR

Arcserve Appliance 9000 Series Specifications											
Appliance Model	9012	9024	9048	9072DR	9096DR	9144DR	9192DR	9240DR	9288DR	9360DR	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	480 GB SSD			2 x 1.9 TB SSD (RAID1)							
Processor	Intel Xeon Silver 4108, 8-CORE, 1.8 GHz			Intel Xeon Silver 4114, 10-CORE, 2.2 GHz							
Number of Processors	1			2							
RAID Card	PERC H730P Low Profile, adaptor, 2 GB NV Cache			PERC H730P, MiniCard, 2 GB NV Cache							
RAID Configuration	RAID-5			RAID-6							
Drive Bays	4			16							
Expansion 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			Broadcom 5720 QP 1 Gb Network Daughter Card SAS 12 Gbps HBA External Controller							Broadcom 5720 QP

	Port 1 Gb LOM		1 GB SAS 12 Gbps HBA External Dual Port 10G Base-T Copper
PCIe Cards (Factory Option)	SAS 12 Gbps HBA External Controller Broadcom 5719 Quad-Port 1G NIC Dual-Port 10G Copper Dual-Port 10G SFP+ Dual-Port FC 16G HBA	Dual-Port 10G Copper Dual-Port 10G SFP+ Dual-Port FC 16G HBA	Dual-Port 10G SFP+ Dual-Port FC 16G HBA
Power Supplies	Dual, Hot-Plug, Redundant Power Supply (1+1), 550 W	Dual, Hot-Plug, Redundant Power Supply (1+1), 750 W	
iDRAC Enterprise	1		

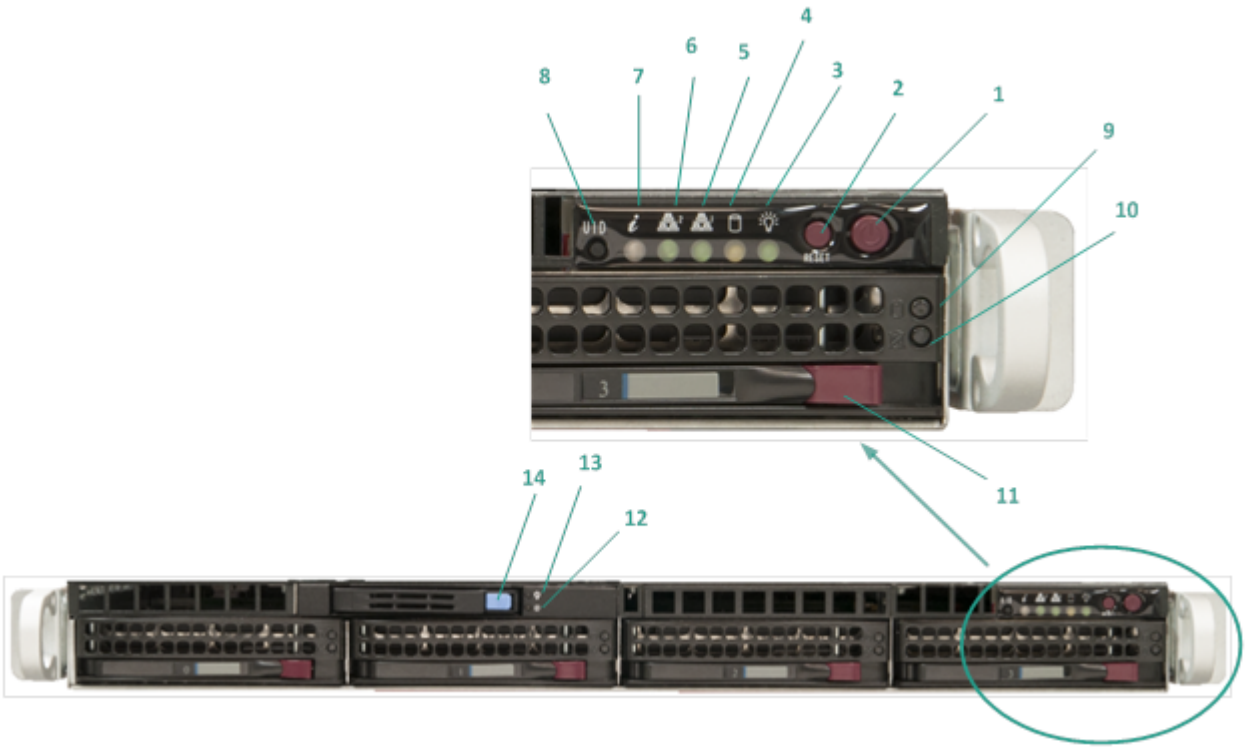
Controls and Indicators

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 7100-7300v
- Front Panel 7400-7600v
- Front Panel 8100-8200
- Front Panel 8300-8400
- Front Panel 9012-9048
- Front Panel 9072 DR-9504 DR
- Rear Panel 7100-7300v
- Rear Panel 7400-7600v
- Rear Panel 8100-8200
- Rear Panel 8300-8400
- Rear Panel 9012-9048
- Rear Panel 9072 DR-9504 DR

Front Panel 7100-7300v

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



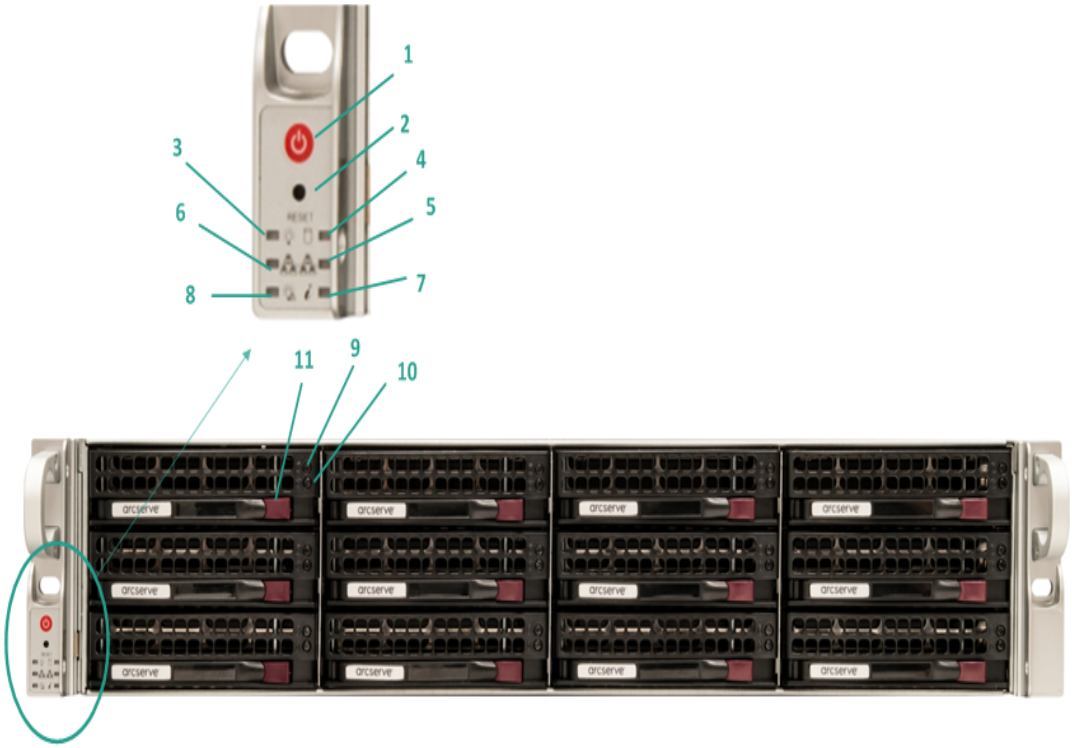
Number	Control / Indicator	Description
1	Power button	Used to turn on and off power from the power supply to the appliance components. When turning off the power, the main power is turned off but standby power is still supplied. Therefore, to ensure power is completely removed from the appliance, unplug the power supply cable before performing maintenance.
2	Reset button	Used to reboot the appliance.
3	Power LED	**Solid Green:** Indicates that the power is being supplied to the power supply of the appliance. This LED should normally be On when the appliance is operating.
4	Device Activity LED	**Blinking Amber**: Indicates activity on at least one of the hard drives.
5	Network Interface Card (NIC1) LED	**Blinking Amber**: Indicates network activity on Network 1 (ETH0 Port).
6	Network Interface Card (NIC2) LED	**Blinking Amber:** Indicates network activity on Network 2 (ETH1 Port).

7	Information LED	**Continuously On and Red:** An overheat condition has occurred. (This can be caused due to cable congestion.) ***Blinking Red - Fast (1 second):** Fan Failure. Check for an inoperative fan. ***Blinking Red - Slow (4 seconds):** Power Failure. Check for an inoperative power supply. **Solid Blue:** Local UID has been activated. Use this function to locate the Server in a rack environment. **Blinking Blue:** Remote UID has been activated. Use this function to locate the Server from a remote location.
8	Unit Identifier (UID) button	Used to turn on or off the Universal Information LED (blue) on both the front and rear appliance panels. When the blue LED is On, the appliance can be easily located in a rack (from either the front or the back).
9	Hard Drive (HDD) LED	**Blinking Green**: Indicates activity on the corresponding drive.
10	Hard Drive (HDD) LED	***Solid Red**: Indicates failure of the corresponding 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.
11	Hard Drive (HDD) Latch	Used to unlock and remove the hard drive.
12	Solid State Drive (SSD) LED	***Solid Red**: Indicates drive failure.
13	Solid State Drive (SSD) LED	**Solid Green**: Indicates drive activity. **Blinking Green**: Indicates the drive is being accessed.
14	Solid State Drive (SSD) Latch	Used to unlock and remove the SSD drive.

*Any Solid or Blinking Red light indicates some kind of failure. To quickly resolve this issue, contact Arcserve Support.

Front Panel 7400-7600v

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



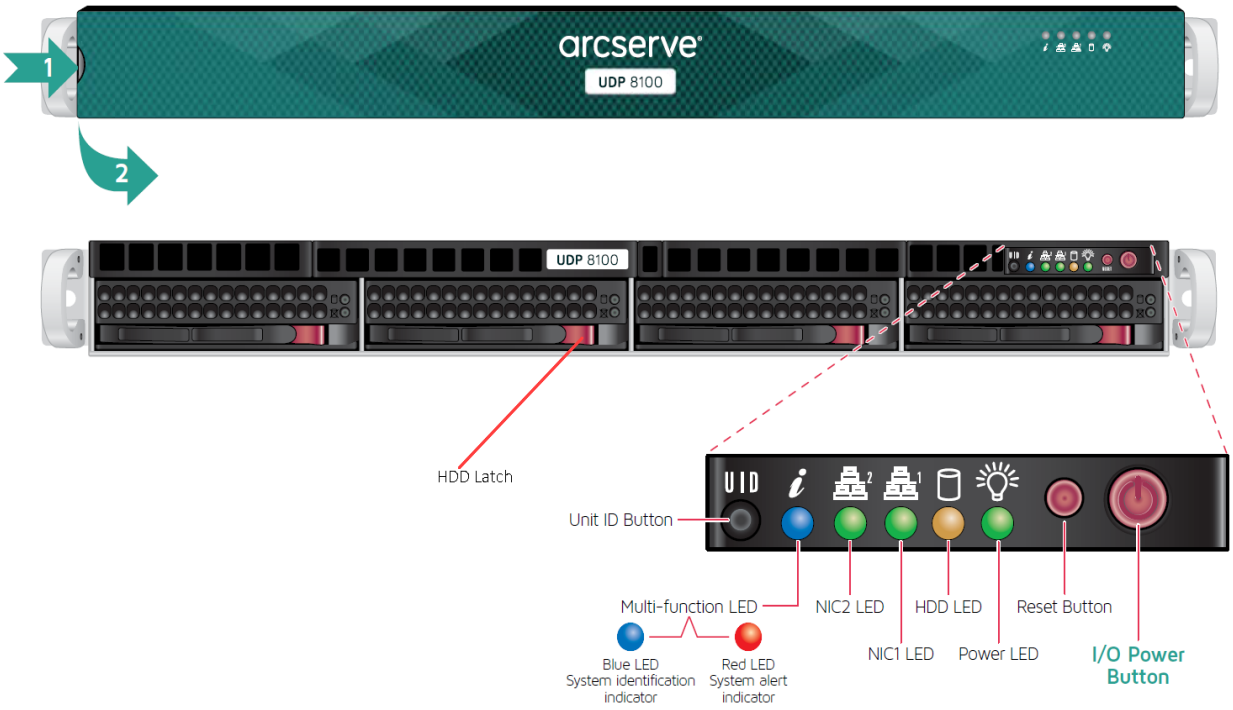
Number	Control / Indicator	Description
1	Power button	Used to turn on and off power from the power supply to the appliance components. When turning off the power, the main power is turned off but standby power is still supplied. Therefore, to ensure power is completely removed from the appliance, unplug the power supply cable before performing maintenance.
2	Reset button	Used to reboot the appliance.
3	Power LED	**Solid Green:** Indicates that the power is being supplied to the power supply of the appliance. This LED should normally be On when the appliance is operating.
4	Device Activity LED	**Blinking Amber**: Indicates activity on at least one of the hard drives.
5	Network Interface Card (NIC1) LED	**Blinking Amber**: Indicates network activity on Network 1 (ETH0 Port).
6	Network Interface Card (NIC2) LED	**Blinking Amber:** Indicates network activity on Network 2 (ETH1 Port).

7	Information LED	**Continuously On and Red:** An overheat condition has occurred. (This can be caused due to cable congestion.) ***Blinking Red - Fast (1 second):** Fan Failure. Check for an inoperative fan. ***Blinking Red - Slow (4 seconds):** Power Failure. Check for an inoperative power supply. **Solid Blue:** Local UID has been activated. Use this function to locate the Server in a rack environment. **Blinking Blue:** Remote UID has been activated. Use this function to locate the Server from a remote location.
8	Unit Identifier (UID) button	Used to turn on or off the Universal Information LED (blue) on both the front and rear appliance panels. When the blue LED is On, the appliance can be easily located in a rack (from either the front or the back).
9	Hard Drive (HDD) LED	**Blinking Green**: Indicates activity on the corresponding drive.
10	Hard Drive (HDD) LED	***Solid Red**: Indicates failure of the corresponding 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.
11	Hard Drive (HDD) Latch	Used to unlock and remove the hard drive.
12	Solid State Drive (SSD) LED	***Solid Red**: Indicates drive failure.
13	Solid State Drive (SSD) LED	**Solid Green**: Indicates drive activity. **Blinking Green**: Indicates the drive is being accessed.
14	Solid State Drive (SSD) Latch	Used to unlock and remove the SSD drive.

*Any Solid or Blinking Red light indicates some kind of failure. To quickly resolve this issue, contact Arcserve Support.

Front Panel 8100-8200

The front panel of the Arcserve Appliance 8100-8200 contains control panel buttons, control panel LEDs, and drive carrier LEDs. The following table describes these items:



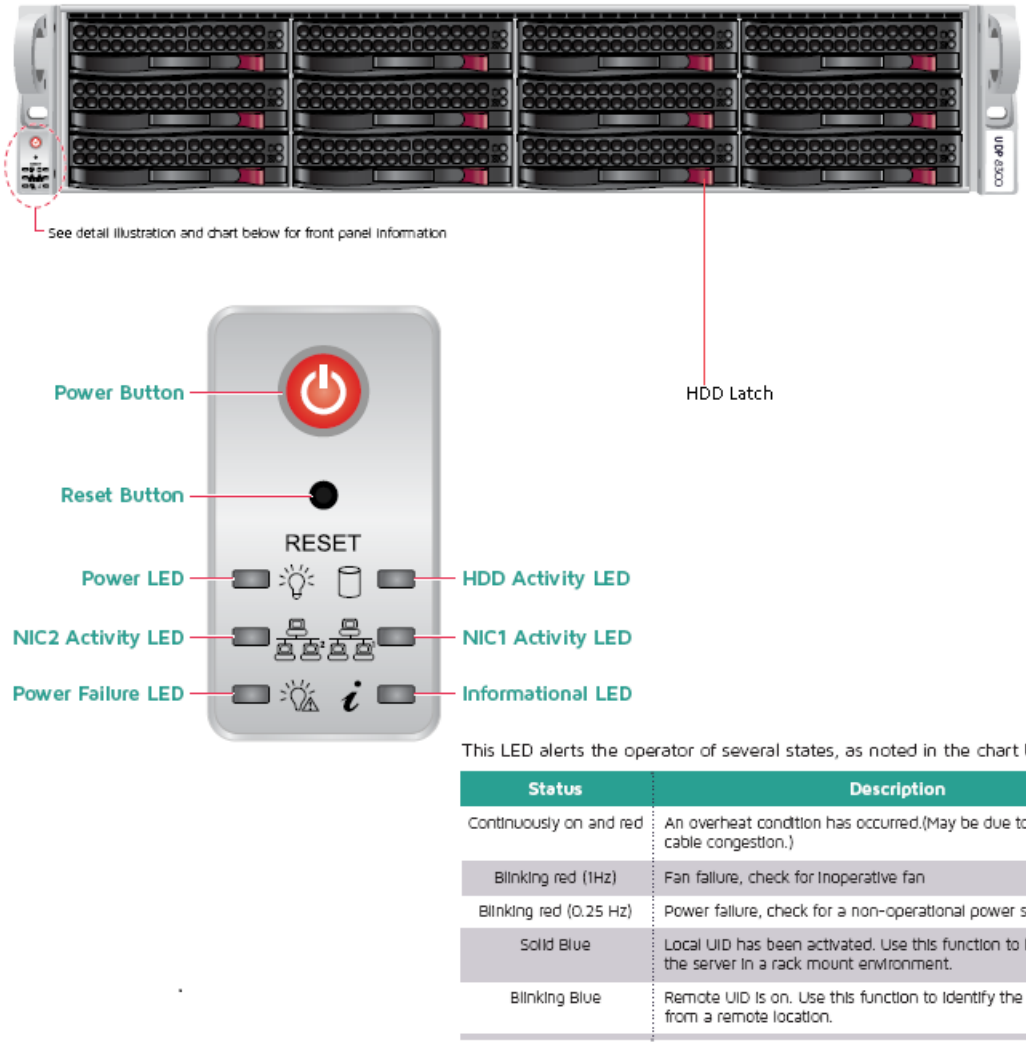
Control/Indicator	Description
I/O Power button	Used to turn on and off power from the power supply to the appliance components. When turning off the power, the main power is turned off but standby power is still supplied. Therefore, to ensure that power is completely removed from the appliance, unplug the power supply cable before performing maintenance.
Reset button	Used to reboot the appliance.
Power LED	**Solid Green:** Indicates that the power is being supplied to the power supply of the appliance. This LED should normally be On when the appliance is operating.
HDD LED	**Blinking Amber**: Indicates activity on at least one of the hard drives.
Network Interface Card (NIC1) LED	**Blinking Amber**: Indicates network activity on Network 1 (ETH0 Port).
Network Interface Card (NIC2) LED	**Blinking Amber:** Indicates network activity on Network 2 (ETH1 Port).
Information LED	**Continuously On and Red:** An overheat condition has occurred. **Note:** A cable congestion may cause this situation.

	***Blinking Red - Fast (1 second):** Fan Failure. Check for an inoperative fan. ***Blinking Red - Slow (4 seconds):** Power Failure. Check for an inoperative power supply. **Solid Blue:** Local UID is activated. Use this function to locate the Server in a rack environment. **Blinking Blue:** Remote UID is activated. Use this function to locate the Server from a remote location.
Unit Identifier (UID) button	Used to turn on or off the Universal Information LED (blue) on both the front and rear appliance panels. When the blue LED is On, the appliance can be easily located in a rack (from either the front or the back).
Hard Drive (HDD) LED	**Blinking Green**: Indicates activity on the corresponding drive.
Hard Drive (HDD) LED	***Solid Red**: Indicates failure of the corresponding 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.
Hard Drive (HDD) Latch	Used to unlock and remove the hard drive.
Solid State Drive (SSD) LED	***Solid Red**: Indicates drive failure.
Solid State Drive (SSD) LED	**Solid Green**: Indicates drive activity. **Blinking Green**: Indicates the drive is being accessed.
Solid State Drive (SSD) Latch	Used to unlock and remove the SSD drive.

*Any Solid or Blinking Red light indicates some kind of failure. To quickly resolve this issue, contact Arcserve Support.

Front Panel 8300-8400

The front panel of the Arcserve Appliance 8300-8400 contains control panel buttons, control panel LEDs, and drive carrier LEDs. The following table describes these items:



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

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

Control/Indicator	Description
Power button	Used to turn on and off power from the power supply to the appliance components. When turning off the power, the main power is turned off but standby power is still supplied. Therefore, to ensure power is completely removed from the appliance, unplug the power supply cable before performing maintenance.
Reset button	Used to reboot the appliance.
Power LED	**Solid Green:** Indicates that the power is being supplied to the power supply of the appliance.

	This LED should normally be On when the appliance is operating.
Network Interface Card (NIC1) LED	**Blinking Amber**: Indicates network activity on Network 1 (ETH0 Port).
Network Interface Card (NIC2) LED	**Blinking Amber:** Indicates network activity on Network 2 (ETH1 Port).
Information LED	**Continuously On and Red:** An overheat condition has occurred. (This can be caused due to cable congestion.) ***Blinking Red - Fast (1 second):** Fan Failure. Check for an inoperative fan. ***Blinking Red - Slow (4 seconds):** Power Failure. Check for an inoperative power supply. **Solid Blue:** Local UID has been activated. Use this function to locate the Server in a rack environment. **Blinking Blue:** Remote UID has been activated. Use this function to locate the Server from a remote location.
Power Failure LED	Indicates a power supply module has failed.
Hard Drive (HDD) LED	**Blinking Green**: Indicates activity on the corresponding drive.
Hard Drive (HDD) LED	***Solid Red**: Indicates failure of the corresponding 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.
Hard Drive (HDD) Latch	Used to unlock and remove the hard drive.

*Any Solid or Blinking Red light indicates some kind of failure. To quickly resolve this issue, contact Arcserve Support.

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. For more information, see

			link.
5	USB port (optional)	SS	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.

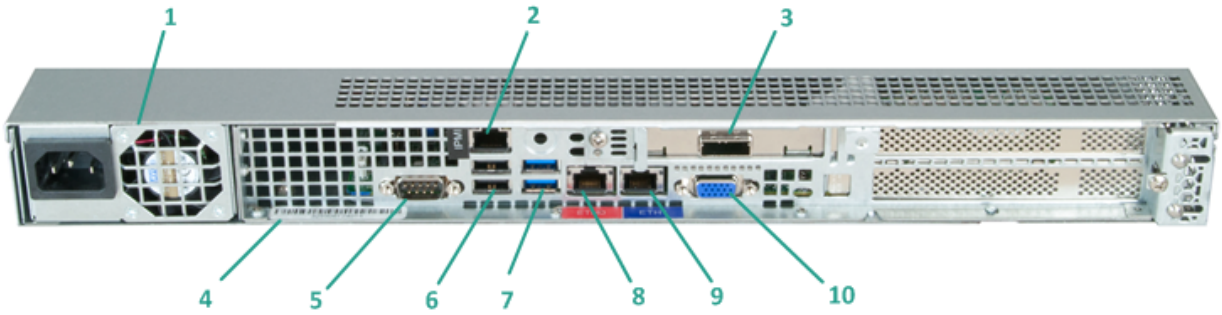
Front Panel 9072 DR - 9504 DR

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.

Rear Panel 7100-7300v

The rear panel contains the power supplies, cable connections, and ports for the appliance.

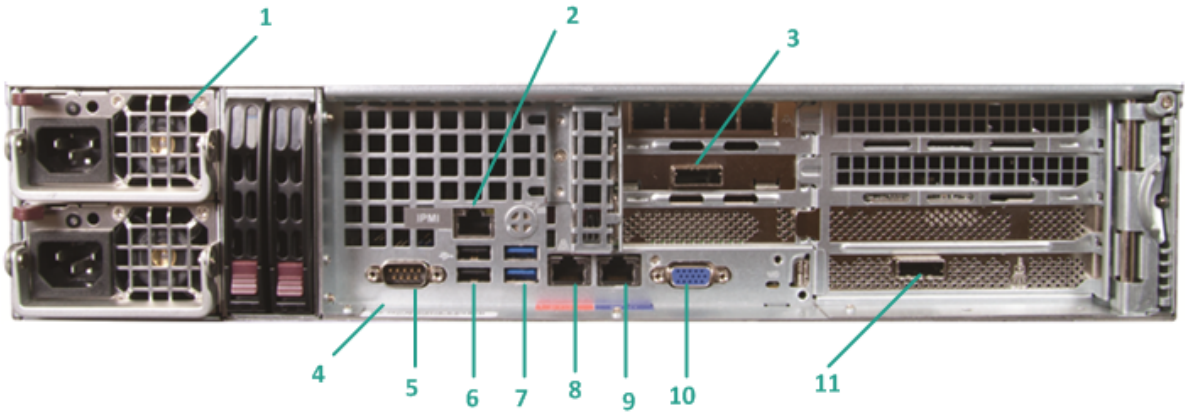


Number	Name of Control/Indicator	Description
1	Power Supply	Provides high-efficiency power supply to the appliance. **Note:** The main power switch is used to apply or remove power from the power supply to the appliance. Turning off the appliance power with this button removes the main power but standby power is still supplied. Therefore, to ensure power is completely removed from the appliance, unplug the power supply cable before performing maintenance.
2	IPMI Port (Remote Management)	The IPMI (Intelligent Platform Management Interface) port is used to monitor the physical health of Servers, such as temperature, voltage, fans, power supplies, and the appliance. **Note**: The default user name/password for IPMI access is ADMIN/ARCADMIN (case-sensitive). We recommend that you change the password as soon as possible. For details about how to change the IPMI password, see How to Change the IPMI Password.
3	External Storage Device Port (SAS port for tape drive)	Used to connect an external storage device (hard drive, tape drive, etc.) to the appliance. These portable external storage devices can be used to store backed-up data for easy transporting from one location to another.

4	Serial Number Label	A unique serial number that is assigned to the appliance.
5	COM1 Serial Port	Communication port that is used to connect a serial device, such as a mouse to the appliance (if needed).
6	USB 2.0 (black)	Used to connect USB 2.0 type devices to the appliance.
7	USB 3.0 (blue)	Used to connect USB 3.0 type devices to the appliance.
8	Network Data I/O Port 1	Used to transfer network data to and from the appliance. (ETH0 for Network 1)
9	Network Data I/O Port 2	Used to transfer network data to and from the appliance. (ETH1 for Network 2)
10	VGA Connector	Used to connect a monitor to the appliance (if needed).

Rear Panel 7400-7600v

The rear panel contains the power supplies, cable connections, and ports for the appliance.

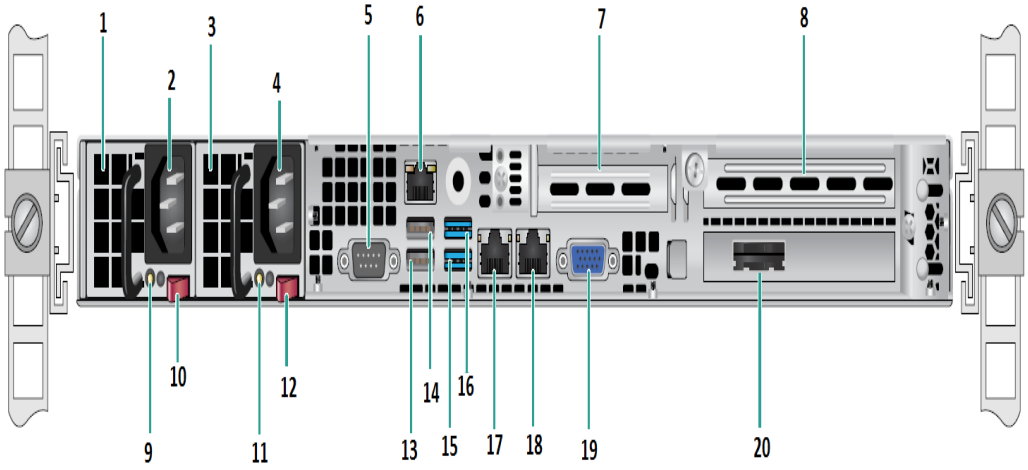


Number	Name of Control/Indicator	Description
1	Dual Power Supply	Provides high-efficiency power supply to the appliance. **Note:** The main power switch is used to apply or remove power from the power supply to the appliance. The benefit of having a dual power supply is if one fails then the other is available for use. Turning off the appliance power with this button removes the main power but standby power is still supplied. Therefore, to ensure power is completely removed from the appliance, unplug the power supply cable before performing maintenance.
2	IPMI Port (Remote Management)	The IPMI (Intelligent Platform Management Interface) port is used to monitor the physical health of Servers, such as temperature, voltage, fans, power supplies, and the appliance. **Note**: The default user name/password for IPMI access is ADMIN/ARCADMIN (case-sensitive). We recommend that you change the password as soon as possible. For details about how to change the IPMI password, see How to Change the IPMI Password.
3	External Storage Device Port (SAS port for tape drive)	Used to connect an external storage device (hard drive, tape drive, etc.) to the appliance. These portable external storage devices can be used to store backed-up data for easy transporting from one loc-

		ation to another.
4	Serial Number Label	A unique serial number that is assigned to the appliance.
5	COM1 Serial Port	Communication port that is used to connect a serial device, such as a mouse to the appliance (if needed).
6	USB 2.0 (black)	Used to connect USB 2.0 type devices to the appliance.
7	USB 3.0 (blue)	Used to connect USB 3.0 type devices to the appliance.
8	Network Data I/O Port 1	Used to transfer network data to and from the appliance. (ETH0 for Network 1)
9	Network Data I/O Port 2	Used to transfer network data to and from the appliance. (ETH1 for Network 2)
10	VGA Connector	Used to connect a monitor to the appliance (if needed).
11	External Storage Device Port (Tap Autoloader/Library) LSI SAS 9212 - 4i4e	Used to connect an external storage device (Tape Autoloader/Library) to the appliance. These portable external storage devices can be used to store backed-up data for easy transporting from one location to another. **Note**: This port is present in the operating system as LSI Adapter SAS2 2008 Falcon.

Rear Panel 8100-8200

The rear panel contains the power supplies, cable connections, and ports for the appliance.

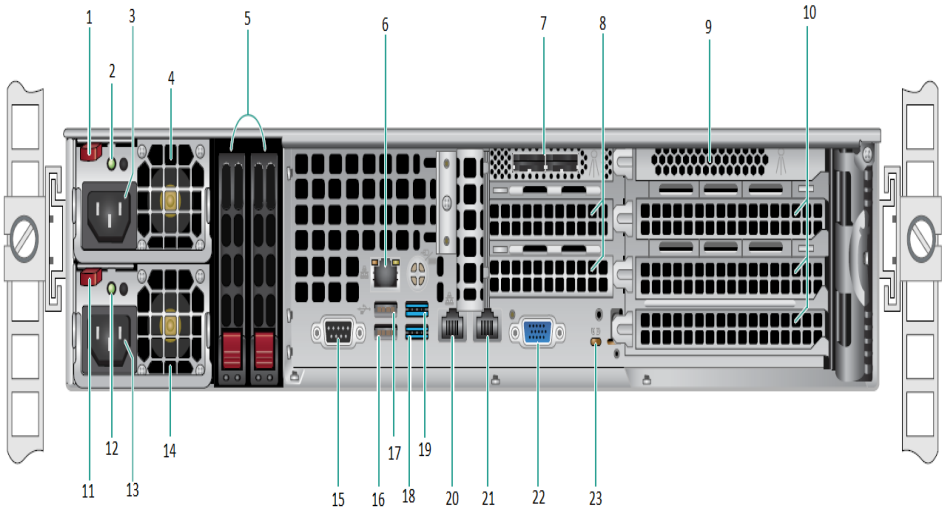


Num-ber	Name of Control/Indicator
1	Power Supply Module #1
2	AC Power Inlet #1
3	Power Supply #2
4	AC Power Inlet #2
5	COM Port
6	PMI Port (Remote Management)
7	Low Profile PCI Expansion Slot
8	PCI Expansion Slot
9	Power Good LED #1
10	Power Supply Lock #1
11	Power Good LED #2
12	Power Supply Lock #2
13	USB 2.0 Port 1 (Black)
14	USB 2.0 Port 2 (Black)
15	USB 3.0 Port 3 (Blue)
16	USB 3.0 Port 4 (Blue)
17	Network Data I/O Port 1 (ETH0 for Network 1)
18	Network Data I/O Port 2 (ETH1 for Network 2)
19	VGA Port

20	External Storage Device Port (SAS port for tape drive option)

Rear Panel 8300-8400

The rear panel contains the power supplies, cable connections, and ports for the appliance.

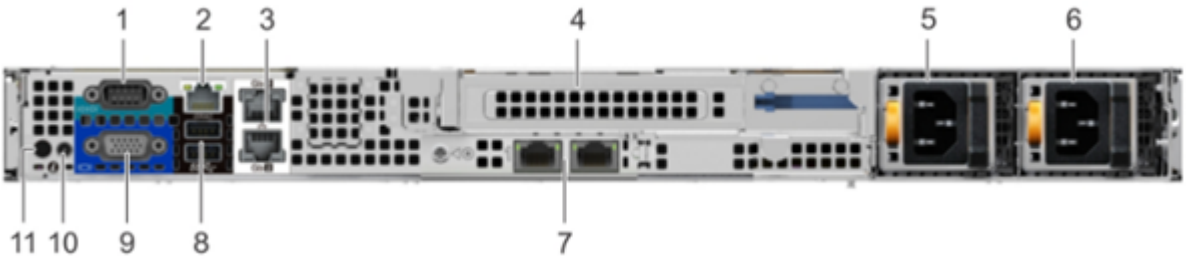


Num-ber	Name of Control/Indicator
1	Power Supply Module #1 Lock
2	Power Supply Module #1 Power Good LED
3	Power Supply Module #1 AC Receptacle
4	Power Supply Module #1 Fan
5	Rear SSDs (optional)
6	IPMI Port (Remote Management)
7	External SAS HBA Ports
8	Half-length PCI Expansion Slots
9	Internal RAID Controller
10	Full-length PCI Expansion Slots
11	Power Supply Module #2 Lock
12	Power Supply Module #2 Power Good LED
13	Power Supply Module #2 AC Receptacle
14	Power Supply Module #2 Fan
15	COM Port
16	USB Port 1 (generation 2)
17	USB Port 2 (generation 2)
18	USB Port 3 (generation 3)
19	USB Port 4 (generation 3)

20	ETH0 (Network 1)
21	ETH1 (Network 2)
22	VGA Port (Monitor)
23	UID LED

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:

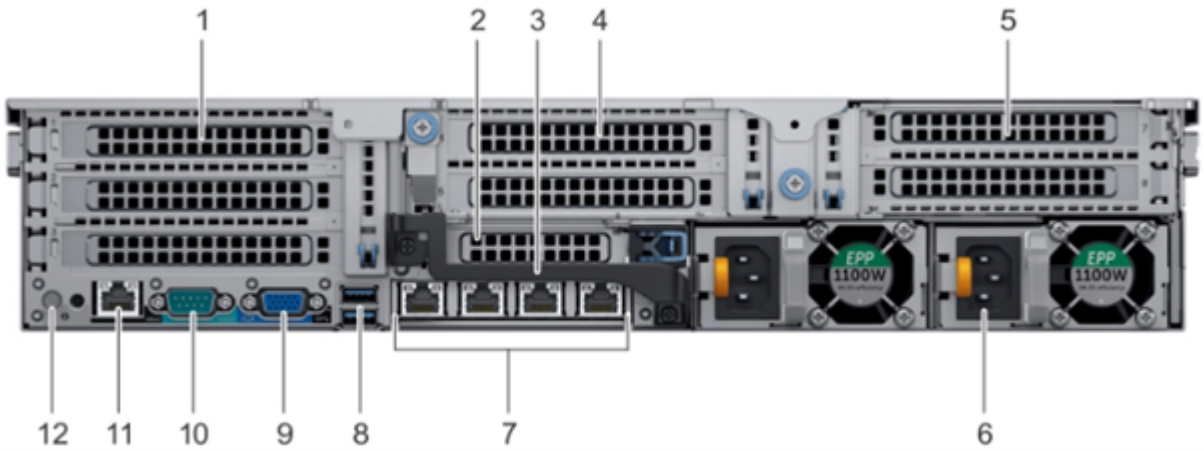


Number	Control / Indicator	Icon	Description
1	Serial port		Use the serial port to connect a serial device to the system. For more information, see link.
2	iDRAC9 dedicated network port		Use the iDRAC9 dedicated network port to securely access the embedded iDRAC on a separate management network. For more 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	LOM riser ports (2)		For more information about the PSU configurations, see link.
7	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.
8	VGA port		Use the VGA port to connect a display to the system. For more information, see link.
9	CMA power port		The Cable Management Arm (CMA) power port enables you to connect to the CMA.
10	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.

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 Data Store Service (GDD). One Arcserve UDP GDD data store will use 3 free ports

				that start from 5000. It is needed when the data store with GDD is enabled for backup or the restore task is used.
6052	TCP	Arcserve Backup GDB	CA.ARCserve.Communication Foundation.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.Communication Foundation.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 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.
8014	TCP	Arcserve UDP Server	httpd.exe	Specifies the default HTTP/HTTPS communication 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 data stores 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 3rd 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 out-going com-munications.
18005	TCP	Arcserve UDP Linux	Java	Used by Tomcat. Can be ignored for firewall settings.

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
4152-3	TCP	CASDiscovery	casdscsvc.exe	Arcserve Discovery Service
4152-4	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.

How to Add Ports to CentOS 6.6 x64 Firewall

If you upgrade the Arcserve Appliance pre-installed Linux Backup Server to v6.5 Update 2, then after the upgrade you need to manually add some ports to Linux that has CentOS 6.6 x64 firewall.

Follow these steps:

1. Navigate to the following path:

   vi /etc/sysconfig/iptables

2. In the *iptables* file, manually add the following lines that are mentioned in bold if not present already:

   # Firewall configuration written by system-config-firewall

   # Manual customization of this file is not recommended.

   **filter*

   :INPUT ACCEPT [0:0]

   :FORWARD ACCEPT [0:0]

   :OUTPUT ACCEPT [0:0]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   -A INPUT -p icmp -j ACCEPT

-A INPUT -i lo -j ACCEPT

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

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

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

COMMIT

3. Save the *iptables* file.
4. Restart the *iptables* service using the following command:

   /etc/init.d/iptables restart

You have added the ports to CentOS 6.6 x64 firewall successfully.

Chapter 3: Installing the Arcserve Appliance

This section contains the following topics:

How to Install Arcserve Backup r17.5 SP1 73

How to Install 8100-8200 Series Appliance 75

How to Install 8300-8400 Series Appliance 76

How to Install 9012-9048 Series Appliance 77

How to Install 9072-9504DR Series Appliance 78

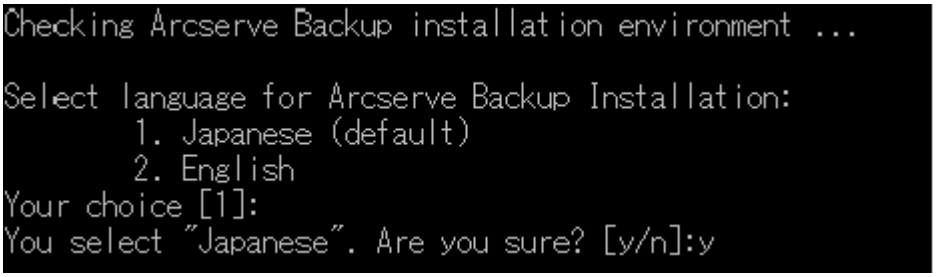
How to Install Arcserve Backup r17.5 SP1

Arcserve Backup r17.5 SP1 is not pre-installed on the appliance. You can install Arcserve Backup r17.5 SP1 using a script called “InstallASBU.bat” located on your desktop.

Follow these steps:

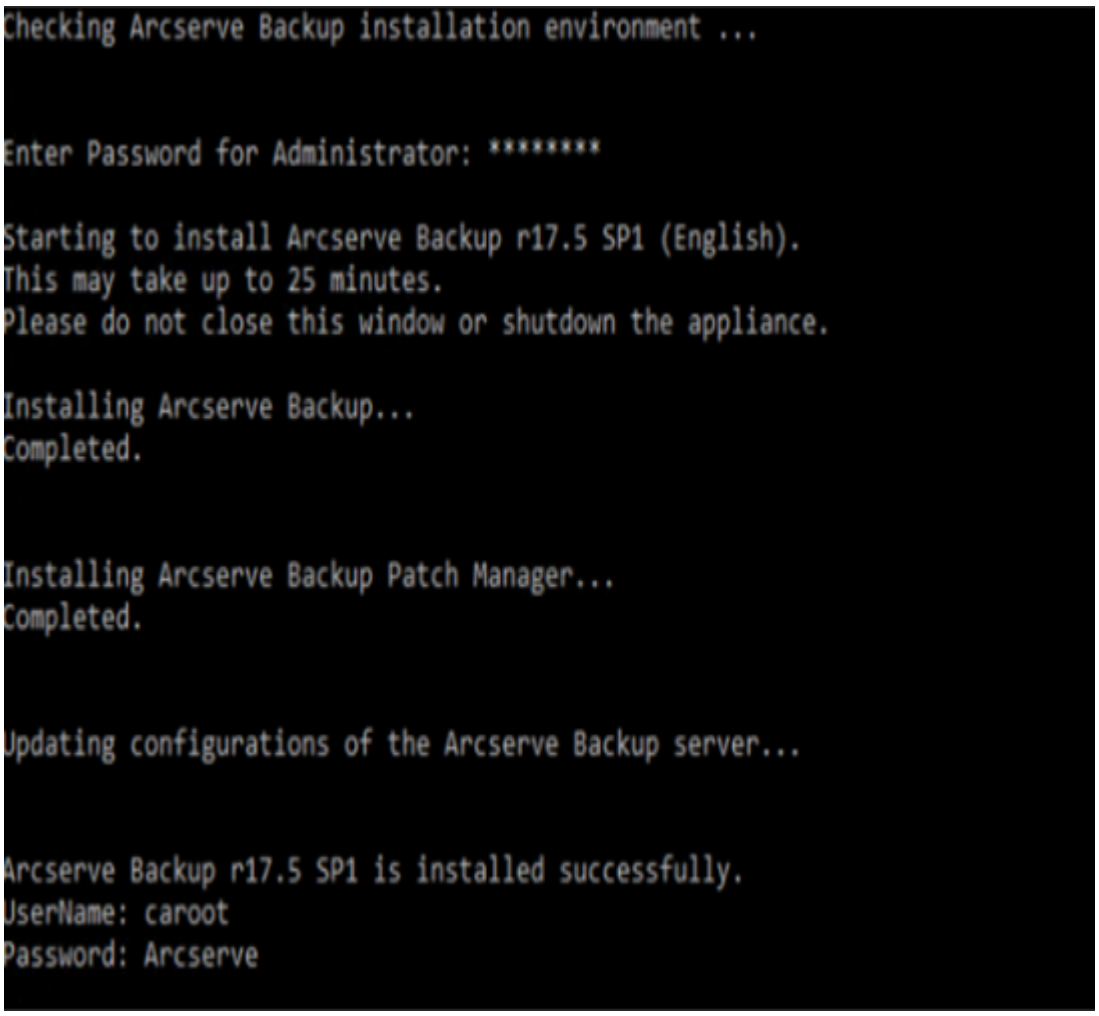
1. From your desktop, locate and launch **InstallASBU.bat**.

   Note: If you are launching the .bat file from a non-English Windows system, the following screen appears. Select the language to install Arcserve Backup r17.5 SP1, otherwise go to step 2.

2. Enter the Administrator password and the script is generated to help install

Arcserve Backup r17.5 SP1.



After installation completes, the Arcserve Backup icon is added to your desktop. You can now log into Arcserve Backup with the following credentials:

- User Name = caroot
- Password = Arcserve

How to Install 8100-8200 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 8100-8200.

How to Install 8300-8400 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 8300-8400.

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.

Chapter 4: Upgrading Arcserve UDP on the Appliance

This section contains the following topics:

How to Apply a License After Upgrading Arcserve Software 80

Upgrade Sequence on the Arcserve Appliance 81

Upgrade Sequence for UDP Console, RPS, and Agent 87

How to Apply a License After Upgrading Arcserve Software

After upgrading Arcserve UDP to v6.5 or upgrading Arcserve Backup to r17.5, the original license key on the Arcserve Appliance will not work. To obtain the new license keys for Arcserve Unified Data Protection v6.5 and Arcserve Backup r17.5, contact your account representative.

For more details about adding a license key for Arcserve UDP, see Arcserve Product Licensing Online Help.

Upgrade Sequence on the Arcserve Appliance

The upgrade from Arcserve Appliance v5.0 to Arcserve UDP v6.5 could involve one of the following sequences:

- 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 the Arcserve Appliance Used as Arcserve UDP Console and RPS

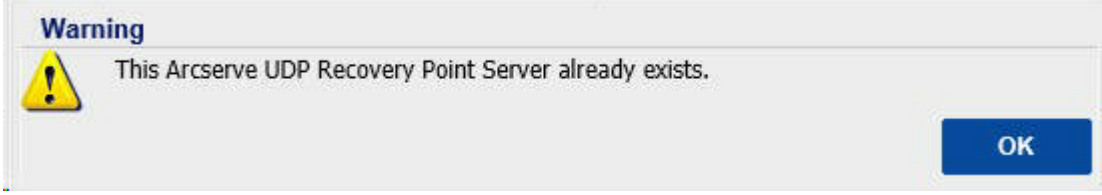
Upgrade this Arcserve Appliance, then follow up the upgrade sequence described to upgrade the environment.

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 Appliances are Used in the Environment

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



Upgrade the Arcserve UDP Linux Agent on the Arcserve Appliance

Follow these steps:

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

For more information, see *Arcserve Unified Data Protection Agent for Linux Online Help*.

Upgrade the Arcserve Backup on the Arcserve Appliance

Refer to the Arcserve Backup Implementation Guide to complete upgrade on the Arcserve Appliance.

Upgrade Sequence for UDP Console, RPS, and Agent

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

1. Upgrade Arcserve UDP Console.
2. Upgrade Arcserve UDP RPS (DR site).
3. Upgrade Arcserve UDP RPS (Data Center).
4. Upgrade Arcserve UDP Agentless Proxy, some Agents in Data Center.
5. Upgrade Arcserve UDP RPS (Remote site).
6. Upgrade Arcserve UDP Agentless Proxy and some Agents at the remote site.

   Note: Repeat Step 5 and 6 for each remote location.
7. Upgrade Arcserve UDP Virtual Standby Monitor.

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

Chapter 5: Configuring the Arcserve Appliance

This section contains the following topics:

How to Configure Network Settings for Arcserve Appliance 89

How to Set up the Arcserve Appliance 94

Configure Arcserve Appliance as Gateway 103

How to Configure Network Settings for Arcserve Appliance

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

Follow these steps:

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

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

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

   Welcome to the Arcserve Appliance Configuration Tool screen appears.

