# **User Guide**

Arcserve® Appliance Version 8.x OTCSETVE®

# **User Guide**

### Arcserve<sup>®</sup> Appliance

#### Version 8.x

The Table of Contents appears on the left pane. To view all topics, click the  $^{\rm OC}$  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.

© 2019 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 <u>arcserve.com/support</u> 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	1
Language Support	2
Product Documentation	3
Chapter 2: Introducing the Arcserve Appliance	5
Introduction	6
Arcserve Unified Data Protection	7
Arcserve Unified Data Protection Agent for Linux	8
Arcserve Backup	9
Arcserve Continuous Availability	10
Safety Precautions	11
What is Included in the Box	12
What is Included in the Box of Appliance 8000 Series	13
What is Included in the Box of Appliance 9000 Series	14
What is Included in the Box of Appliance X Series	14
What is Not Included in the Box	17
Available Models	18
Models 7100-7300v	19
Models 7400-7600v	21
Models 8100-8400	23
Models 9012 - 9504DR	24
Model X Series	25
Controls and Indicators	28
Front Panel of 7100-7300v	29
Front Panel of 7400-7600v	31
Front Panel of 8100-8200	33
Front Panel of 8300-8400	35
Front Panel of 9012-9048	36
Front Panel of 9072DR - 9504DR	38
Front Panel of X Series	38
Rear Panel of 7100-7300v	
Rear Panel of 7400-7600v	41
Rear Panel of 8100-8200	43
Rear Panel of 8300-8400	45

Rear Panel of 9012-9048	46
Rear Panel of 9072DR-9504DR	48
Rear Panel of X Series	49
Ports Used by the Appliance	50
Arcserve UDP	51
Components installed on Microsoft Windows	52
Components installed on Linux	57
Node protected by UDP Linux remotely	59
Arcserve Backup	60
Appliance for Linux Support	61
How to Add Ports to CentOS 6.6 x64 Firewall	62
Chapter 3: Installing the Arcserve Appliance	64
How to Install Arcserve Backup 18.0	65
How to Install 8100-8200 Series Appliance	67
How to Install 8300-8400 Series Appliance	
How to Install 9012-9048 Series Appliance	
How to Install 9072-9504DR Series Appliance	68
How to Install X Series Appliance	
Chapter 4: Upgrading Arcserve UDP on the Appliance	69
How to Apply a License After Upgrading Arcserve Software	70
Upgrade Sequence on Arcserve Appliance	71
Upgrade the Arcserve Appliance Used as Arcserve UDP Console and RPS	72
Upgrade the Arcserve Appliance Used as Arcserve UDP RPS	73
Upgrade Steps When Two or More Arcserve Appliance Are Used in the Environment	74
Upgrade the Arcserve UDP Linux Agent on the Arcserve Appliance	75
Upgrade the Arcserve Backup on the Arcserve Appliance	76
Upgrade Sequence for UDP Console, RPS, and Agent	77
Chapter 5: Configuring the Arcserve Appliance	78
How to Configure Network Settings for Arcserve Appliance	79
How to Set Up the Arcserve Appliance	83
Configure Arcserve Appliance as Gateway	92
Chapter 6: Working with Arcserve Appliance	93
Activate Arcserve Product on the Appliance	94
Create a Plan Using Arcserve Appliance Wizard	95
Add Nodes to a Plan	96

Add Nodes by Active Directory	99
Add vCenter/ESX Nodes	. 101
Add Hyper-V Nodes	
Create a Backup Plan for Linux Nodes	106
Create a Backup Plan to a Tape Device	107
Create an On-Appliance Virtual Standby Plan	108
Create Plan to Backup the Linux Backup Server	109
Setting-up to Perform Linux Instant VM Job to Local Appliance Hyper-V	113
Migrate Arcserve UDP Console Using ConsoleMigration.exe	114
Migrate Pre-installed Linux Backup Server to CentOS 7.4	116
Perform Migration between Arcserve Appliances	118
Solution 1	119
Solution 2	124
Modify the Input Source of Pre-installed Linux Backup Server	127
Chapter 7: Monitoring the Appliance Server Remotely	. 131
Working with IPMI	132
How to Change IPMI Password	133
How to Upgrade IPMI Firmware	136
Working with Integrated Dell Remote Access Controller (iDRAC)	137
Monitor and Manage Integrated Dell Remote Access Controller (iDRAC)	138
Find the IP address of Integrated Dell Remote Access Controller for 9000 Series (iDRA	C) 140
Find the IP address of Integrated Dell Remote Access Controller for X Series (iDRAC) .	142
Configure DHCP or Static IP address of iDRAC	144
Chapter 8: Restoring or Repairing the Arcserve Appliance	. 151
Debug Factory Reset	152
Apply Arcserve UDP Factory Reset Using Boot Option in 7000-8000 Series Appli- ance	154
Apply Arcserve UDP Factory Reset Using Boot Option in 9012-9504DR Series App ance	oli- 157
Apply Arcserve UDP Factory Reset Using Boot Option in X Series Appliance	159
Clear Configuration and Apply Appliance Factory Reset	162
Replace Factory Reset Image Using Set Appliance Image Utility	164
Remove and Replace a Hard Drive	167
Perform Bare Metal Recovery (BMR) without Preserving Data	169
Perform Bare Metal Recovery (BMR) and Preserving Data	184
Chapter 9: Performing Appliance Capacity Expansion	. 192
Working with Arcserve Appliance Expansion Kit - X Series Models	