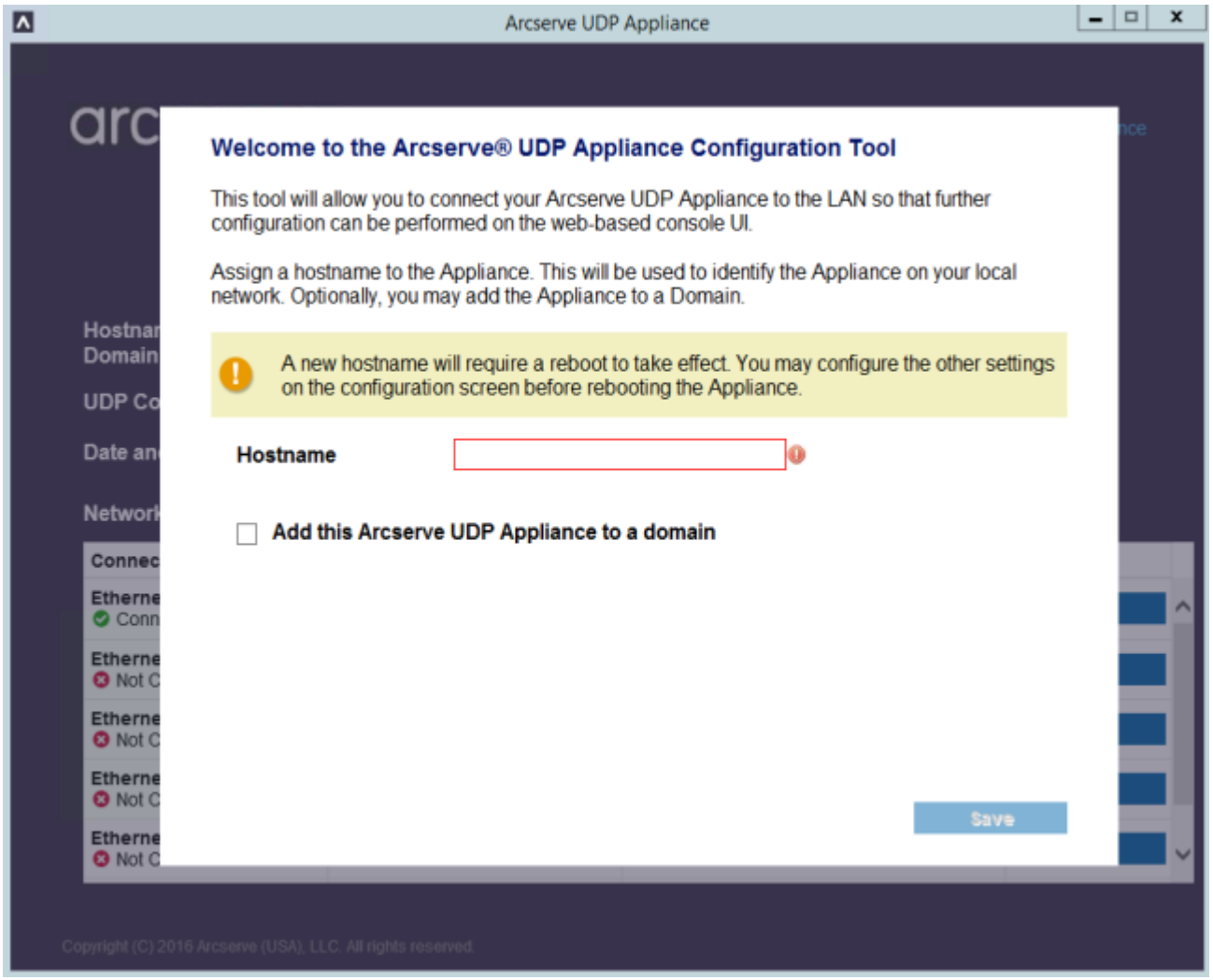
3. Enter the following details:

   Hostname

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

   Add this Arcserve Appliance to a domain

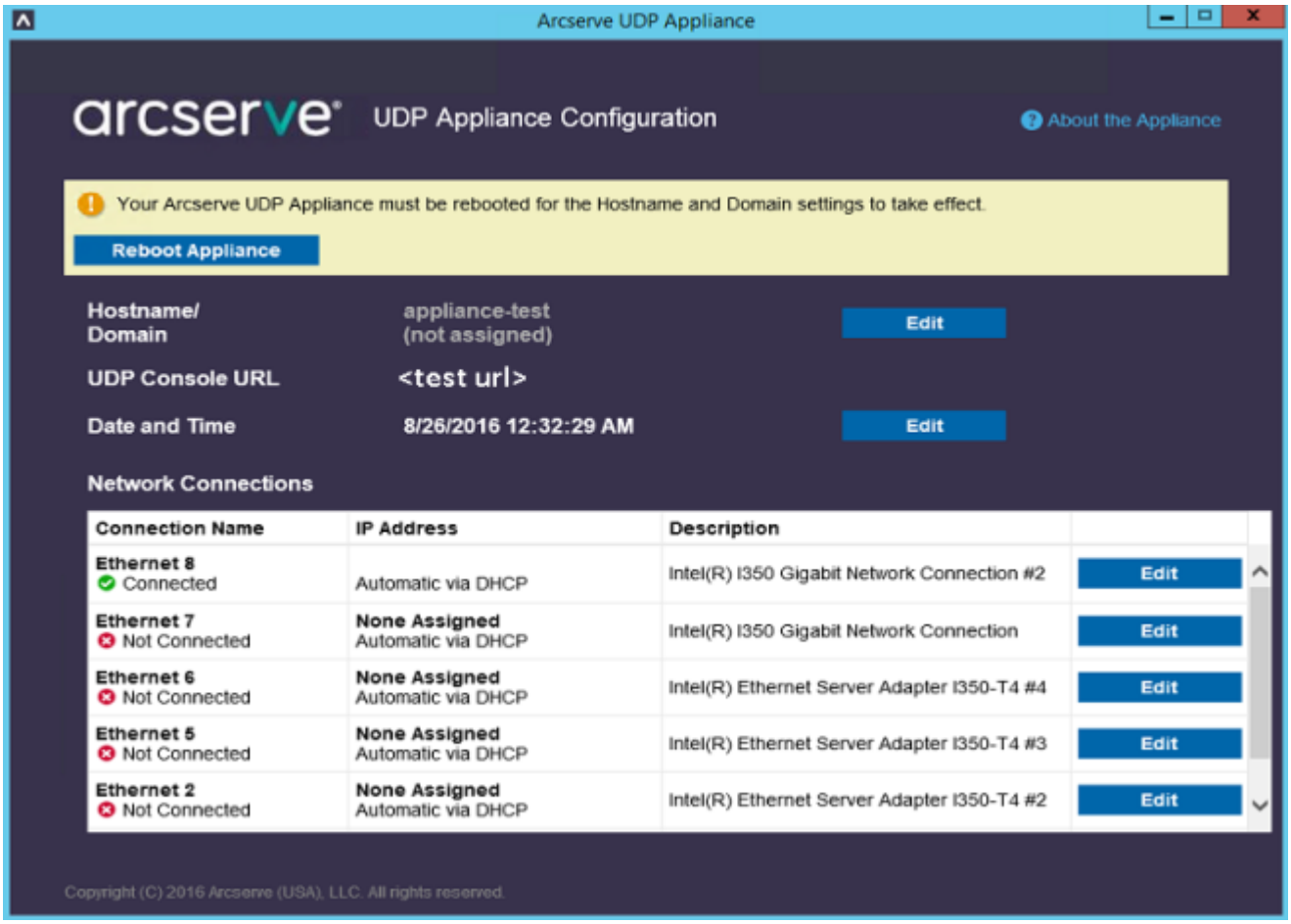
   Select the check-box to make your appliance a member of a domain in your network. Specify the values in Domain, Username, and Password fields that are displayed when the option is selected.



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*.

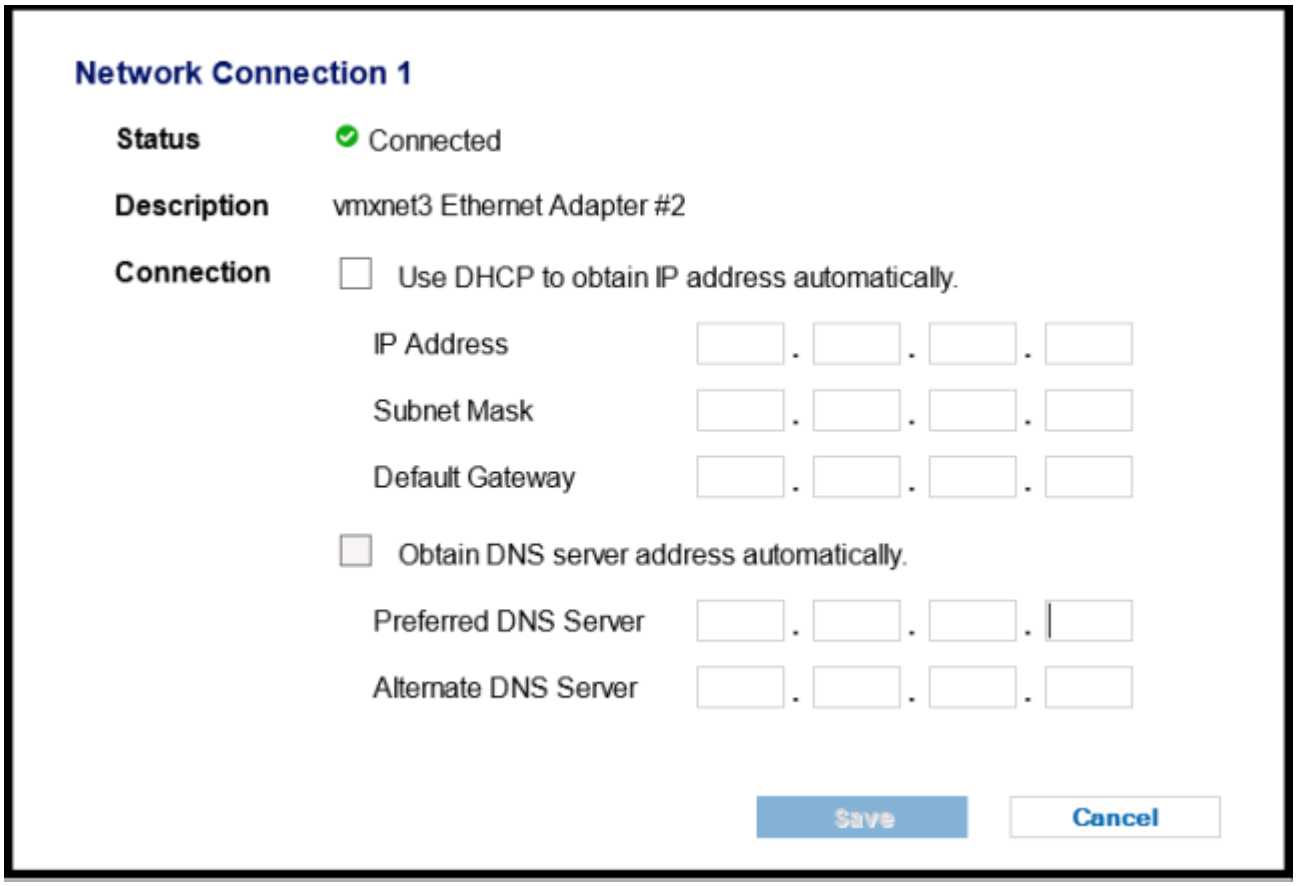
4. Click **Save**.

   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.

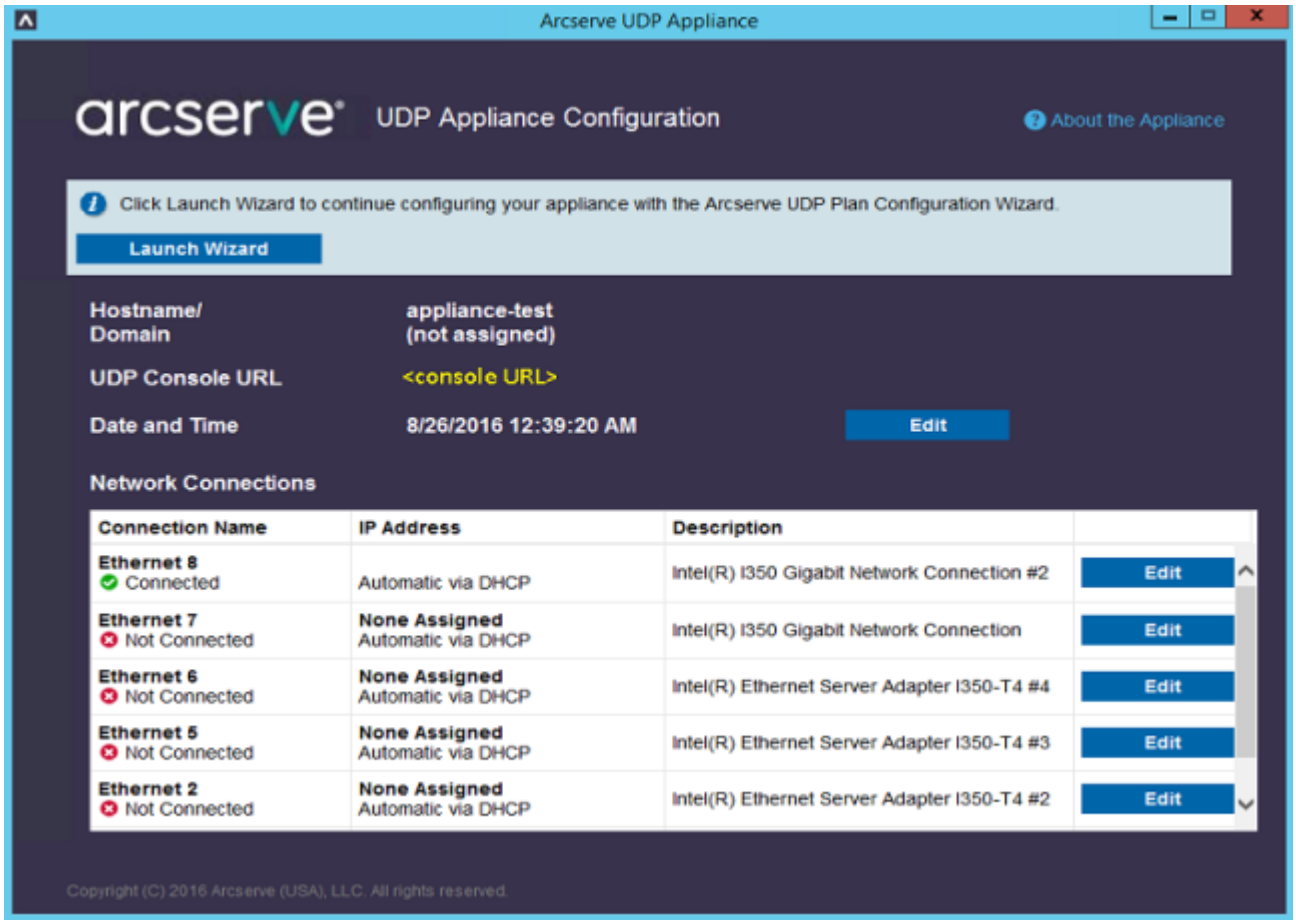
7. To apply the changes, click **Reboot Appliance** to restart the appliance.

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 UDP Appliance
arcserve
UDP Appliance Configuration
About the Appliance
Click Launch Wizard to continue configuring your appliance with the Arcserve UDP Plan Configuration Wizard.
Launch Wizard
Hostname/ Domain
appliance-test (not assigned)
UDP Console URL
<console URL>
Date and Time
8/26/2016 12:39:20 AM
Edit
Network Connections
Connection Name
IP Address
Description
Ethernet 8
Connected
Automatic via DHCP
Intel(R) I350 Gigabit Network Connection #2
Edit
Ethernet 7
Not Connected
None Assigned
Automatic via DHCP
Intel(R) I350 Gigabit Network Connection
Edit
Ethernet 6
Not Connected
None Assigned
Automatic via DHCP
Intel(R) Ethernet Server Adapter I350-T4 #4
Edit
Ethernet 5
Not Connected
None Assigned
Automatic via DHCP
Intel(R) Ethernet Server Adapter I350-T4 #3
Edit
Ethernet 2
Not Connected
None Assigned
Automatic via DHCP
Intel(R) Ethernet Server Adapter I350-T4 #2
Edit
Copyright (C) 2016 Arcserve (USA), LLC. All rights reserved.

How to Set up the Arcserve Appliance

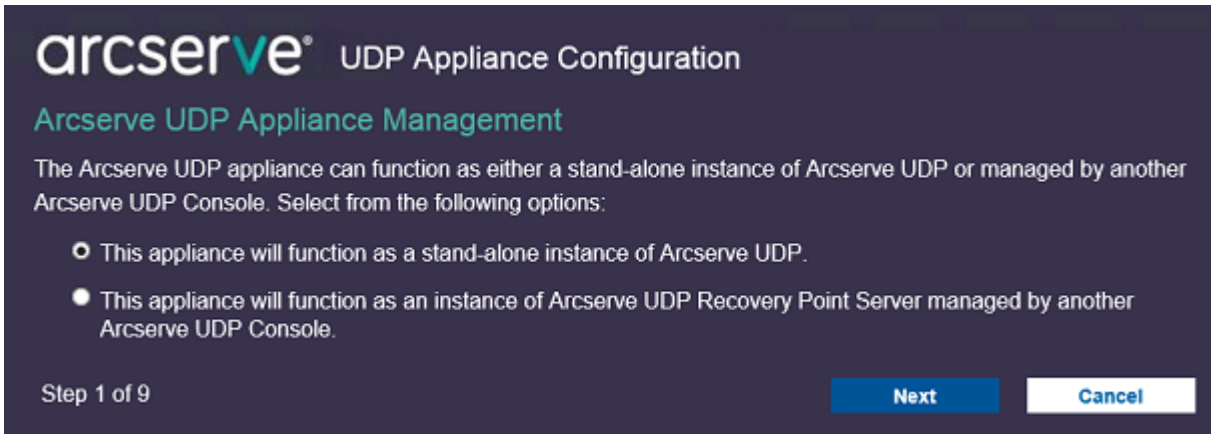
After the appliance restarts with the new hostname, the Unified Data Protection wizard opens. The wizard lets you create a basic plan to schedule backups. The plan lets you define the nodes that you want to protect and schedule when to run backups. The backup destination is the appliance Server.

Note: All the steps on the Arcserve Appliance Configuartion wizard are optional, you can skip 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.

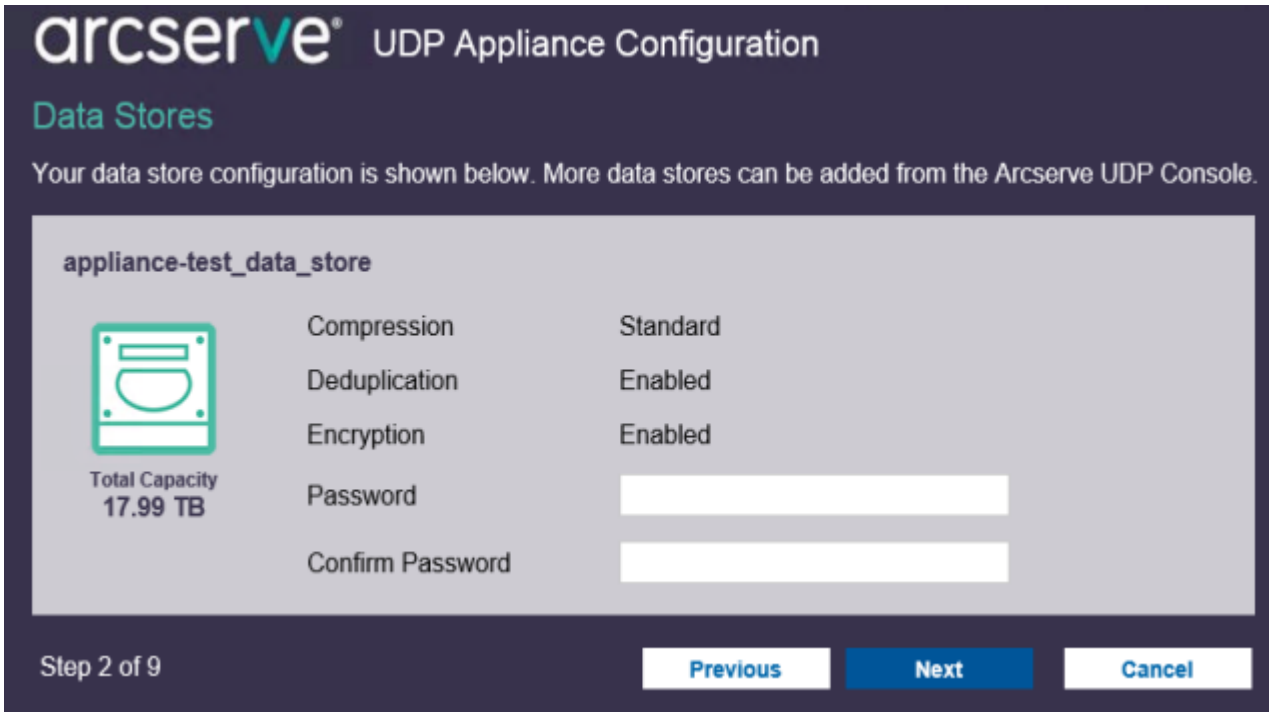


2. Select whether you want to manage the appliance locally (default) or from another UDP console. If the appliance is managed from another UDP console, then specify the UDP console URL, username, and password.
3. Click **Next**.

   The **Data Stores** dialog opens. A data store is a physical storage area on the appliance and is used as the destination for your backups.

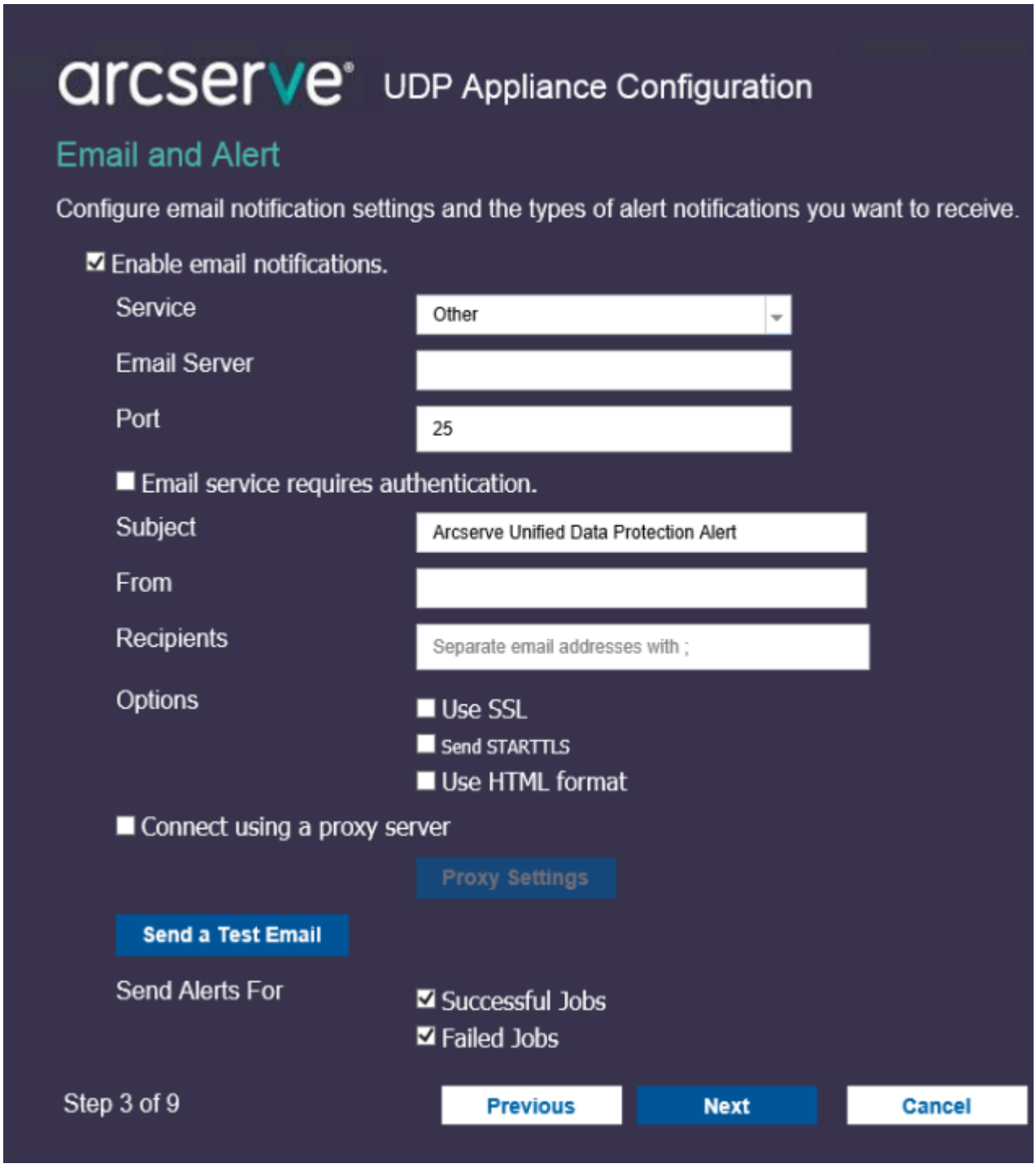
   By default, Arcserve UDP creates a data store called <hostname>_data_store. This data store is deduplication and encryption enabled. For more information about deduplication and encryption, see *Data Deduplication* in Arcserve UDP Solutions Guide.

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



4. Enter and confirm the encryption password for this data store.
5. 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.



6. 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

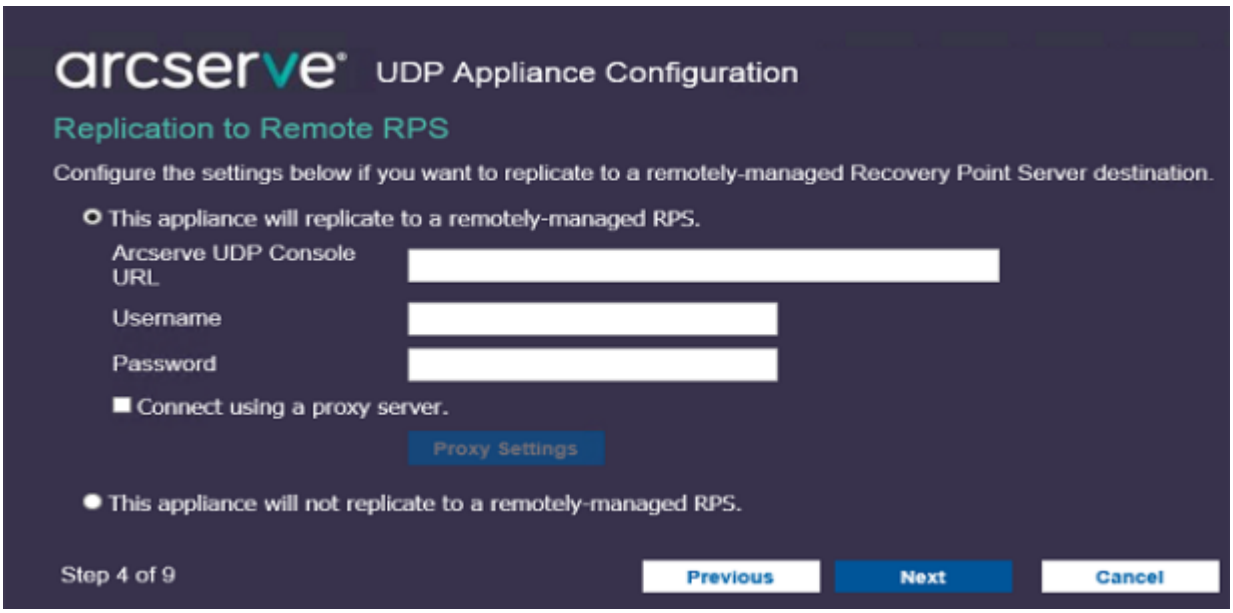
Specifies the proxy Server user name and port number if you are connecting to the mail Server through a proxy Server. Also, specify a username and password if the proxy Server requires authentication.

Send a Test Email

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

7. Click **Next**.

8. The **Replication to Remote RPS** dialog opens.



9. 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.

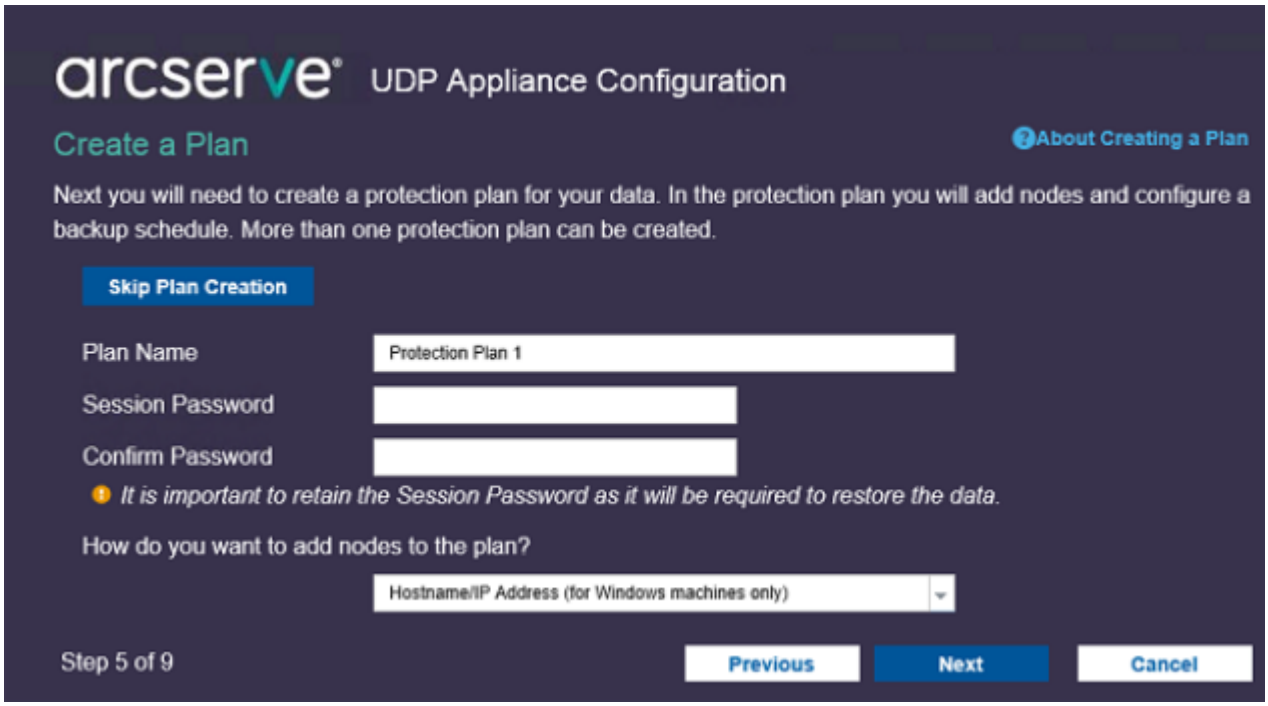
   Connect using a proxy Server

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

10. 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.

11. 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.

12. 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.

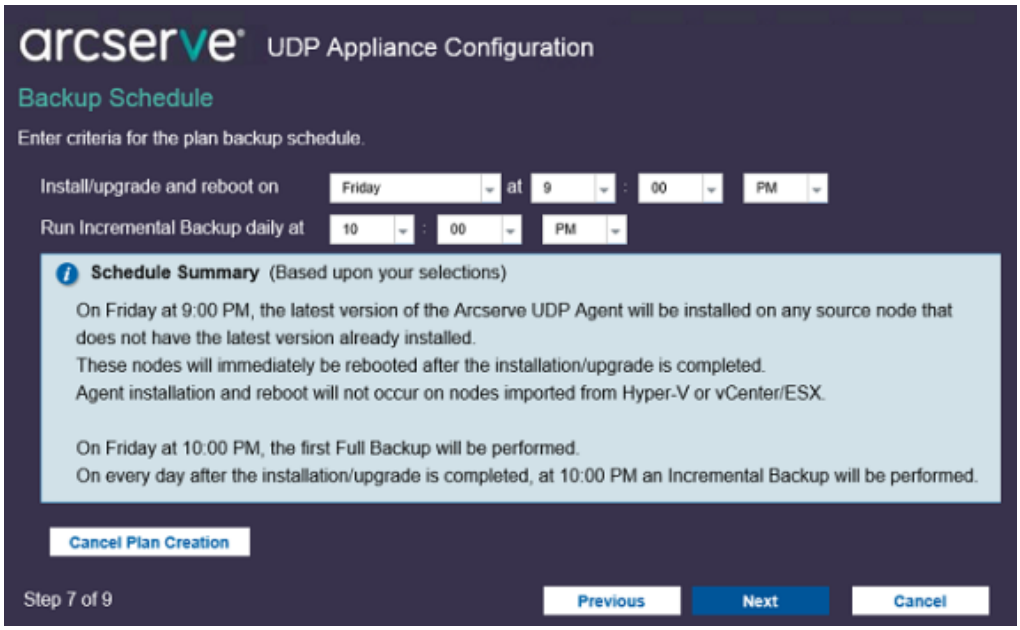
- Importing from a Hyper-V Server

  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.

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

The **Backup Schedule** dialog opens.



14. Enter the following schedule:

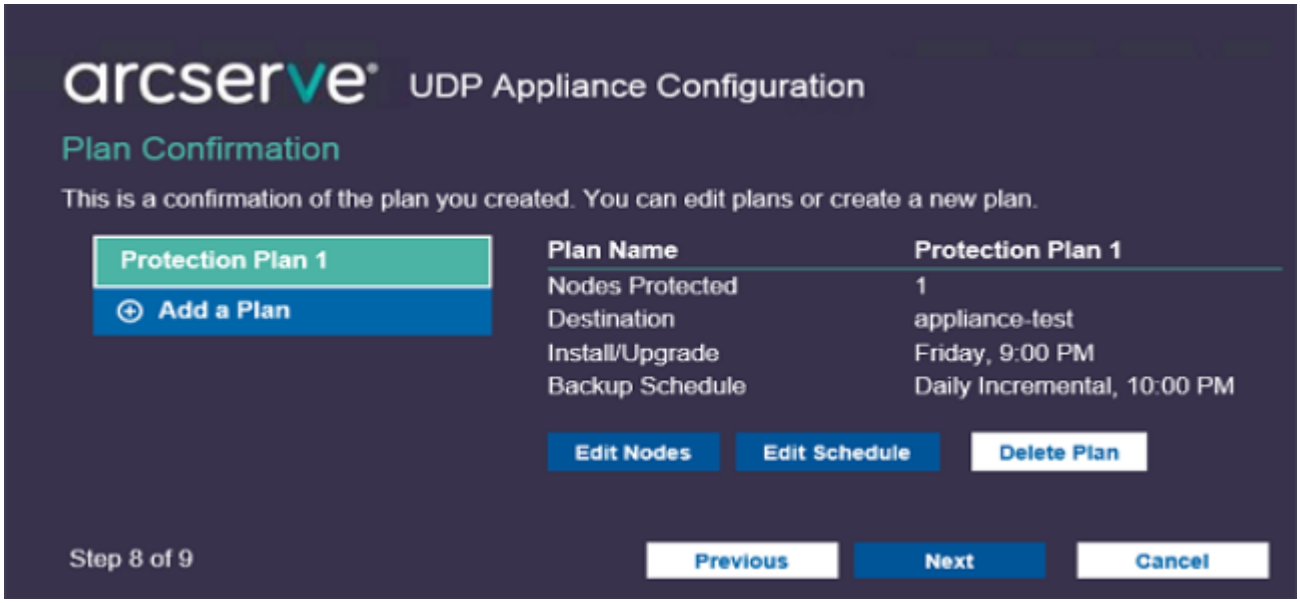
- **Arcserve UDP agent install or upgrade schedule:** The latest version of the Arcserve UDP agent is installed on source nodes that do not have the agent installed. Any previous agent installations is upgraded to the latest version.
- **Incremental backup schedule:** A full backup is performed for the 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**.

15. Click **Next**.

The **Plan Confirmation** dialog opens.



16. From the 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.

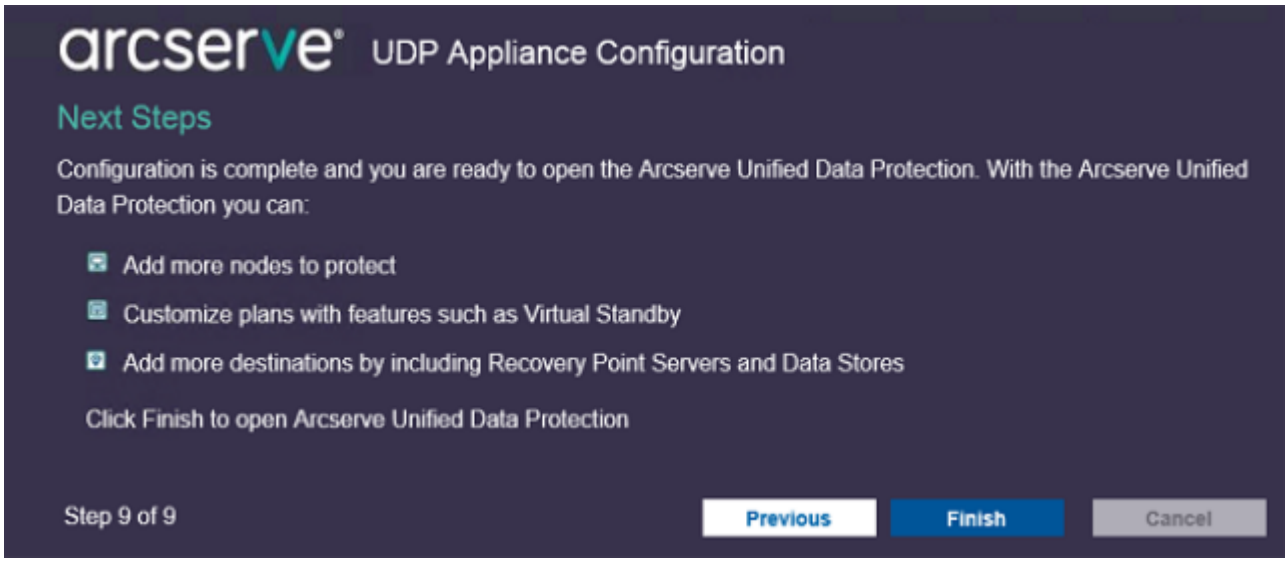
Edit Schedule

Modifies the backup schedule.

17. 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 Data Stores.



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

Configure Arcserve Appliance as Gateway

You can configure the Arcserve Appliance as Gateway.

Follow these steps:

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

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

Chapter 6: Working with Arcserve Appliance

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

This section contains the following topics:

Activate Arcserve Product on the Appliance 105
Create a Plan Using Arcserve Appliance Wizard 106
Add Nodes to a Plan 107
Create a Backup Plan for Linux Nodes 116
Create a Backup Plan to a Tape Device 117
Create an On-Appliance Virtual Standby Plan 118
Create Plan to Backup the Linux Backup Server 119
Setting-up to Perform Linux Instant VM Job to Local Appliance Hyper-V 124
Migrate Arcserve UDP Console Using ConsoleMigration.exe 125
Migrate Pre-installed Linux Backup Server to CentOS 7.4 127
Perform Migration between Arcserve Appliances 129
Modify the Input Source of Pre-installed Linux Backup Server 138

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

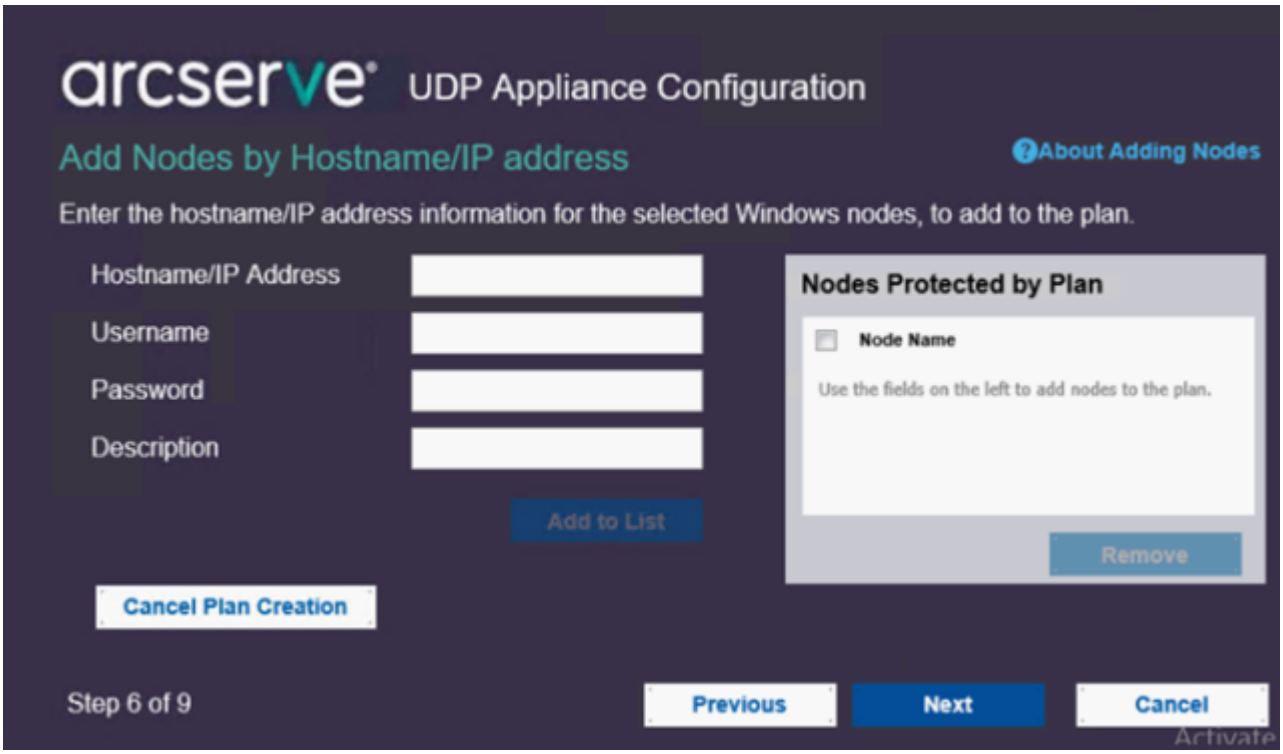
  (Add Hyper-V Nodes)

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 UDP Agent (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**.

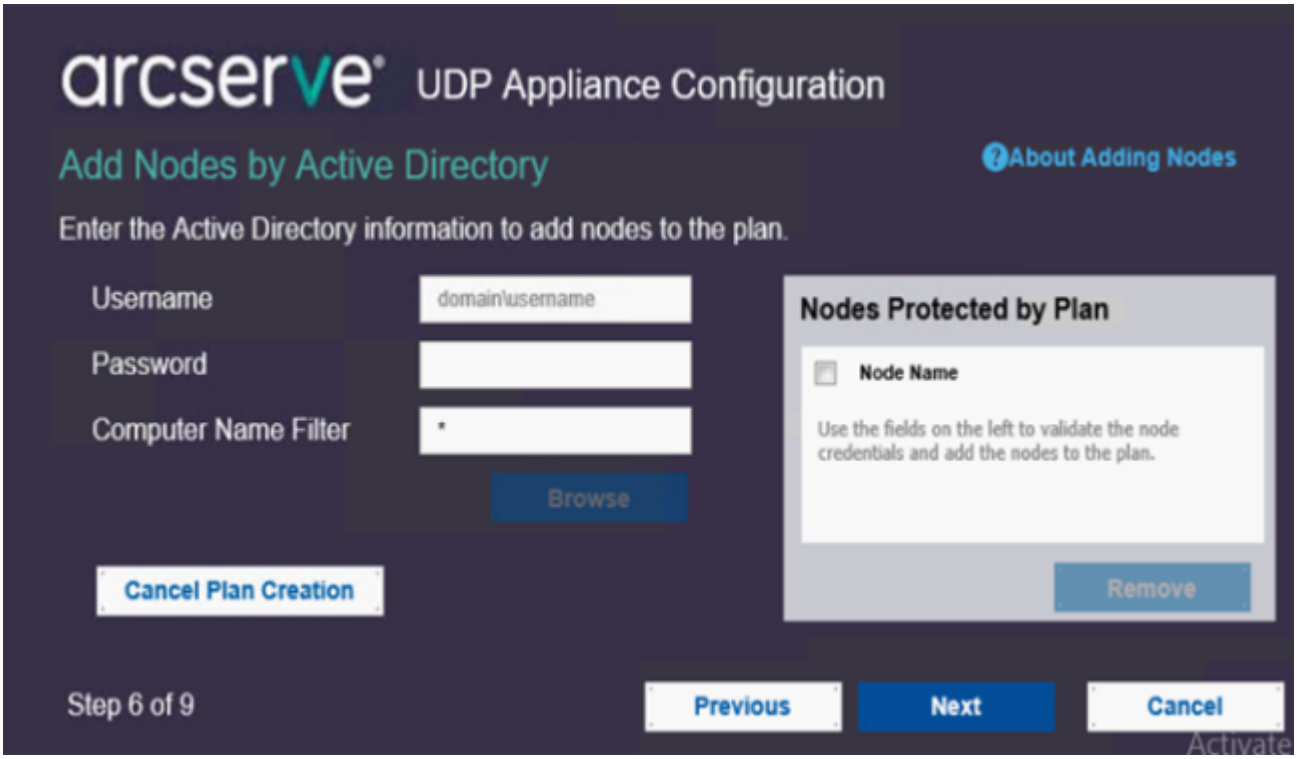
   The nodes are added to the plan.

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

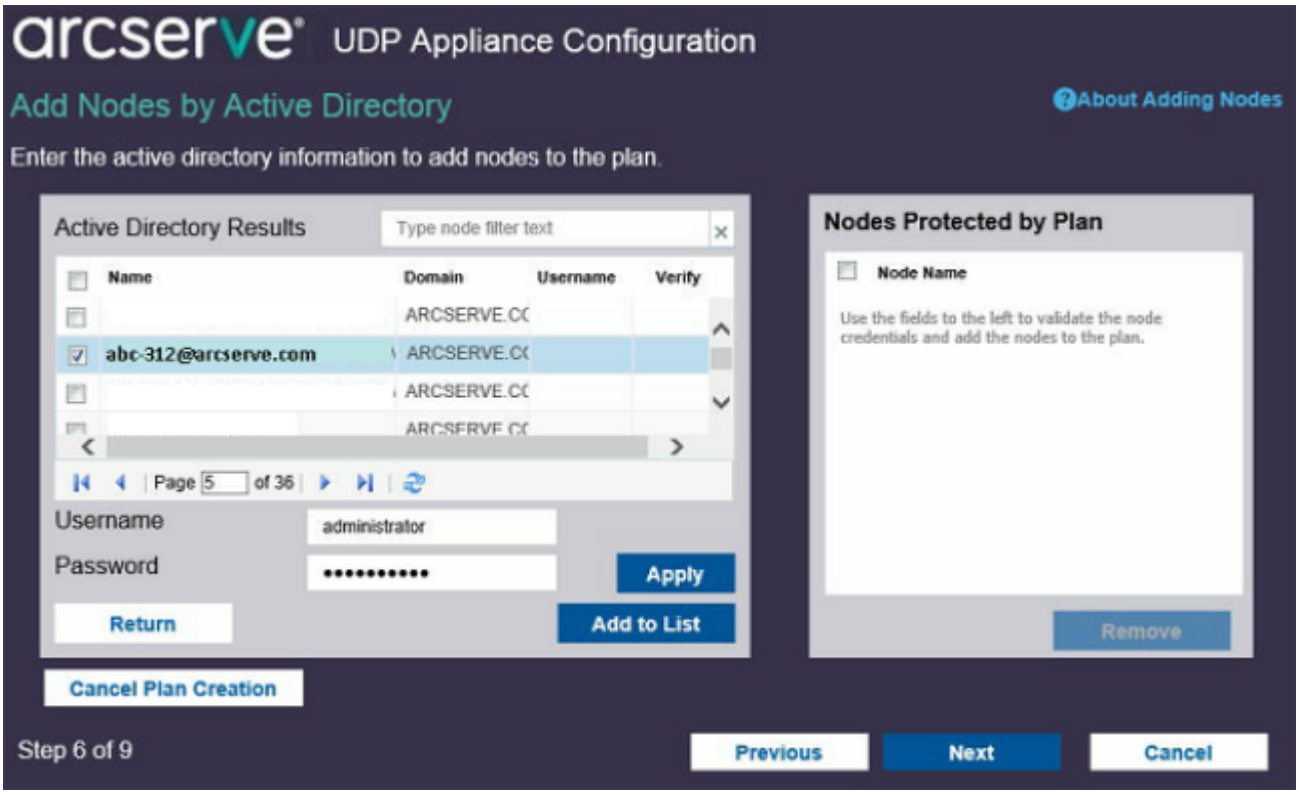
Specifies the filter to discover node names.

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

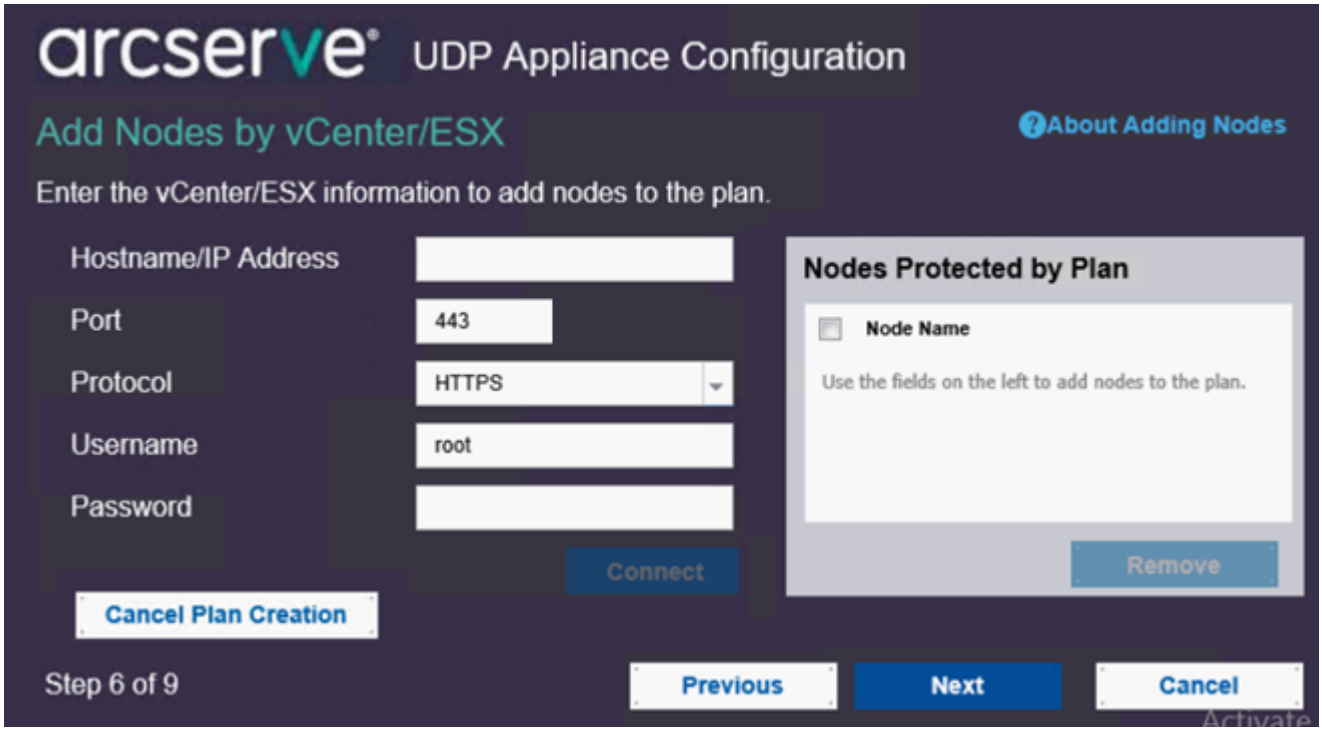
Specifies a user name of the Server.

Password

Specifies the user password.

Cancel Plan Creation

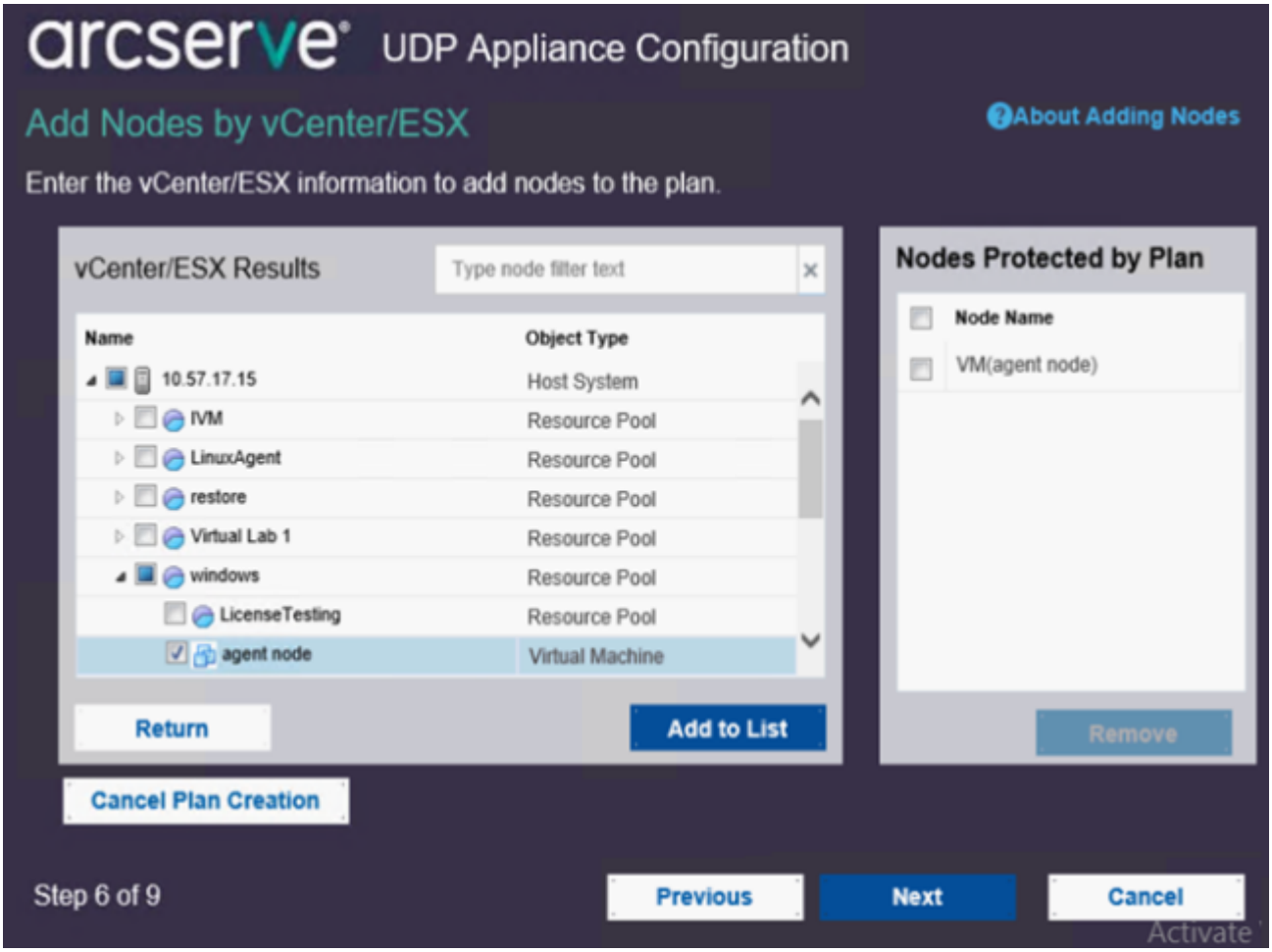
Cancels the plan that you just created.



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**.

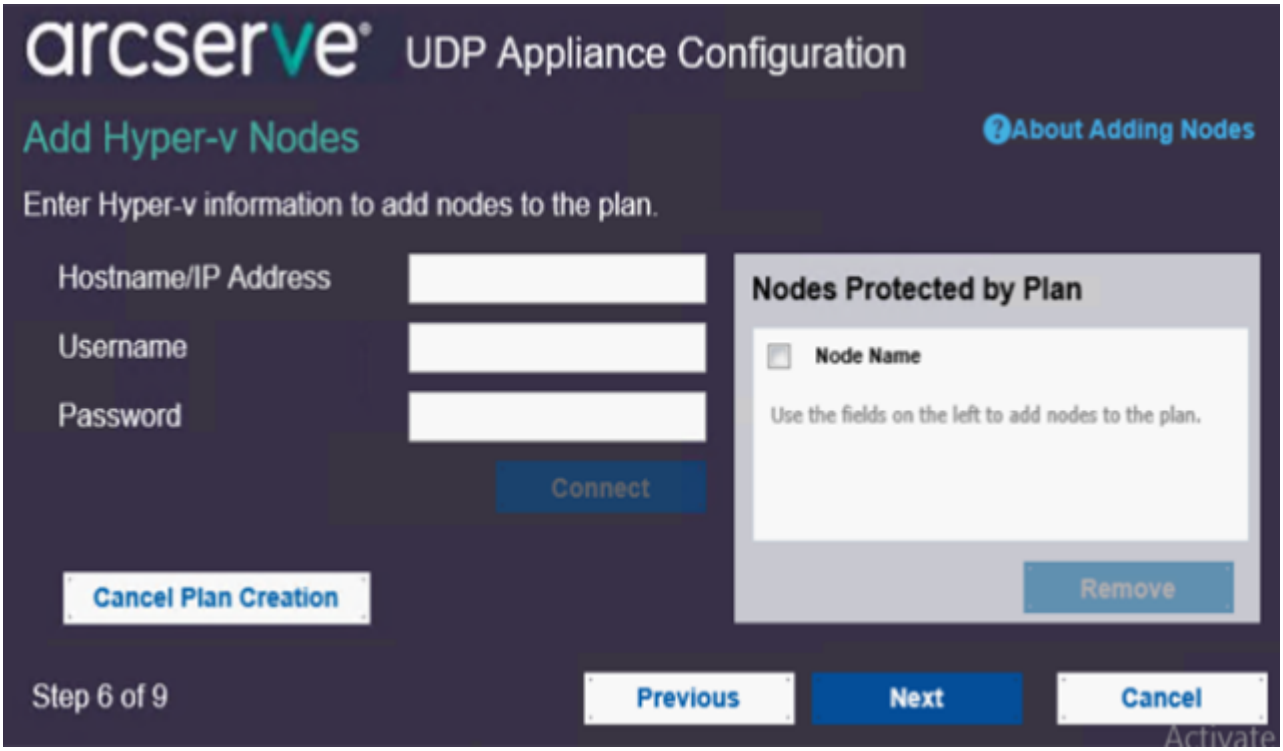
   The nodes are added to the plan.

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

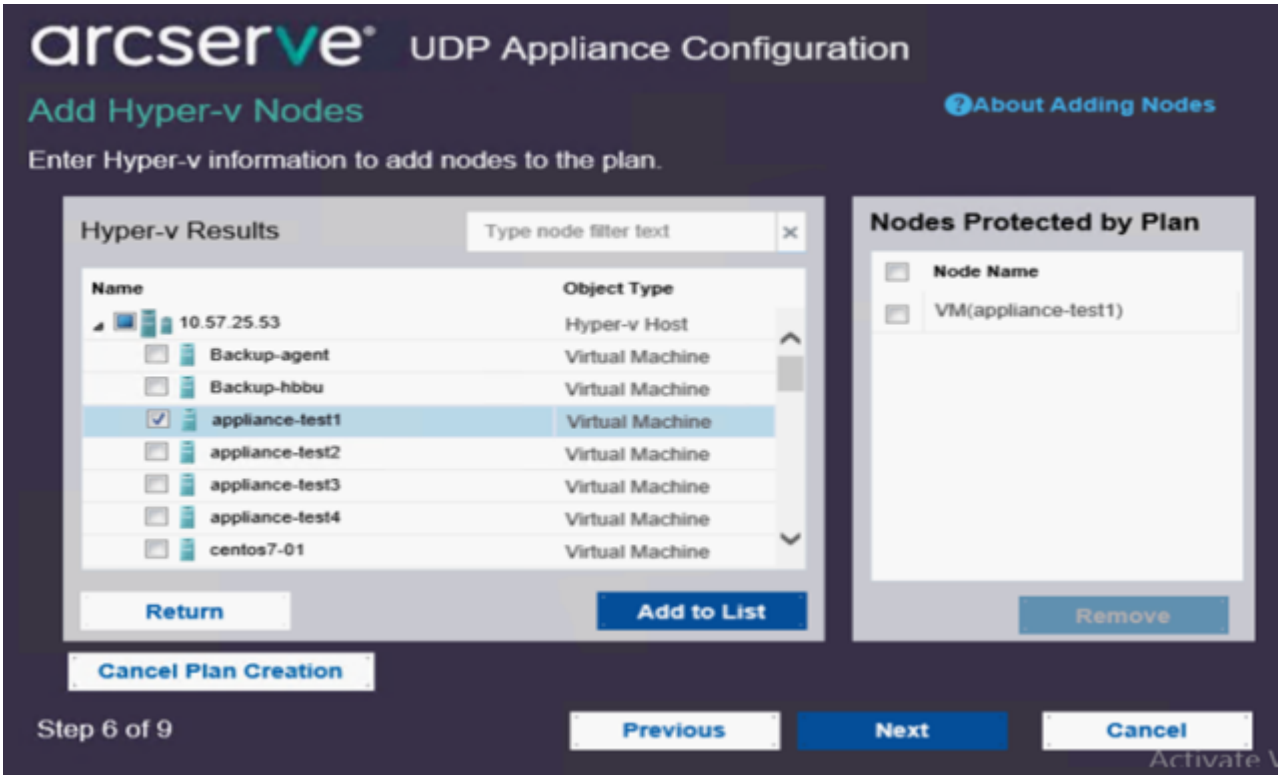
Specifies the password of user name.

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 data store using the UDP backup plan, and the destination is a tape device. You need to use Arcserve Backup Manager to manage your backup jobs to a tape.

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

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

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

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

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

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

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

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

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

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

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

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

Create an On-Appliance Virtual Standby Plan

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

Follow these steps:

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

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

6. Save and run the plan.

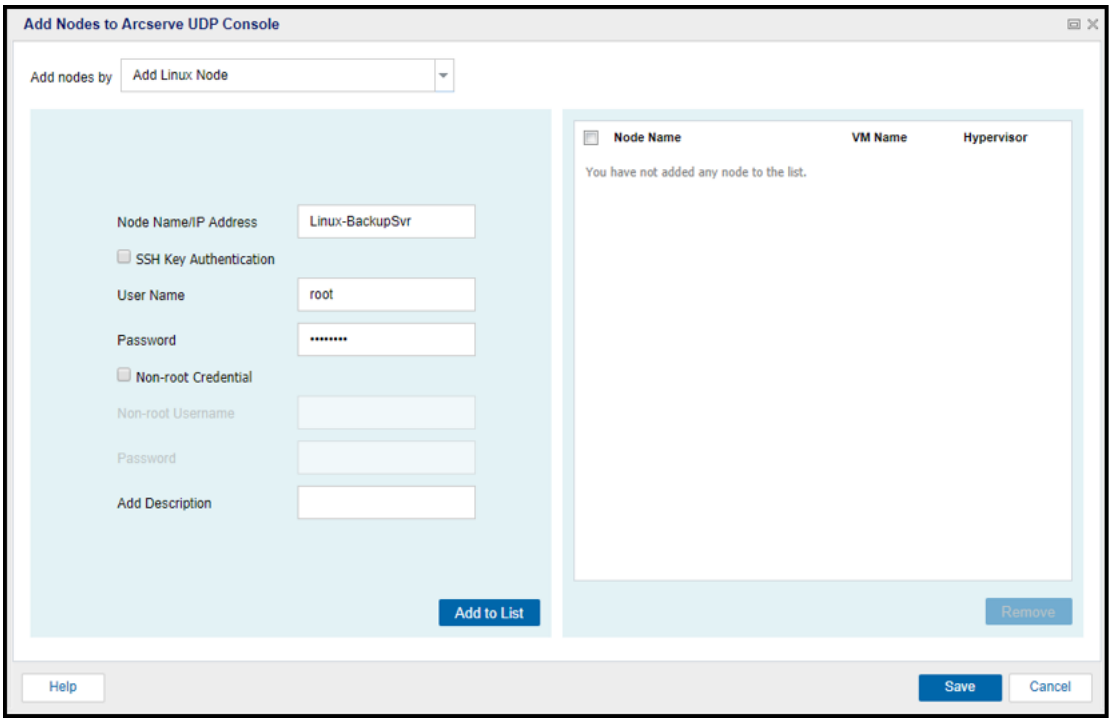
Create Plan to Backup the Linux Backup Server

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

Follow these steps:

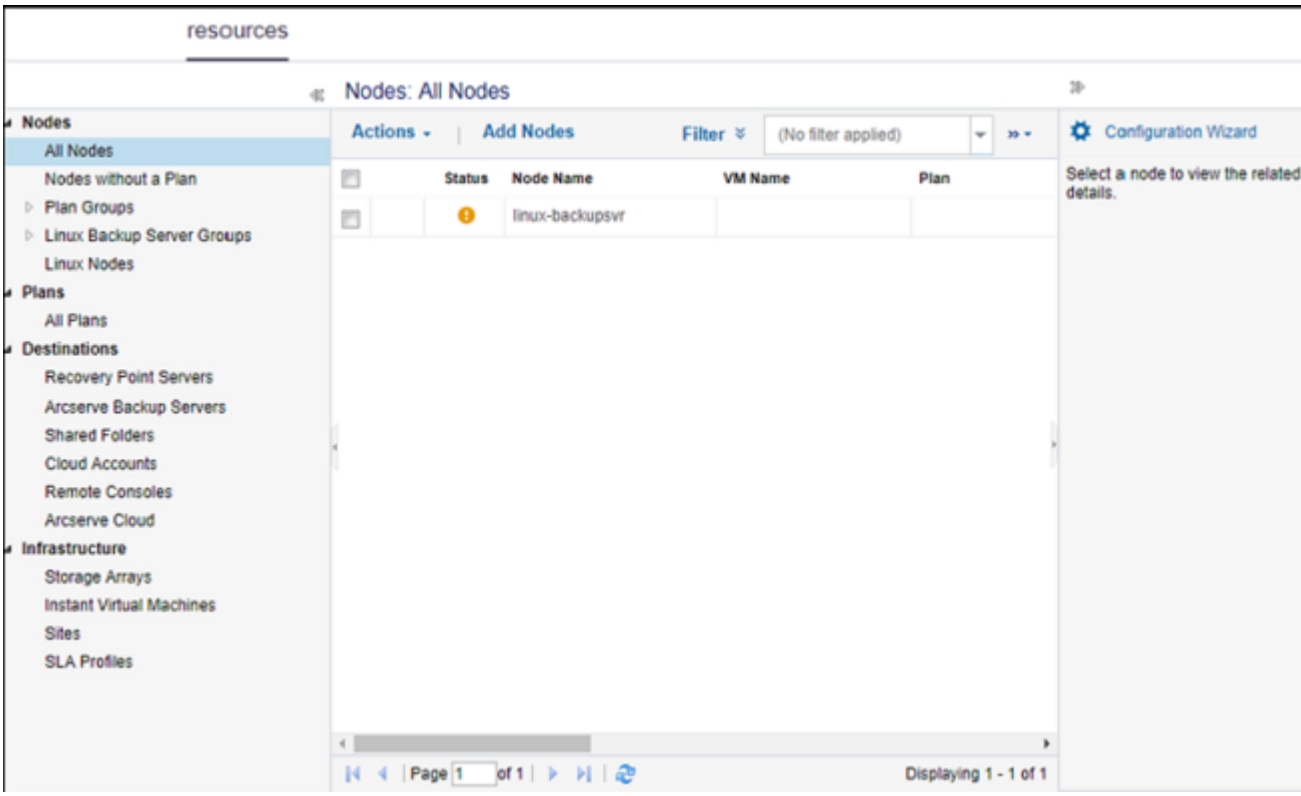
1. From Arcserve UDP Console, click the **resources** tab.
2. Click **All Nodes** in the right pane.
3. From the center pane, click **Add Nodes**.

   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**.



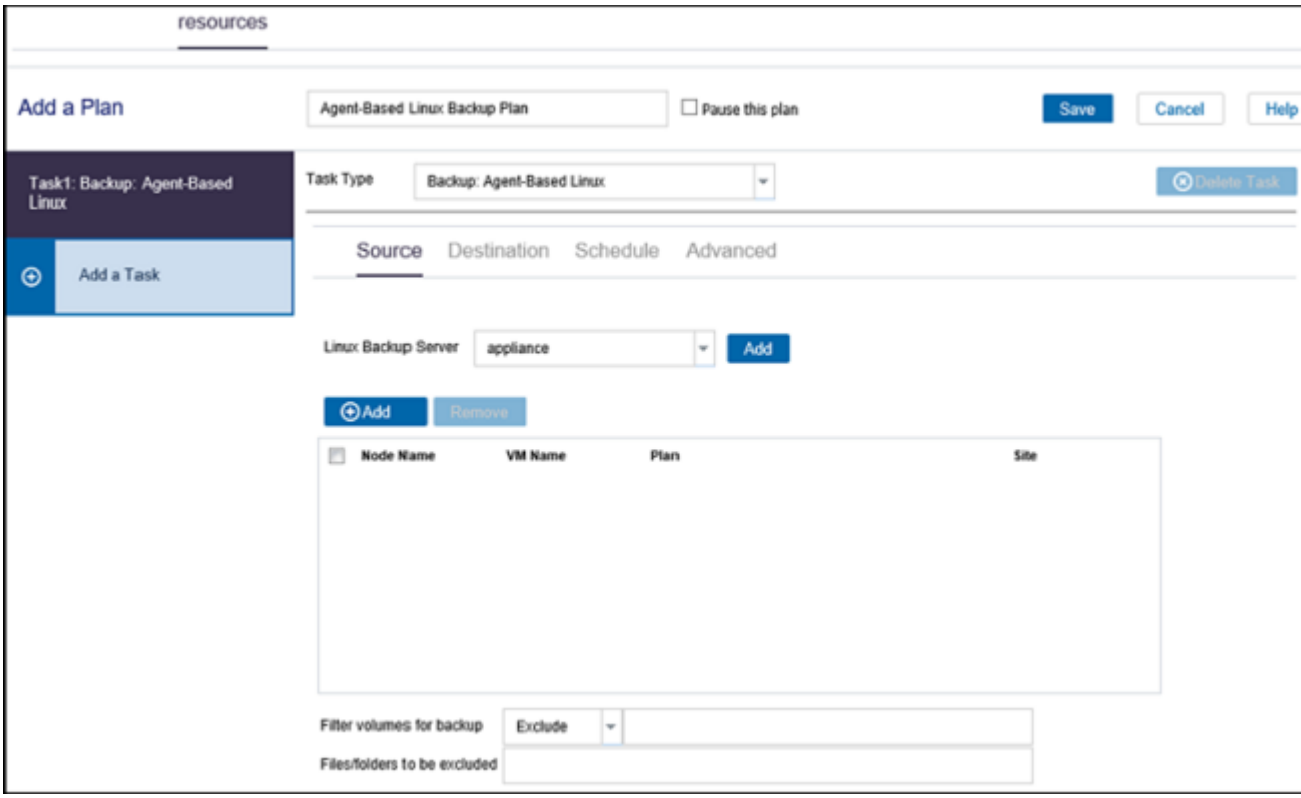
6. Click **Save**.

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

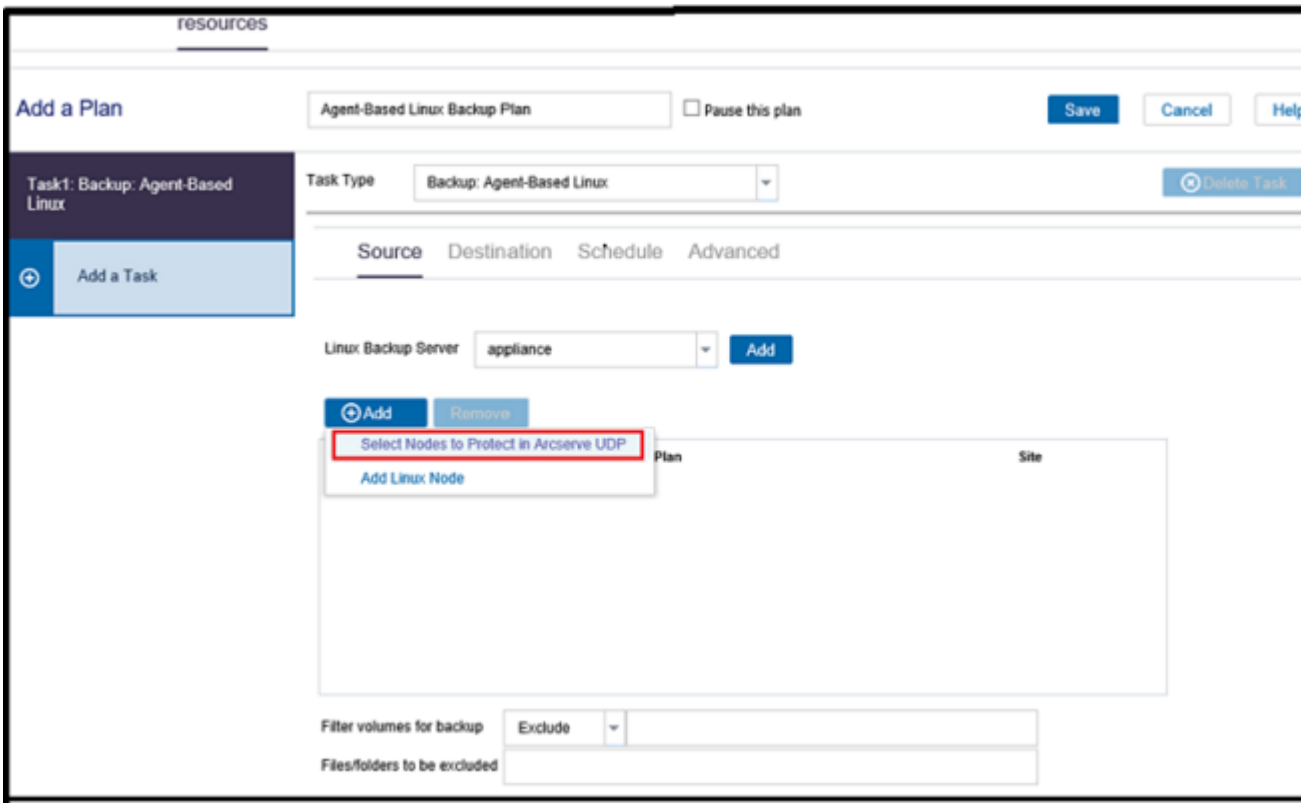


7. Navigate to **All Plans** and create an Agent-based Linux plan.

The **Source** tab appears.

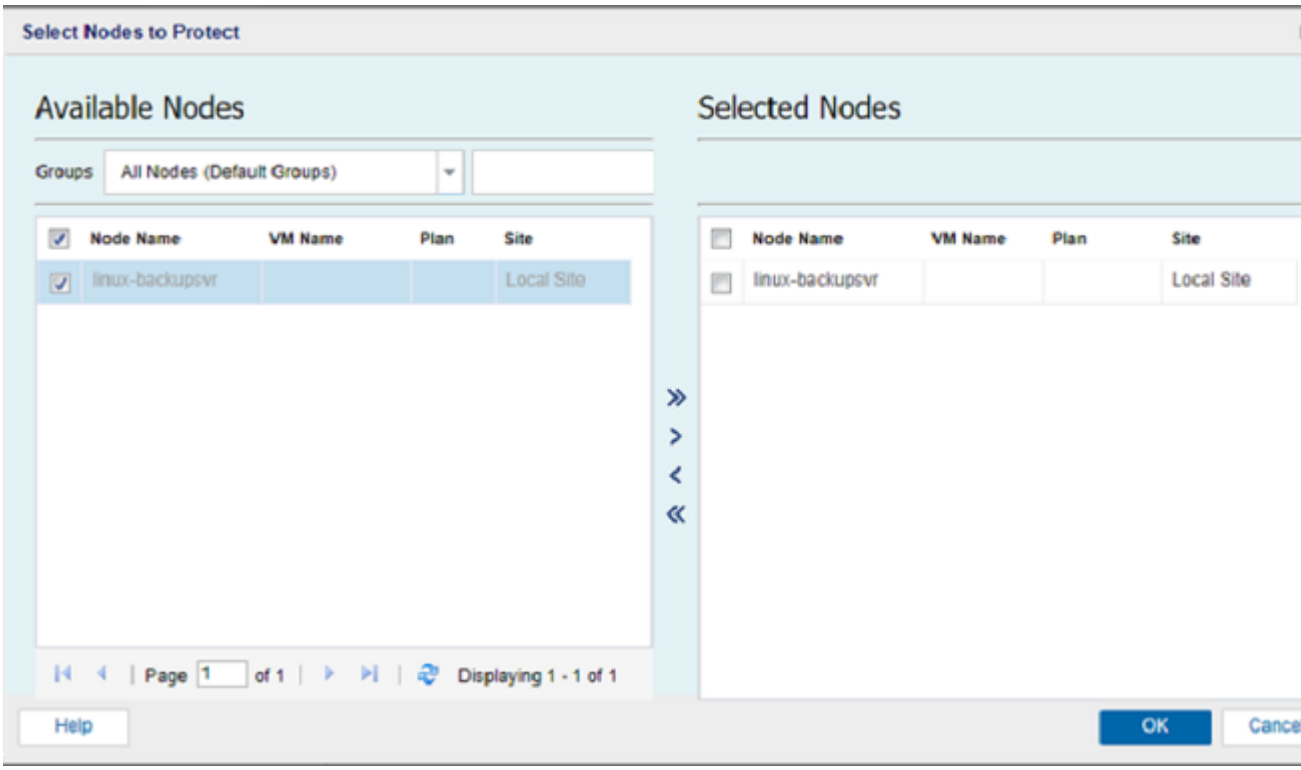


8. From the **Add** drop-down list, select *Select Nodes to Protect in Arcserve UDP*.



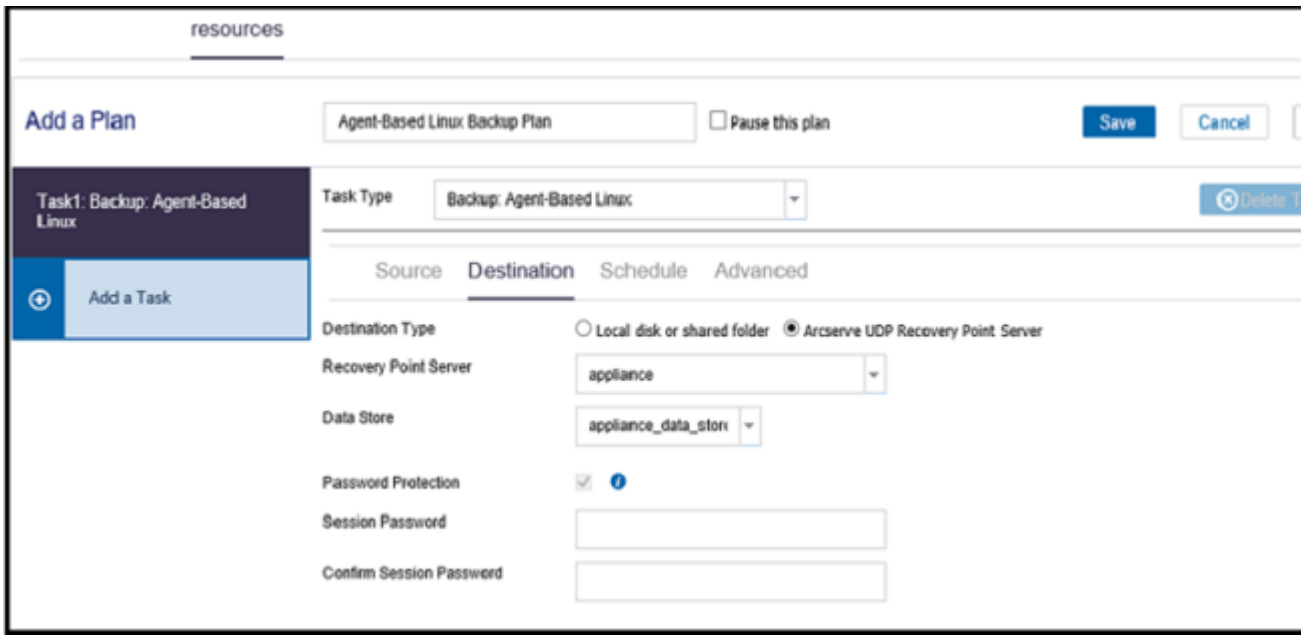
The **Select Nodes to Protect** dialog opens.

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

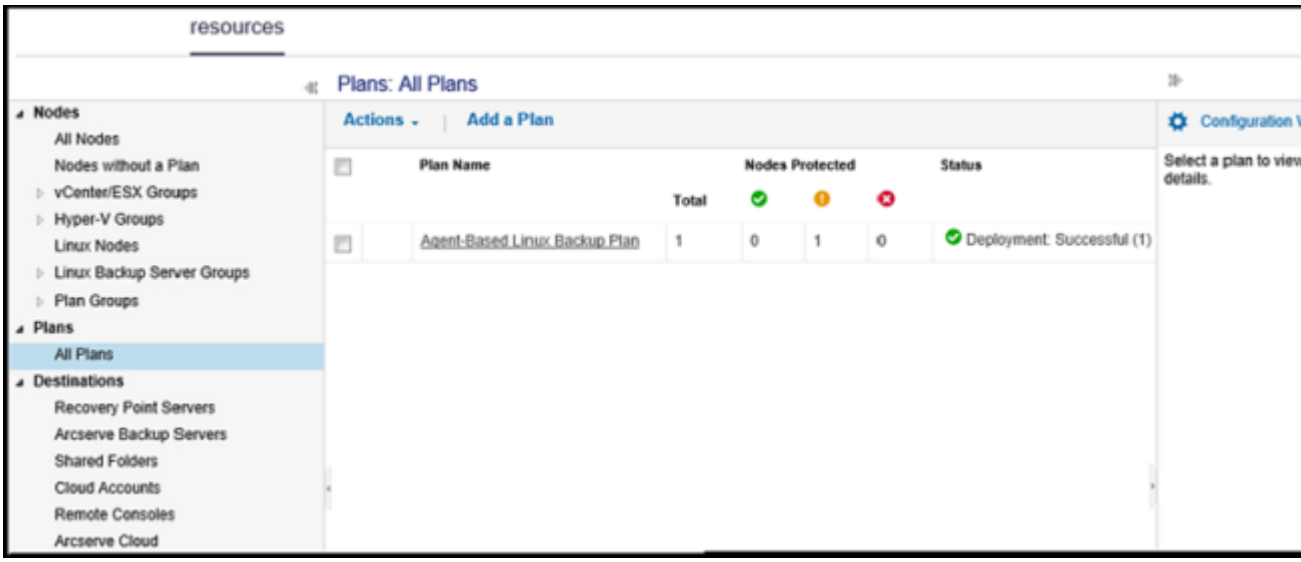


The **Destination** tab appears.

10. The default destination displayed is the data store 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**.



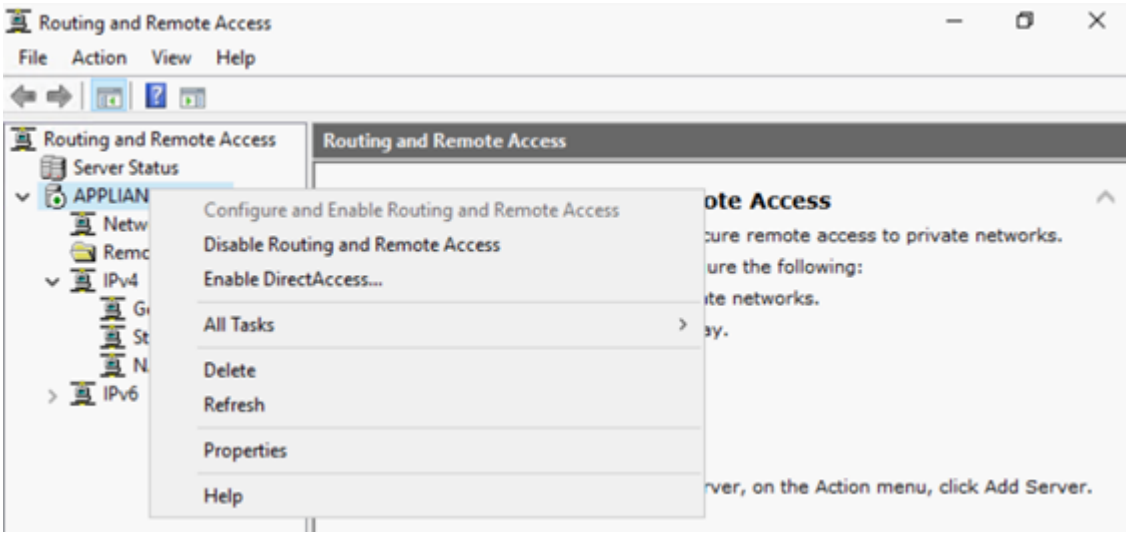
You can perform backup for the added Linux Backup Server successfully.

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. Open Routing and Remote Access and click **Disable Routing and Remote Access**.



4. Run the following command with PowerShell to reconfigure Routing and Remote Access for the newly added virtual network switch in step 1 using DOS command line:

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

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

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.

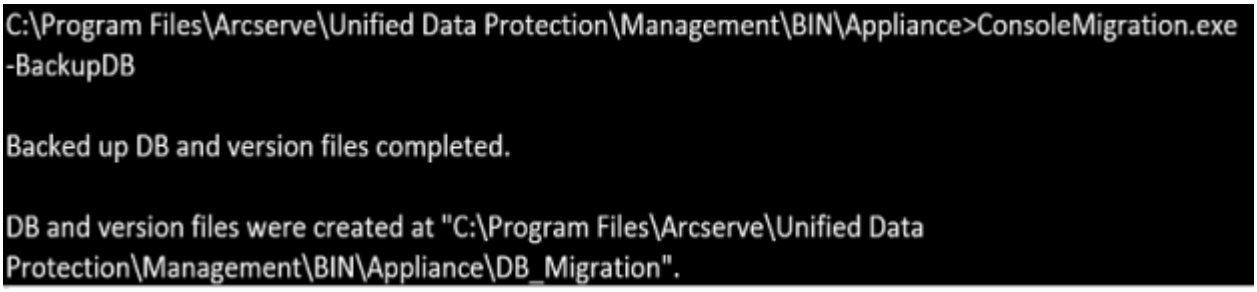
Migrate Arcserve UDP Console Using ConsoleMigration.exe

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:

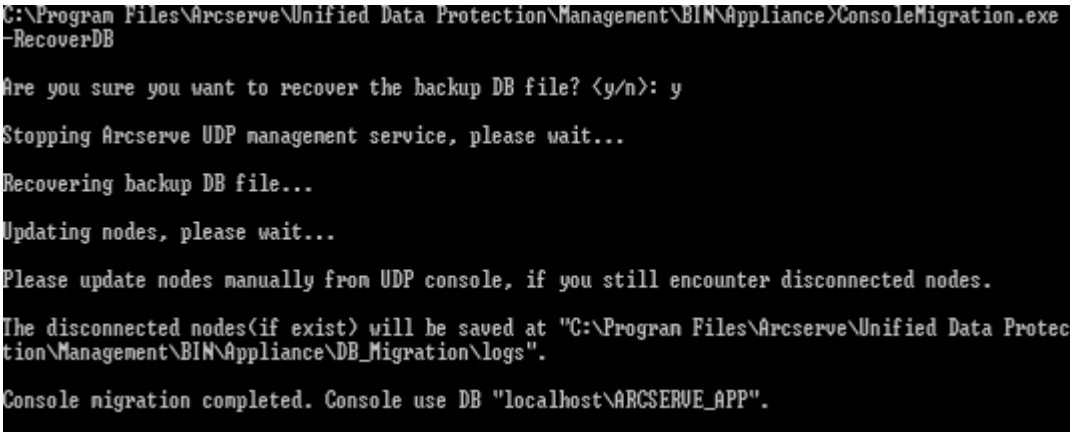
   <UDP_Home> *Management**BIN**Appliance*\

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: In Arcserve UDP v6.5 Update 4, ***-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.

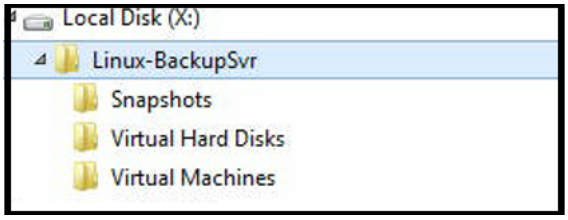
Migrate Pre-installed Linux Backup Server to CentOS 7.4

Important! The Linux Migration Tool is available only from Arcserve UDP v6.5 Update 4 or higher version.

Linux Migration tool (Linux_migration.ps1) is a new feature introduced from Arcserve UDP v6.5 Update 4 that lets you migrate the pre-installed Linux Backup Server of the Arcserve Appliance from the previous version of CentOS such as CentOS 6.6 to CentOS 7.4.

Follow these steps:

1. Log into Arcserve Appliance using the credentials of administrator.
2. Upgrade the previous versions of Arcserve UDP in Arcserve Appliance and Linux Backup Server to Arcserve UDP v6.5 Update 4 or higher version.
3. Download the *Linux-BackupSvr.zip* from the link (the MD5 for this download is *0A51C1020CB8EA569B9DCEAF7BF226E0*) and extract the files to the local drive. For example, if you extract the files to drive X, the path is displayed as below.



4. Open the PowerShell command line and enter the following command to change the directory path to the folder that includes Linux_migration.ps1 file:

   cd C:\Program Files\Arcserve\Unified Data Protection\Engine\bin\Appliance

5. Run the following command to execute the migration:

   Linux_migration.ps1 –path X:\Linux-BackupSvr

   Note: *X:\Linux-BackupSvr* is the path where the files from *Linux-BackupSvr.zip* are extracted to your local drive.

   The command line displays the progress of the migration process.

   After the migration process is completed successfully, the old Linux backup server is powered off and the name of old Linux backup server is modified to *Linux-BackupSvr-CentOS<version number>-<hhmm>*. The import of new Linux

Backup Server (CentOS 7.4) is completed and the name is modified as *Linux-BackupSvr* in the Hyper-V manager successfully.

6. Update the Linux backup server from the Arcserve UDP Console.

   After the migration of Linux Backup Server to CentOS 7.4, all the Linux backup server settings such as Linux backup plans, Linux nodes, and Linux jobs are migrated and configured in the Arcserve Appliance Console successfully.

Perform Migration between Arcserve Appliances

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

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

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

  For more information on Console migration, refer the How to Migrate Arcserve UDP Console Using ConsoleMigration.exe topic.

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

- Solution 1
- Solution 2

Solution 1

Bare Metal Recovery (BMR) solution

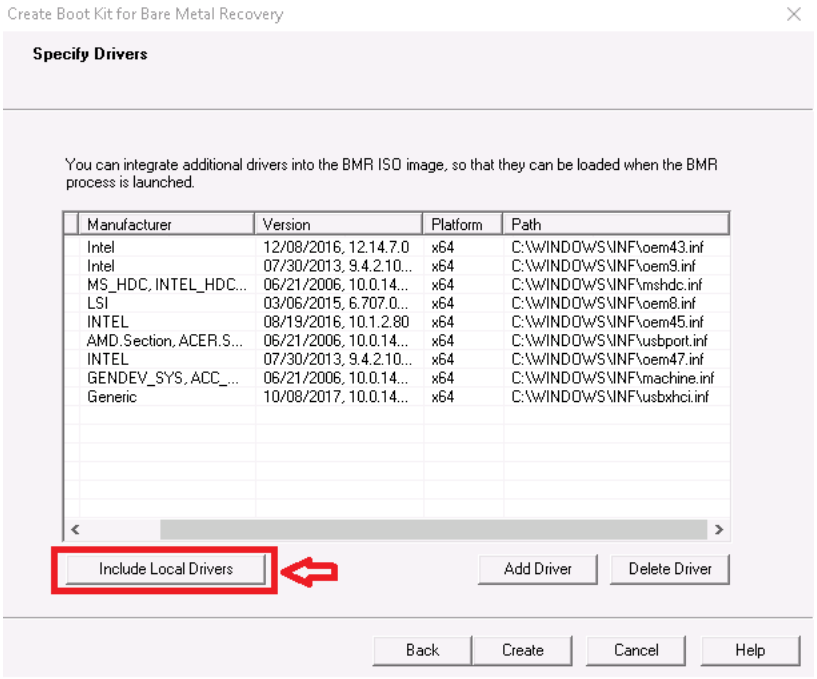
To perform BMR from existing Arcserve Appliance to another fresh Arcserve Appliance, follow these steps:

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

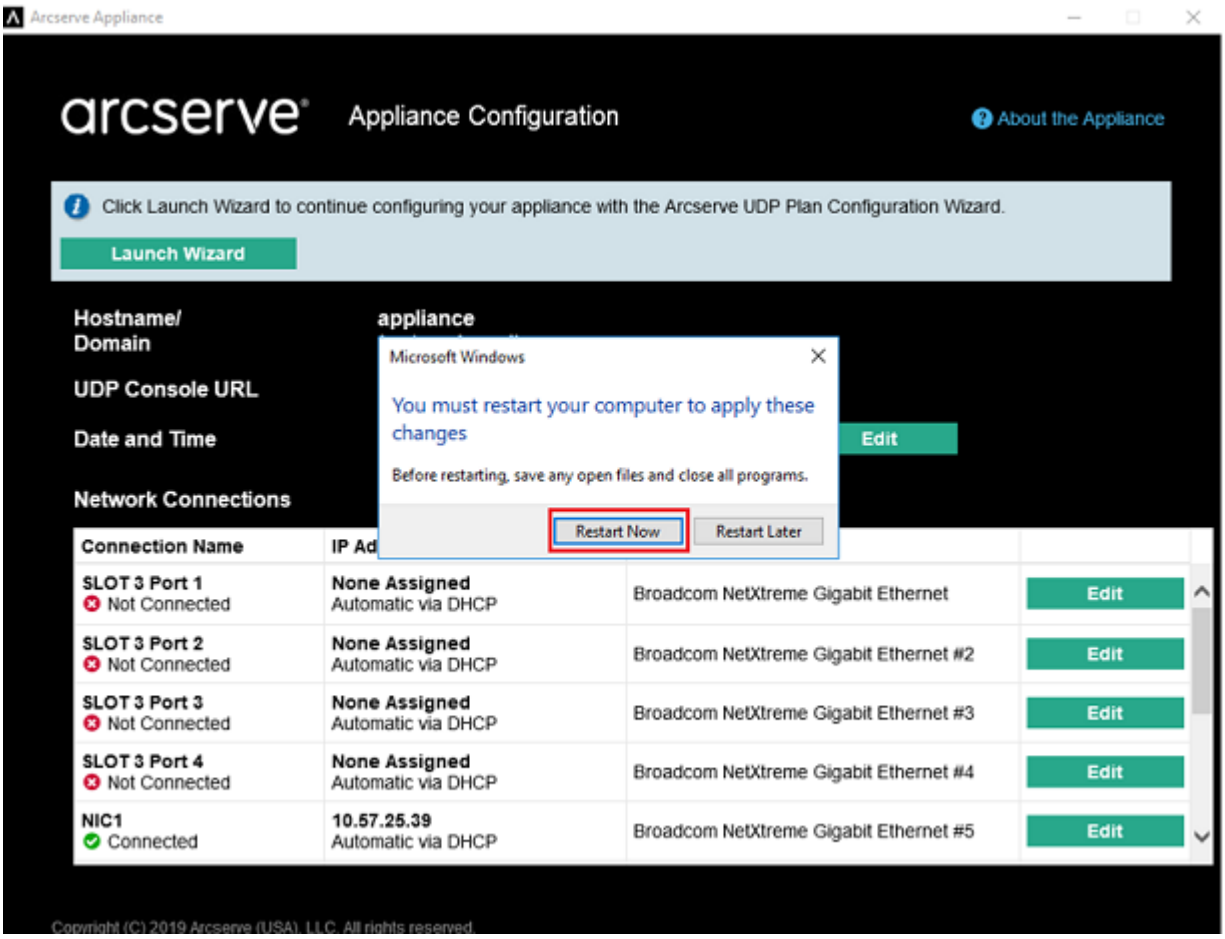
   Note: You can just ignore the following warning:

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

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



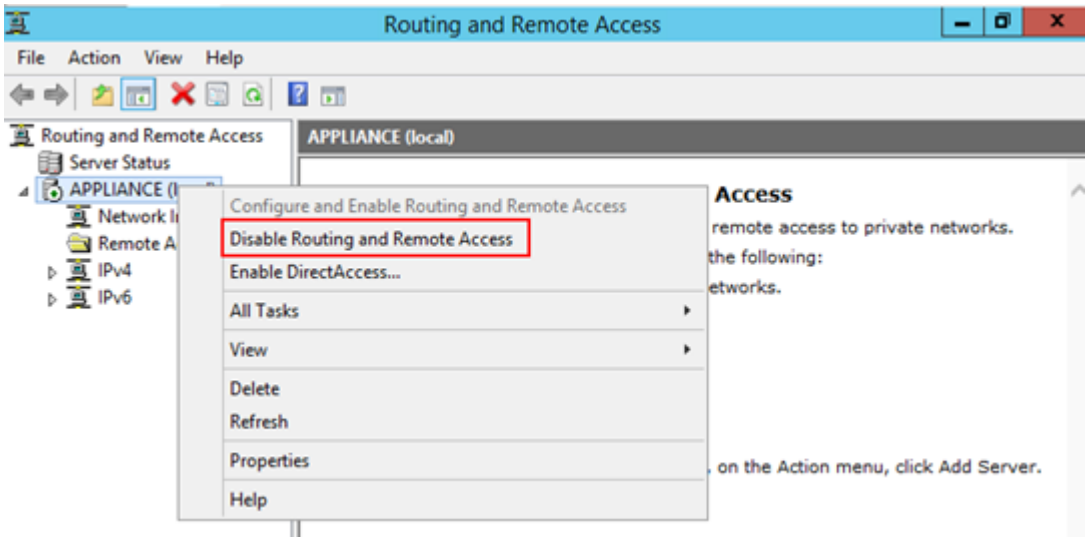
3. After the BMR, restart the Appliance 8400 according to the system prompt.