Working with SSD Flash Expansion Kit in Arcserve X Series Appliance	196
Working with Expansion Kit in Arcserve Appliance 9072-9504 DR Models	206
Working with SSD Flash Expansion Kit in Arcserve Appliance 9072-9504 DR Models	211
Connecting Appliance Expansion Shelf to the Appliance Server (8000)	
Appliance Infield Expansion for all the Available Models	
What is included in the box	227
How to Connect the Appliance Expansion Shelf to the Appliance Server	230
How to Modify Arcserve UDP Data store	. 238
Adding a Data Path on Expansion Shelf to Arcserve UDP Data Store	239
Migrating Hash Destination to the new SSD	240
Checking the Overall Capacity of Data Store from Arcserve UDP Console	241
Resuming all the plans from Arcserve UDP Console	242
Chapter 10: Working with Network Configuration	244
Understanding the Network Configuration Details	245
How to Configure the NIC Teaming Process	250
How to Disable DHCP Server	252
How to Configure IP Address for the Preinstalled Linux Backup Server	253
How to Enable Round Robin on the DNS Server to Balance Load	255
How to Check Network Status on Appliance	256
Chapter 11: Understanding Safety Precautions	257
General Safety Precautions	258
Electrical Safety Precautions	260
FCC Compliance	261
Electrostatic Discharge (ESD) Precautions	262
Chapter 12: Activating Sophos on the Arcserve Appliance for 9000 Series	263
Method 1: Activate Sophos on the Arcserve Appliance using the email	264
Method 2: Activate Sophos on the Arcserve Appliance using script	265
Manually Installing Sophos Intercept X Advanced for Server on Arcserve UDP $\dots$	267
Chapter 12: Activating Sophos on the Arcserve Appliance for X Series	271
Manually Installing Sophos Intercept X Advanced for Server on Arcserve UDP $\dots$	271
Chapter 12: Upgrading Firmware for Arcserve Appliance 9000 Series	275
Upgrade BIOS Firmware for Arcserve Appliance 9000 Series	
Viewing BIOS Firmware Version	275
Method 1: View BIOS firmware version from iDRAC Web Interface	

Method 2: View BIOS firmware version from BIOS Arcserve Appliance 9000 series	
Download the Updated Package for BIOS	
Upgrade BIOS	277
Verify Updated BIOS	
Verify Updated BIOS using System Logs	
Verify Updated BIOS from iDRAC Web Interface or BIOS	
Upgrade iDRAC Firmware for Arcserve Appliance 9000 Series	279
Viewing iDRAC Firmware Version	279
View iDRAC firmware version from iDRAC Web Interface	
Method 2: View iDRAC firmware version from BIOS Arcserve Appliance 9000 series	
Download the Updated Package for iDRAC	
Upgrade iDRAC	
Verify Updated iDRAC	
Verify Updated iDRAC using System Logs	
Verify Updated iDRAC from iDRAC Web Interface or BIOS	
Upgrade Firmware for Arcserve Appliance X Series	
Upgrade BIOS Firmware for Arcserve Appliance X Series	285
Viewing BIOS Firmware Version	
Method 1: View BIOS firmware version from iDRAC Web Interface	
Method 2: View BIOS firmware version from BIOS Arcserve Appliance X series	
Download the Updated Package for BIOS	
Upgrade BIOS	
Verify Updated BIOS	
Upgrade iDRAC Firmware for Arcserve Appliance X Series	
Viewing iDRAC Firmware Version	
Method 1: View iDRAC firmware version from iDRAC Web Interface	
Method 2: View iDRAC firmware version from BIOS Arcserve Appliance X series	
Download the Updated Package for iDRAC	291
Upgrade iDRAC	
Verify Updated iDRAC	292
Chapter 13: Troubleshooting	
Linux Backup Server Fails to Connect from the Console	
Backing Up Arcserve Appliance from Another Appliance Reports Duplicated N	lodes295
Linux Backup Server Cannot Communicate with Any Node in the Network $\ldots$	
Linux Backup Server Cannot Get the Network DNS Suffix	298
Default Time Zone on the Appliance	

Licenses Error even when the licenses are available	
Arcserve UDP Console Shows Error while adding Remote Console in Replicat Remotely Managed RPS Task	
Unable to Perform VSB Task Using Another Appliance as Monitor	
Chapter 14: Applying Best Practices	
Best Practices for Network Configuration	
Best Practices for Windows Defender with PowerShell cmdlets	
Configure Preinstalled Linux Backup Server to External Network	
Best Practices for replacing Factory Reset Image When Secured by Sophos	
Best Practice for Creating Deduplication Data Store across Volumes	319
Chapter 15: Acknowledgements	321
PuTTY	

## **Chapter 1: About Arcserve Appliance Documentation**

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

This section contains the following topics:

Language Support	2
Product Documentation	3

#### Language Support

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
- Korean
- Portuguese (Brazil)
- Spanish

#### **Product Documentation**

For all Arcserve UDP related documentation, click this link for the <u>Arcserve Docu-</u><u>mentation</u>.