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

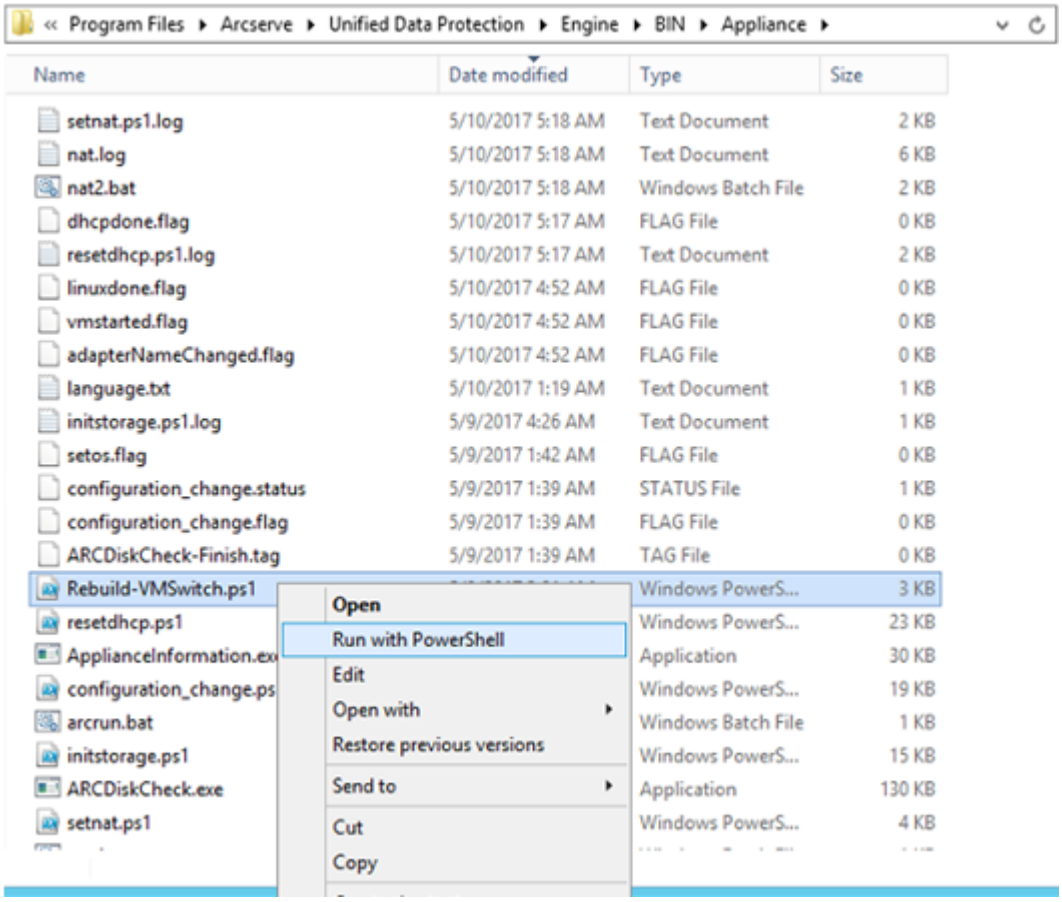
   Follow these steps:

   a. Open Routing and Remote Access and click **Disable Routing and Remote Access**.



   b. Run the following command with PowerShell:

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

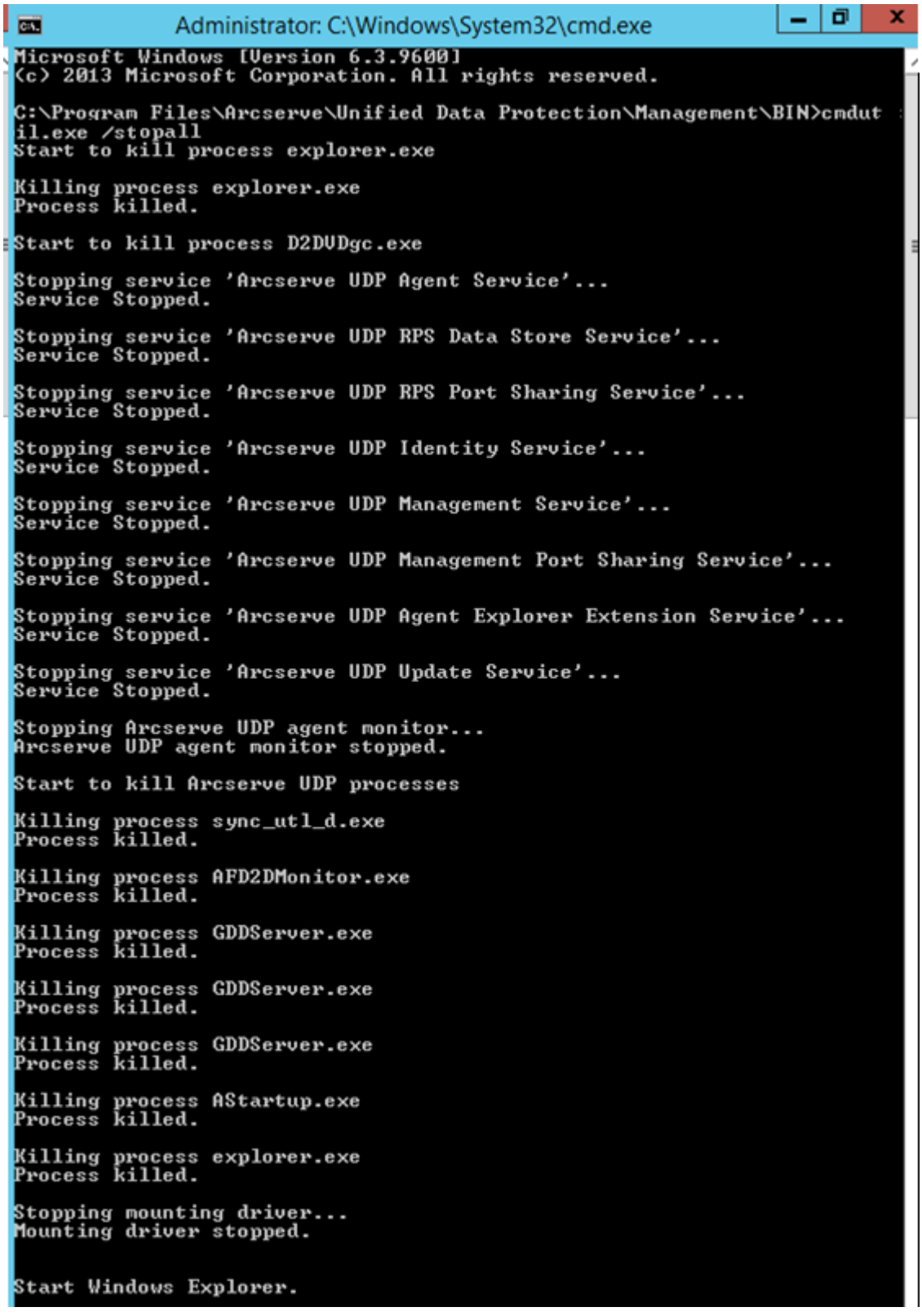


5. Now, follow these steps to copy the data on 8200 Appliance to 8400 Appliance and import the data on to 8400 Appliance:

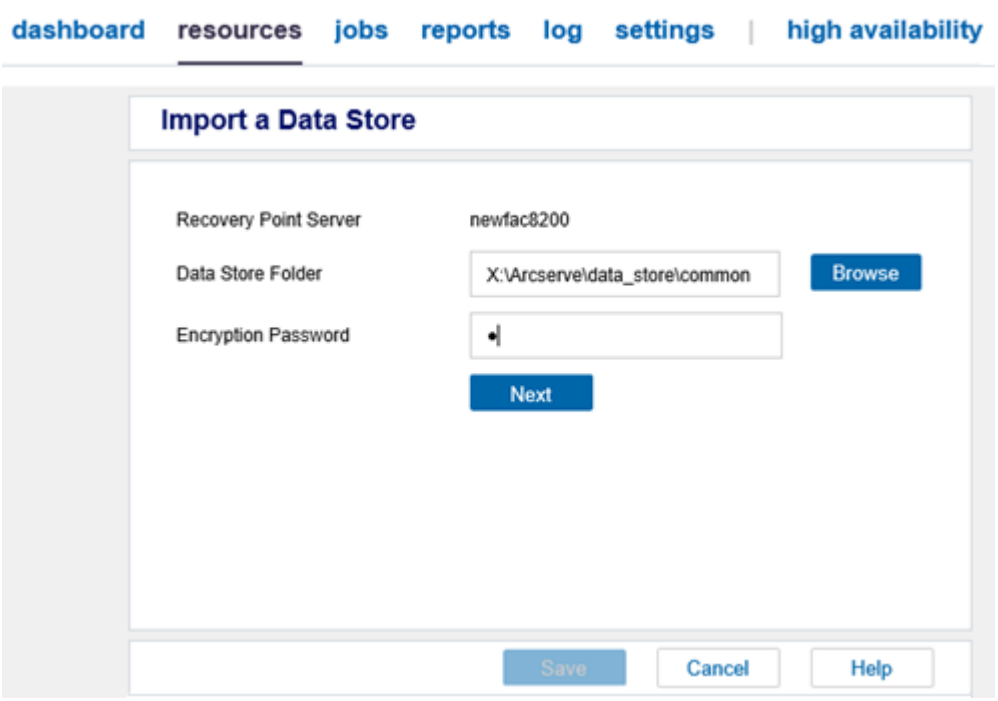
   a. Stop all the UDP services on Arcserve Appliance 8200 using the following command in the command line:

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

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



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


dashboard
resources
jobs
reports
log
settings
high availability
Import a Data Store
Recovery Point Server
newfac8200
Data Store Folder
X:\Arcserve\data_store\common
Browse
Encryption Password
Next
Save
Cancel
Help

Solution 2

Migrate Arcserve Appliance solution

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

Prerequisites:

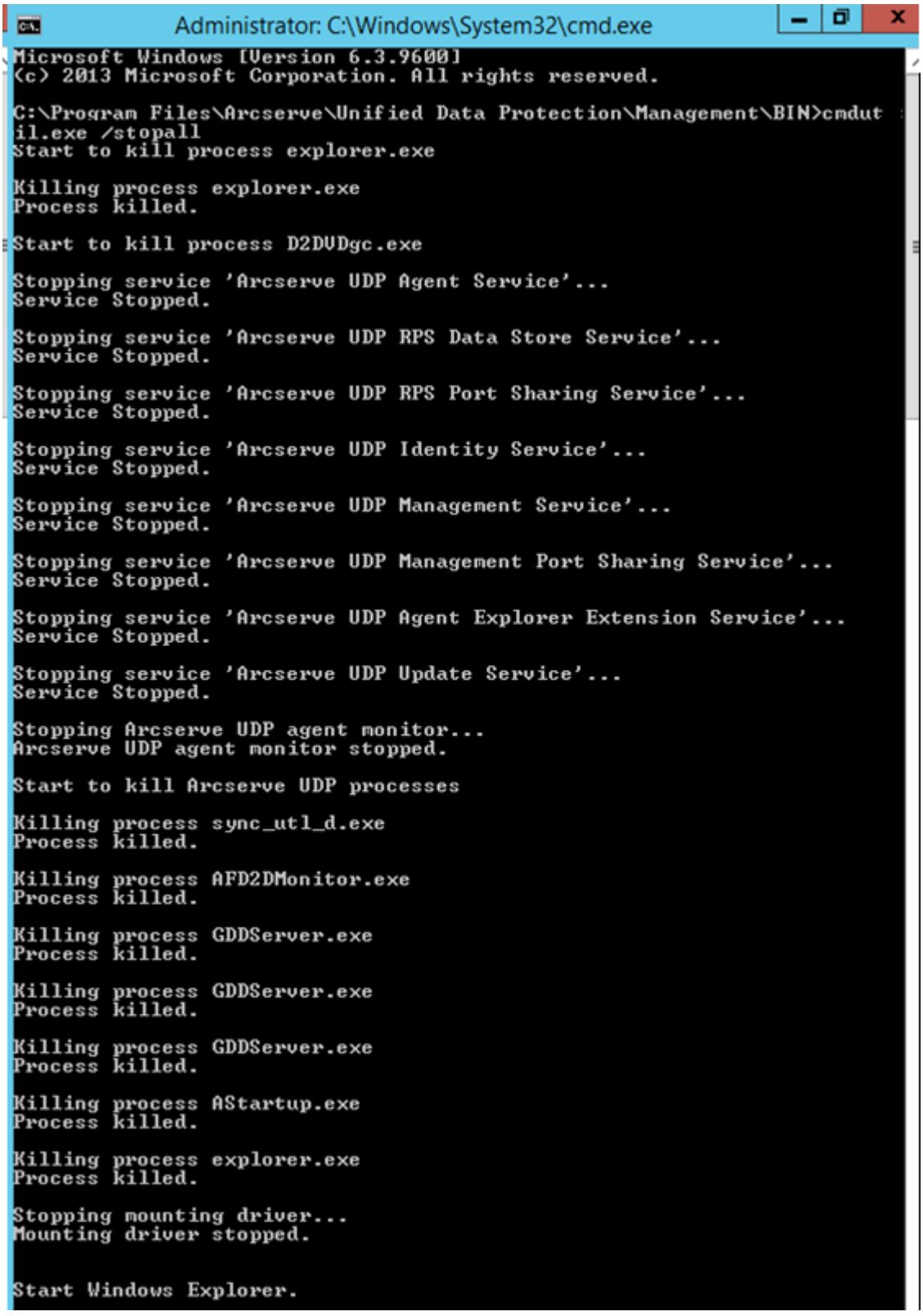
- On Arcserve Appliance 8200, ensure that no job runs.
- You have migrated the Arcserve UDP Console from Arcserve Appliance 8200 to 8400.

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

Follow these steps:

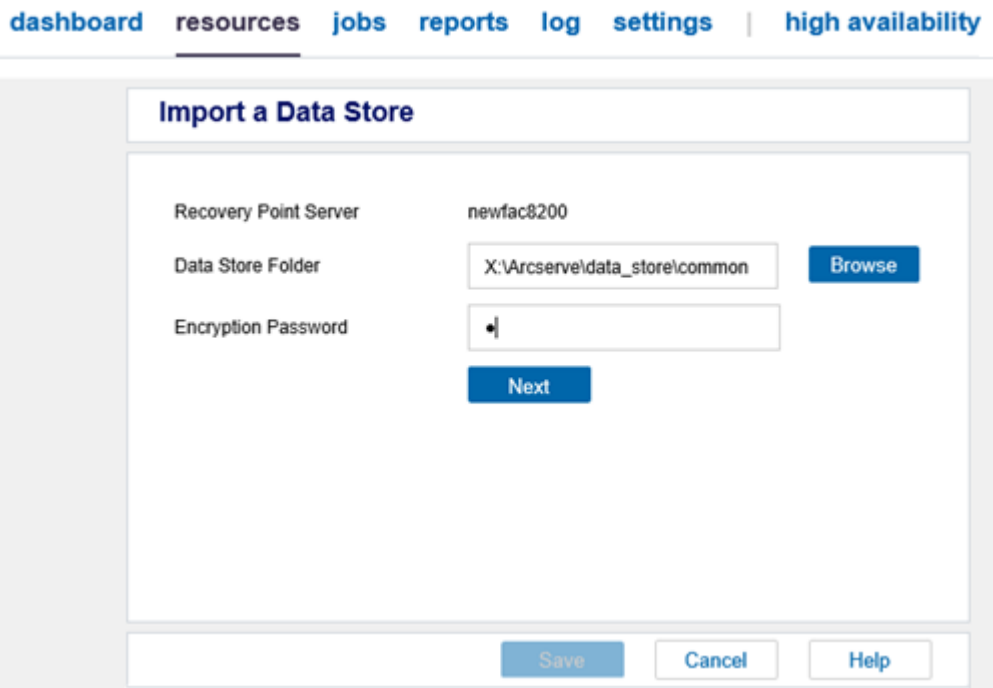
1. Stop all the Arcserve UDP services on Arcserve Appliance 8200 using the following command in the command line:

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



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

3. On 8400 Appliance, start all Arcserve UDP services and then import the data stores copied from 8200 Appliance.



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

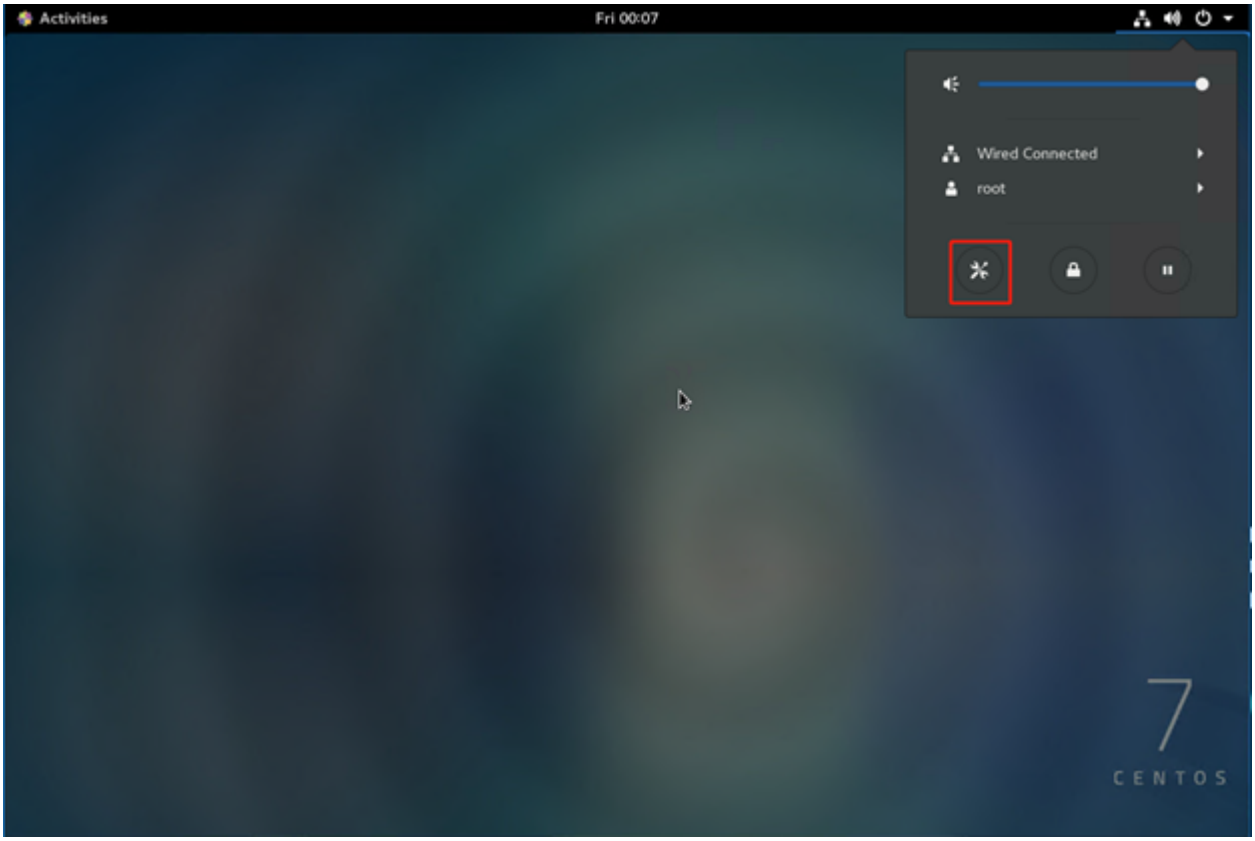
You have migrated the existing Arcserve Appliance to another fresh Arcserve Appliance successfully.

Modify the Input Source of Pre-installed Linux Backup Server

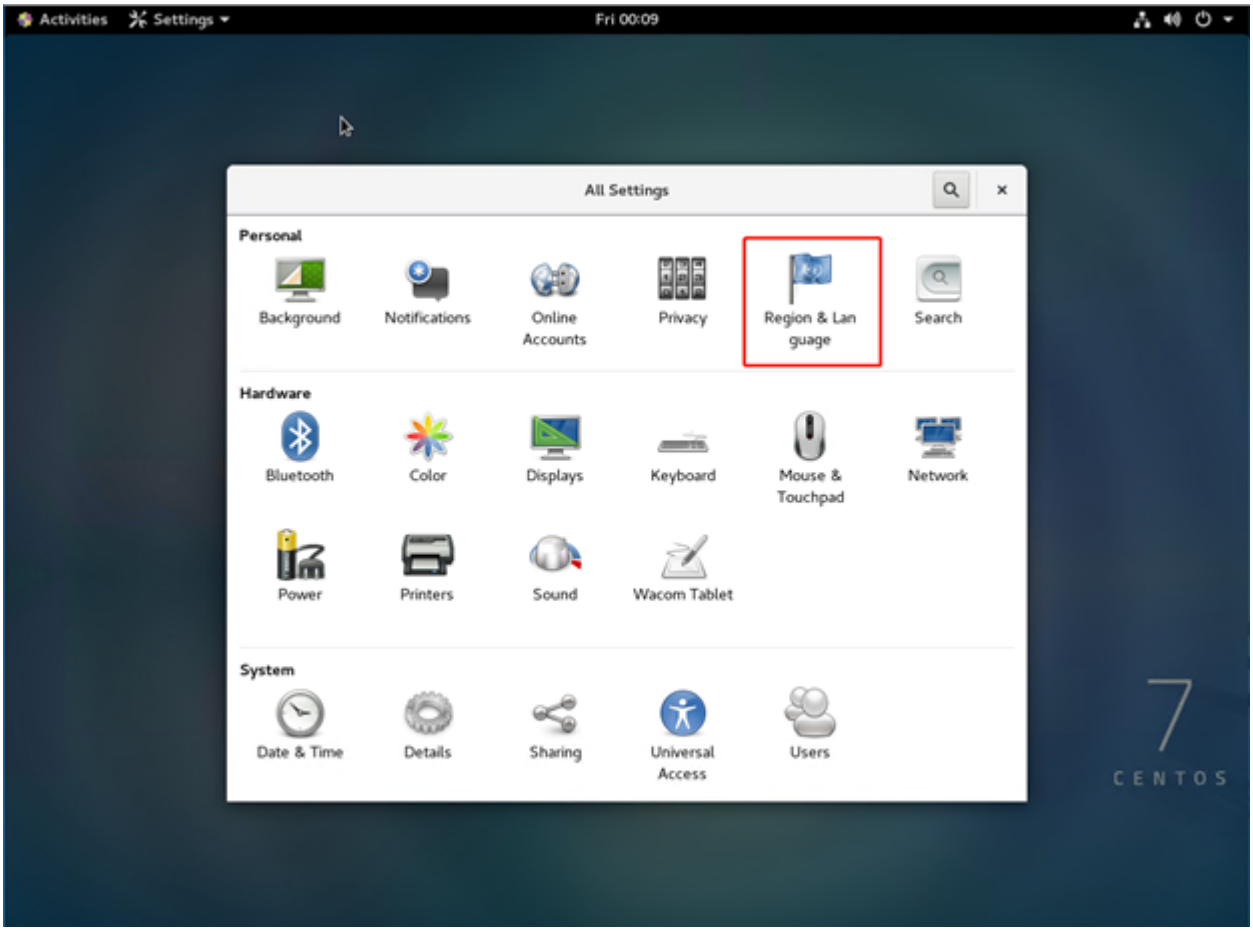
You can change the Keyboard of pre-installed Linux Backup Server.

Follow these steps:

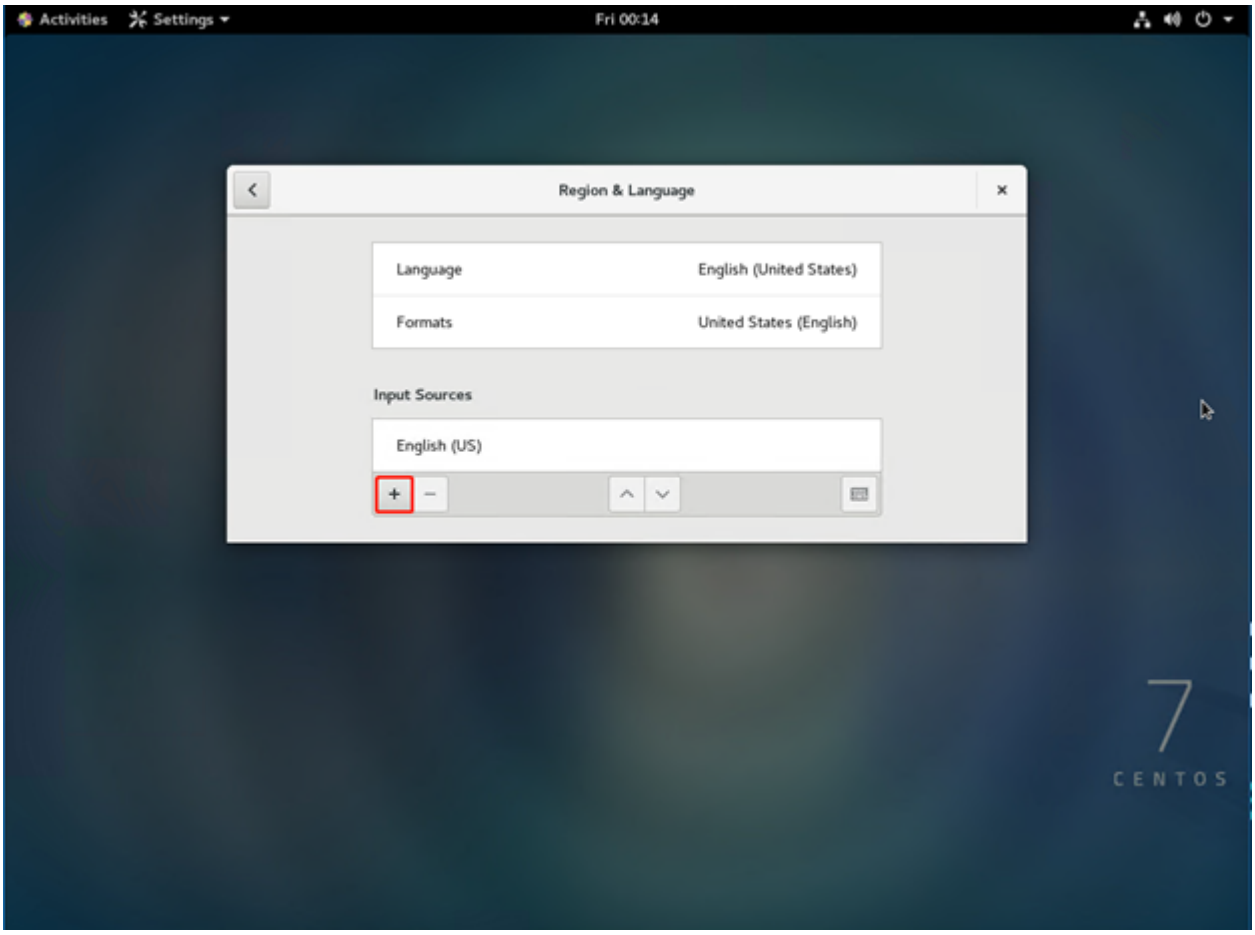
1. Log into Arcserve Appliance as administrator.
2. Click **Settings**.



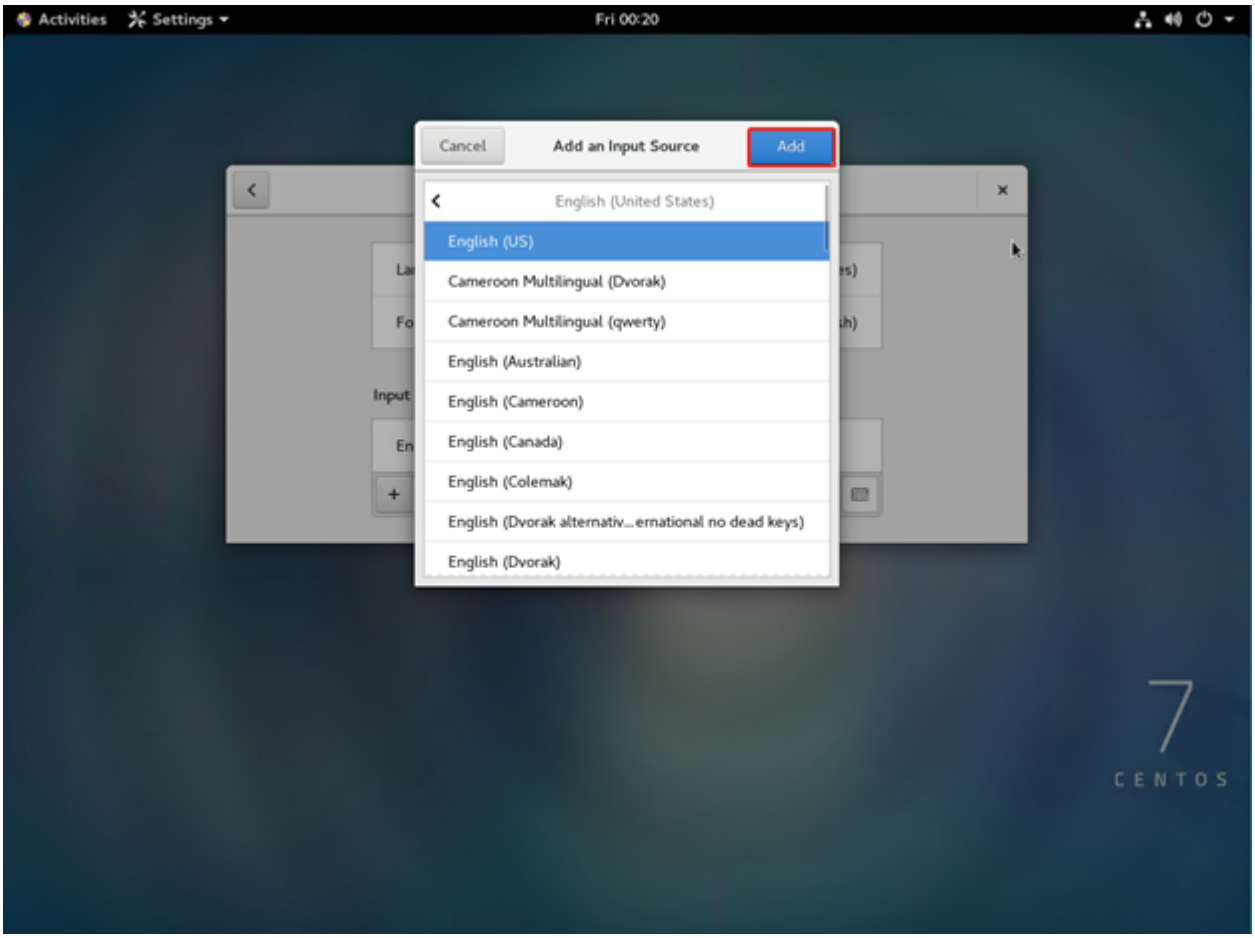
3. Click **Region & Language**.



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



5. Select the language and keyboard layout.



6. Click **Add**.

   Input source is successfully added.

Chapter 7: Monitoring the Appliance Server Remotely

You can monitor Arcserve Appliance remotely.

This section contains the following topics:

Working with IPMI 143

Working with Integrated Dell Remote Access Controller (iDRAC) 148

Working with IPMI

This section contains the following topics:

How to Change IPMI Password

Before changing the IPMI password, you need to access the BIOS setup screen to obtain the IP address.

Follow these steps:

1. Boot up your system.

   The Bootup screen appears.

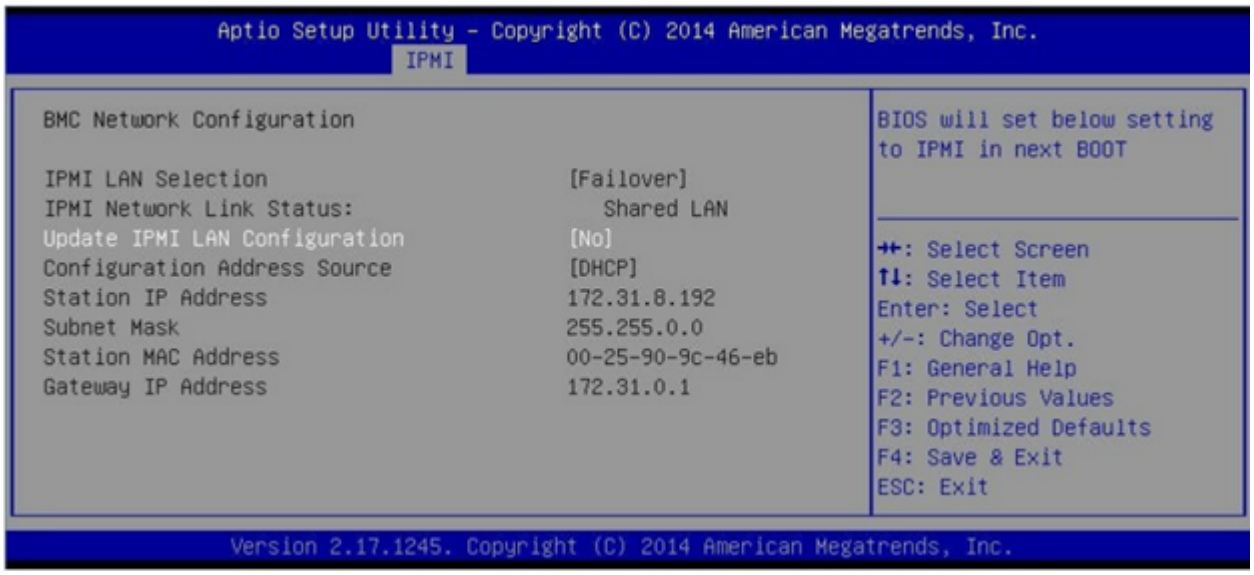
2. Press the **Delete** key.

   The BIOS setup screen is displayed.

   Note: To navigate, use the arrow keys and press **Enter**. To go back to the previous screens, press **Escape** key.

3. Select the **IPMI** tab at the top of the main BIOS screen.

   Note: By default, the configuration address source is set to DHCP.



4. Verify that the IP address is correct. You can connect to the IPMI interface using your web browser only if your Server is on the same network.
5. Note the **Station IP Address**.
6. Enter the Station IP address on your web browser.

   After you are connected to the remote Server via the IPMI port, the IPMI login screen is displayed.

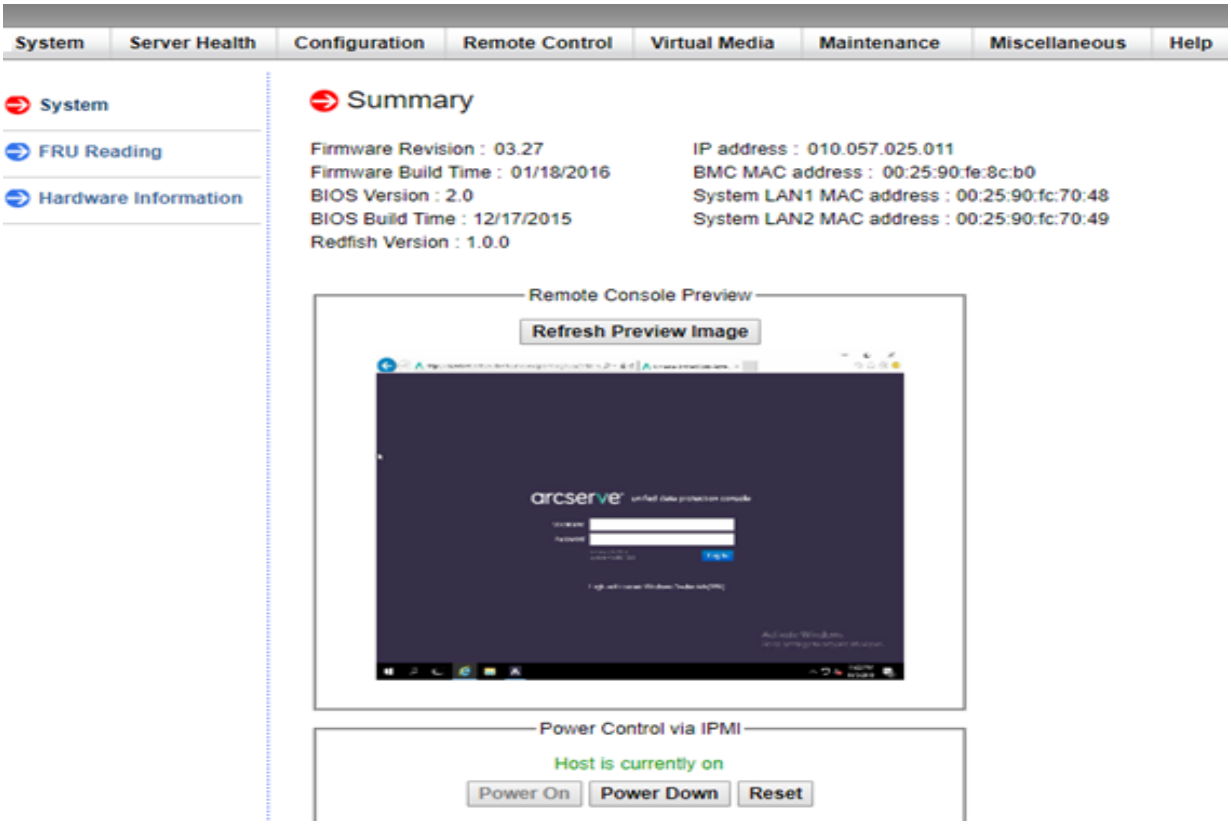
7. Enter your user name in the Username field.

   Default: ADMIN

8. Enter your password in the Password field.

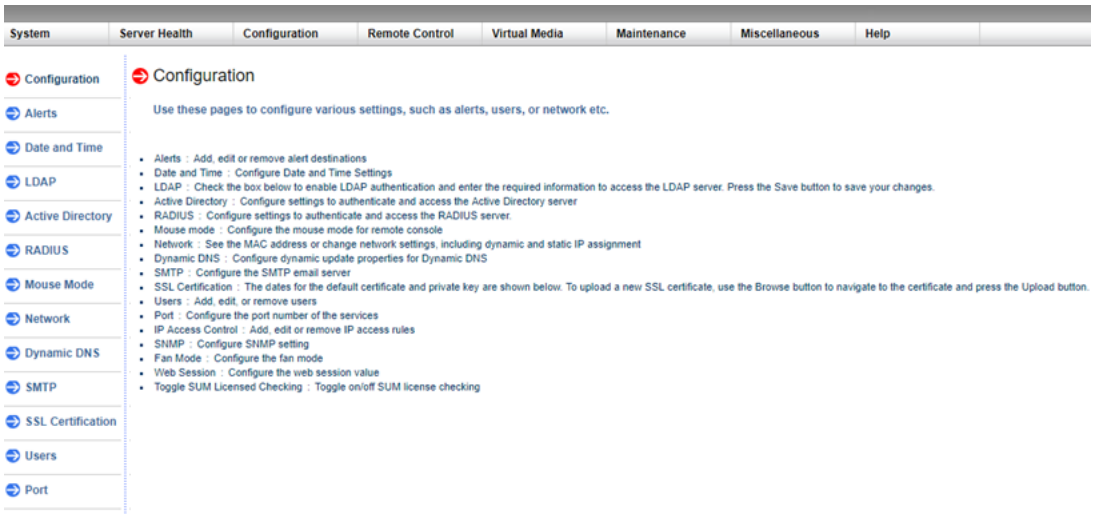
   Default: ARCADMIN

   The home page (IPMI main screen) is displayed.



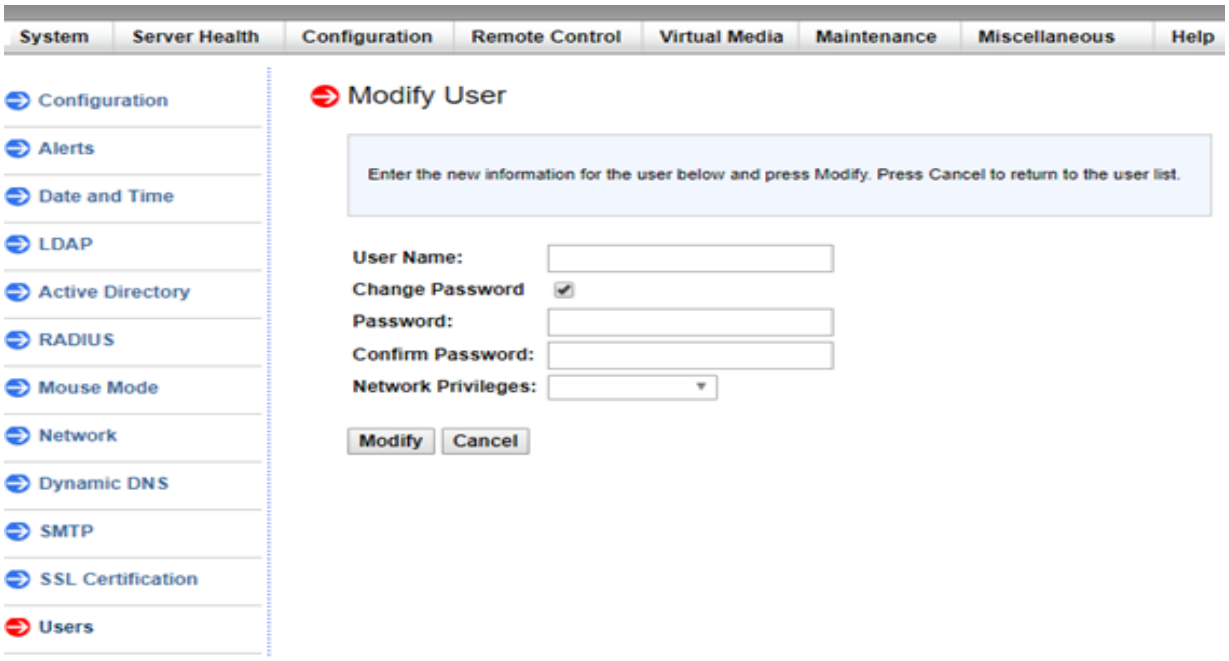
9. Click the **Configuration** option from the top bar.

   The Configuration screen is displayed.



10. Click the **Users** option in the Configuration sidebar.
11. Select the User: (ADMN) from the Users List.
12. Click **Modify User**.

    The Modify User screen is displayed.



13. Enter your user name (ADMIN).
14. Select the **Change Password** option.

    The password field is enabled.
15. Enter the new password and confirm.
16. Click **Modify** to save the changes.

    Your IPMI password is successfully changed.

How to Upgrade IPMI Firmware

Supermicro IPMI Utilities help you to upgrade the IPMI as per your organization requirement.

Follow these steps:

1. Login to **IPMI**, navigate to the **Maintenance** tab, and click **Firmware Update**.

   Firmware Update screen appears.

2. Click **Enter Update Mode**.

   Message from webpage pop-up window appears.

3. Click **OK**.

   BIOS & IPMI download screen appears.

4. Click the **.zip** file corresponding to the revision of IPMI model.

   The file downloads and Firmware Upload screen appears.

5. Extract files from the downloaded **.zip** file.
6. Click **Browse** on the Firmware Upload screen and select the **.bin** file from the extracted files.
7. Click **Upload Firmware**.

   Firmware Image uploads.

8. Click **Start Upgrade**.

   Firmware upgrade completes and reboots IPMI.

   You can view the upgraded Firmware version on the Summary screen.

Working with 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.

Restoring or Repairing the Arcserve Appliance

This section contains the following topics:

Apply Arcserve UDP Factory Reset Using Boot Option in 7000-8000 Series Appliance ..151

Apply Arcserve UDP Factory Reset Using Boot Option in 9012-9504DR Series Appliance ..154

Clear Configuration and Apply Appliance Factory Reset ..157

How to Replace Factory Reset Image Using Set Appliance Image Utility ..160

Remove and Replace a Hard Drive ..163

How to Perform Bare Metal Recovery (BMR) without Preserving Data ..166

How to Perform Bare Metal Recovery (BMR) and Preserving Data ..179

Apply Arcserve UDP Factory Reset Using Boot Option in 7000-8000 Series Appliance

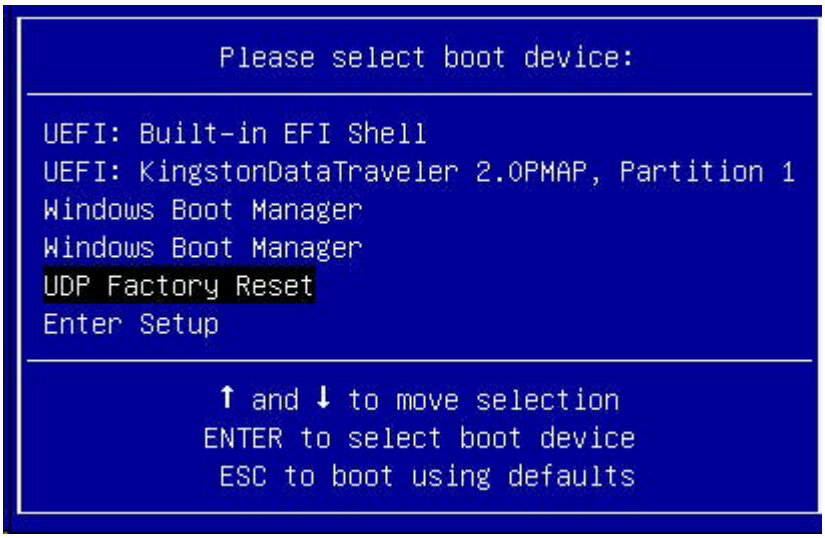
You can apply UDP factory reset from the Boot Menu of the Arcserve Appliance. Using UDP factory reset, you can return your Arcserve Appliance to clean and non-configured status.