The Arcserve UDP Knowledge Center consists of the following documentation:

#### Arcserve UDP Solutions Guide

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

#### Arcserve UDP Release Notes

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

#### Arcserve UDP Agent for Windows User Guide

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

#### Arcserve UDP Agent for Linux User Guide

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

# **Chapter 2: Introducing the Arcserve Appliance**

This section contains the following topics:

Introduction	6
Safety Precautions	
What is Included in the Box	
What is Not Included in the Box	
Available Models	
Controls and Indicators	
Ports Used by the Appliance	

#### Introduction

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

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

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

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

Arcserve Appliance is defined with Hardware Warranty. Please visit <u>arc</u>-<u>serve.com/arcserve-appliance-warranty</u> 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 <u>Compatibility</u> <u>Matrix</u>.

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 <u>Arcserve UDP Solution Guide</u>.

#### **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 preinstalled in a virtual machine within the appliance. This virtual machine becomes the Linux Backup Server. Arcserve Unified Data Protection Agent for Linux is installed at the default installation path in the Arcserve Appliance.

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

**Note:** For more information about creating backup plans and restoring Linux machines, see <u>Arcserve UDP Agent for Linux User Guide</u>.

The Linux Backup Server uses the following default login information:

- Username root
- Password Arcserve

Note: We recommend to change the default password.

#### **Arcserve Backup**

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

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

Arcserve Appliance includes integration with Arcserve Backup for performing a backup to tape. Arcserve Backup 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 <u>doc</u>-<u>umentation</u>.

Arcserve Backup Server uses the following default login information:

- Username -- caroot
- Password -- Arcserve

#### **Arcserve Continuous Availability**

Arcserve Continuous Availability is a solution based on asynchronous real-time replication and automated application switchover and switchback to provide costeffective business continuity for virtual environments on Windows Servers. For more information about supported operating systems, see <u>Compatibility Matrix</u>.

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

**Note:** Arcserve Continuous Availability is not pre-installed in the Appliance. For more information about how to install and configure Arcserve Continuous Availability, see <u>Installation Guide</u>

#### **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 <u>Safety Precautions</u> <u>Appendix</u>.

# What is Included in the Box

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

- 8000 Series
- 9000 Series
- X Series

### What is Included in the Box of Appliance 8000 Series

The following items are included in the box:

- Arcserve Appliance (serial number label is located on rear side 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 <u>Arcserve Support</u>.

## What is Included in the Box of Appliance 9000 Series

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

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

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

**Note:** Inspect the box that the appliance was shipped in and ensure that no items are missing from the box and that there are no visible signs of damage. If any items are missing or damaged, retain all packaging materials and contact <u>Arcserve Support</u>.

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

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

### What is Included in the Box of Appliance X Series

Arcserve Appliance X series contains the following items:

- Appliance X Series Compute Node:
  - MICROSOFT
  - WIN SVR EMB STD 2019 16-CORE

Compute Node Accessory box:

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

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

#### Appliance X series Storage Node

The 5U storage system box includes the following:

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

ME4084 Accessory boxes:

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

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

**Note:** Inspect the box that the appliance was shipped in and ensure that no items are missing from the box and that there are no visible signs of damage. If any items are missing or damaged, retain all packaging materials and contact <u>Arcserve Support</u>.

#### 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
- Model X Series

## 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 capa- city*	3 TB	6 ТВ	6 TB	9 ТВ 9 ТВ			
Usable backup capacity**	2.8 TB	5.8 TB	5.8 TB	8.8 TB 8.8 T			
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 manageme backups, compress support, agentless backups, granular	sion, encrypt backup, rem	ion, WAN optim	nized replication dby, tape sup	on, advanced	virtualization		
On-Appliance Vir- tual Standby	N/A	N/A	Up to 3 VMs	N/A	Up to 3 VMs		
Warranty and Tech	nnical Specific	ations					
Full System Depot Warranty			3 Years				
Physical Dimen- sions (H x W x D in Inches)	1.7" x	17.2" x 25.6" (1	LU - 19" Rack	Mount rails pi	rovided)		
Remote man- agement and net- work interface ports	Remote man- agement and net- vork interface						
Hard Disk type and RAID con- figuration	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 Con- nectivity (SAS, SATA, FC)	1 x PASS						
Total system RAM	1 16 GB 16 GB 32 GB 32 GB 48 GB						
SSD drive	120 GB SSD	120 GB SSD	120 GB SSD	240 GB SSD	240 GB SSD		

					-		
(For dedu-							
plication hash							
tables)							
Maximum weight			41 lbs				
(lbs)		41 105					
Power Supplies							
(Single or redund-			1 x 600W				
ant)							
Power con-							
sumption	02/446/442	122/10/11/12	125/1077/1115	425/467/445	120/100/152		
(Watts @ idle/-	93/116/143	122/164/143	125/16//145	125/16//145	129/188/152		
load/startup)							
AC voltage & fre-			100 - 240v		·		
quency range			100 - 2400				
Ampere rating			7.5 Amp Max				
*1 TB = 1,000,000,	.000,000 byte	es.					
** 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,							
· · · · ·	, , -	, 5 - 11		// /	. ,, ,		

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 Cap	Backup Storage Capacity							
Raw Storage capa- city*	16 TB	16 TB	20 TB	20 TB	30 ТВ	30 ТВ		
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 managemer compression, encry agentless backup, re granular restore, un On-Appliance Vir-	ption, WAN emote virtua ified report	optimized repl al standby, tap ing and dashbo	lication, adv e support, a pard.	anced virtu	alization sup onsistent ba	oport,		
tual Standby	N/A	Up to 6 VMs	N/A	VMs	N/A	VMs		
Warranty and Techr	nical Specifica	ations		1	1			
Full System Depot Warranty			3 Yea	ars				
Physical Dimen- sions (H x W x D in Inches)	3.5'	' x 17.2" x 25.6	" (2U - 19"	Rack Moun	t rails provi	ded)		
Remote man- agement and net- work interface ports	nt and net- 1 x IPMI & 2 x 1 GbF (RI45) and 4 x 1GbF (RI45). 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 Con- nectivity (SAS, SATA, FC)	1 x PASS							
Total system RAM	64 GB	96 GB	64 GB	96 GB	128 GB	192 GB		
SSD drive	240 GB SSD	240 GB SSD	480 GB SSD	480 GB SSD	480 GB SSD	480 GB SSD		

	т	r	1		r		
(For deduplication							
hash tables)							
Maximum weight		52 lbs					
(lbs)			52 11	72			
Power Supplies							
(Single or redund-			2 x 92	20w			
ant)							
Power con-							
sumption	208/257/	208/257/	208/257/	208/257/	240/296/	240/296/	
(Watts @ idle/-	358	358	358	358	369	369	
load/startup)							
AC voltage & fre-			100 - 2	2401			
quency range			100 - 2	.400			
Ampere rating			11 Amp	Max			
*1 TB = 1,000,000,0	*1 TB = 1,000,000,000 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*	12TB-18TB	24TB-36TB	48TB-128TB	96TB-240TB						
System RAM	32GB	32GB	64GB	128GB						
Max RAM**	64GB/960	GB/160GB	96GB/128GB/192GB	160GB/192GB/256GB						
SSD drive	120GB SSD	200GB SSD	480GB SSD	1.2TB SSD						
Processor	E5-2609 V4, 8-CORE, 1.7GHZ	E5-2620 V4, 8-CORE, 2.1 GHZ	E5-2640 V4, 10- CORE, 2.4GHZ	E5-2650 V4, 12-CORE, 2.2GHZ						
RAID Card	936	1-4i	9361-8i							
RAID Con- figuration	RAID-5 v	vith BBU	RAID-6 with BBU							
Drive Bays	2	1	12							
Drives		3x 4TB SAS	6x 4TB SAS 12G 7x 4TB SAS 12G	6x 8TB SAS 12G 7x 8TB SAS 12G						
	12G 4x 2TB SAS 12G	12G	8x 4TB SAS 12G 9x 4TB SAS 12G 10x 4TB SAS 12G	8x 8TB SAS 12G 9x 8TB SAS 12G 10x 8TB SAS 12G						
			11x 4TB SAS 12G 12x 4TB SAS 12G	11x 8TB SAS 12G 12x 8TB SAS 12G						
DIMMs / Max DIMMs	4x 8GB DD	R4-2400/ 8	4x 16GB DDR4- 2400/ 8	4x 32GB DDR4-2400/ 8						
Cards	LSI SAS9200-8E									
Power Sup- plies	2x hot swap 500W AC	redundant Platinum	Two x 920W hot swap redundant high-effi- ciency 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 Appliance has additional RAM in order 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 9000 Series Specifications													
Appliance Model	901 <sup>.</sup> 2	902 4	904 8	9072- DR	9096- DR	9144- DR	9192- DR	9240- DR	9288- DR	9360- DR	9504DR			
Usable capacity	4 TB	8 TB	16 TB	24 TB	32 TB	48 TB	64 TB	80 TB	96 TB	120 TB	168 TB			
Source Backup	12 TB	24 TB	48 TB	72 TB	96 TB	144 TB	192 TB	240 TB	288 TB	360 TB	504 TB			
System RAM	6 x 8 GB (48 GB)		12 x 16 GB (192 GB)							12 x 32 GB (384 GB)				
Max RAM / DIMMS	176 GB / 10 DIMMS			576 GB / 24 DIMMS							768 GB / 24 DIMMS			
SSD drive	480	)GB S	SSD	2 x 1.9 TB SSD (RAID1)										
Processor	Intel Xeon Sil- ver 4108, 8- CORE, 1.8 GHz			Intel Xeon Silver 4114, 10-CORE, 2.2 GHz										
Number of Processors	1			2										
RAID Card	Low ada	C H7 v Pro apto NV Ca	file, r, 2	PERC H730P, MiniCard, 2 GB NV Cache										
RAID Con- figuration	RAID-5		RAID-6											
Drive Bays	4			16										
Expansion Kit	NA		11	10	8	6	4	6	4	NA				
RAID 2	NA		6											
Drives	3 x 2 TB	3 x 4 TB	3 x 8 TB	5 x 8 TB	6 x 8 TB	8 x 8 TB	10 x 8 TB	12 x 8 TB	10 x 12 TB	12 x 12 TB	16 x 12 TB			