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

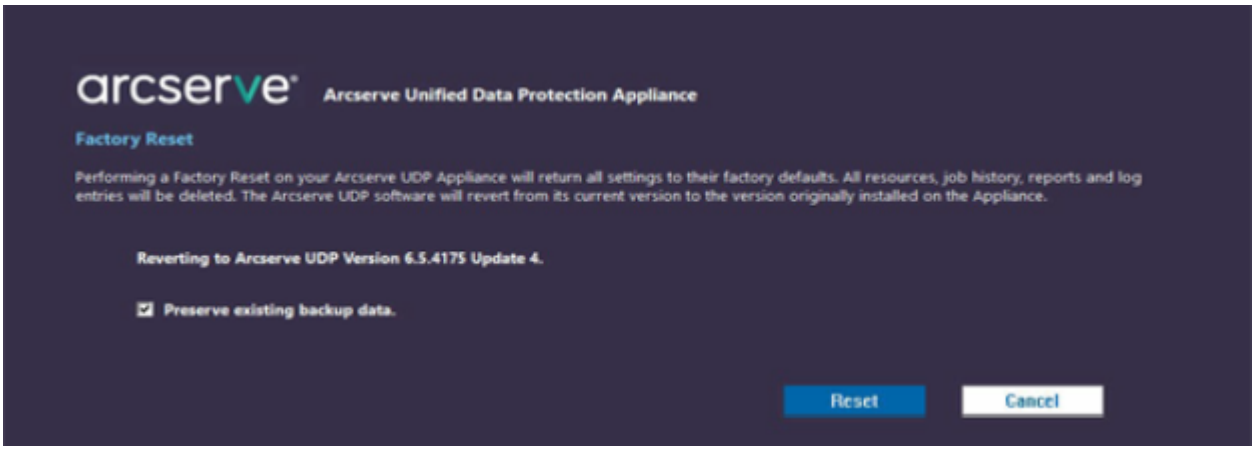
Follow these steps:

1. Press F11 to invoke Boot Menu.

2. Select the boot option UDP Factory Reset.



A page about factory reset is displayed.

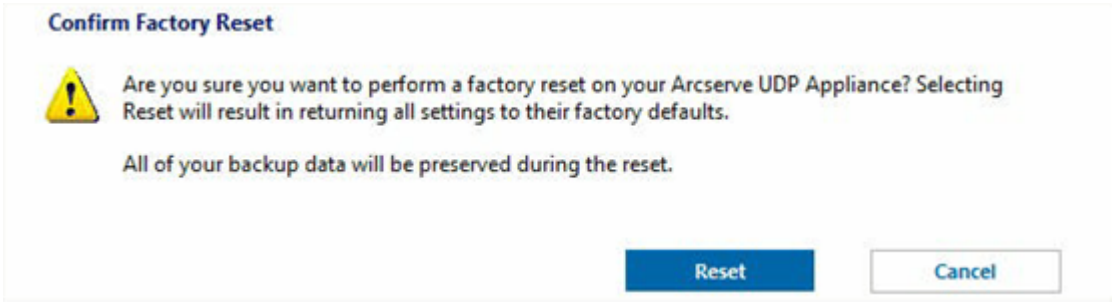


Notes:

- 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 remains 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.

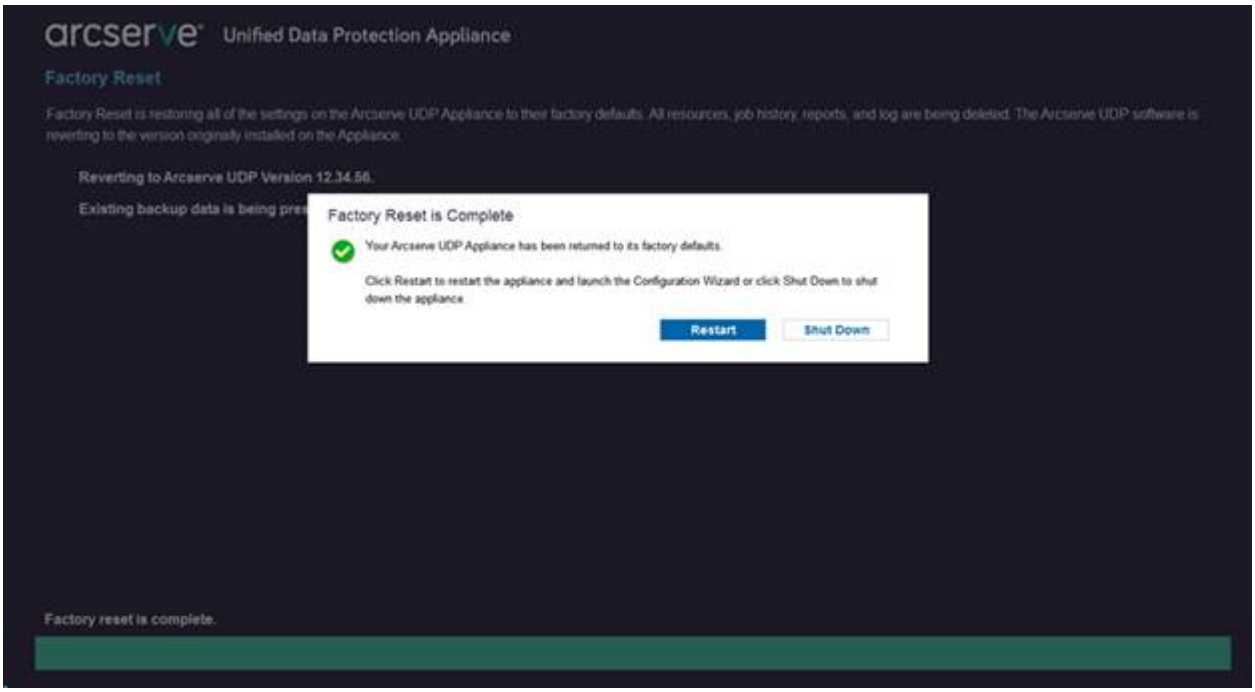
3. Click **Reset**.

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.


arcserve Unified Data Protection Appliance
Factory Reset
Factory Reset is restoring all of the settings on the Arcserve UDP Appliance to their factory defaults. All resources, job history, reports, and log are being deleted. The Arcserve UDP software is reverting to the version originally installed on the Appliance.
Reverting to Arcserve UDP Version 12.34.56.
Existing backup data is being pres
Factory Reset is Complete
Your Arcserve UDP Appliance has been returned to its factory defaults.
Click Restart to restart the appliance and launch the Configuration Wizard or click Shut Down to shut down the appliance.
Restart
Shut Down
Factory reset is complete.

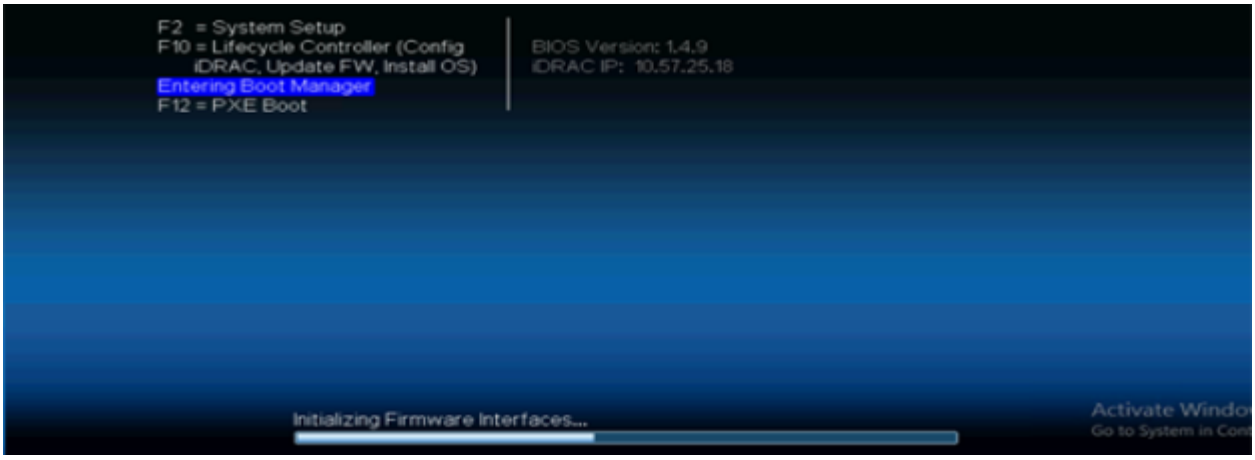
Apply Arcserve UDP Factory Reset Using Boot Option in 9012-9504DR Series Appliance

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.

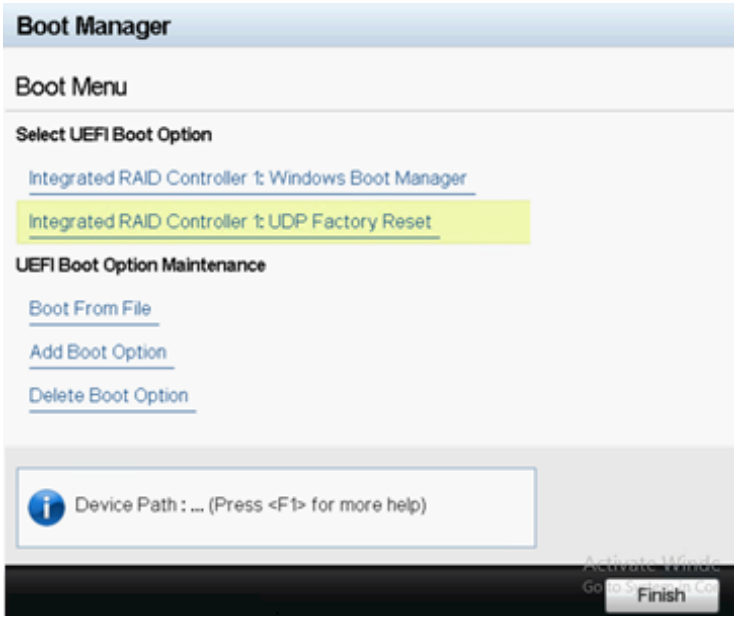
Note: You can also select the Preserve the backup data option while running UDP factory reset.

Follow these steps:

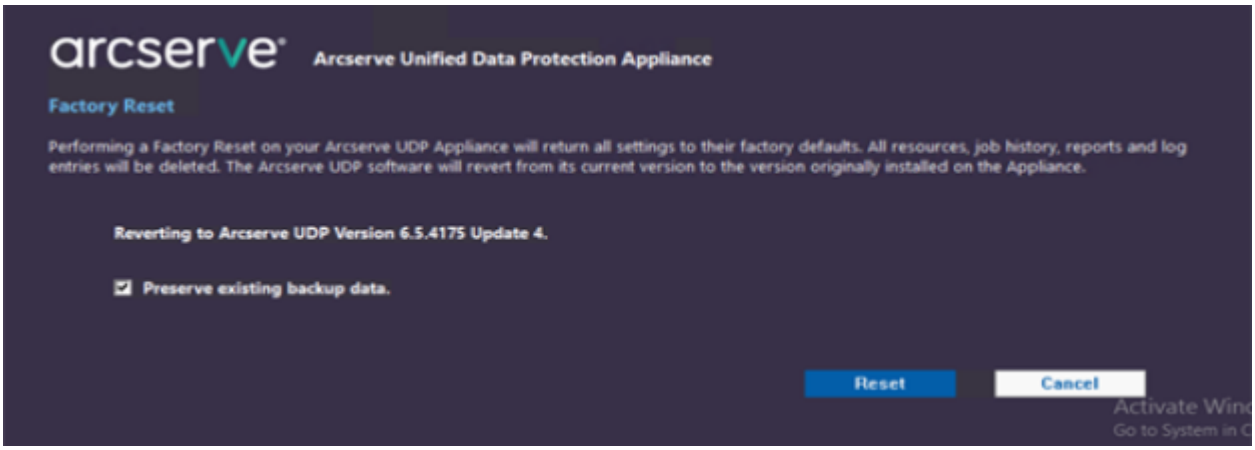
1. Press F11 on the keyboard to invoke Boot Menu.



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



A page about factory reset is displayed.

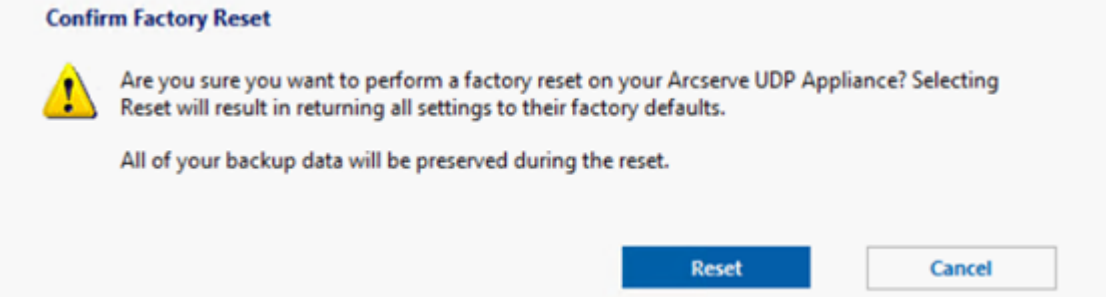


Notes:

- 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.

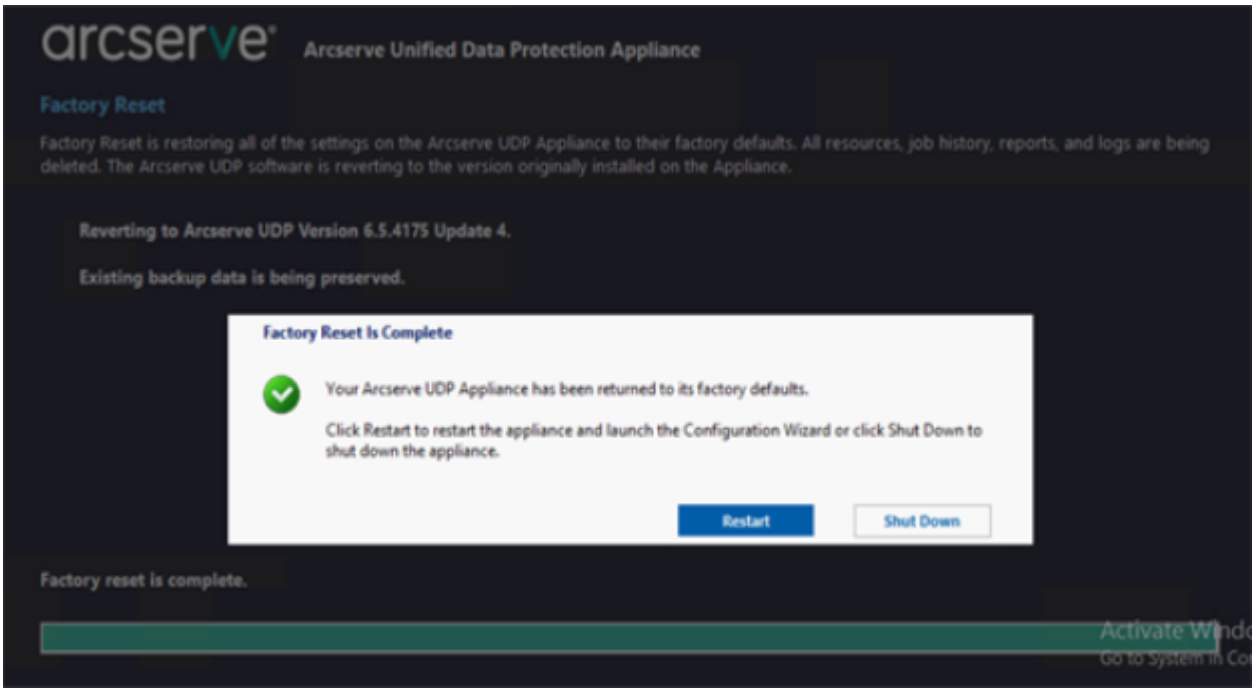
3. Click **Reset**.

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.

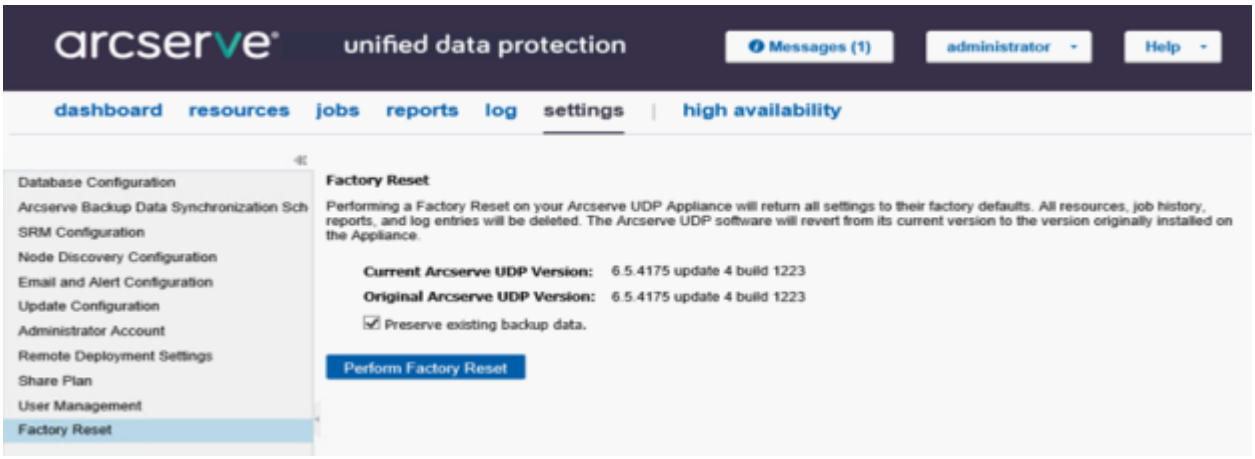

arcserve
Arcserve Unified Data Protection Appliance
Factory Reset
Factory Reset is restoring all of the settings on the Arcserve UDP Appliance to their factory defaults. All resources, job history, reports, and logs are being deleted. The Arcserve UDP software is reverting to the version originally installed on the Appliance.
Reverting to Arcserve UDP Version 6.5.4175 Update 4.
Existing backup data is being preserved.
Factory Reset Is Complete
Your Arcserve UDP Appliance has been returned to its factory defaults.
Click Restart to restart the appliance and launch the Configuration Wizard or click Shut Down to shut down the appliance.
Restart
Shut Down
Factory reset is complete.

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.

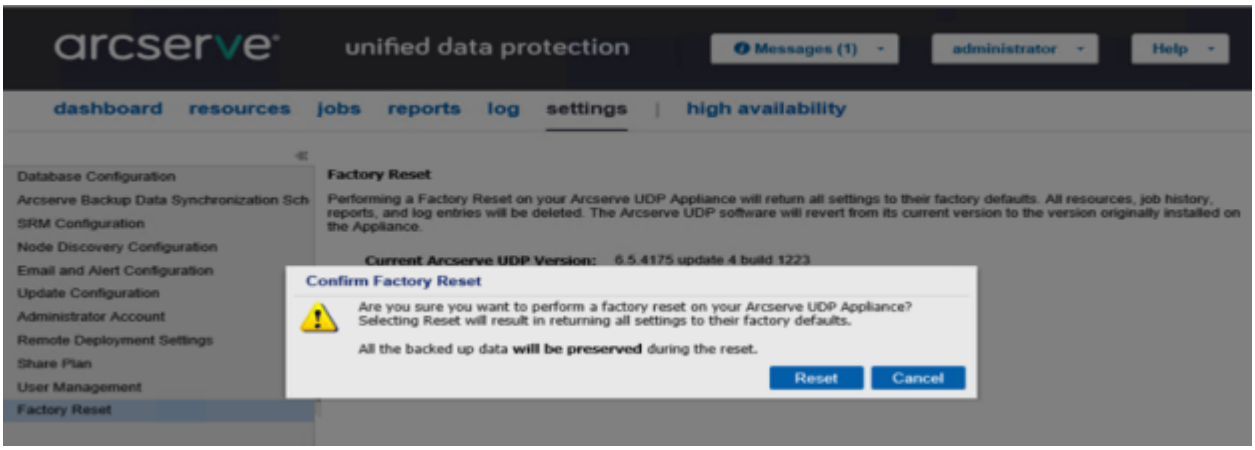
   Notes:

   Arcserve UDP provides the **Preserve existing backup data** option to help you preserve the existing data store.

   - 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.

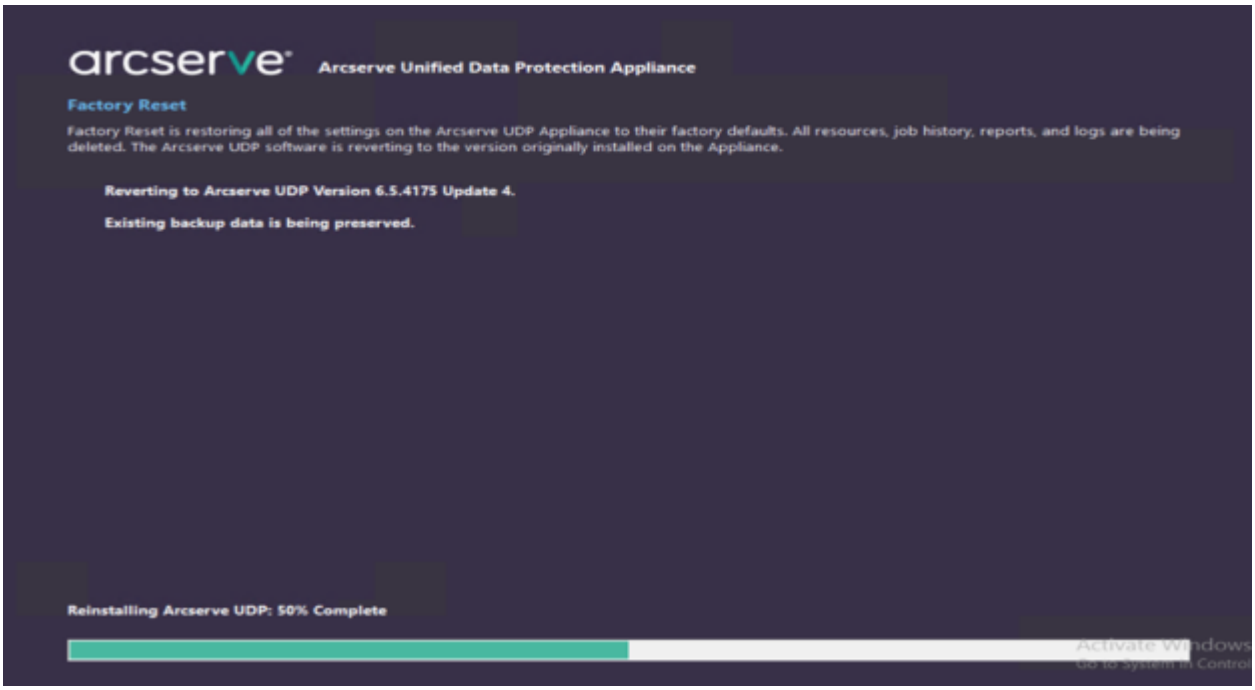
2. Click **Perform Factory Reset**.

   A confirmation dialog is displayed.



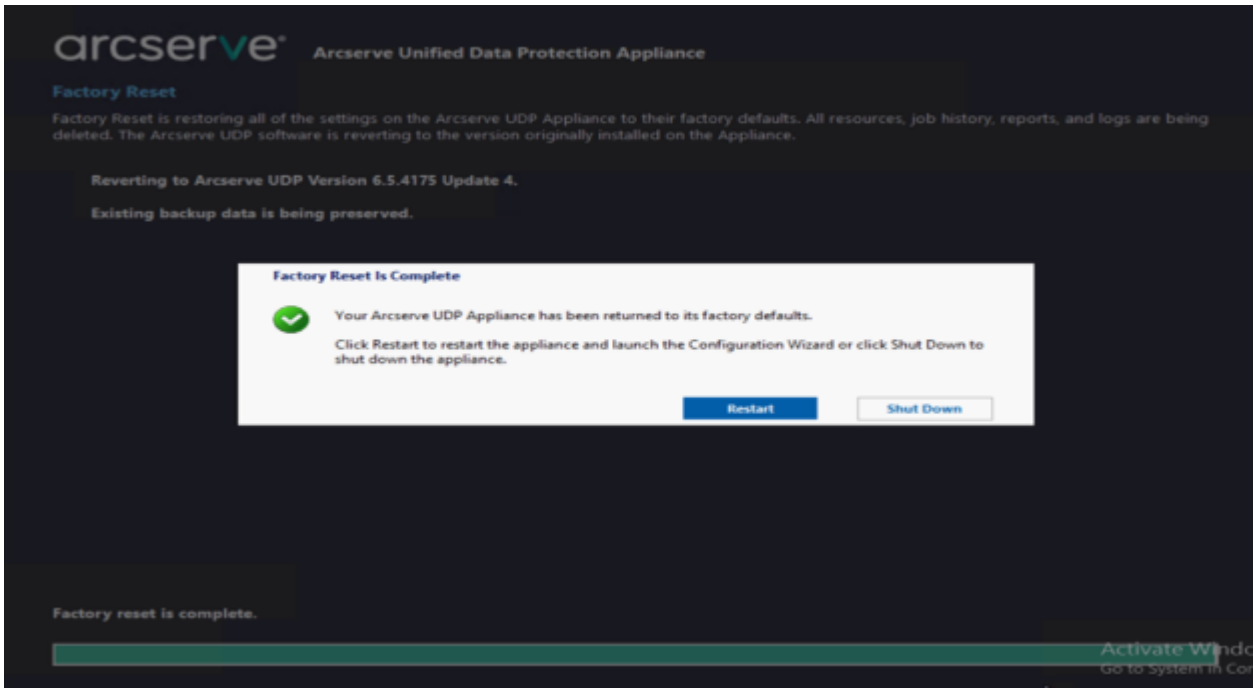
3. From the confirmation dialog, click **Reset** to launch the factory reset.

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



   Completion of factory reset displays a confirmation dialog.

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



How to Replace Factory Reset Image Using Set Appliance Image Utility

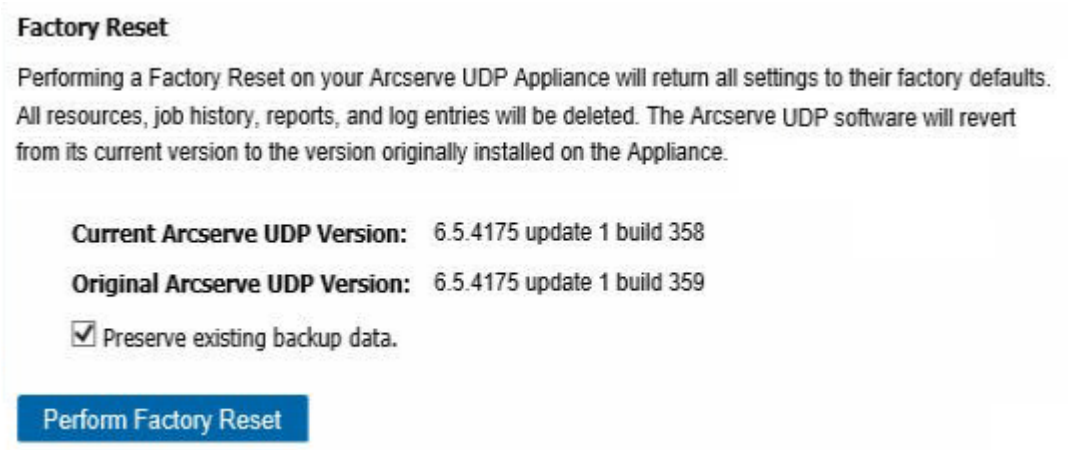
Set Appliance Image Utility tool helps you to replace the original Appliance image in current system with desired Appliance image of Arcserve Appliance available versions.

Note: Replacing the Arcserve Appliance image with a different Windows operating system version is not supported. For example, if you are using Arcserve Appliance v6.5 Update 1 that is running on Windows 2012 R2 and want to replace Arcserve Appliance v6.5 Update 1 with Arcserve v6.5 Update 2, you can apply Arcserve Appliance v6.5 Update2 image that is running on Windows 2012 R2 only. The same way, if you are using Arcserve Appliance v6.5 Update 3 that is running on Windows 2016 and want to replace Arcserve Appliance v6.5 Update 3 with Arcserve v6.5 Update 4, you can apply Arcserve Appliance v6.5 Update 4 image that is running on Windows 2016 only.

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

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

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



Note: The above screen refers to Arcserve Appliance v6.5 Update1 GUI and may vary from other release versions of Arcserve Appliance.

Example scenario to replace factory reset image for UDP v6 Update 1 with factory reset image for UDP v6.5 Update 1

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

How to Use Set Appliance Image Utility to revert from Arcserve Appliance v6 Update 1 to Arcserve Appliance v6.5 Update 1

If the installed Arcserve UDP release version on Appliance is Arcserve UDP v6 Update 1, then you can upgrade the Appliance to Arcserve UDP v6.5 Update 1.

Follow these steps:

1. Download the Appliance image of Arcserve Appliance v6.5 Update 1, and execute the Set Appliance Image Utility. Perform the following steps to use set Appliance Image Utility:
   a. To download the 6.5 factory reset image, contact Arcserve support.
   b. Open the Windows command line and run the following command:

      C:\Program files\Arcserve\Unified Data Protection\Management\bin\Appliance\SetImage.exe –applianceimage <Full-path of the appliance image just downloaded>

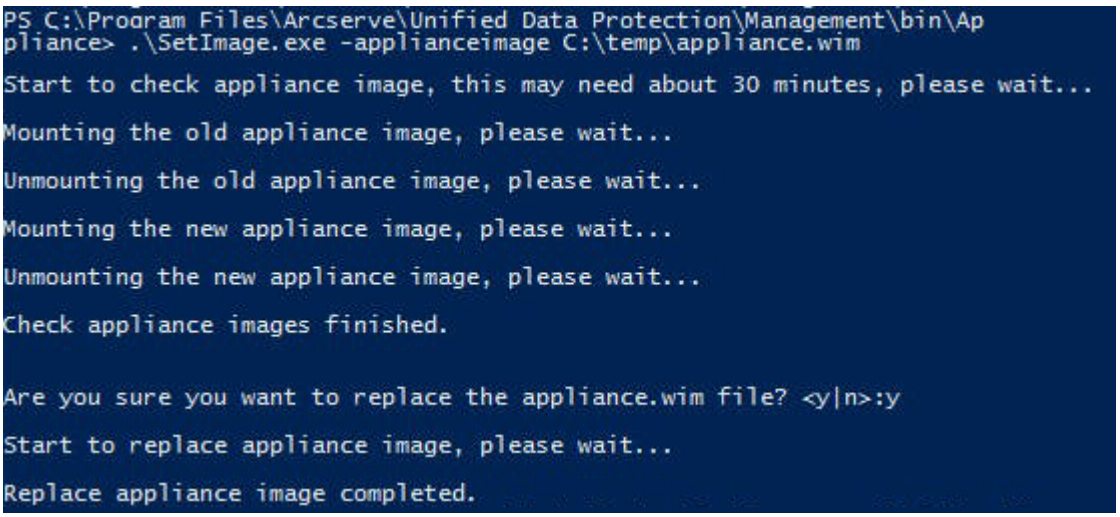
      After *checking appliance images finished* step is complete, you can view the following query:

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

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

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

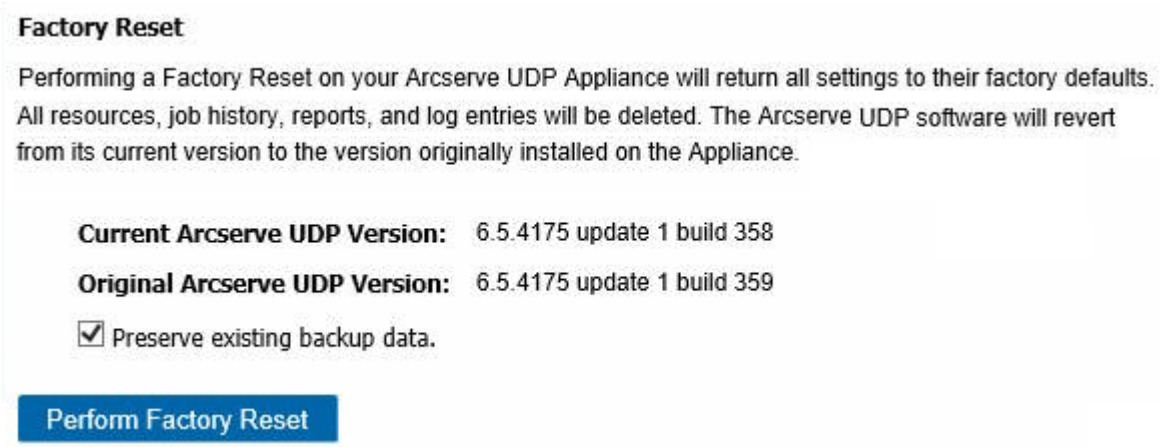
      Replace appliance image completed.



2. Perform the following steps to revert to Update 1 version of Appliance:

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

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



The *Original Arcserve UDP Version* changes to Arcserve Appliance v6.5 Update 1.

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

b. Click **Perform Factory Reset** to revert from current version of Appliance to the new Arcserve Appliance v6.5 Update 1 version.

For more information about Factory Reset, refer the link.

Remove and Replace a Hard Drive

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

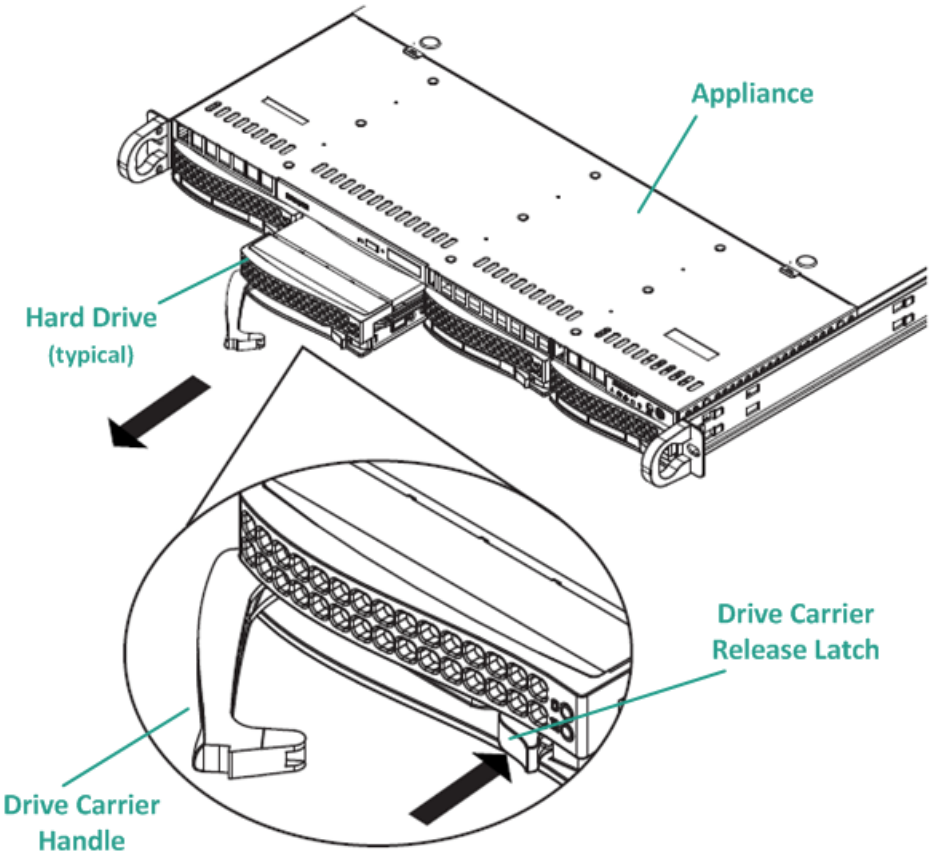
The Arcserve Appliance contains four hard drive carriers which are labeled 0, 1, 2 and 3 from left to right. If you replace more than one hard drive at a time, you should label the replacement hard drives so that you know which drive is placed into each drive carrier. You should also label the hard drives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

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

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

Follow these steps:

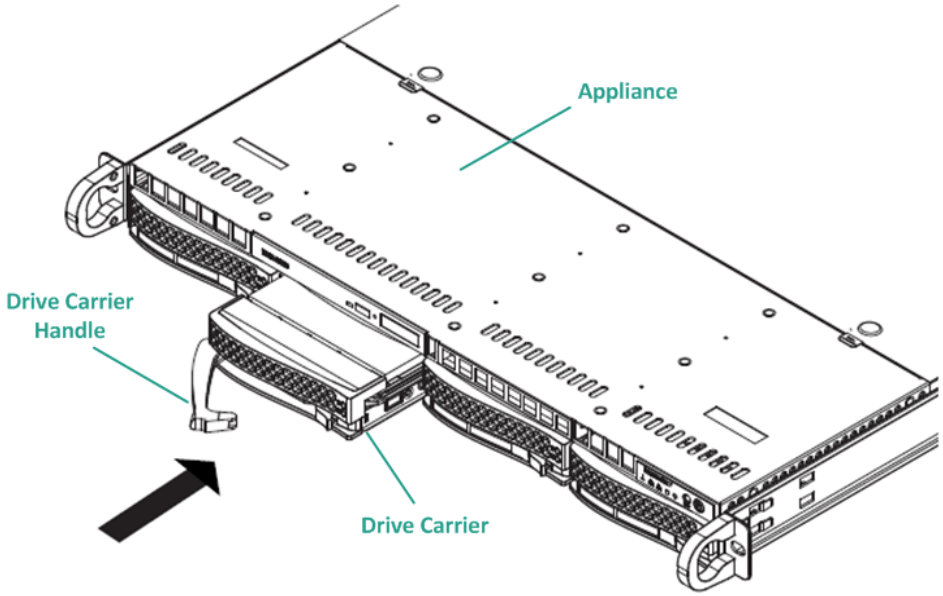
1. To gain access to the drive holders, you first need to remove the faceplate:
    a. Unlock the faceplate lock.
    b. Press the release knob to retract the faceplate pins.
    c. Carefully remove the faceplate (using two hands).
2. Press the release latch on the drive carrier. This extends the drive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



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

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

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



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

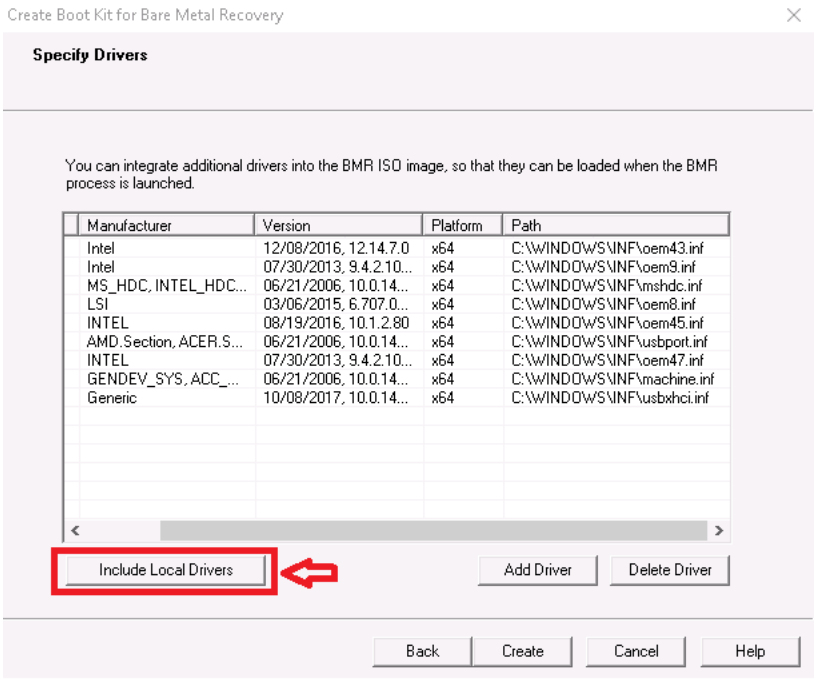
How to Perform Bare Metal Recovery (BMR) without Preserving Data

On the 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.

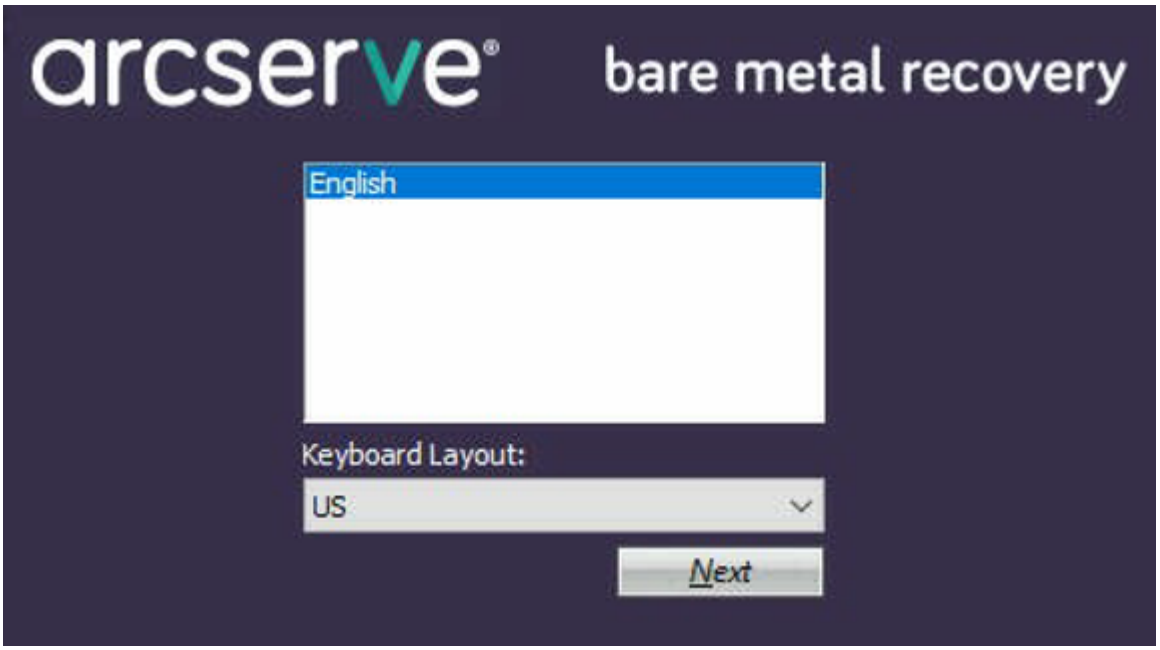
   Note: You need to include the local drivers for the ISO image. To include the local drivers, select the **Include Local Drivers** option in the **Create Boot Kit for Bare Metal Recovery** window. For more information on how to create boot kit, refer link.



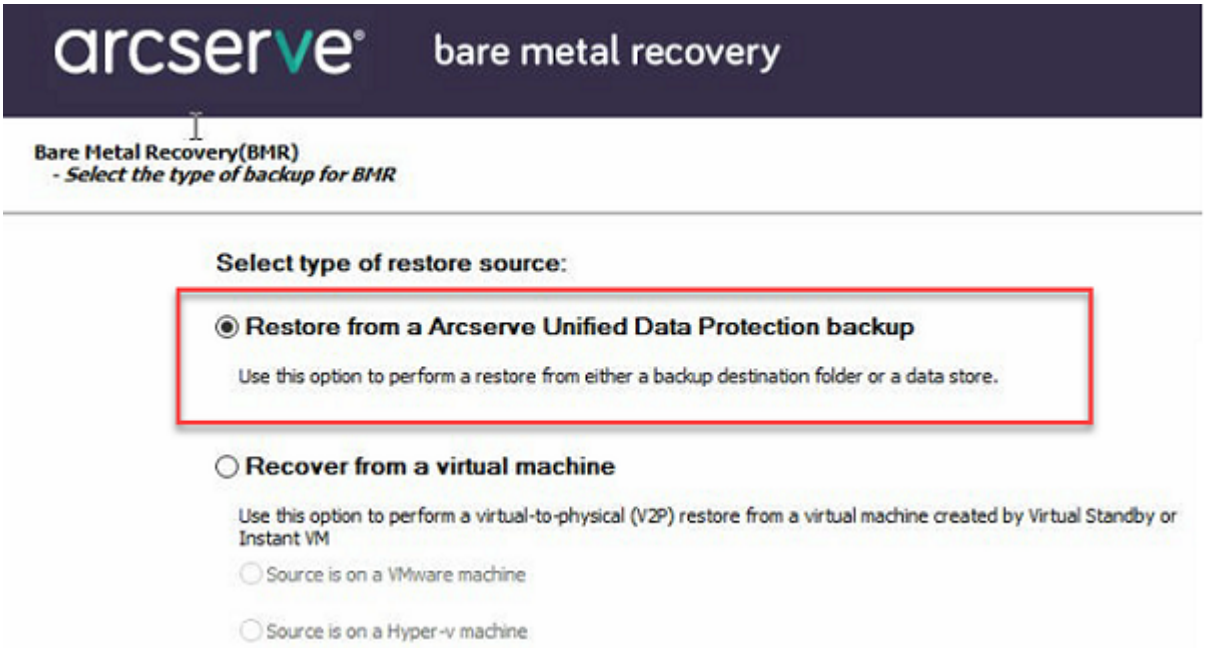
2. Boot the Arcserve Appliance using BMR ISO image or USB Stick.