Arcserve Appliance Models 9012 - 9504DR

Base PCIe	On-Board Broadcom	Broadcom 5720 QP 1Gb Network Daughter Card	Broad- com 5720 QP 1Gb SAS 12Gbps HBA
Cards	5720 Dual Port 1Gb LOM	_	External Dual Port 10G Base-T Copper
	SAS 12Gbps		
	HBA External		
	Controller		
	Dreedeere	Dual-Port 10G Copper Dual-Port 10G SFP+ Dual-Port FC 16G HBA	Dual-
	Broadcom 5719 Quad-		Port
PCIe Cards	Port 1G NIC		10G
(Factory			SFP+
Option)	Dual-Port		Dual-
option	10G Copper		Port FC
	Dual-Port		16G
	10G SFP+		НВА
	Dual-Port FC		
	16G HBA		
	Dual, Hot- Plug Podund		
Power Sup- plies	Plug, Redund- ant Power	Dual, Hot-Plug, Redundant Power Supply (1+1),	750 \/
	Supply (1+1),		750 VV
	550 W		
iDRAC Enterprise		1	

# **Model X Series**

Arcserve Appliance Model X Series

Arcserve Appliance X Series Specifications					
Appliance Model	X1000DR	X1500DR	X2000DR	X2500DR	X3000DR
Effective Capacity (TB) <sup>1</sup>	1,056	1,584	2,112	2,640	3,168
Maximum Effective Capa- city with Expansion Kits	3,168				

Note: Effective capacity takes global source deduplication into account and is approximately 3x the usable capacity of the HDDs and does not include SSDs. The actual backup capacity may vary based on factors such as data types, backup type, schedule, and so on.Disk Imaging and Disaster Recovery SoftwareArcserve UDP Premium Edition included Cybersecurity SoftwareTape Integration SoftwareArcserve Backup includedCybersecurity SoftwareSophos Intercept X Advanced for Server includedContinuous Availability with Automated FailoverArcserve UDP Cloud Hybrid Secured by SophosDisaster Recovery Add-onCompute NodeCPUDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVME SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External ControllerOptionalIntel X510 Qual Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 2G50 SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+F C AdapterOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Disipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	(TB) <sup>1</sup>	
actual backup capacity may vary based on factors such as data types, backup type, schedule, and so on. Disk Imaging and Disaster Recovery Software Tape Integration Software Cybersecurity Software Optional Cloud Backup and Disaster Recovery Add-on Continuous Availability with Automated Failover Optional Cloud Backup and Disaster Recovery Add-on CPU Default RAM Arcserve UDP Cloud Hybrid Secured by Sophos Dual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W) Default RAM 1,024 GB (16 x 64) DDR4-3200 RDIMM Max RAM 2,048 GB DIMM Slots 24 NVMe SSD Dive Bays 24 x 2.5" Enterprise NVMe SSD SAS 12Gbps HBA External Controller Intel X50 Quad Port 10G Base-T Adapter Broadcom 57414 Dual Port 25G SFP28 Adapter Broadcom 57414 Dual Port 2GB SFP28 Dual Port 10G SFP+FC Adapter Dual, Hot-plug, Redundant Power Supply (1+1), 1100W Heat Dissipation Arcserve UDP Cloud Port 20 Dual, Hot-plug, Redundant Power Supply (1+1), 1100W Heat Dissipation Arcserve UDP Cloud Port 20 Dual, Hot-plug, Redundant Power Supply (1+1), 1100W Heat Dissipation (excludes bezel, front 26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)		es global source deduplication into account and is
schedule, and so on.Disk Imaging and Disaster Recovery SoftwareArcserve UDP Premium Edition includedTape Integration SoftwareSophos Intercept X Advanced for Server includedContinuous Availability with Automated FailoverArcserve Continuous Availability optionalOptional Cloud Backup and Disaster Recovery Add-onArcserve UDP Cloud Hybrid Secured by SophosCPUDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24 x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External ControllerIncludedIntel X550 Quad Port 10G Base-T AdapterOptionalRedoctor S7414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight751bs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	approximately 3x the usable	capacity of the HDDs and does not include SSDs. The
Disk Imaging and Disaster Recovery SoftwareArcserve UDP Premium Edition includedTape Integration SoftwareArcserve Backup includedCybersecurity SoftwareSophos Intercept X Advanced for Server includedContinuous Availability with Automated FailoverArcserve Continuous Availability optionalOptional Cloud Backup and Disaster Recovery Add-onArcserve UDP Cloud Hybrid Secured by SophosCompute NodeDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External ControllerIncludedIntel X550 Quad Port 10G Base-T AdapterOptionalBroadcom 57414 Dual Port 12Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	actual backup capacity may	vary based on factors such as data types, backup type,
Arcserve UDP Premium Edition includedTape Integration SoftwareArcserve Backup includedCybersecurity SoftwareSophos Intercept X Advanced for Server includedContinuous Availability with Automated FailoverArcserve Continuous Availability optionalOptional Cloud Backup and Disaster Recovery Add-onArcserve UDP Cloud Hybrid Secured by SophosCPUDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External ControllerIncludedIntel X550 Quad Port 10G Base-T AdapterOptionalSreadcom 57414 Dual Port 12Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalRemote Hardware Man- agementDual, Hot-plug, Redundant Power Supply (1+1), 1100WPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bzel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	schedule, and so on.	
Recovery SoftwareArcserve Backup includedTape Integration SoftwareSophos Intercept X Advanced for Server includedCybersecurity SoftwareSophos Intercept X Advanced for Server includedContinuous Availability with Automated FailoverArcserve Continuous Availability optionalOptional Cloud Backup and Disaster Recovery Add-onArcserve UDP Cloud Hybrid Secured by SophosCPUDual Intel Xeon Gold 6258R 2.7G, 28C/S6T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External ControllerDaticudedIntel X50 Quad Port 10G Base-T AdapterOptionalRroadcom 57414 Dual Port 26Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalGlobe Fibre Channel HBA Remote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight7Slbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Disk Imaging and Disaster	Arcsonyo LIDP Promium Edition included
Cybersecurity SoftwareSophos Intercept X Advanced for Server includedContinuous Availability with Automated FailoverArcserve Continuous Availability optionalOptional Cloud Backup and Disaster Recovery Add-onArcserve UDP Cloud Hybrid Secured by SophosCompute NodeCPUDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External ControllerOptionalIntel X550 Quad Port 10G SGS FP28 AdapterIncludedBroadcom 57414 Dual Port 2GGb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Recovery Software	Alcselve obr Freihlum Edition Included
Continuous Availability with Automated FailoverArcserve Continuous Availability optionalOptional Cloud Backup and Disaster Recovery Add-onArcserve UDP Cloud Hybrid Secured by SophosCompute NodeCPUDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterOptionalBroadcom 57414 Dual Port 1GGb Fibre Channel HBAOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Tape Integration Software	Arcserve Backup included
Automated FailoverArcserve Continuous Availability optionalOptional Cloud Backup and Disaster Recovery Add-onArcserve UDP Cloud Hybrid Secured by SophosCompute NodeDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 12Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G GSFP+ FC AdapterOptionalQLogic 2692 Dual Port 1GGb Fibre Channel HBADual, Hot-plug, Redundant Power Supply (1+1), 1100WPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Cybersecurity Software	Sophos Intercept X Advanced for Server included
Automated FalloverArcserve UDP Cloud Hybrid Secured by SophosOptional Cloud Backup and Disaster Recovery Add-onArcserve UDP Cloud Hybrid Secured by SophosCPUDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 2GGb SFP28 AdapterOptionalIntel X10 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Continuous Availability with	Areconyo Continuous Availability entional
Disaster Recovery Add-onArcserve UDP Cloud Hybrid Secured by SophosCompute NodeCPUDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G GFP+ FC AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalIntel X710 Dual Port 10G SFP+ StreamentOptionalPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Automated Failover	Arcserve continuous Availability optional
Compute NodeCPUDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalGlogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Optional Cloud Backup and	Areconyce UDD Cloud Unbrid Secured by Sechos
CPUDual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s, 38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVME SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Disaster Recovery Add-on	Arcserve ODP Cloud Hybrid Secured by Sophos
CPU38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G GSFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)		Compute Node
38.5M Cache, Turbo, HT (205W)Default RAM1,024 GB (16 x 64) DDR4-3200 RDIMMMax RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G GSFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	CDU	Dual Intel Xeon Gold 6258R 2.7G, 28C/56T, 10.4GT/s,
Max RAM2,048 GBDIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware Man- agementDual, Hot-plug, Redundant Power Supply (1+1), 1100WPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	CPU	38.5M Cache, Turbo, HT (205W)
DIMM Slots24NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Default RAM	1,024 GB (16 x 64) DDR4-3200 RDIMM
NVMe SSD2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware Man- agementDual, Hot-plug, Redundant Power Supply (1+1), 1100WPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Max RAM	2,048 GB
Drive Bays24x 2.5" Enterprise NVMe SSDSAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware Man- agementDual, Hot-plug, Redundant Power Supply (1+1), 1100WPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 25Ibs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	DIMM Slots	24
SAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware ManagementDual, Hot-plug, Redundant Power Supply (1+1), 1100WPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 25lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	NVMe SSD	2 x 1.6TB (RAID-1) and 6 x 4TB (RAID-5)
SAS 12Gbps HBA External Controller2x IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware ManagementDual, Hot-plug, Redundant Power Supply (1+1), 1100WPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 25lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Drive Bays	24x 2.5" Enterprise NVMe SSD
ControllerZx IncludedIntel X550 Quad Port 10G Base-T AdapterIncludedBroadcom 57414 Dual Port 25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	SAS 12Gbps HBA External	
Base-T AdapterIncludedBroadcom 57414 Dual PortOptional25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10GOptionalSFP+ FC AdapterOptionalQLogic 2692 Dual PortOptional16Gb Fibre Channel HBAOptionalRemote Hardware ManagementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	•	2x Included
Base-T AdapterBroadcom 57414 Dual Port25Gb SFP28 AdapterIntel X710 Dual Port 10GSFP+ FC AdapterQLogic 2692 Dual Port16Gb Fibre Channel HBARemote Hardware ManagementOptionalPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat DissipationVeight75lbs (34kg)Form FactorIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Intel X550 Quad Port 10G	
25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Base-T Adapter	Included
25Gb SFP28 AdapterOptionalIntel X710 Dual Port 10G SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Broadcom 57414 Dual Port	
SFP+ FC AdapterOptionalQLogic 2692 Dual Port 16Gb Fibre Channel HBAOptionalRemote Hardware Man- agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	25Gb SFP28 Adapter	Optional
SFP+ FC AdapterOptionalQLogic 2692 Dual PortOptional16Gb Fibre Channel HBAiDRAC Enterprise IncludedRemote Hardware ManagementDual, Hot-plug, Redundant Power Supply (1+1), 1100WPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Intel X710 Dual Port 10G	Ontional
16Gb Fibre Channel HBAOptionalRemote Hardware ManagementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	SFP+ FC Adapter	Ορτιοπαι
16Gb Fibre Channel HBAiDRAC Enterprise IncludedRemote Hardware ManagementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	QLogic 2692 Dual Port	Ontional
agementiDRAC Enterprise IncludedPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	16Gb Fibre Channel HBA	Optional
agementDual, Hot-plug, Redundant Power Supply (1+1), 1100WPower SuppliesDual, Hot-plug, Redundant Power Supply (1+1), 1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Remote Hardware Man-	iDPAC Enterprise Included
Power Supplies1100WHeat Dissipation4100 BTU/hrWeight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	agement	
Weight75lbs (34kg)Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Power Supplies	
Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Heat Dissipation	4100 BTU/hr
Form Factor2UIn-rack Dimensions (excludes bezel, front26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)	Weight	75lbs (34kg)
In-rack Dimensions (excludes bezel, front 26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)		
(excludes bezel, front 26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)		
		26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)
	panel, and power supply	, , , , , , , , ,