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

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

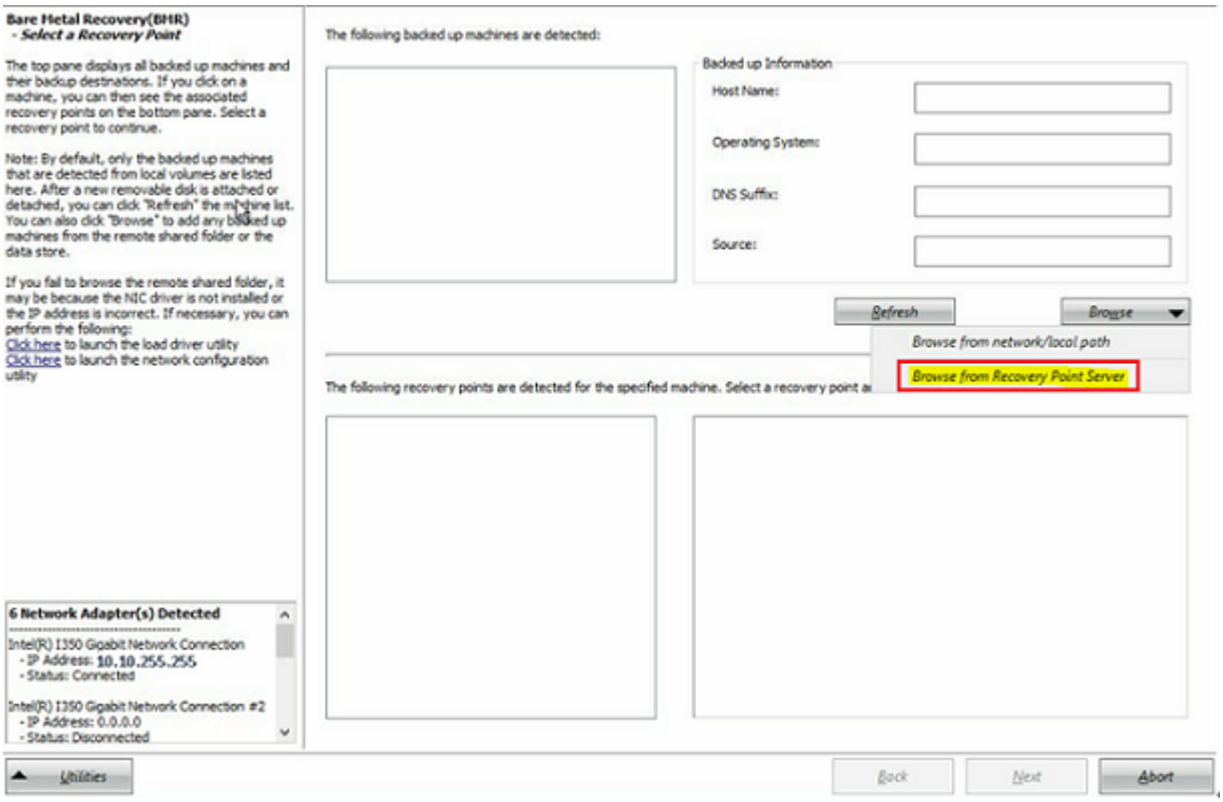


4. Select the **Restore from a Arcserve Unified Data Protection backup** option and click **Next**.



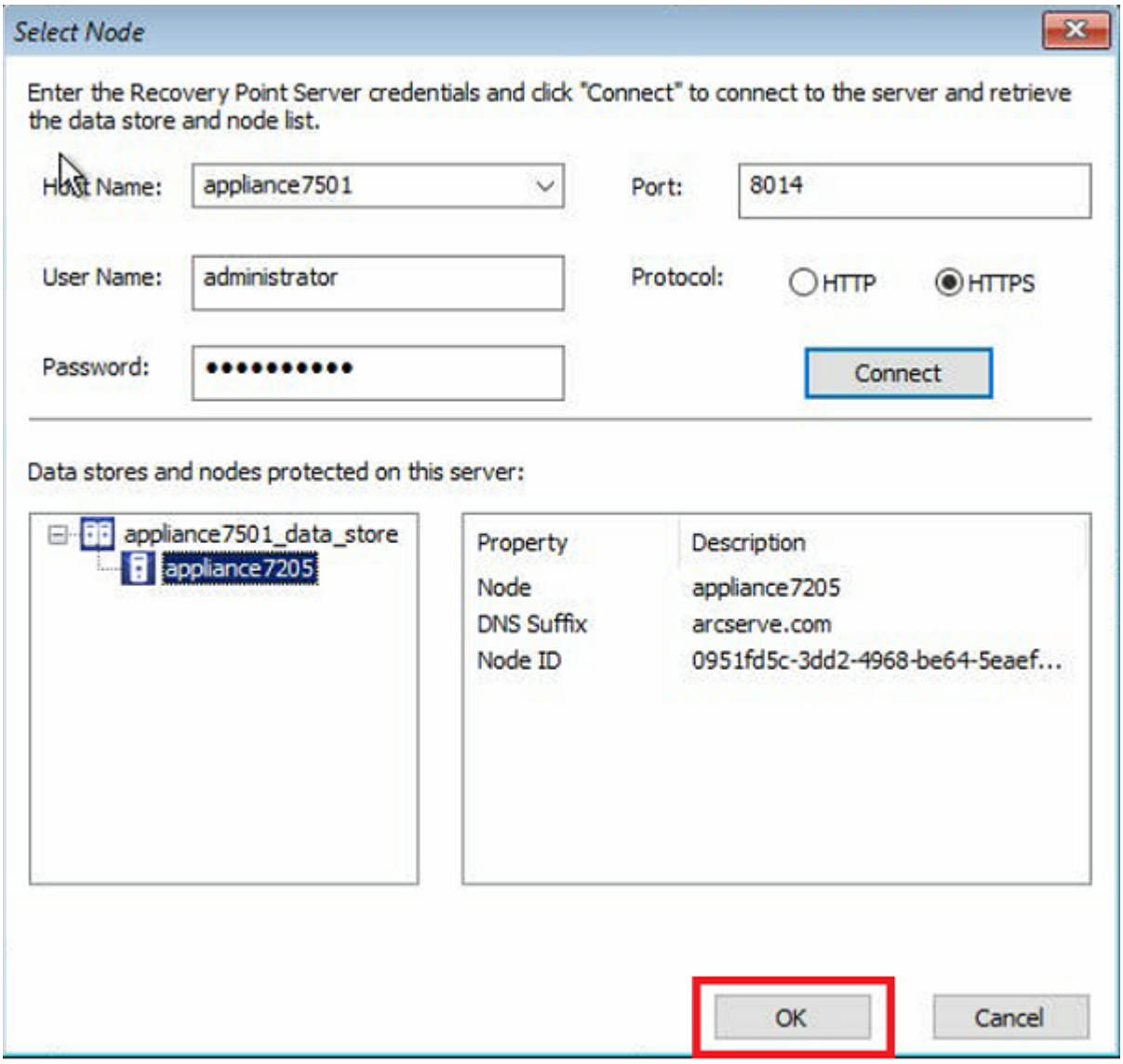
The **Select a Recovery Point wizard** window appears.

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



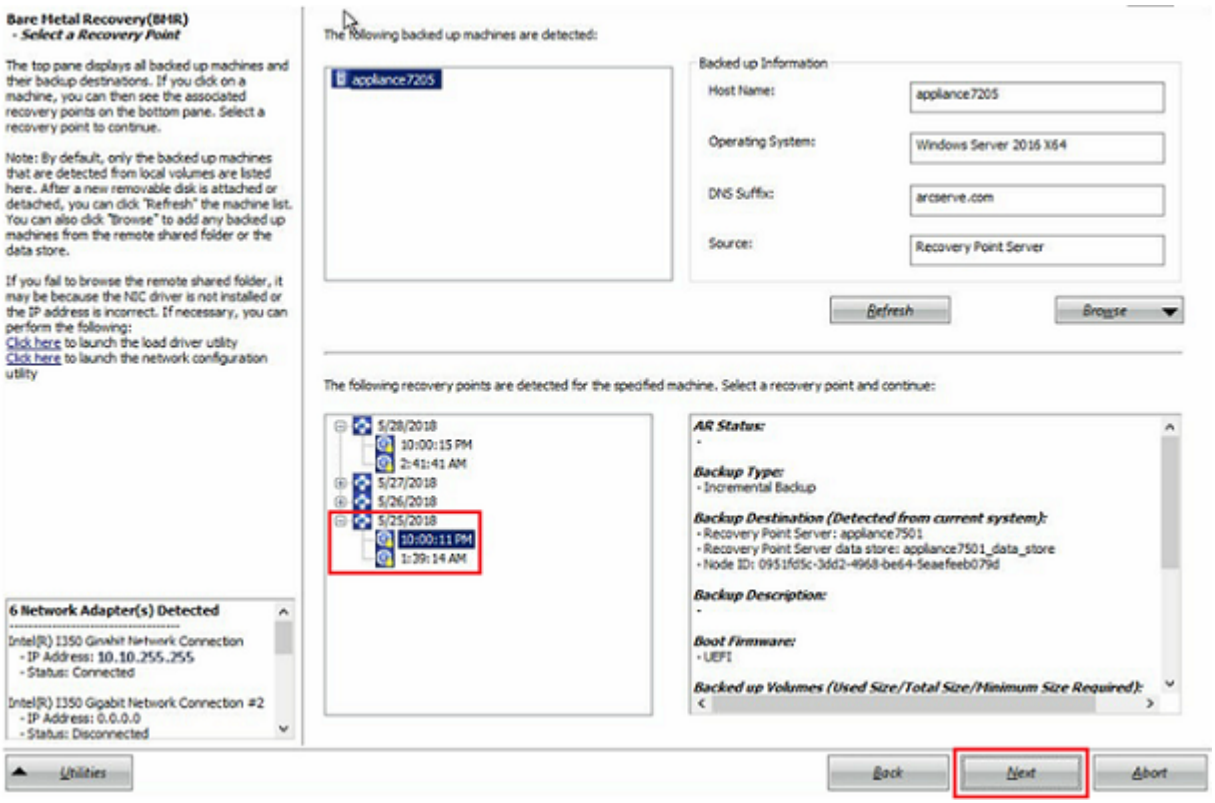
The **Select Node** window appears.

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.

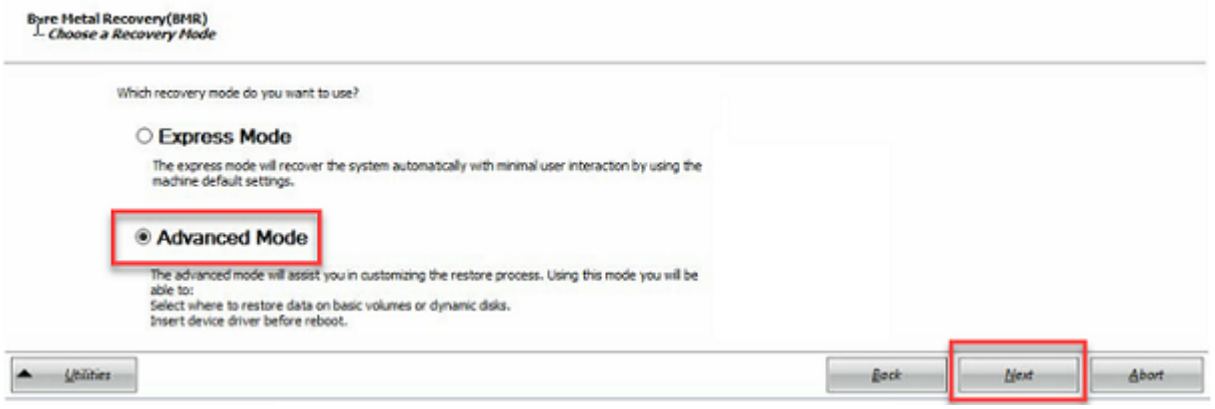
9. Select the recovery point to restore and click **Next**.



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

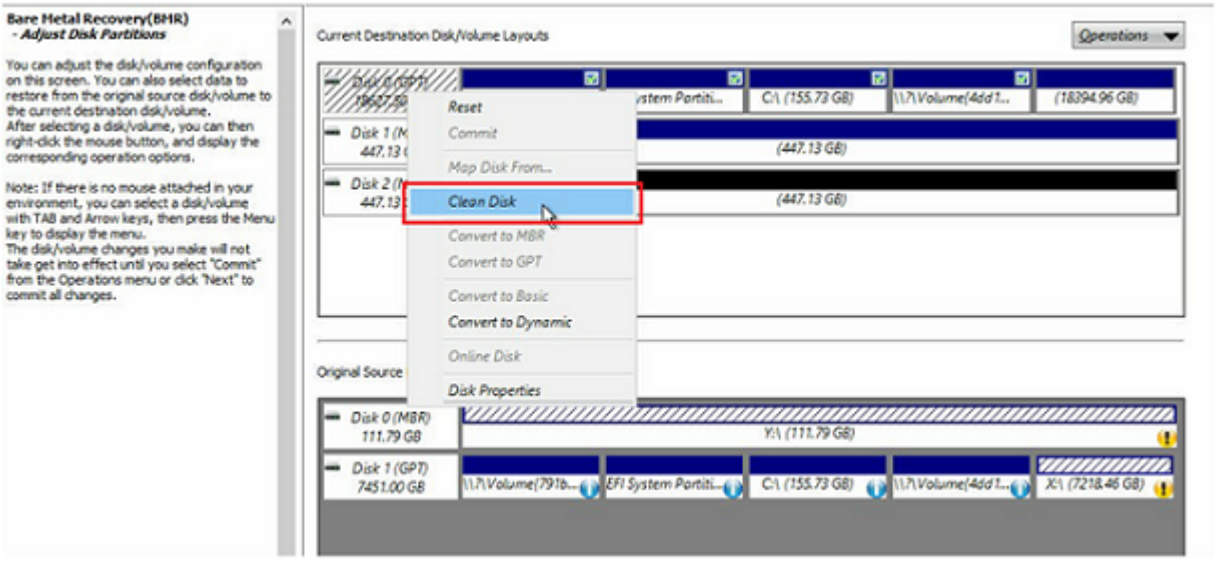
The **Bare Metal Recovery(BMR)- Choose a Recovery Mode** dialog appears.

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

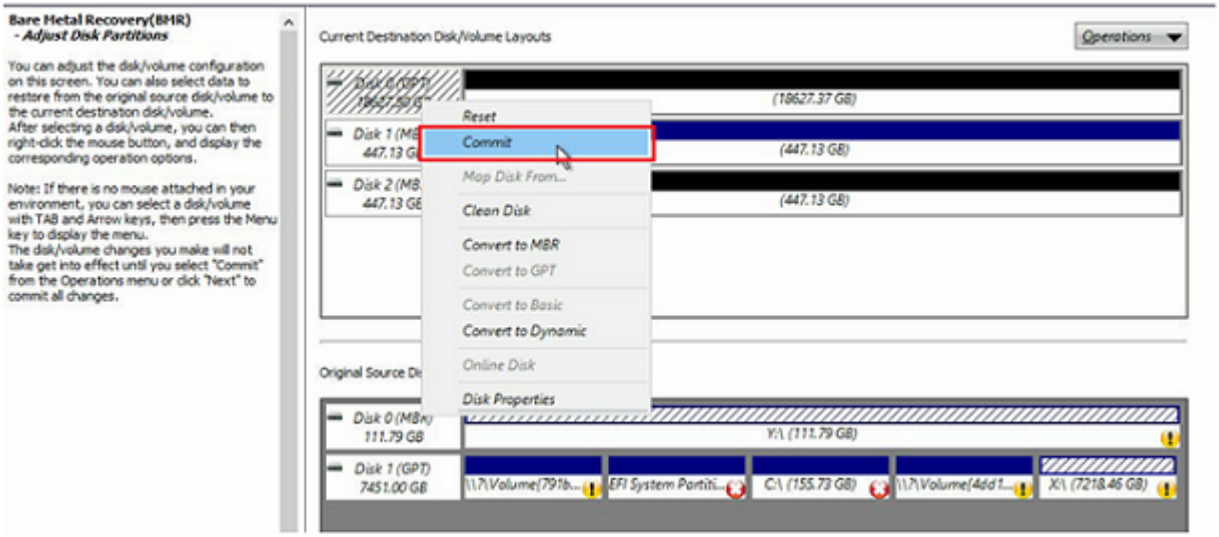


The **Bare Metal Recovery(BMR)- Adjust Disk Partitions** dialog appears.

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

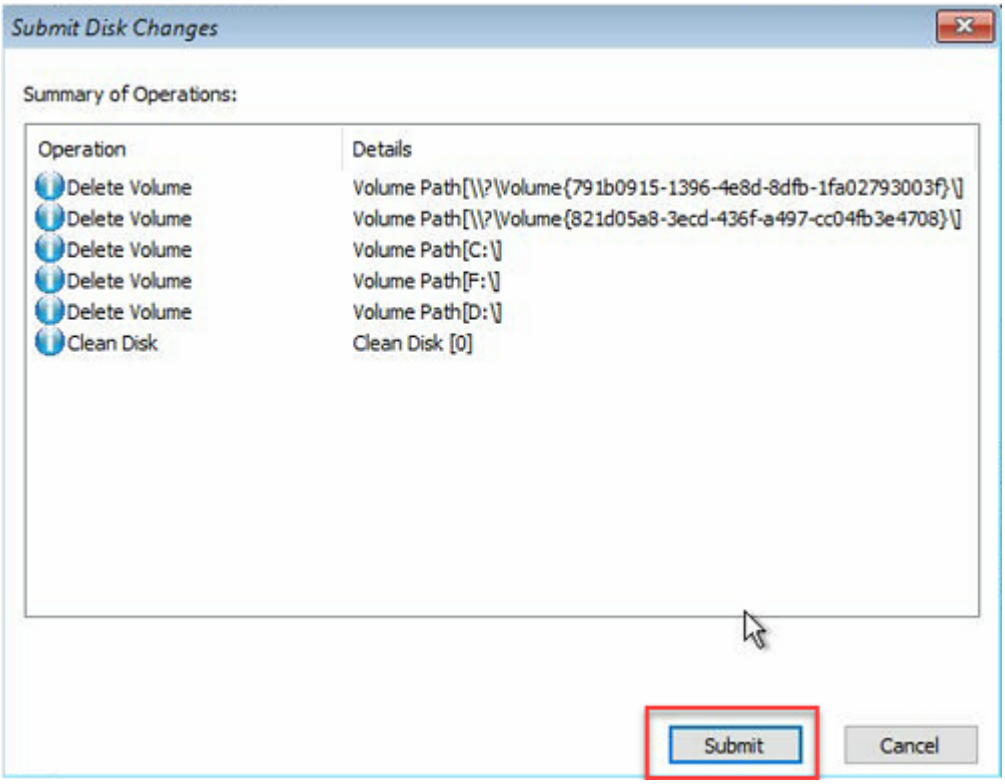


13. After cleaning the disk, right click on the same disk and click **Commit**.

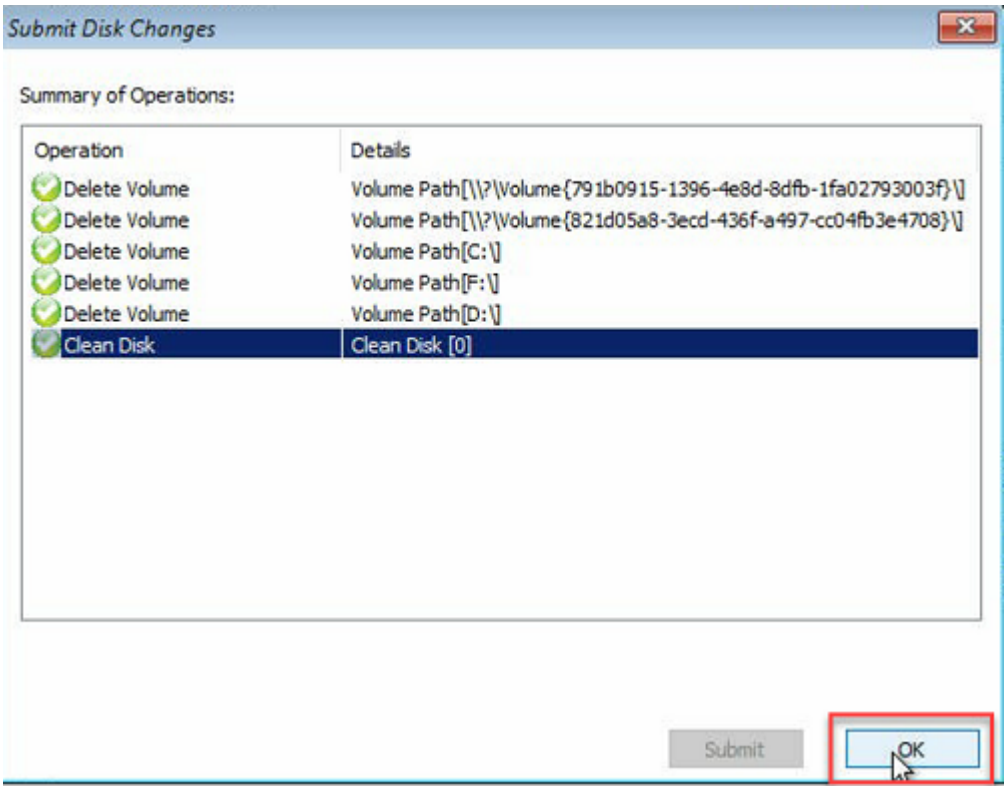


The **Submit Disk Changes** window appears.

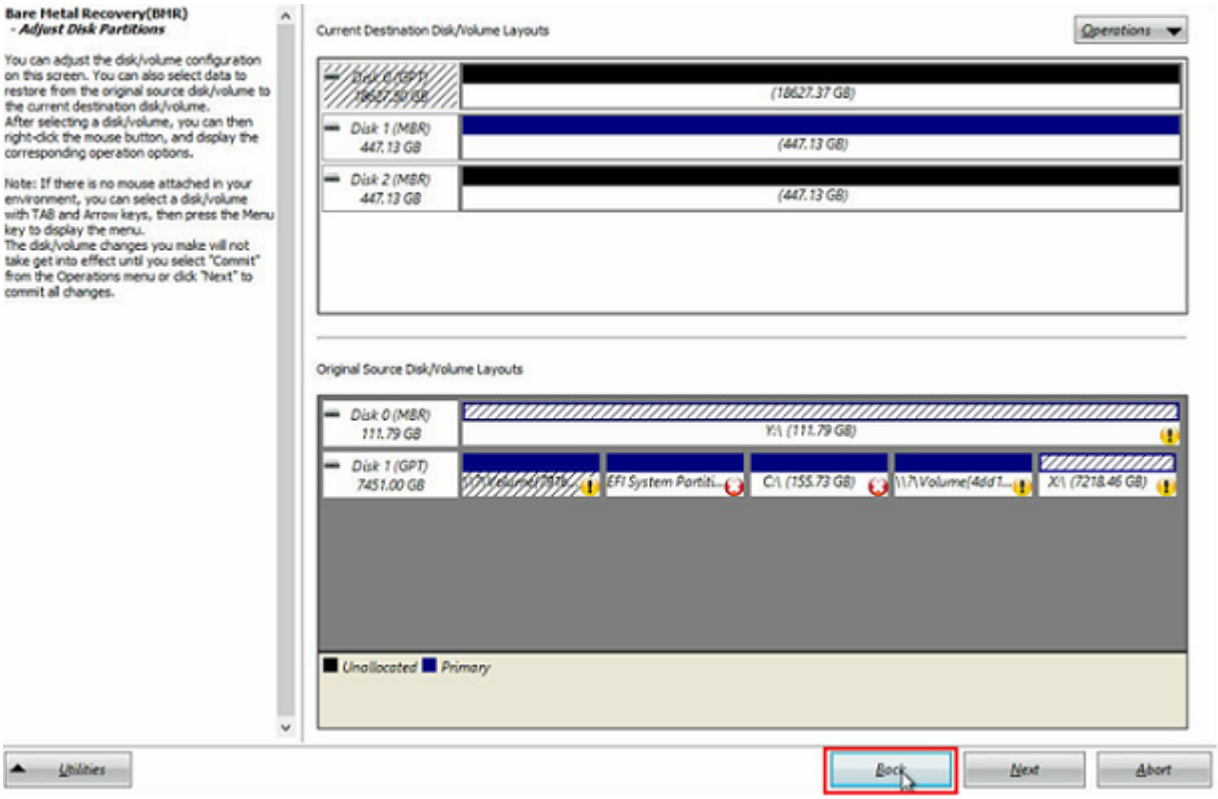
14. Click **Submit**.



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

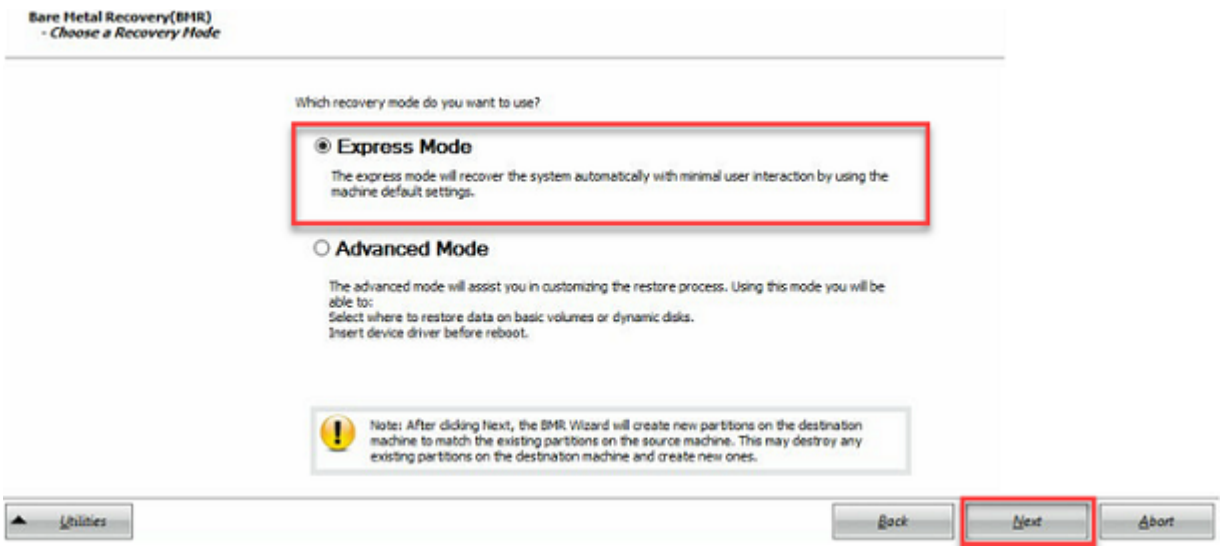


16. From the **Bare Metal Recovery(BMR)- Adjust Disk Partitions** dialog, click **Back**.



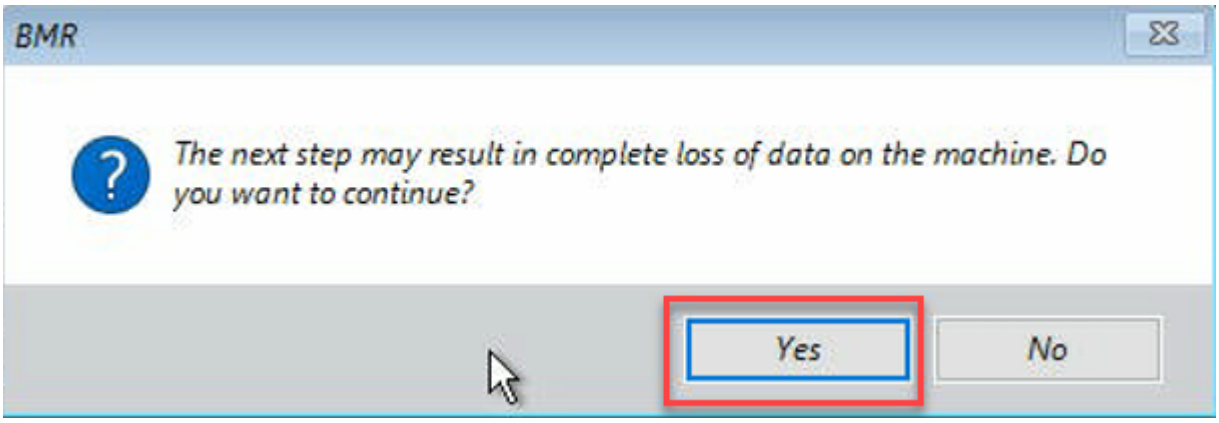
The **Bare Metal Recovery(BMR)- Choose a Recovery Mode** dialog appears.

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



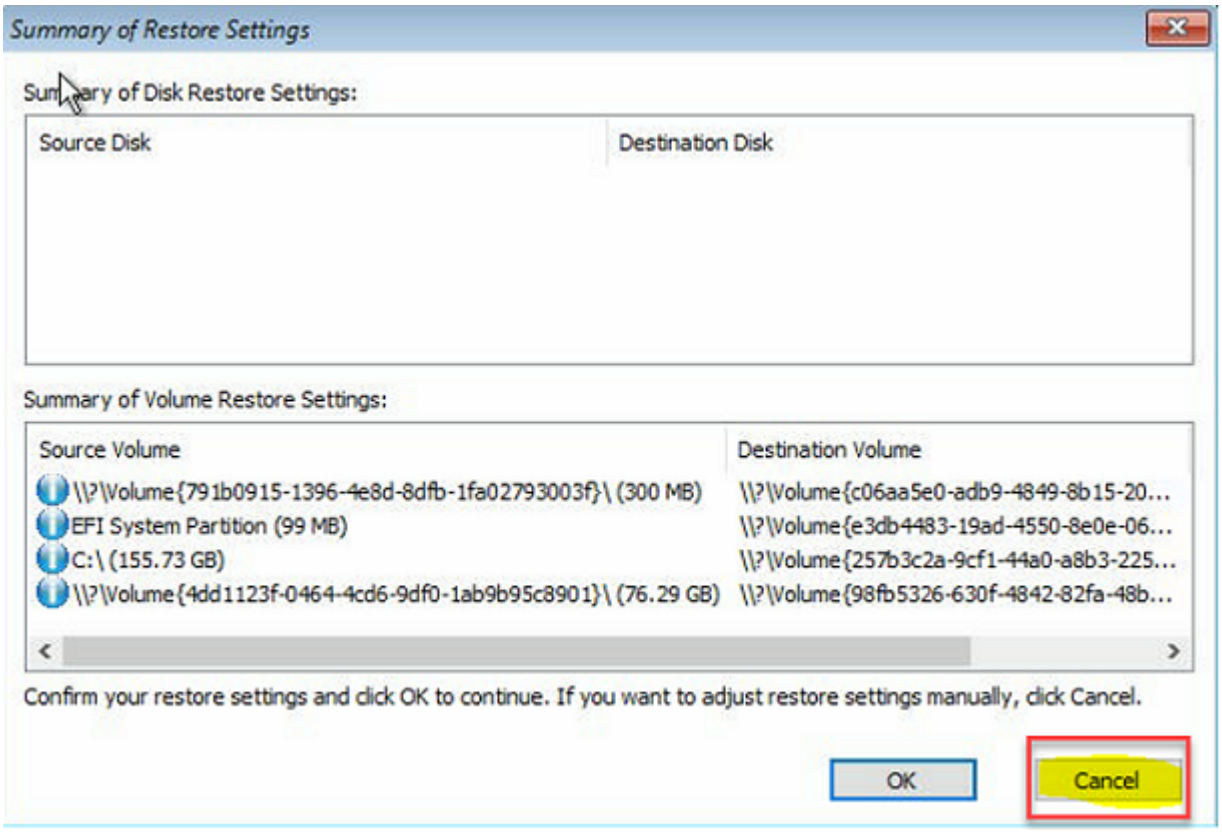
The **BMR** dialog appears.

18. Click **Yes**.



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

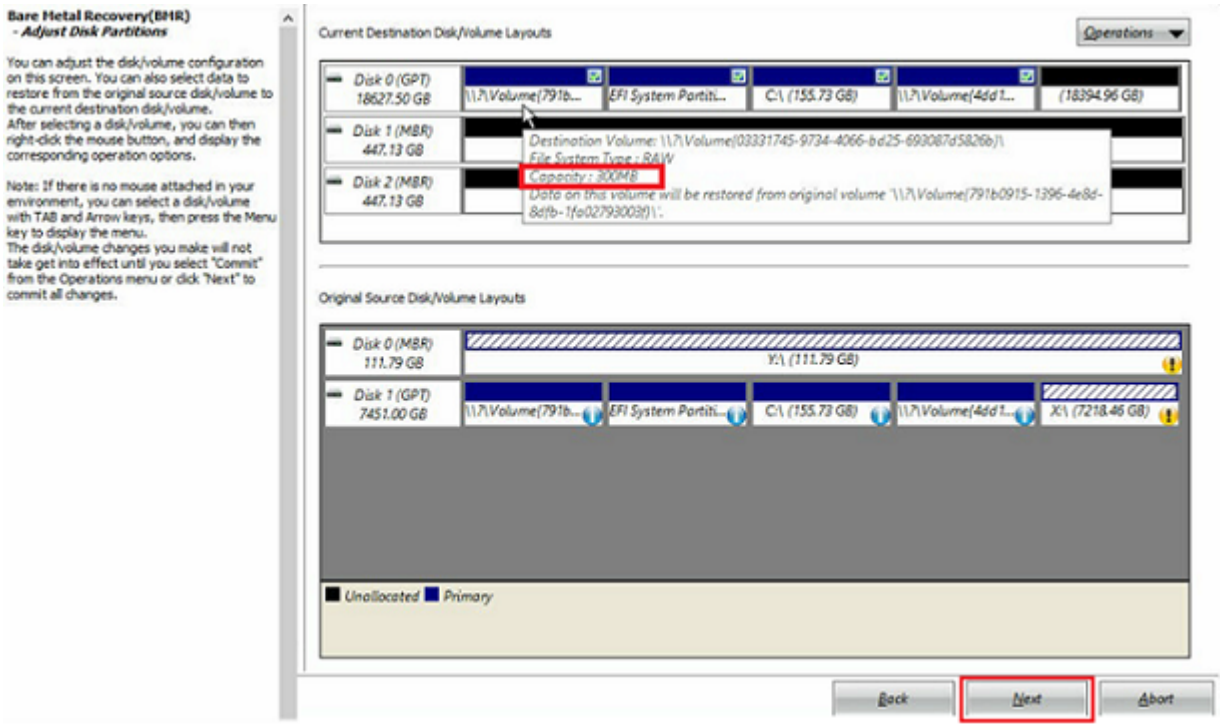
19. Click **Cancel**.



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

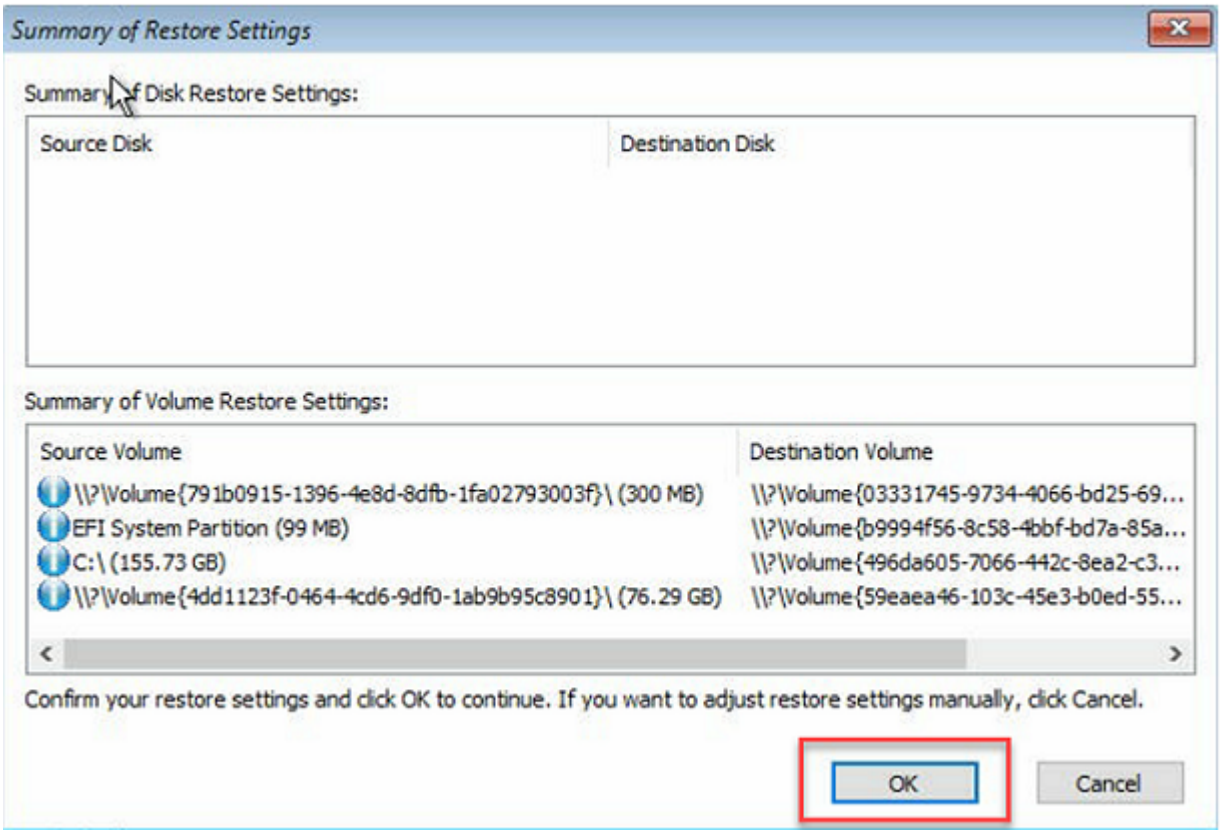
20. Compare and verify if the capacity of the first four partitions available in the **Current Destination Disk/Volume Layouts** tab matches with the largest GPT disk available in the **Original Source Disk/Volume Layouts** tab and click **Next**.

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



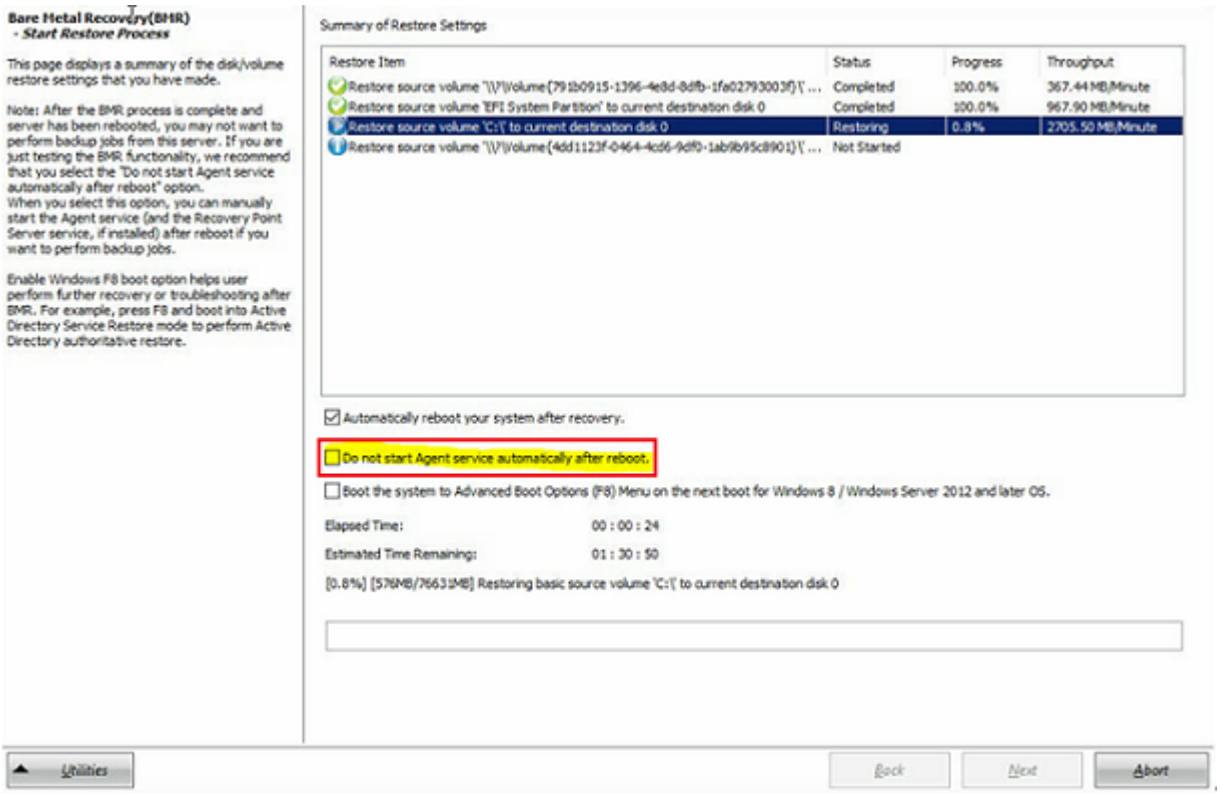
The **Summary of Restore Settings** dialog appears.

21. Click **OK**.



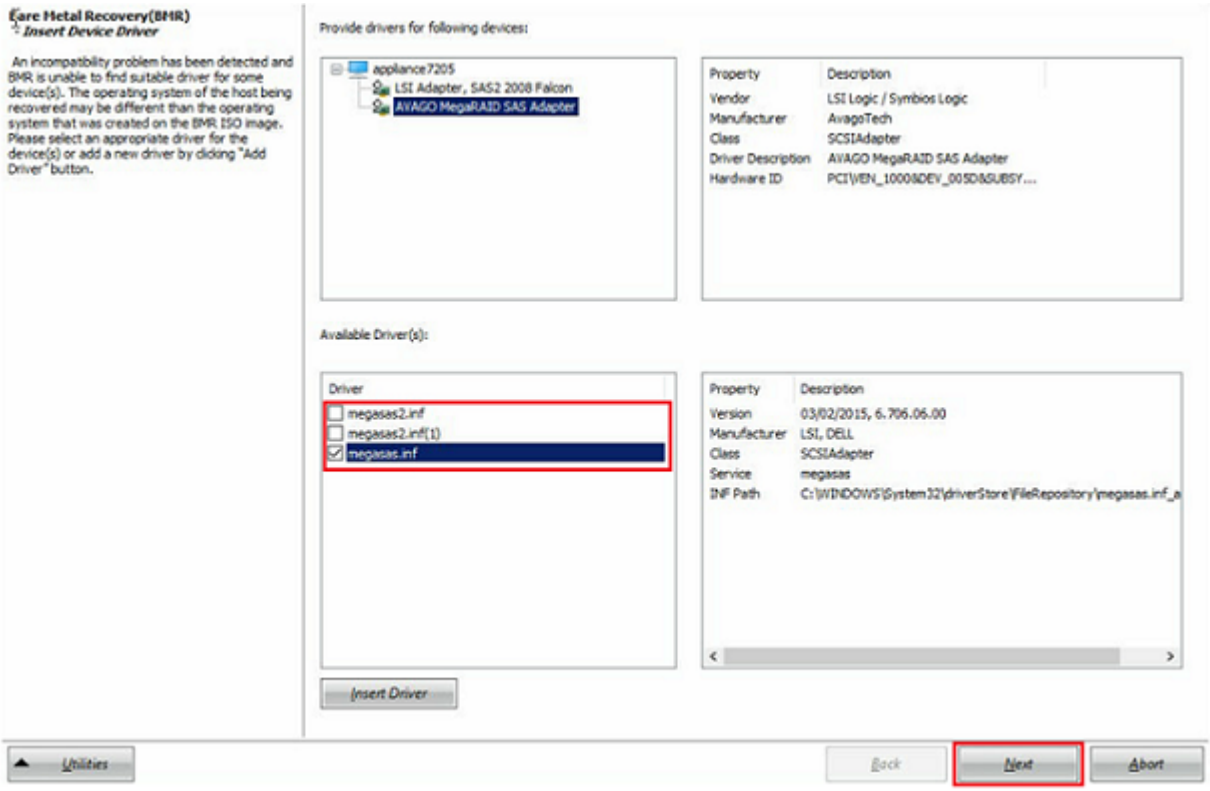
The **Bare Metal Recovery(BMR)- Start Recovery Process** dialog appears.

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

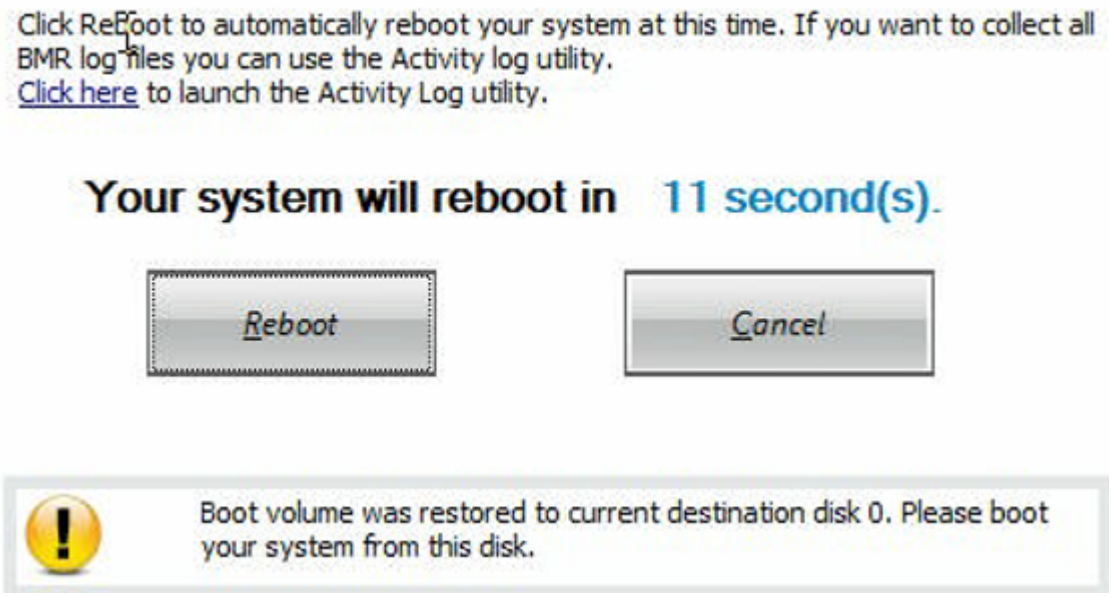


The **Bare Metal Recovery(BMR)- Insert Device Driver** dialog appears.

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.

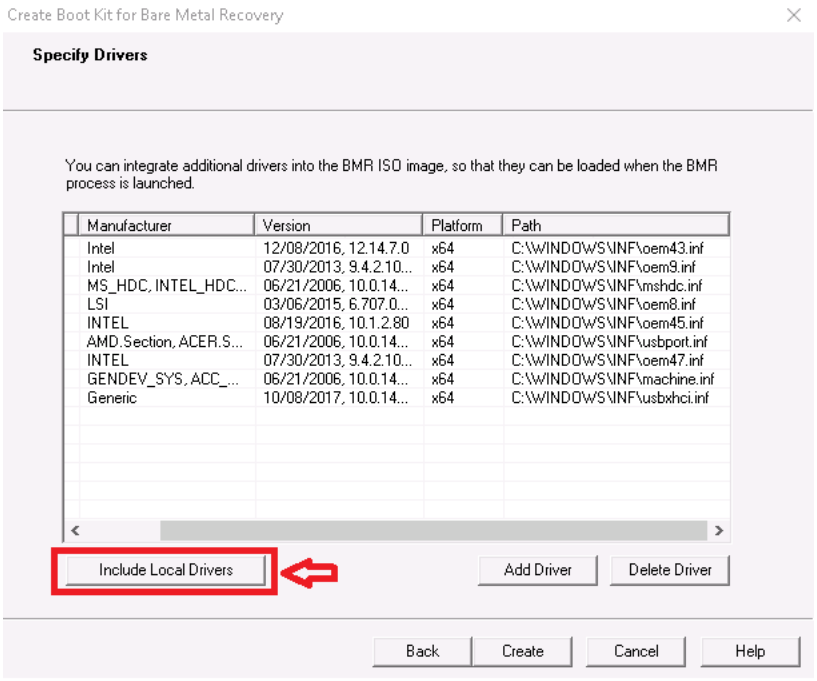
How to Perform Bare Metal Recovery (BMR) and Preserving Data

On the 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.