handles)					
Outer Dimensions (includes					
bezel, front panel, and	29.6″ x	19.0" x 3.4"	(75.1 cm >	( 48.2 cm )	( 8.7cm)
power supply handles)					
Packaging Dimensions	38′	" x 26" x 12'	" (97cm x <del>6</del>	66cm x 30c	:m)
	Stora	ge Node			
16TB SAS 12G Hot-Plug	28	42	56	70	84
HDD	20	42	50	70	04
Minimum Usable Capacity	352	528	704	880	1056
Linear Expansion Capability	$\checkmark$	$\checkmark$	$\checkmark$	1	
with Optional Kits	V	V	V	$\checkmark$	
RAID Level	RAID-ADAPT				
RAID Controller	Dual 8-port SAS 12Gb Controller				
Hot-spare space on HDDs	Up to 64 TB				
Power Supplies	Dual, Redundant (1+1), 2200W				
Heat Dissipation	7507 BTU				
Weight	From 141lbs (64kg) to 298lbs (135kg)				
Form Factor	5U				
Outer Dimensions (includes	20 21"	v 10 01" v 0		7cm x 49 '	
bezel, front panel, and	38.31" x 19.01" x 8.75" (97.47cm x 48.30cm x				
power supply handles)			22.23cm)		

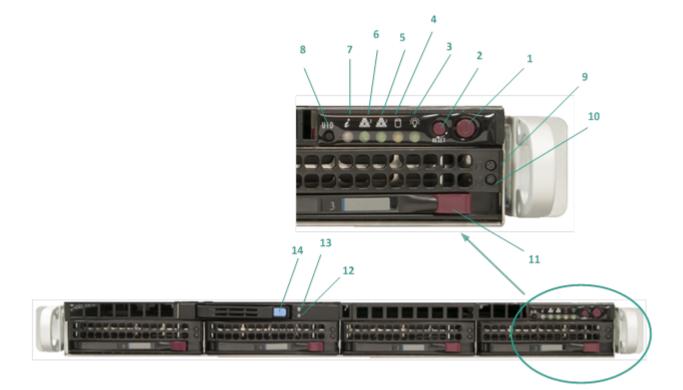
## **Controls and Indicators**

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

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

#### Front Panel of 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.



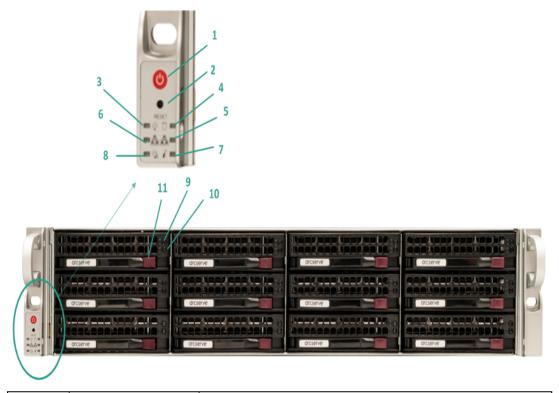
Number	Control / Indicator	Description
		Used to turn on and off power from the power supply
		to the appliance components. When turning off the
1	Power button	power, the main power is turned off but standby
1		power is still supplied. Therefore, to ensure power is
		completely removed from the appliance,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

		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.
7	Information LED	*Blinking Red - Slow (4 seconds): Power Failure. Check
/		for an inoperative power supply.
		Solid Blue: Local UID has been activated. Use this func-
		tion 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.
		Used to turn on or off the Universal Information LED
8	Unit Identifier (UID)	(blue) on both the front and rear appliance panels.
0	button	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.
	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
10		data is lost and the appliance continues to work nor-
		mally. Therefore, to guard against any problems asso-
		ciated 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.
<u>++</u>	Solid State Drive (SSD)	
12	LED	*Solid Red: Indicates drive failure.
13	Solid State Drive (SSD)	Solid Green: Indicates drive activity.
	LED	Blinking Green: Indicates the drive is being accessed.
14	Solid State Drive (SSD) Latch	Used to unlock and remove the SSD drive.
L	1	1