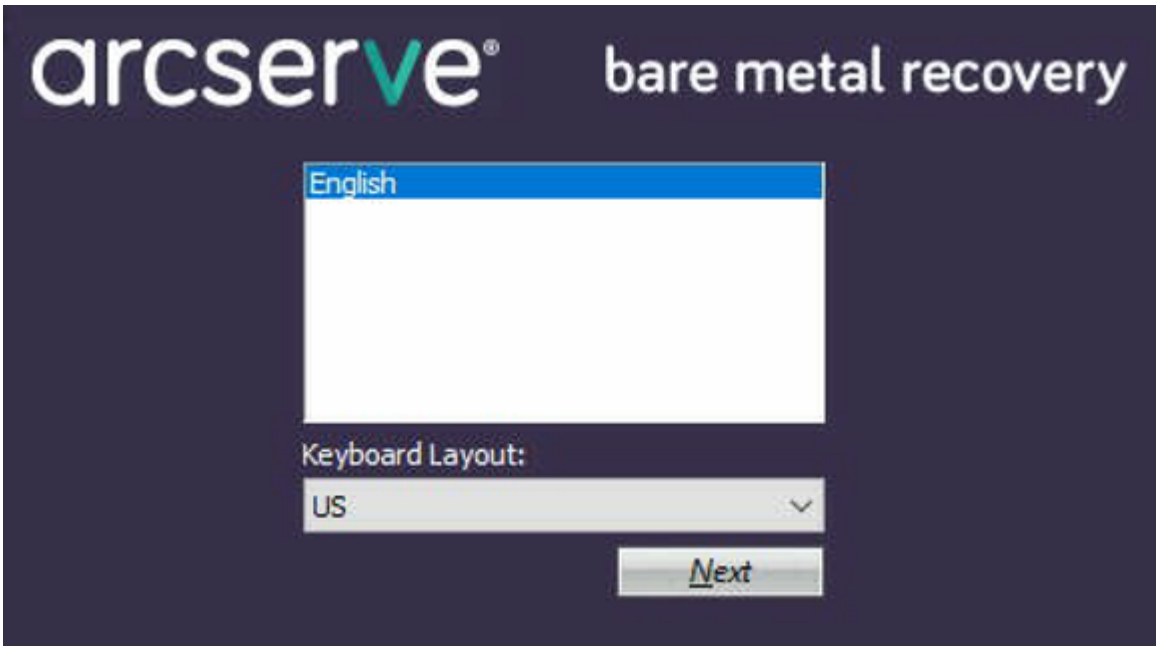
   Note: You need to include the local drivers for the ISO image. To include the local drivers, select the **Include Local Drivers** option in the **Create Boot Kit for Bare Metal Recovery** window. For more information on how to create boot kit, refer link.



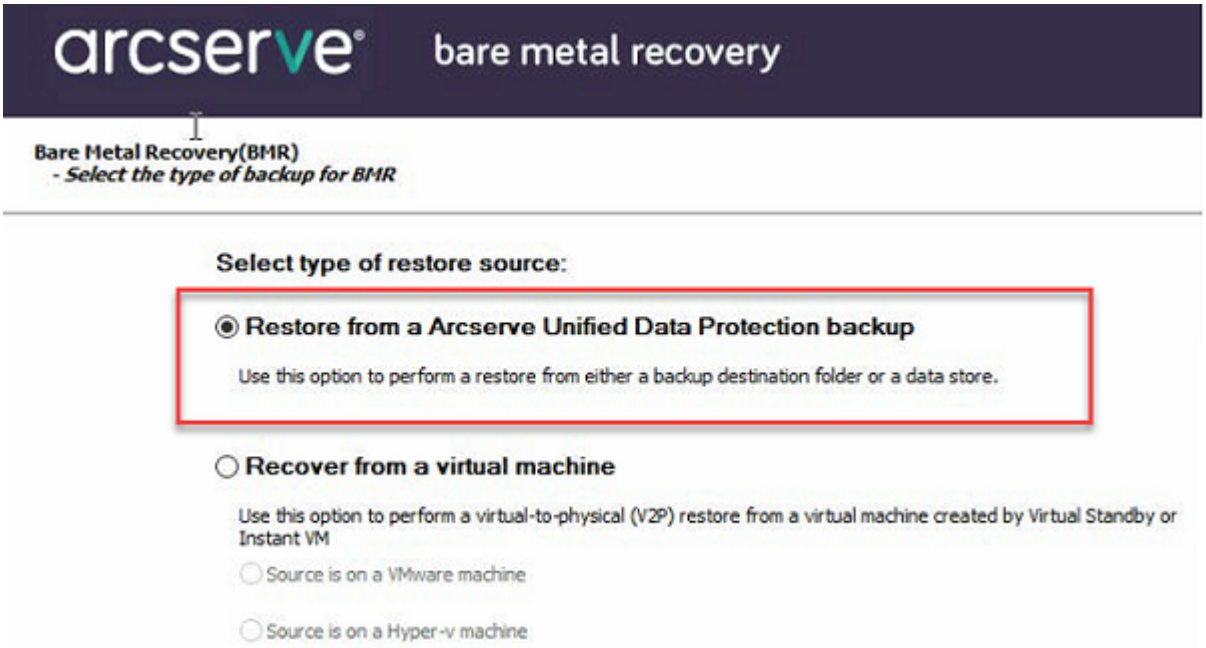
2. Boot the Arcserve Appliance using BMR ISO image or USB Stick.

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

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

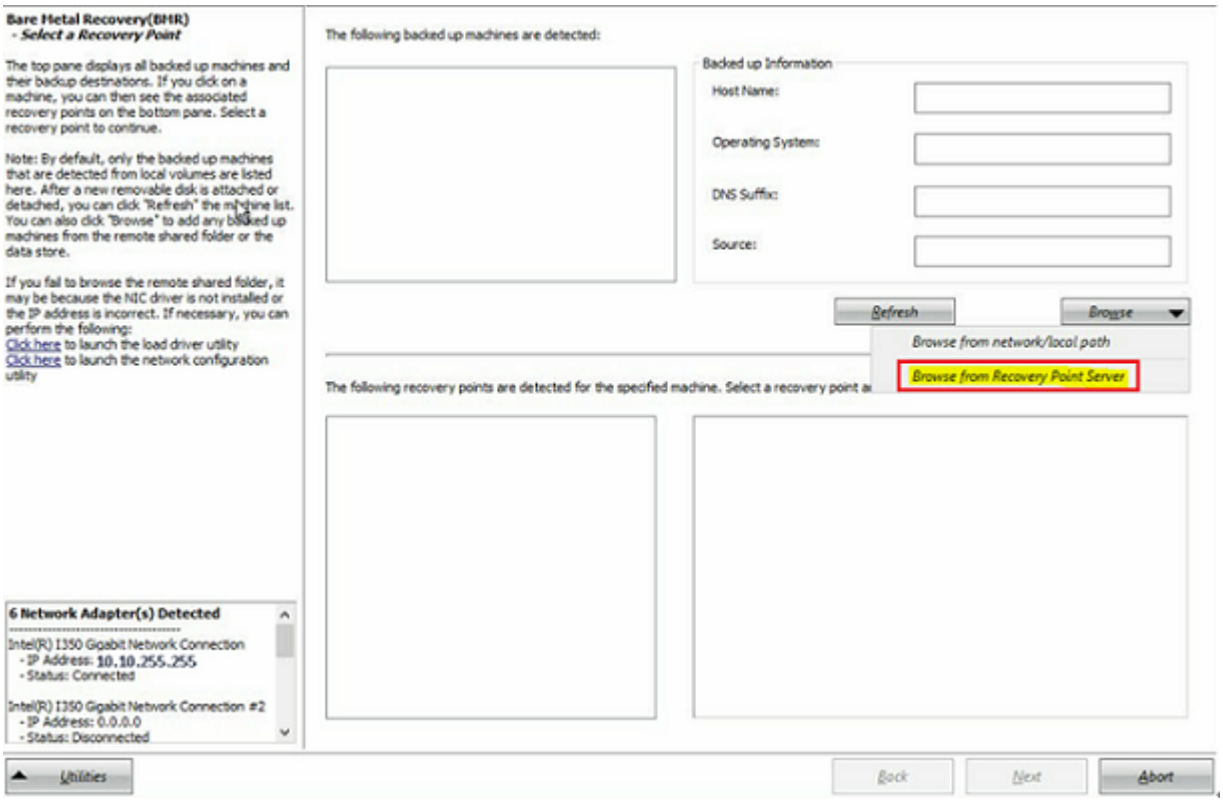


4. Select the **Restore from a Arcserve Unified Data Protection backup** option and click **Next**.



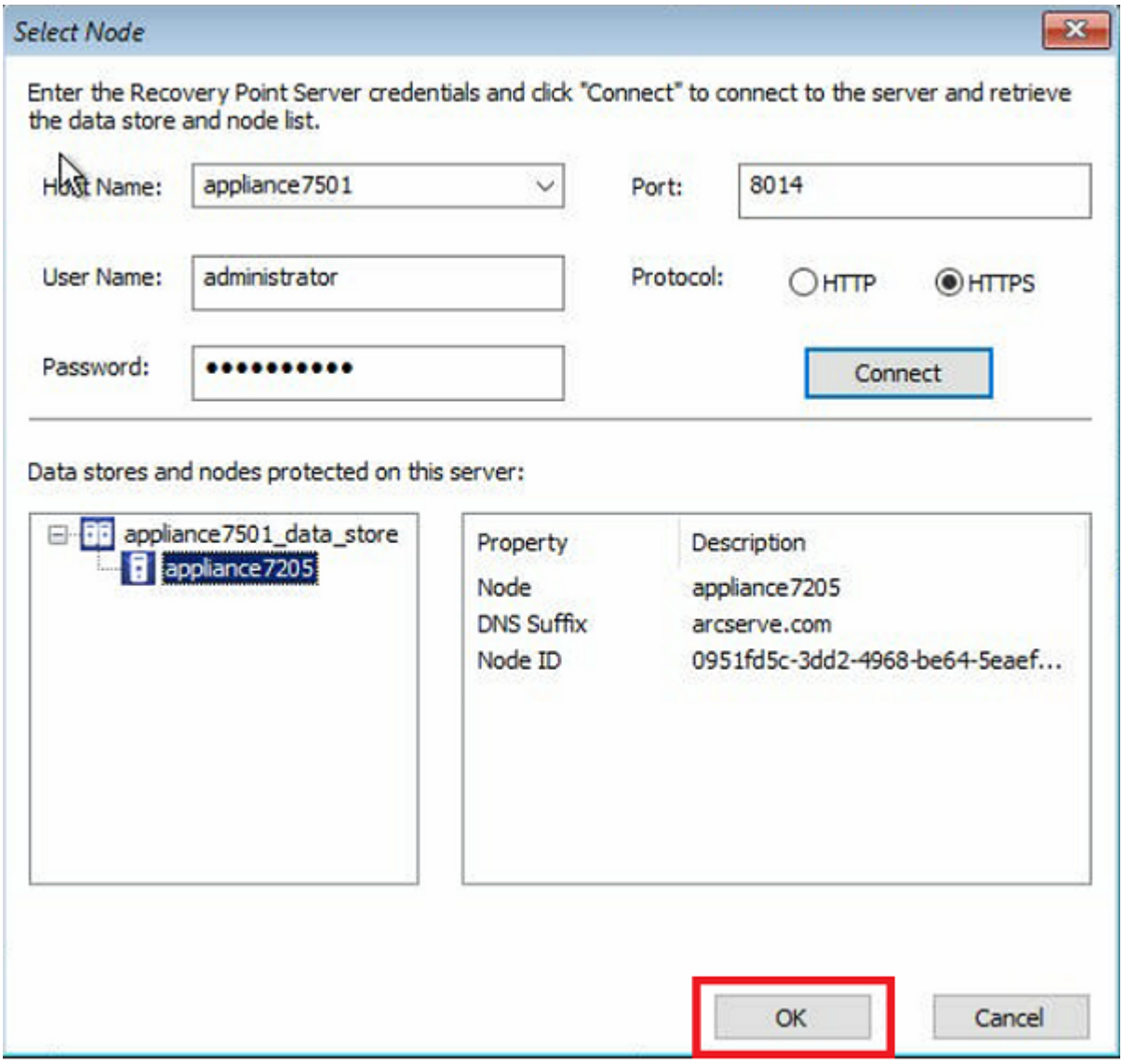
The **Select a Recovery Point wizard** window appears.

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



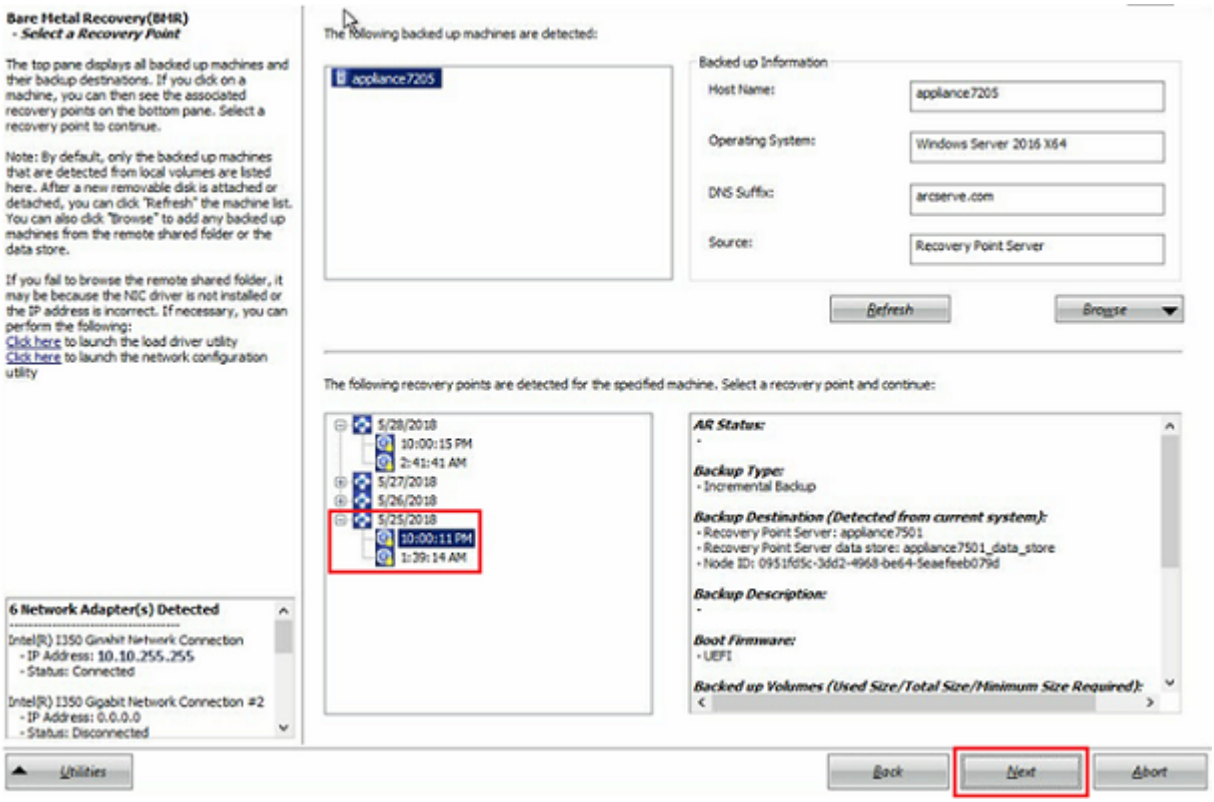
The **Select Node** window appears.

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.

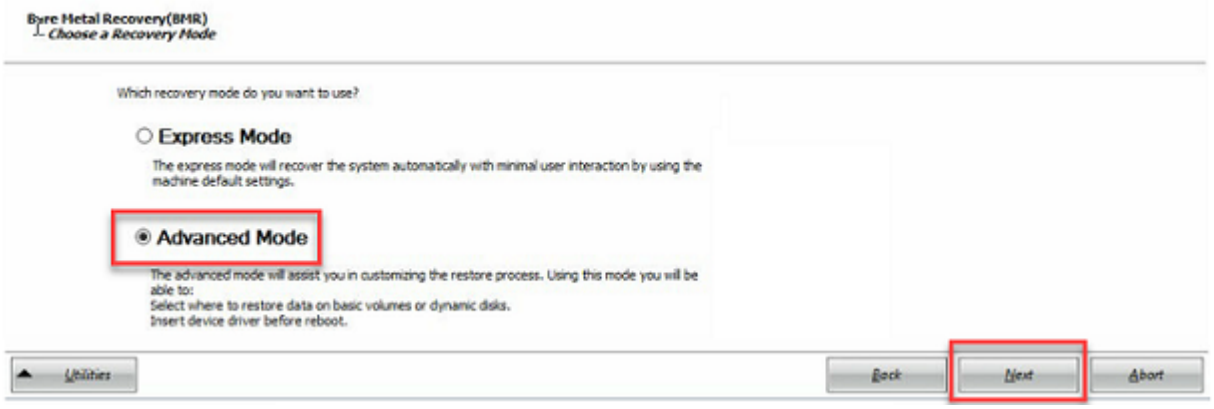
9. Select the recovery point to restore and click **Next**.



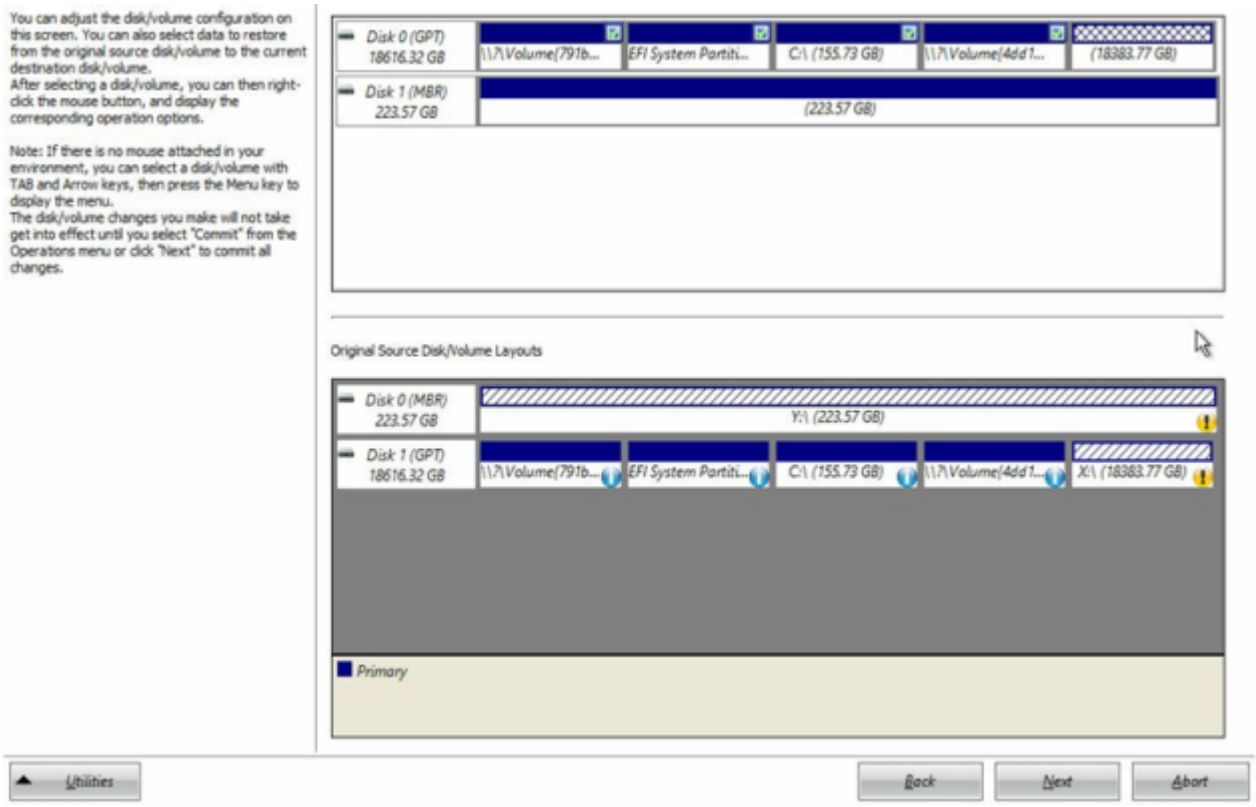
10. (Optional) Enter the session password if prompted, and click **OK**.

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

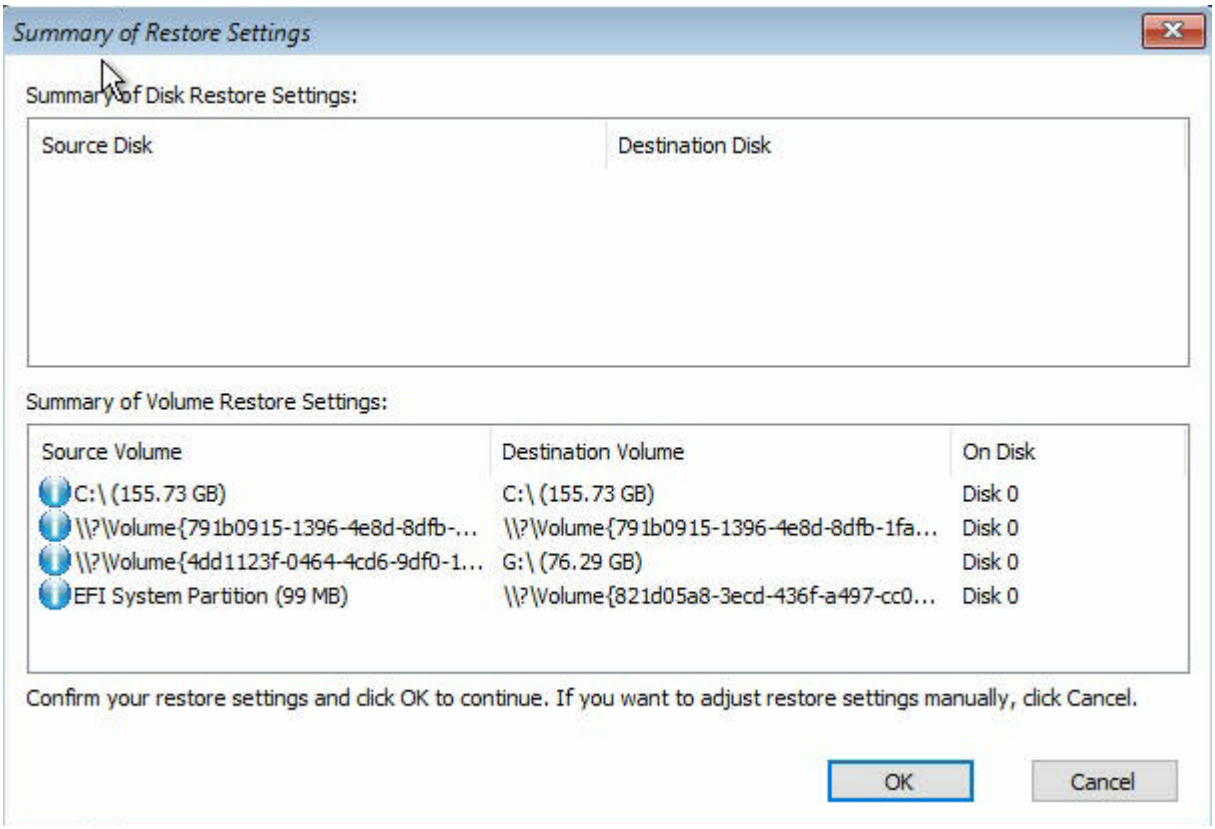
11. Select **Advanced Mode** and click **Next**.



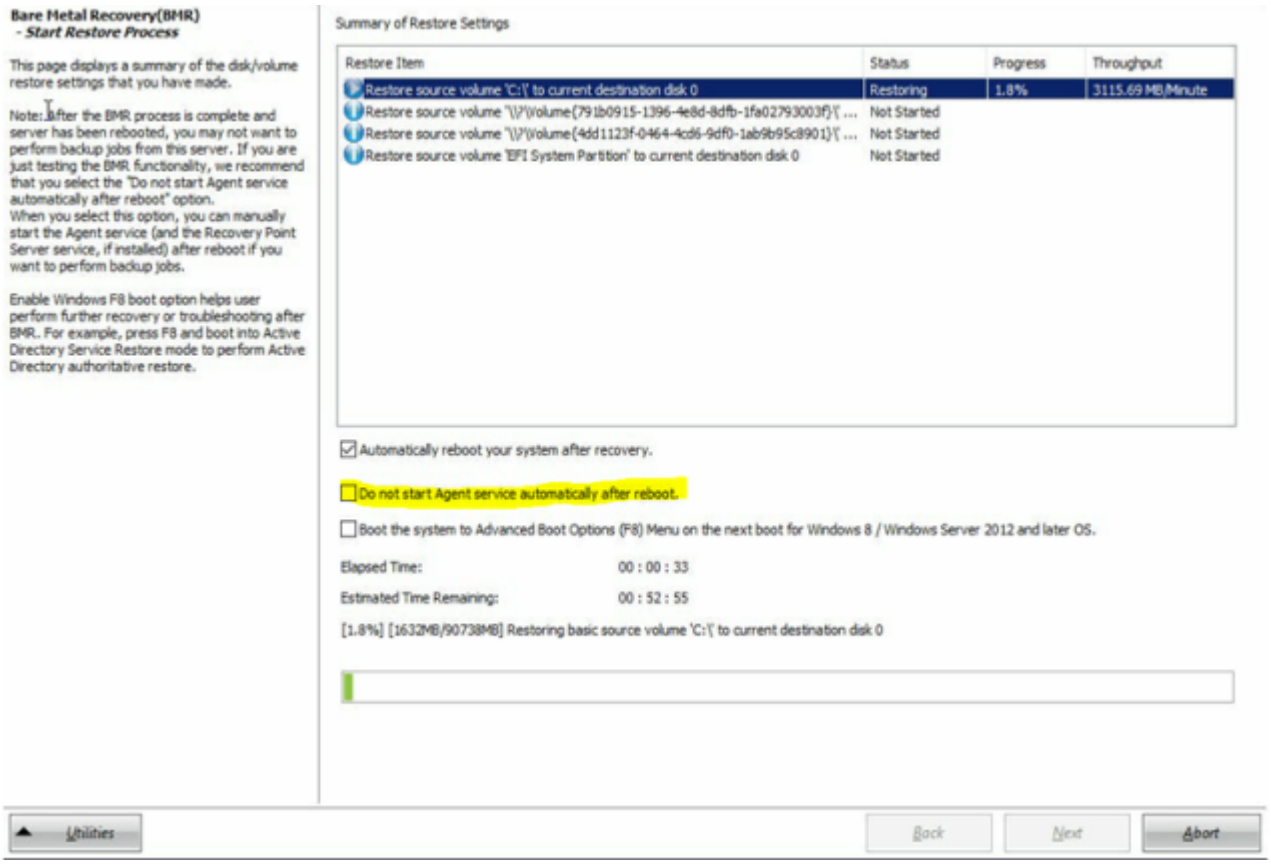
12. On the **Bare Metal Recovery(BMR)- Adjust Disk Partitions** dialog, click **Next**.



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 9012-9504 DR Models 189

Connecting Appliance Expansion Shelf to the Appliance Server 195

Working with Expansion Kit in Arcserve Appliance 9012-9504 DR Models

Arcserve Expansion Kit lets you expand the data capacity in Arcserve Appliance 9012-9504DR 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.

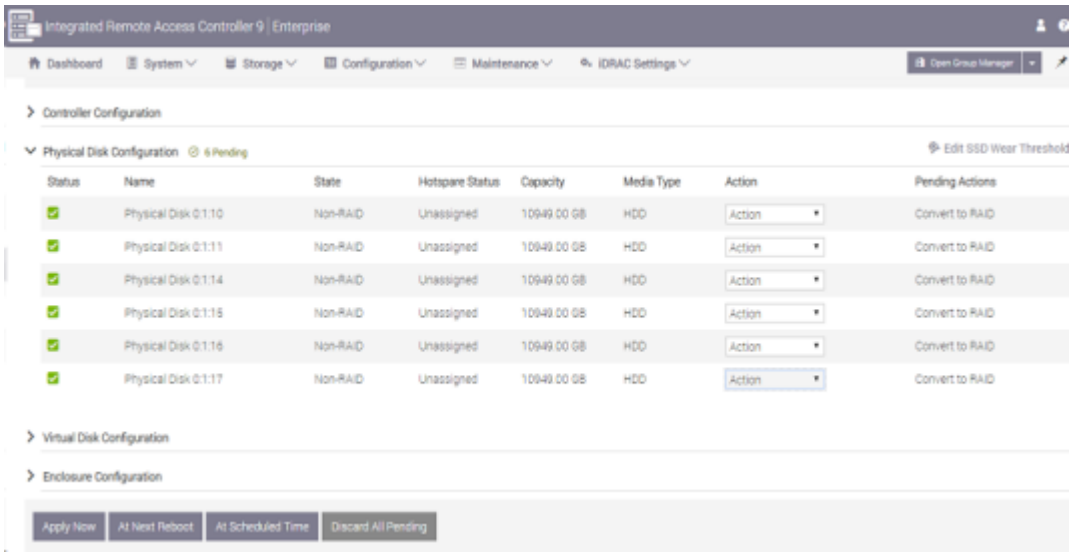
    A dialog appears to display the following warning message:

    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:

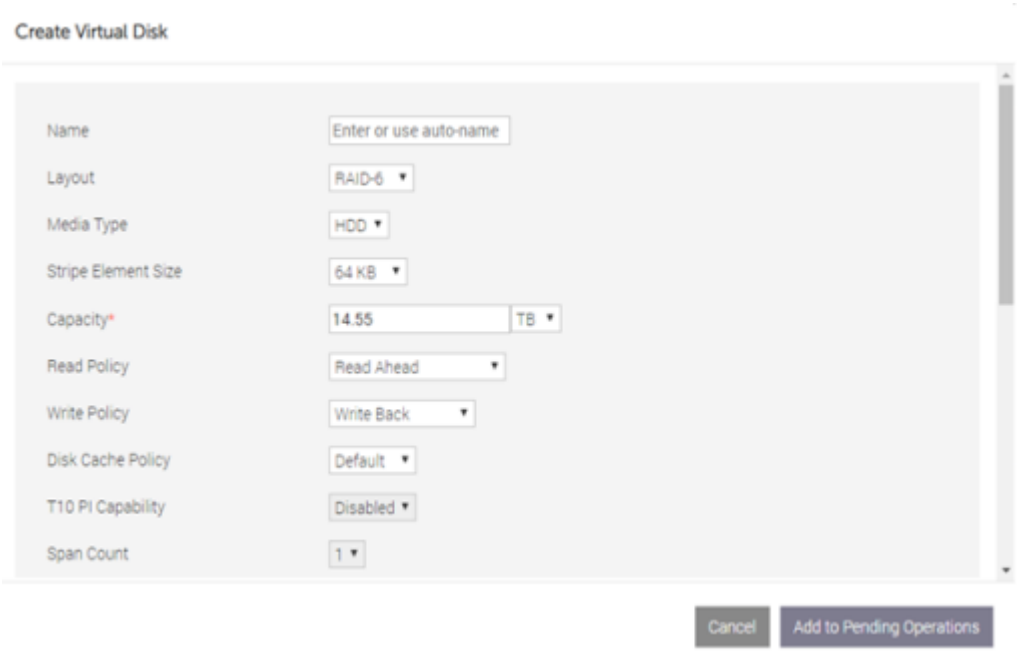
a. Navigate to Configuration, Storage Configuration and Virtual Disk Configuration.

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**.

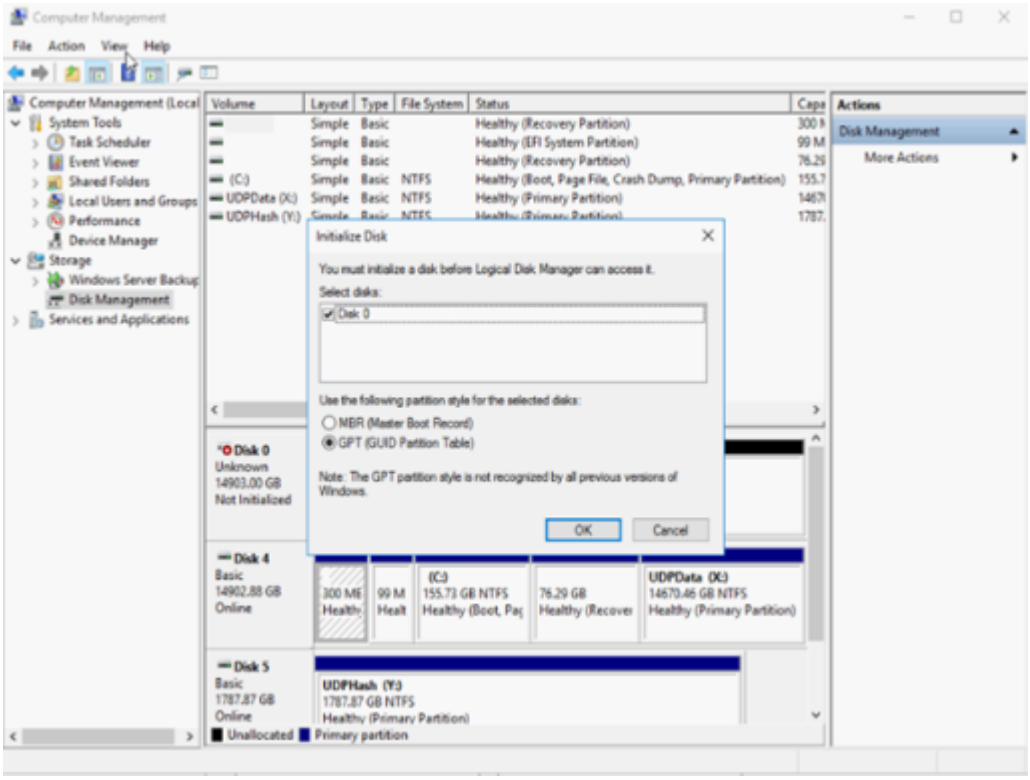
j. Double click the new virtual disk that you added.

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 data store:

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.

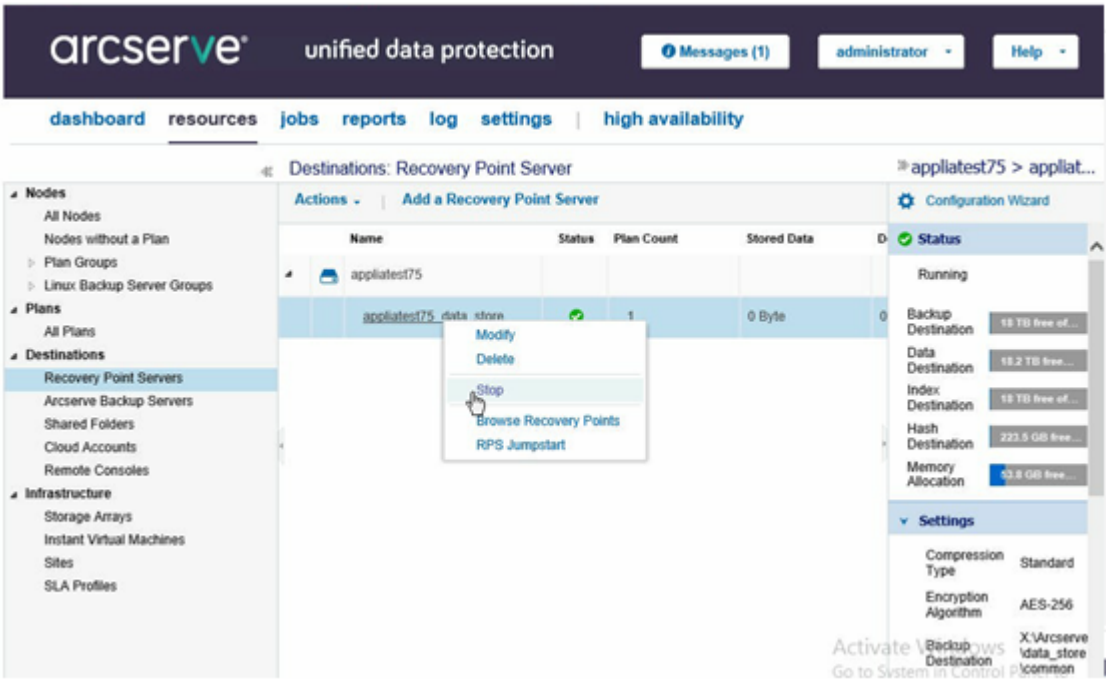
c. Click **Launch UDP Console**.

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 Data Store 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 <data store 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 <data store 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 data store.

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

i. Right click the Data Store and click **Start**.

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

Data capacity of the Arcserve Appliance is successfully expanded.

Connecting Appliance Expansion Shelf to the Appliance Server

This section contains the following topics:

Appliance Infield Expansion for all the Available Models

Model	Current Capacities \TB	Expansion Shelf Capacity	Current SSD - GB	New SSD REQ - GB	Free Slots	Add-on Cards	DESCRIPTION
8100	4, 6	8 (6x2 TB Disks)	120	8 TB - 140	2, 3	LSI SAS 9200 -8E HBA Qlogic Dual port HBA Quad-Port 1G NIC Dual port 10G SPF+ Dual Port 10G Copper Infield Expansion - (MegaRAID SAS 9380-8e)	1. 8100 model supports only 8 TB Infield Expansion. 2. 8100 - 8 TB Expansion Shelf comes with comes with inbuilt and pre-configured SSD 240 GB. 3. 8100 has 2 and 3 as optional slots . One free slot is mandatory for Appliance Infield Expansion / MegaRAID SAS 9380-8e. 4. If both the optional slots are

							filled with add-on Cards, then you need to free at least one slot , pre-ferrably slot 3 in order to use Infield Expansion. 5. SAS con-nection is used between the Appli-ance and Expansion shelf. 6. 8100 - Expansion shelf comes with RAID-6. 7. Expansion Shelf comes with Dual PSU. 8. Follow **Add data path instruc-tions** given in Expan-sion guide after con-necting the expansion shelf.

							9. Wherever a new SSD is required follow the **Migrate HASH destination to new SSD** instructions given in the Expansion Guide.
8200	8, 12	8 (6x2 TB Disks) OR 16 (6x4 TB Disks)	220	8 TB - NA 16 TB - 280	2, 3	LSI SAS 9200 -8E HBA Qlogic Dual port HBA Quad-Port 1G NIC Dual port 10G SPF+ Dual Port 10G Copper Infield Expansion (MegaRAID SAS 9380-8e)	1. 8200 model supports either 8 TB or 16 TB Infield Expansion. Client can connect only one expansion shelf any time. 2. 8200 - 16 TB Expansion Shelf comes with inbuilt and pre-configured SSD 480 GB. 3. 8200 has 2 and 3 as optional slots. One free slot is mandatory for Appli-

							ance Infield Expansion / MegaRAID SAS 9380-8e. 4. If both the optional slots are filled with add-on Cards, then you need to free at least one slot, pre-ferrably slot 3 in order to use Infield Expansion. 5. SAS con-nection is used between the Appli-ance and Expansion shelf. 6. Expansion shelf comes with RAID-6. 7. Expansion Shelf comes with Dual PSU 8. Follow **Add data path instruc-**

							tions given in Expansion guide after connecting the expansion shelf. 9. Wherever a new SSD is required follow the **Migrate HASH destination to new SSD** instructions given in the Expansion Guide.
8300	16,20,24,28,32,36,40	8 (6x2 TB Disks) OR 16 (6x4 TB Disks) OR 40 (12x4 TB Disks)	480	8 TB - NA 16 TB - 560 40 TB - 790	2, 5, 6	LSI SAS 9200 -8E HBA Qlogic Dual port HBA Quad-Port 1G NIC Dual port 10G SPF+ Dual Port 10G Copper Infield Expansion (MegaRAID SAS 9380-8e)	1. 8300 model supports either 8 TB or 16 TB OR 40 Infield Expansion. Client can connect only one expansion shelf any time. 2. 8300 - 16 TB / 40 TB Expansion Shelf comes with inbuilt and pre-configured SSD 1.9 TB.

							3. 8300 has 2 , 5, and 6 as optional slots . One free slot is mandatory for Appli-ance Infield Expansion / MegaRAID SAS 9380-8e. 4. If both the optional slots are filled with add-on Cards, then you need to free at least one slot, pre-ferrably slot 2 in order to use Infield Expansion. 5. SAS con-nection is used between the Appli-ance and Expansion shelf. 6. Expansion shelf comes with RAID-6 (6x4 TB

							Disks). 7. Expansion Shelf comes with Dual PSU. 8. Follow **Add data path instructions** given in Expansion guide after connecting the expansion shelf. 9. Wherever a new SSD is required follow the **Migrate HASH destination to new SSD** instructions given in Expansion Guide. (Only for Appliance 8300 connect with 40 TB Appliance expansion shelf, there is one unattached 2 TB SSD that you need to place in

							Base appliance and not expansion shelf. Check expansion guide from details).
8400	32,40,48,56,64,72,80	8 (6x2 TB Disks) OR 16 (6x4 TB Disks) OR 40 (12x4 TB Disks)	1200	8 TB - NA 16 TB - NA 40 TB - NA	2, 5, 6	LSI SAS 9200 -8E HBA Qlogic Dual port HBA Quad-Port 1G NIC Dual port 10G SPF+ Dual Port 10G Copper Infield Expansion (MegaRAID SAS 9380-8e)	1. 8400 model supports either 8 TB or 16 TB OR 40 TB Infield Expansion . Client can connect only one expansion shelf any time. 2. 8400 - Requires no addtional SSD. 3. 8400 has 2 , 5, and 6 as optional slots. One free slot is mandatory for Appliance Infield Expansion / MegaRAID SAS 9380-8e. 4. If both the optional

							slots are filled with add-on Cards, then you need to free at least one slot, preferrably slot 2 in order to use Infield Expansion. 5. SAS connection is used between the Appliance and Expansion shelf. 6. Expansion shelf comes with RAID-6. 7. Expansion Shelf comes with Dual PSU. 8. Follow the **Add data path instructions** given in the Expansion guide after connecting the expansion shelf.

What is included in the box

The following items are included in the box:

Note: If you notice that any items in the box are damaged, contact Arcserve Support.

- Appliance Expansion Shelf

  Note: The number of available disks in the expansion shelf depends on the capacity of the Appliance Expansion shelf.

- CVPM02 Module (CacheVault Power Module02) and Cable

- MegaRAID SAS 9380-8e RAID Controller

- SAS Cables

  Two SAS Cables which are used to connect the MegaRaid Controller in the Appliance Expansion Shelf and Appliance Server.

- SSD (optional)

  Note: For Appliance 8300 only, you need to connect with 40 TB Appliance expansion and you have one unattached 2 TB SSD.

How to Connect the Appliance Expansion Shelf to the Appliance Server

Follow these steps:

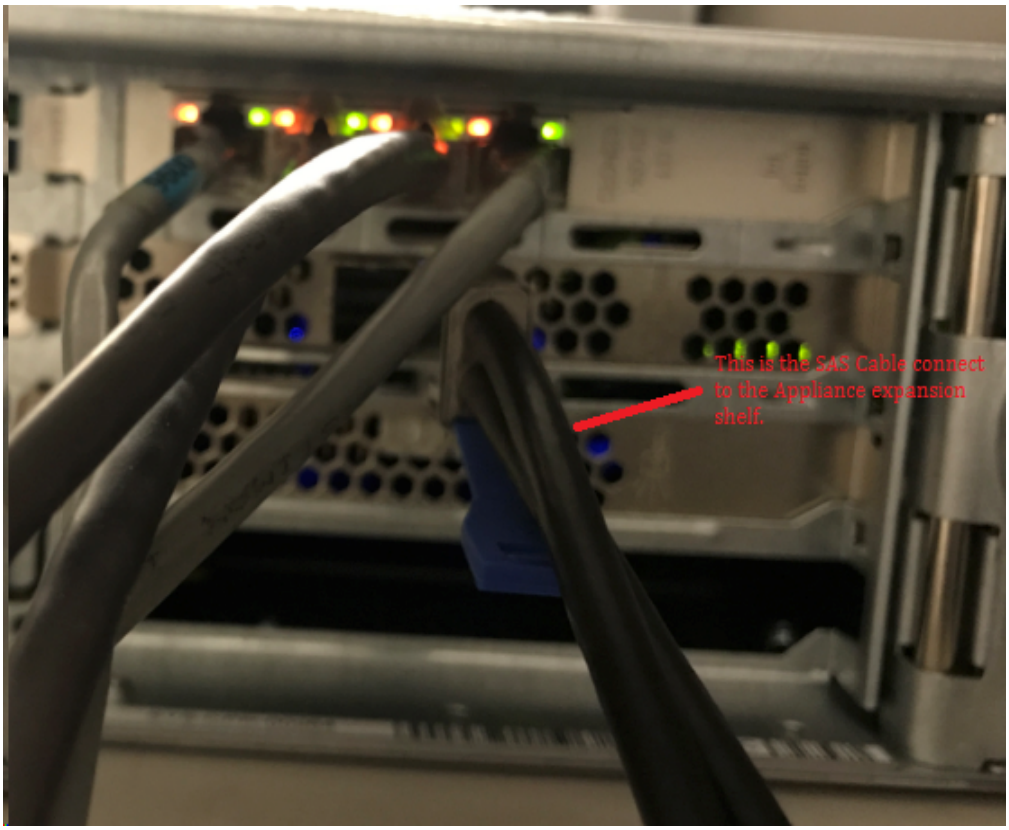
1. Prepare the Appliance expansion shelf and place it close to the Appliance Server.
2. Connect the *CacheVault Power Module02 (CVPM02)* to *MegaRAID Controller 9380-8e*.

3. Pause all the Arcserve UDP plans and ensure that there are no running jobs on the Appliance Server.
4. Power off the Appliance Server and disconnect the power cord from the power supply.

   Note: Disconnect the computer from the power supply to avoid the risk of damaging the system or electric shock.
5. Remove the cover of the Appliance Server chassis.

6. Perform the following steps to insert the *MegaRAID Controller 9380-8e* into an available PCI-e slot of the Appliance Server:
   a. Locate an empty PCI-e slot.
   b. Remove the blank bracket panel on the backside of the computer that aligns with the empty PCIe slot.
   c. Save the bracket screw, if applicable.
   d. Align the MegaRAID Controller 9380-8e to a PCIe slot.
   e. Press down gently but firmly to seat the raid controller correctly in the slot.

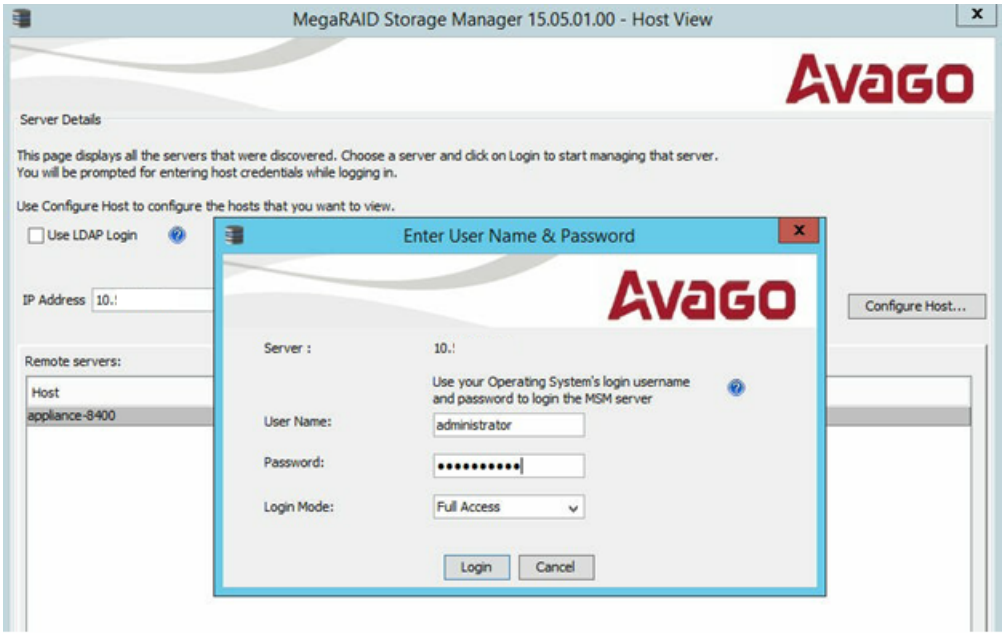
7. Secure the *MegaRAID Controller 9380-8e* bracket to the chassis of the system.
8. Replace the cover of the Appliance Server chassis.
9. Connect the *MegaRAID Controller 9380-8e* in the Appliance Server and the *MegaRAID Controller* in the Appliance expansion shelf with the SAS cable.



10. Insert SSD (only for Appliance 8300 + 40 TB expansion shelf).

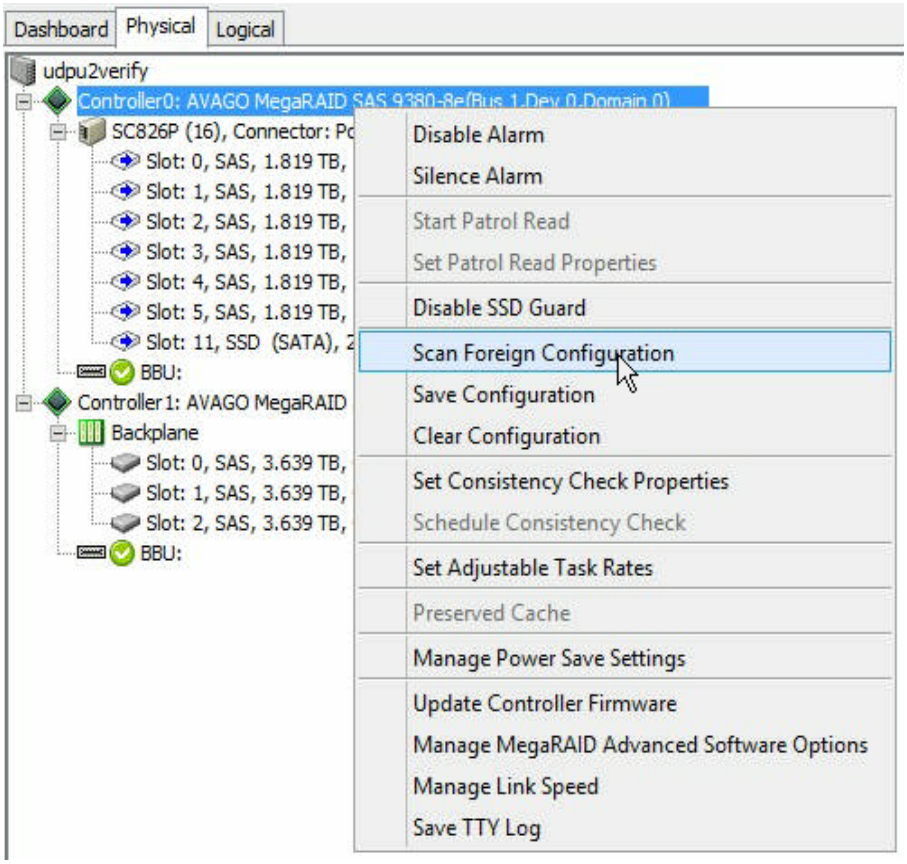
Note: If a 40 TB Appliance Expansion Shelf connected to an Appliance 8300, plug the 2 TB SSD (shipped with the Appliance Expansion Shelf) into the empty SATA slot at the rear panel of the Appliance 8300.

11. Connect the power cords of Appliance Expansion Shelf and power on the Appliance Expansion Shelf.
12. Reconnect the power cords of the Appliance Server and power on the Appliance Server.
13. Log into the Appliance Server, open the MegaRAID Storage Manager and login as administrator.



14. Perform the following steps to verify the raid controller from MegaRAID Storage Manager:
    a. Navigate to the **Physical** tab where the two controllers are listed.
    b. Select the **Controller 9380-8e** and ensure that all the disks connected to the controller 9380-8e are online and available.

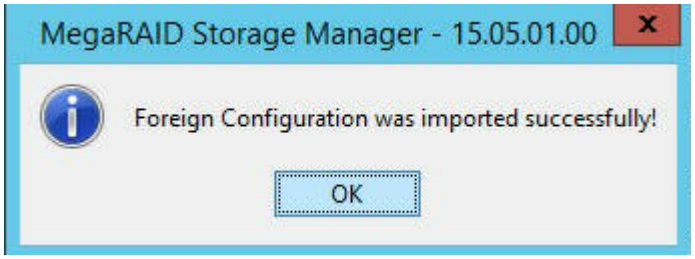
       Note: If there are any disks that are not online, right click and select **Scan Foreign Configuration**.



c. Select the **Import: Import logical configuration from all foreign drives** option and click **OK**.

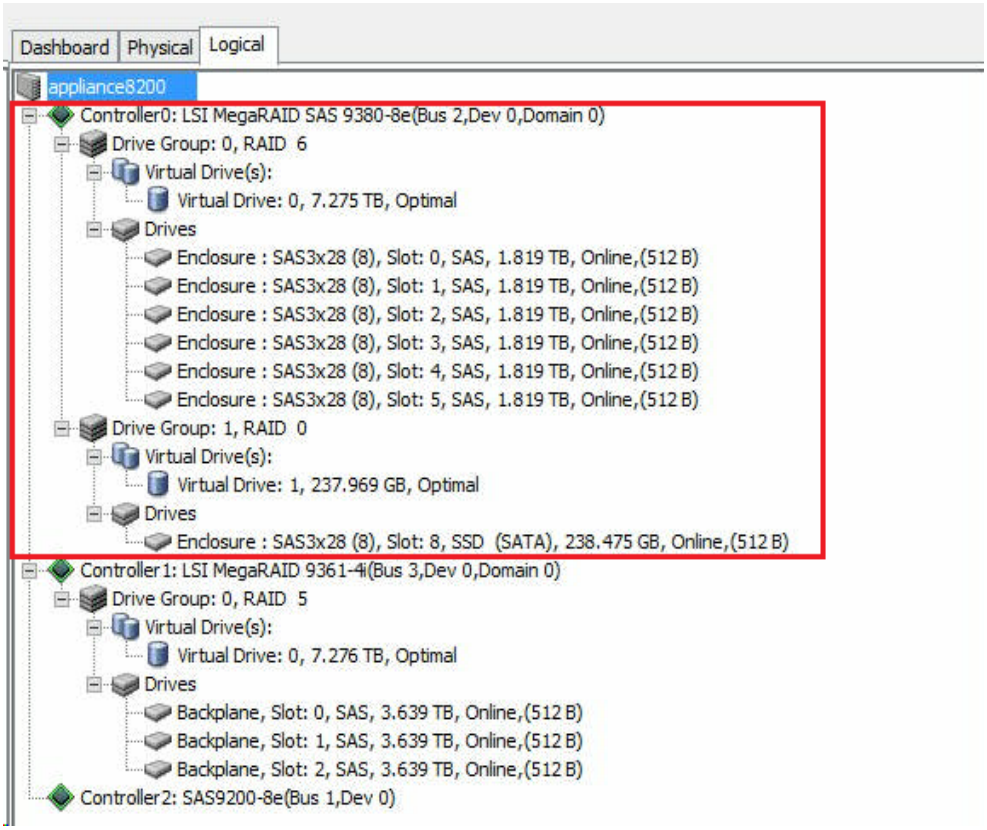
d. Click **Yes** to initiate the import process.

e. Click **OK**.



All the disk drives on the expansion shelf are online now.

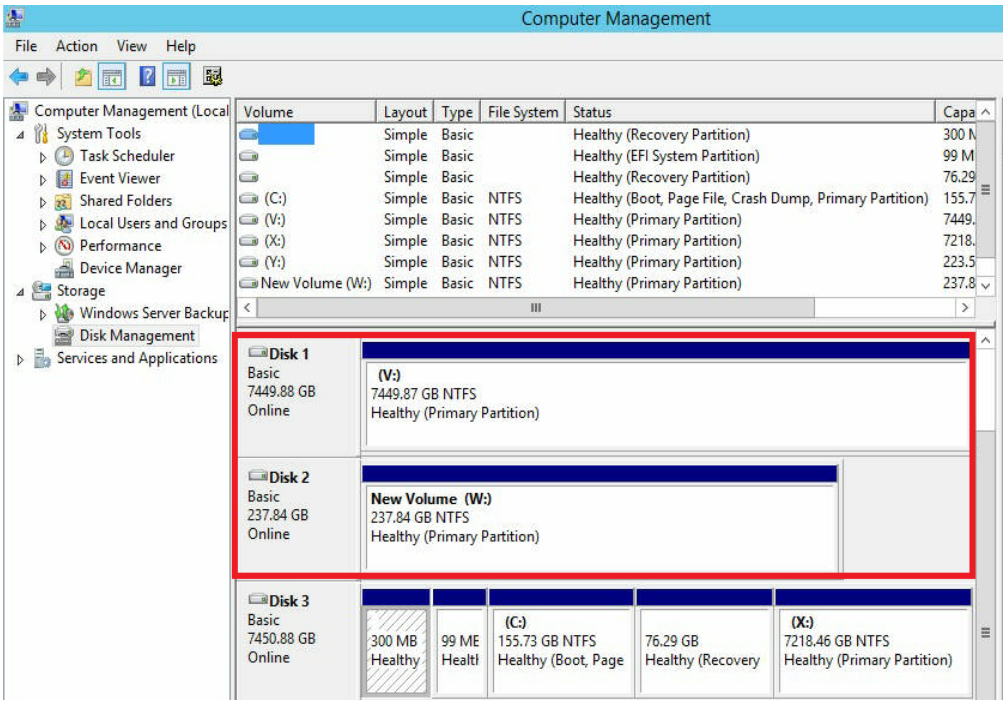
15. Navigate to the Logical tab where you can see the following disks are configured with RAID-6. For other modules of the expansion shelf, one SSD is set as RAID-0 and listed under *LSI MegaRAID SAS 9380-8e*.
    - Appliance server 8100 + 8 TB expansion shelf
    - Appliance server 8200 + 16 TB expansion shelf
    - Appliance server 8300 + 16 TB expansion shelf



16. Open Computer Management and navigate to Disk Management and perform the following steps:

    a. Format the Appliance Expansion Shelf assembled disk as NTFS and assign a drive letter. For example, “V:”.

b. Format the SSD as NTFS and assign a drive letter. For example, “W:”.



You have connected the Appliance Expansion Shelf to the Appliance Server successfully.

How to Modify Arcserve UDP Data store

This section contains the following topics:

- Adding a data path on the expansion shelf to the Arcserve UDP data store
- Migrating Hash Destination to the new SSD
- Checking the Overall Capacity of Data Store from Arcserve UDP Console
- Resuming all the plans from Arcserve UDP Console

Adding a Data Path on Expansion Shelf to Arcserve UDP Data Store

Follow these steps:

1. Create a folder in the volume on the Appliance expansion shelf, such as “V:\data”.
2. Stop the data store and use the following command to expand the data store to the Appliance expansion shelf:

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

as_gddmgr.exe –DataPath Display <data store name>

Migrating Hash Destination to the new SSD

Note: This step is required only when you use a new SSD for the following expansion shelf:

- Appliance server 8100 + 8 TB expansion shelf;
- Appliance server 8200 + 16 TB expansion shelf;
- Appliance server 8300 + 16 TB expansion shelf;
- Appliance server 8300 + 40 TB expansion shelf;

Follow these steps:

1. Create a hash folder on the new SSD such as *W:\Arcserve\data_store\hash*.
2. Ensure the data store is stopped. If not, stop the data store from the Arcserve UDP Console.
3. Modify the data store from the Arcserve UDP Console and set the Hash Destination to *W:\Arcserve\data_store\hash*.
4. Save the modification of the data store.
5. Start the data store from the Arcserve UDP Console.

Checking the Overall Capacity of Data Store from Arcserve UDP Console

The overall capacity is the capacity of the Appliance server plus the capacity of the Appliance expansion shelf.

Resuming all the plans from Arcserve UDP Console

Resume all the paused plans from the Arcserve UDP Console.

Chapter 10: Working with Network Configuration

This section contains the following topics:

Understanding the Network Configuration Details 223
How to Configure the NIC Teaming Process 228
How to Disable DHCP Server 230
How to Configure IP Address for the preinstalled Linux Backup Server 231
How to Enable Round Robin on the DNS Server to Balance Load 233

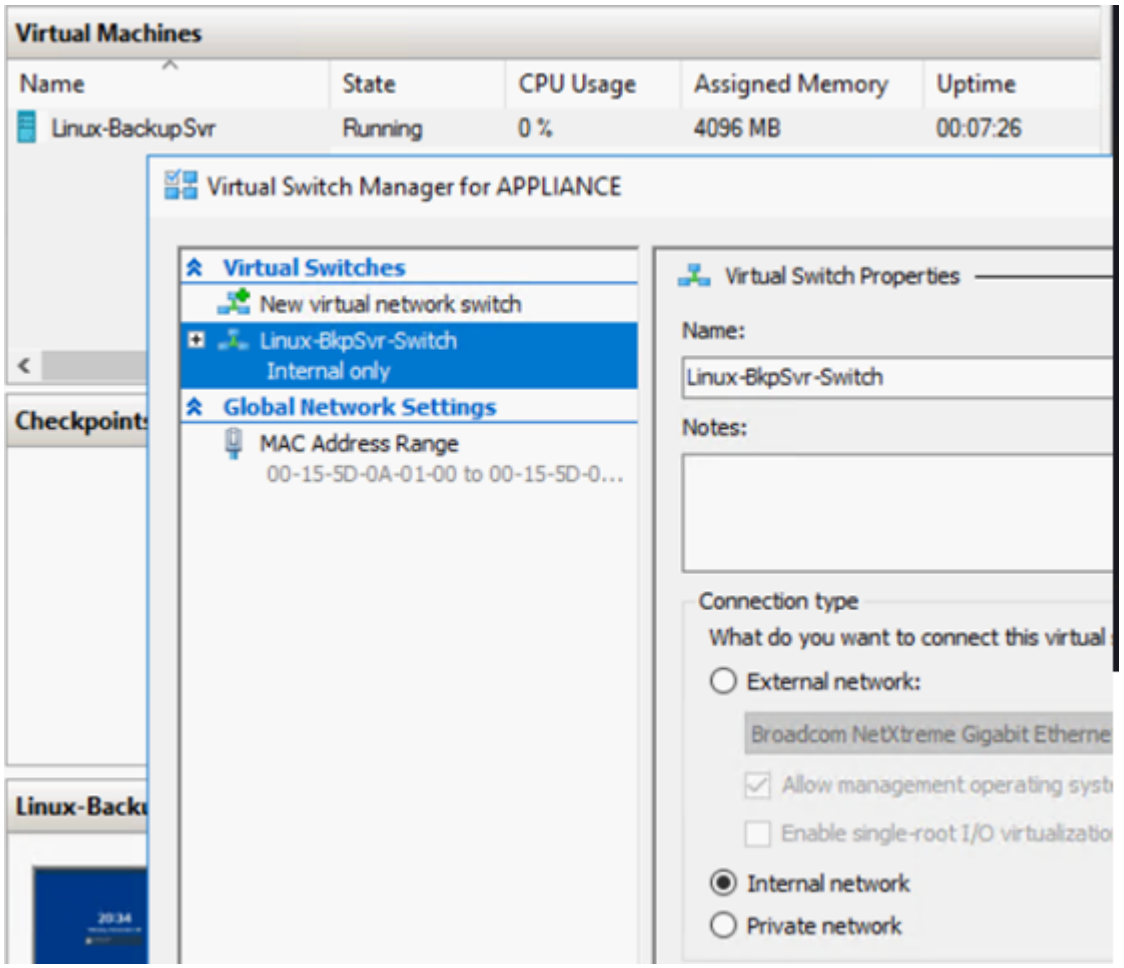
Understanding the Network Configuration Details

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:

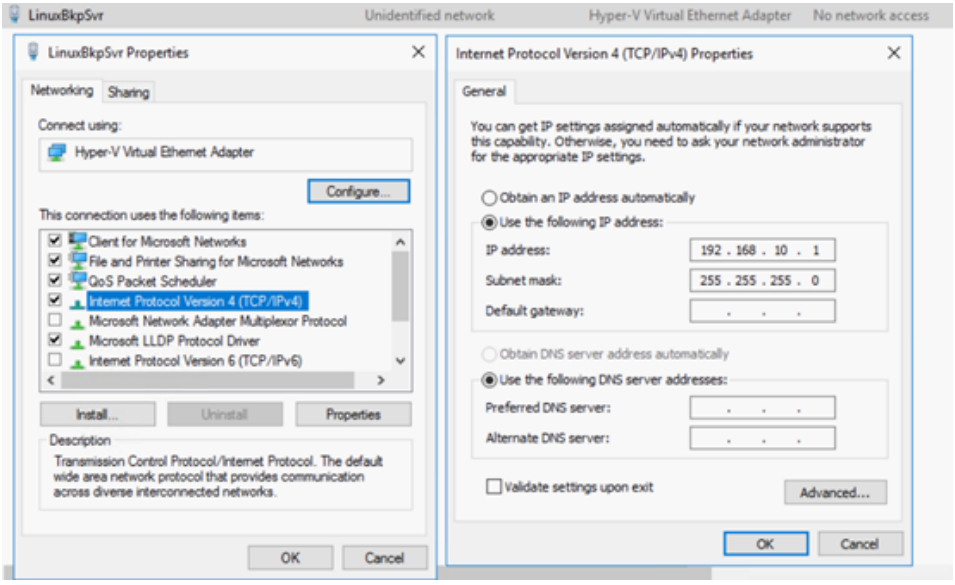
- User does not need to change the host name of the built-in Linux.
- User saves an IP on the network for the Linux Backup Server.
- The Linux Backup Server can connect to any machine on the public network.
- Any machine on the public network can connect to the Linux Backup Server through the special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

Network Configuration Details:

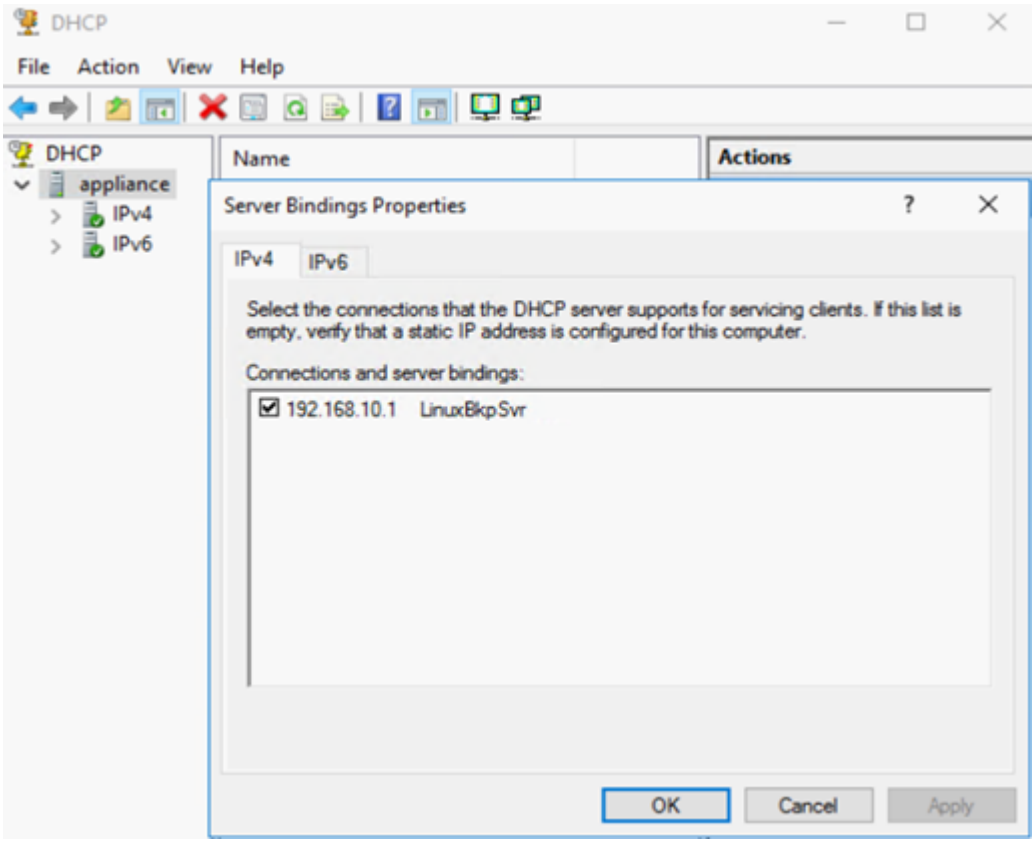
- On the Hyper-V Manager, an internal only virtual switch – *Linux-BkpSvr-Switch* is available that is used only by Linux-BackupSvr.



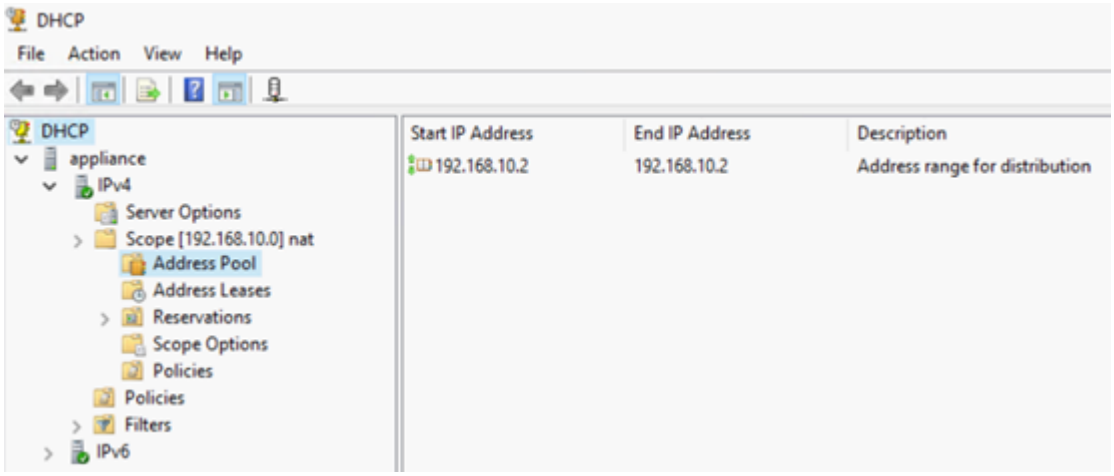
- In the *Control Panel\Network and Internet\Network Connections*, you can see "Hyper-V Virtual Ethernet Adapter" named as "LinuxBkpSvr". You have configured the IPv4 for this switch as "192.168.10.1" by default as below.



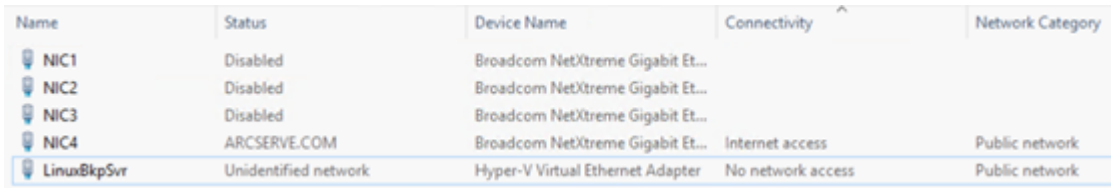
- You have configured DHCP Server on the appliance machine by default. The DHCP Server works only on the Hyper-V virtual adapter.



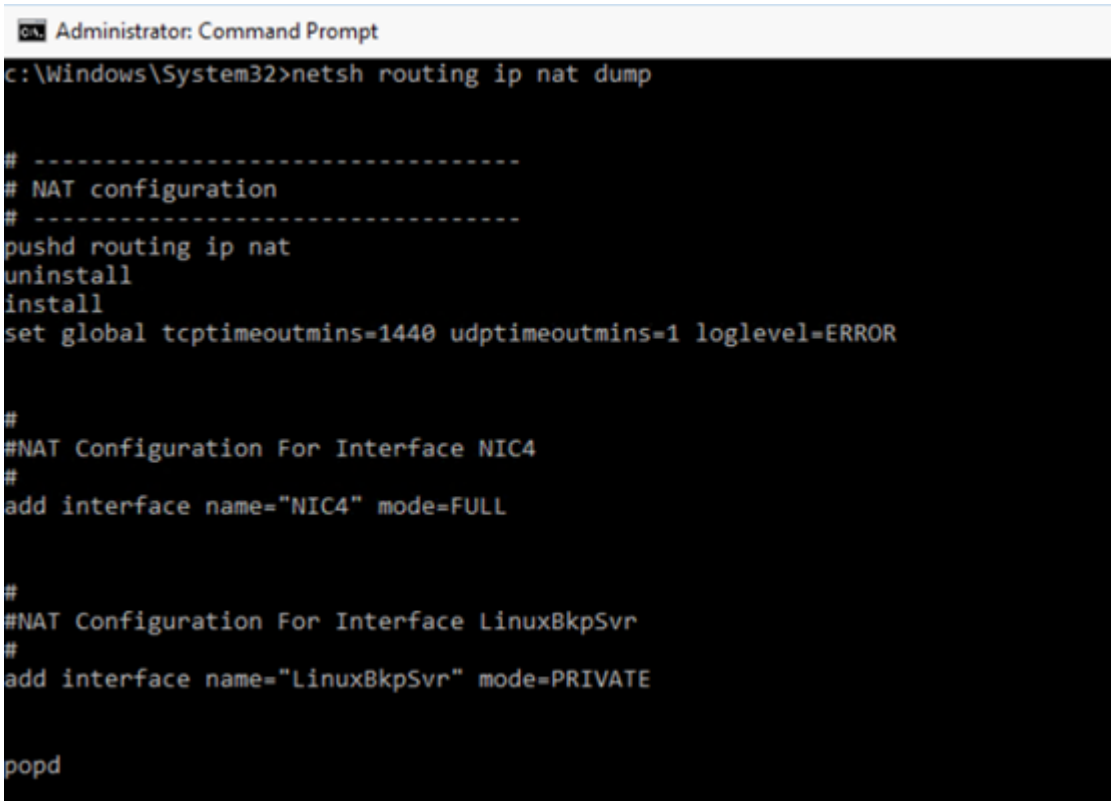
- By default, only one 192.168.10.2 in the Address Pool to ensure the built-in Linux Backup Server can get the IP 192.168.10.2.



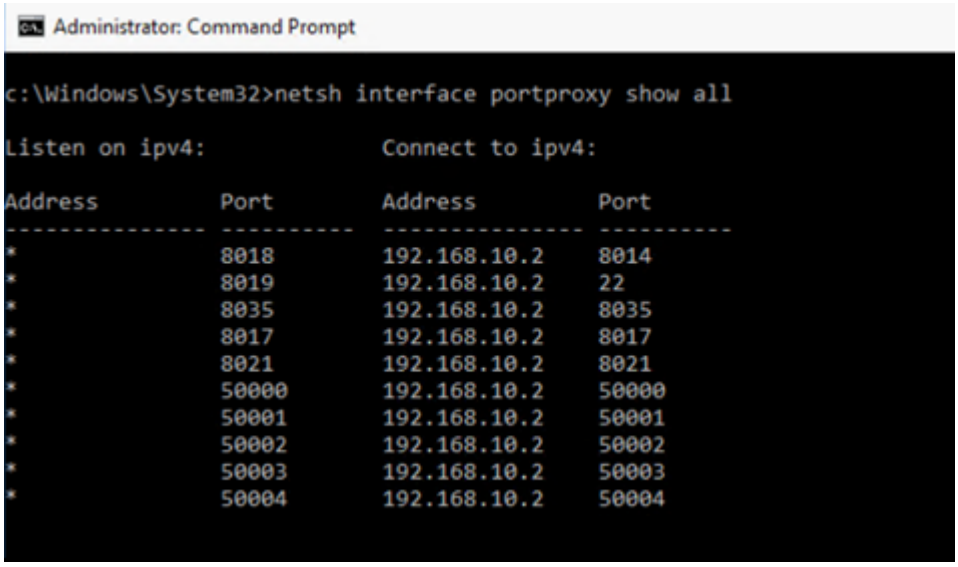
- We have configured NAT on the Appliance machine.



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 Configure the NIC Teaming Process

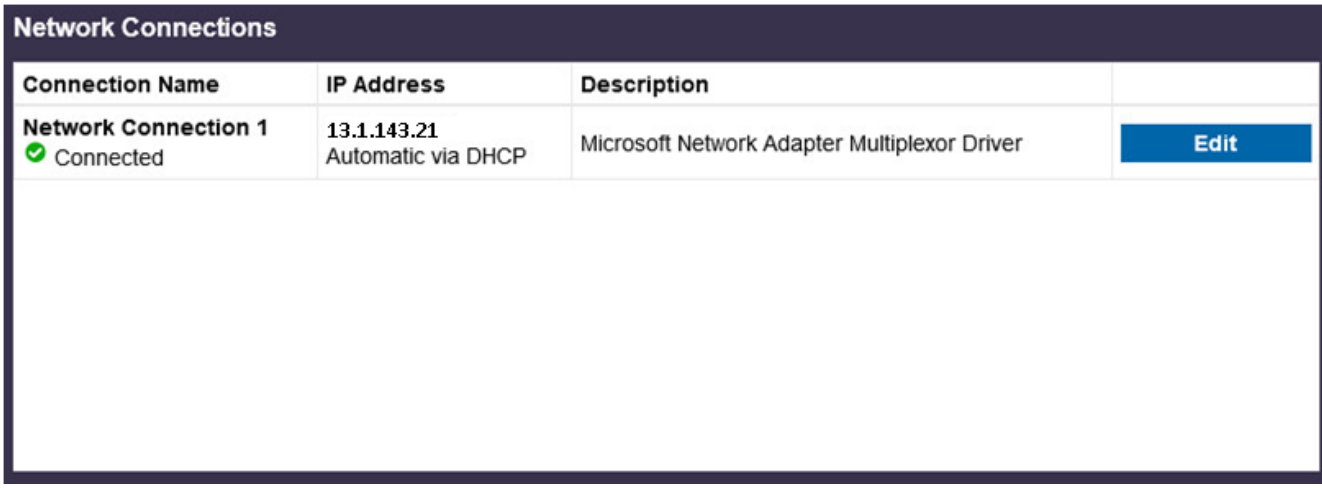
The Arcserve Appliance contains built-in Ethernet ports. To use these ports, an Ethernet NIC teaming needs to be configured. NIC Teaming allows multiple network adapters placed into a team for bandwidth aggregation and traffic failover to maintain connectivity in the event of a network component failure.

To configure a working NIC Team, a network switch supporting the link aggregation is required. Consult your network switch vendor and Microsoft Windows Configuration document to configure the NIC Team.

After the network switch is configured, follow these steps:

1. From Windows desktop, launch the Arcserve Appliance Wizard.

   Note: If a DHCP or static IP address is used, you can configure the IP address for the NIC Team in the Network Connections screen. Ensure that a valid IP address is assigned to the NIC Team and is available on your network.



2. From the Server Manager, select Tools > Routing and Remote Access. The Routing and Remote Access dialog opens.
3. Right-click the node of the Appliance Server and select Disable Routing and Remote Access.

   Note: If other routing and remote access functions are configured for other purposes, we recommend to reconfigure them again after completing these steps.

4. Click Yes on the confirmation dialog to disable the router and remove the configuration.

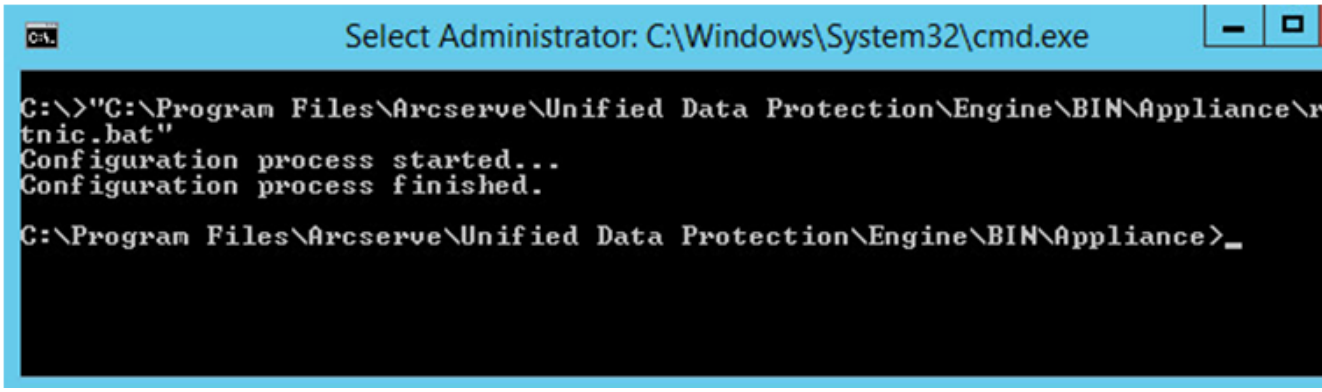
5. Right-click the node of the Appliance Server and select Configure and Enable Routing Remote Access.

   The Routing and Remote Access Server Setup Wizard opens.

6. Click **Cancel** and open a Windows Command prompt window.
7. Run the following command:

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

   The configuration completes and the following message appears.



   To verify that the configuration is working, log into the Linux Backup Server in the Hyper-V Manager and ping the IP address for the specific computers on your intranet. If this fails, review and repeat this procedure.

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

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

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

1. Open file *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Configuration\Appliance.properties*.
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.

   Note:

   - 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.
   - Please ensure “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 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 reset the IP address for network interface LinuxBkpSvr and the preinstalled Linux Backup Server.

   Note:

The preinstalled Linux Backup Server will shut down and restart during the process if you change the Linux_IPAddress.

6. Run the following command from the command prompt:

C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance>powershell .\resetdhcp.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 obtain IPAddress1 when sending a query for Altname1 and always obtain IPAddress2 when sending a query for Altname2.

Chapter 11: Understanding Safety Precautions

This section contains the following topics:

General Safety Precautions 235
Electrical Safety Precautions 237
FCC Compliance 238
Electrostatic Discharge (ESD) Precautions 239

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 that the appliance was shipped in 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 or on a table so that they will not be accidentally step on the components.

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

Electrical Safety Precautions

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

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

FCC Compliance

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

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

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

Electrostatic Discharge (ESD) Precautions

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

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

Chapter 12: Troubleshooting

This section contains the following topics:

Linux Backup Server Fails to Connect from the Console 241

Backing Up Arcserve Appliance from Another Appliance Reports Duplicated Nodes ... 242

Linux Backup Server Cannot Communicate with Any Node in the Network 244

Linux Backup Server Cannot Get the Network DNS Suffix 246

Default Time Zone on the Appliance 247

Licenses Error even when the licenses are available 248

Arcserve UDP Console Shows Error while adding Remote Console in Replicate to a Remotely Managed RPS Task 249

Unable to Perform VSB Task Using Another Appliance as Monitor 251

IVM Job Fails to Create Linux IVM to ESXi Server with HBBU Session on Appliance Data Store 253

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 data store 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 Data Store 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 data store 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. Navigate to the following location and launch Routing and Remote Access management:

   ```
   Server Manager > Tools > Routing and Remote Access
   ```

5. 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.

6. Right click the server name and select *Disable Routing and Remote Access*.
7. After disabling Routing and Remote Access, close the Routing and Remote Access management console.
8. Delete the file *dhcpdone.flag* from the following location:

   ```
   C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance
   ```

9. 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-08:00) Pacific Time (US & Canada) 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

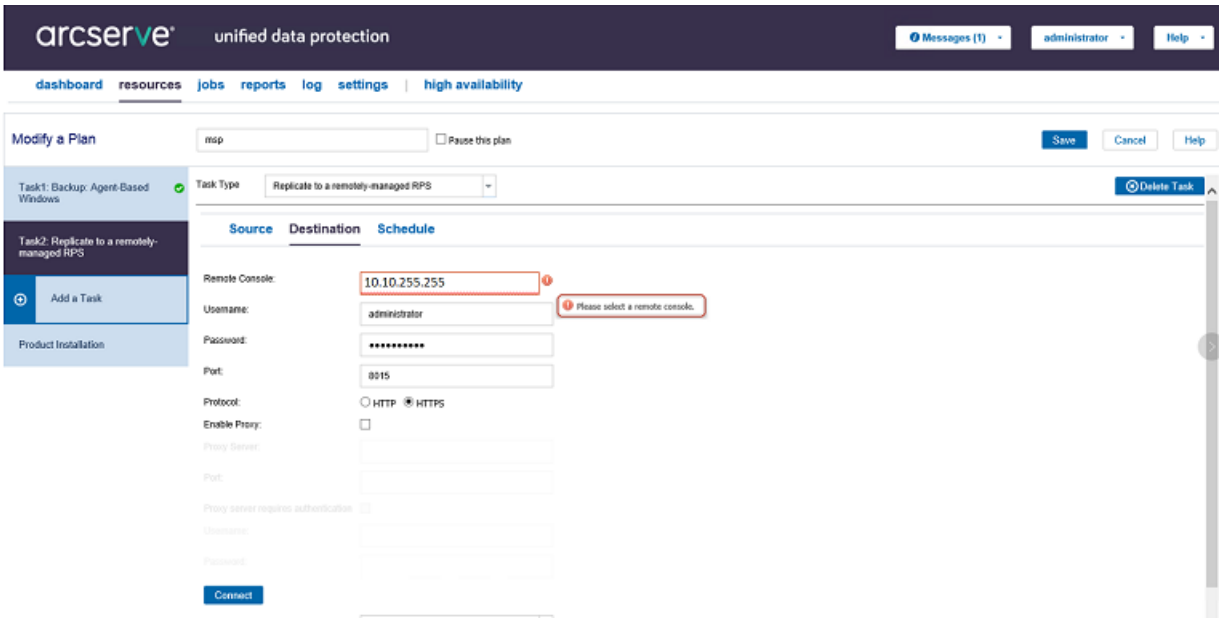
For more information on license related errors in the Appliance even when the licenses are available, refer the link.

Arcserve UDP Console Shows Error while adding Remote Console in Replicate to a Remotely Managed RPS Task

In Arcserve Appliance v6.5 Update1 if you add a *Replicate to a remotely managed RPS* task and enter the hostname/IP of a different appliance machine as Recovery Point Server (RPS) in the *Remote Console* field, then the below error message is displayed in the Arcserve UDP Console.

Note: This issue is fixed in Arccserve Appliance that has default version of Arcserve UDP v6.5 Update 3 or higher.

Error message: *Please select a remote console*



This issue is caused due to the use of same GUID on local console and remote console.

To support remotely managed RPS task to another appliance, follow these steps:

1. Delete the GUID in local Appliance from the following registry path:

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

2. Delete the GUID from the database using the following commands in PowerShell:

```
$database = 'arcserveUDP'
$server = 'localhost\arcserve_app'
```

```
$sqlconn = New-Object System.Data.SqlClient.SqlConnection
$sqlconn.ConnectionString = "Data Source=$server;Initial Cata-
log=$database;Integrated Security=SSPI;"
$sqlconn.Open()
$sqlcmd = New-Object System.Data.SqlClient.SqlCommand
$sqlcmd.Connection = $sqlconn
$sqlcmd.CommandText = "delete from as_edge_configuration where Para-
mKey='ConsoleUuid'"
$sqlcmd.ExecuteNonQuery()
$sqlconn.Close()
```

3. Restart UDP management service on the local appliance machine.
4. Perform the following steps, in the UDP Console of local machine:
    a. Select **All nodes** in Nodes view.
    b. Right click and click **Update**.
    c. Click **OK** to update all the nodes.
5. Select all RPS nodes in Recovery Point Servers view, right click and click **Update** to update all RPS nodes.

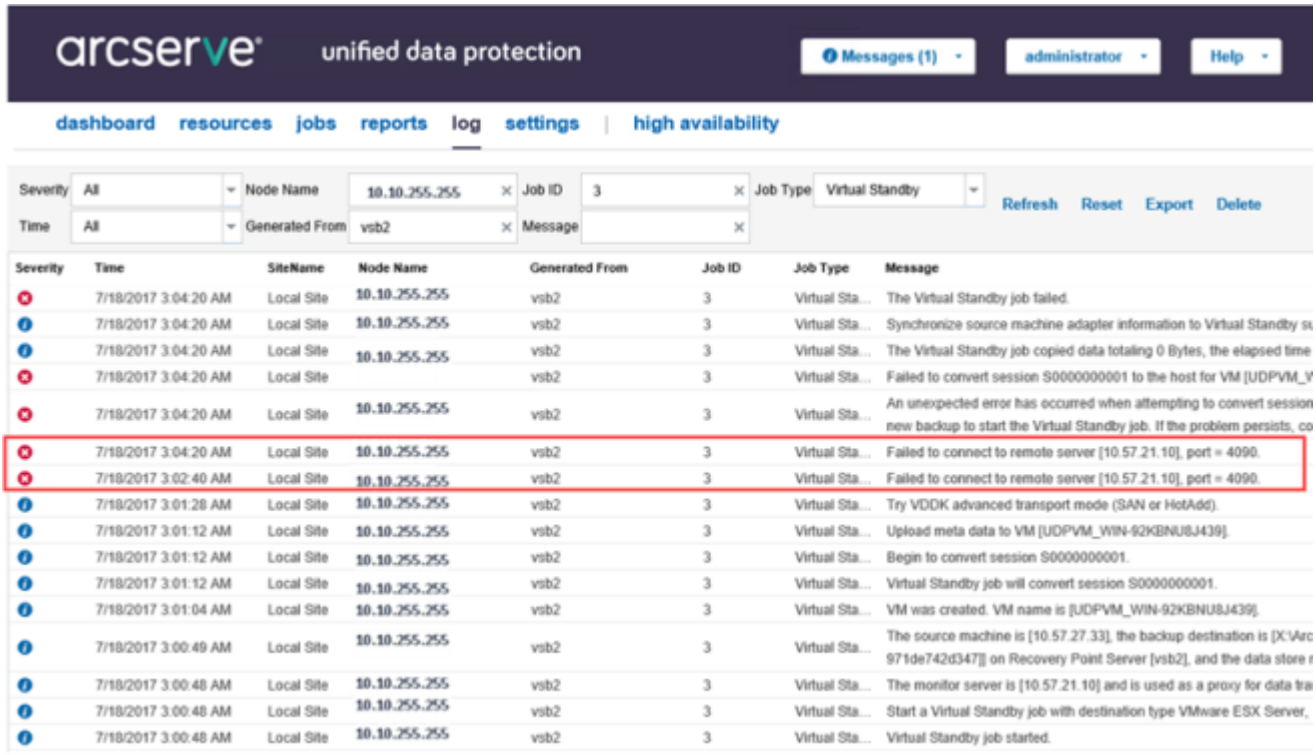
The *Replicate to a remotely managed RPS* task is supported successfully between two Appliance machines.

Unable to Perform VSB Task Using Another Appliance as Monitor

On the Arcserve Appliance> v6.5 Update1 if you perform VSB task and use another Appliance as monitor, the VSB task fails and the below error message is displayed in the activity log.

Note: This issue is fixed on Arcserve Appliance that has default version of Arcserve UDP v6.5 Update 3 or higher.

Error message: *Failed to connect to remote server [IP], port = 4090.*



This issue is caused due to the same GUID present in both monitor Appliance and Arcserve UDP RPS Appliance machine.

To support VSB task, follow these steps:

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

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

2. Delete the GUID from local Appliance using the following registry path:

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

3. Start all the UDP services on Arcserve UDP RPS Appliance using the following command in the command line:

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

4. From the UDP Console of local machine, follow these steps:
   a. Select **All plans** in Plans view.
   b. Right click and click **Deploy Now**.
   c. Click **OK** to deploy all plans.

The Virtual Standby task is now supported.

IVM Job Fails to Create Linux IVM to ESXi Server with HBBU Session on Appliance Data Store

Symptom

The instant virtual machine (IVM) job fails when you create IVM to ESXi Server for Linux virtual machine and the following error appears in the job activity log:

Failed to create data store. Please verify if the same data store already exists on the ESXi Server.

Solution

This issue occurs if the Linux virtual machine is located on the ESXi Server with Host-Based Backup Session (HBBU) on Appliance Data Store.

Follow these steps:

1. Log into Linux backup server as root user.
2. Navigate to the following path:

   /opt/Arcserve/d2dserver/configfiles
3. Create a file with the name *server.env*.
4. Add the following text in the *server.env* file:

   export HBBU_VM_RESTORE_DISABLE=1
5. Save and close the *server.env* file.
6. Run the following command to restart the service:

   #/opt/Arcserve/d2dserver/bin/d2dserver start

Chapter 13: Applying Best Practices

This section contains the following topics:

Best Practices for Network Configuration 255

Best Practices for Windows Defender with PowerShell cmdlets 258

Best Practices for Network Configuration

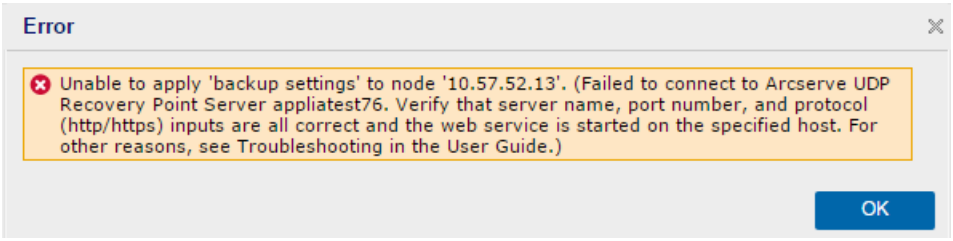
- If multiple network interfaces are connected in the production environment, ensure that each network adapter is connected to different sub network.
- If Linux node is not available in the production environment to protect, we recommend to stop the VM Linux-BackupSvr, DHCP Server service and RRAS on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

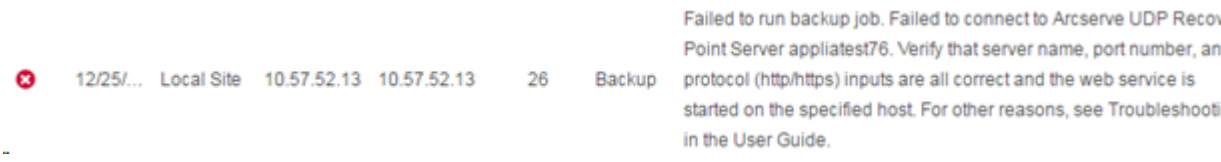
  Symptom

  If both the Appliance and Agent node 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 and RRAS 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:

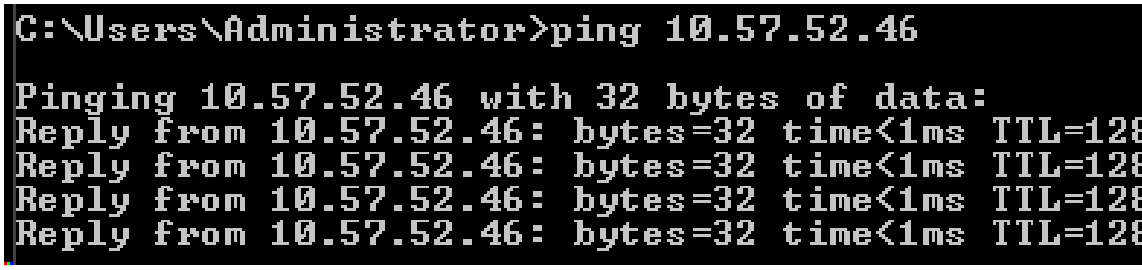
  Steps to be followed on Appliance:

  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  Me
          0.0.0.0          0.0.0.0      10.57.52.1      10.57.52.46
          0.0.0.0          0.0.0.0      10.57.52.1      10.57.52.35
          0.0.0.0          0.0.0.0      10.57.52.1      10.57.52.45
          0.0.0.0          0.0.0.0      10.57.52.1      10.57.52.47
       10.57.52.0    255.255.255.0         On-link      10.57.52.46
       10.57.52.0    255.255.255.0         On-link      10.57.52.35
       10.57.52.0    255.255.255.0         On-link      10.57.52.45
```

  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 Power-Shell 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.

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
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 1997-2015 Simon Tatham.* *Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, and CORE SDI S.A.* *Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:* *The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.* *THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND*

	NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Copyright Text	http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html *PuTTY is copyright 1997-2015 Simon Tatham.* *Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, and CORE SDI S.A.* *Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:* *The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.* *THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.*
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