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

#### Front Panel of 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.



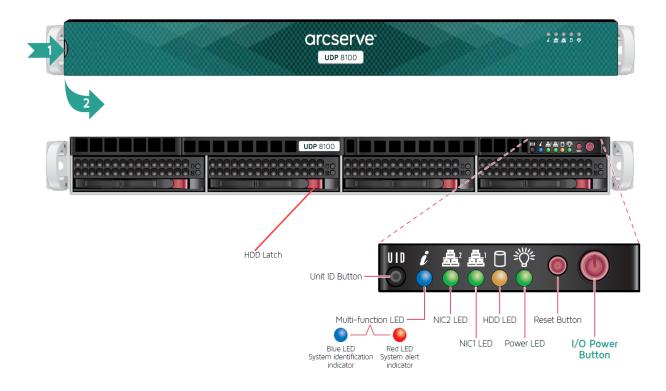
Number	Control/Indicator	Description
1	Power button	Used to turn on and off power from the power supply to the appliance components. When turning off the power, the main power is turned off but standby power is still sup- plied. Therefore, to ensure power is completely removed from the appliance, unplug 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 oper- ating.
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 (ETHO 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

	1	r
		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	Power Fail	Indicates a power supply module has failed.
9	Hard Drive (HDD) LED	Blinking Green: Indicates activity on the corresponding
5		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
10		of the drives will kick in immediately to ensure no data is
		lost and the appliance continues to work normally. There-
		fore, to guard against any problems associated with mul-
		tiple 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)	Used to unlock and remove the hard drive.
<u> </u>	Latch	

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

#### Front Panel of 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:



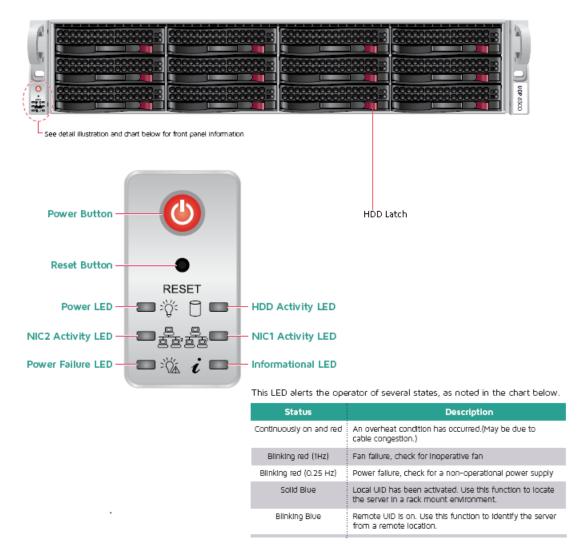
Control/Indicator	Description
I/O Power button	Used to turn on and off power from the power supply to the appli- ance components. When turning off the power, the main power is turned off but standby power is still supplied. Therefore, to ensure that power is completely removed from the appliance, unplug 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 (ETHO 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 inop-
	erative 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.
	Used to turn on or off the Universal Information LED (blue) on both
Unit Identifier (UID)	the front and rear appliance panels.
button	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.
	*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 appli-
Hard Drive (HDD) LED	ance 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	*Solid Red: Indicates drive failure.
(SSD) LED	
Solid State Drive	Solid Green: Indicates drive activity.
(SSD) LED	Blinking Green: Indicates the drive is being accessed.
Solid State Drive	Used to unlock and remove the SSD drive.
(SSD) Latch	

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

#### Front Panel of 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:



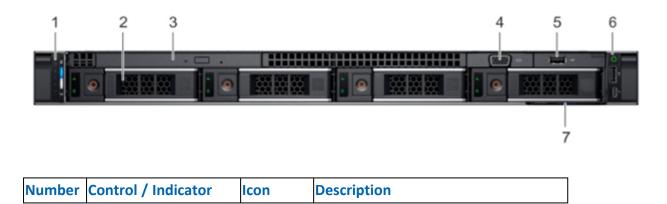
Control/Indicator	Description
	Used to turn on and off power from the power supply to the appli-
	ance components. When turning off the power, the main power is
Power button	turned off but standby power is still supplied. Therefore, to ensure
	power is completely removed from the appliance, unplug the power
	supply cable before performing maintenance.
Reset button	Used to reboot the appliance.
	Solid Green: Indicates that the power is being supplied to the power
Power LED	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).	
	<b>Continuously on and Red:</b> 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.	
Information LED	*Blinking Red - Slow (4 seconds): Power Failure. Check for an inop- erative power supply.	
	<b>Solid Blue:</b> 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.	
	*Solid Red: Indicates failure of the corresponding hard drive.	
Hard Drive (HDD) LED	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 appli- ance 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 <u>Arcserve Support</u>.

# Front Panel of 9012-9048

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



1	Left control panel	NA	<ul> <li>Contains the system health and system ID, status LED, and the iDRAC Quick Sync 2 (wireless) indicator.</li> <li>NOTE: The iDRAC Quick Sync 2 indicator is available only on certain configurations.</li> <li>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.</li> <li>Quick Sync 2 (wireless): Indicates a 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</li> </ul>
2	Drive slots	NA	more information, see <u>link</u> . Enable you to install drives that are sup- ported on your system. For more inform- ation about drives, see <u>link</u> .
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 <u>link</u> .
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 Inform- ation tag also contains the iDRAC secure default password.

# Front Panel of 9072DR - 9504DR

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



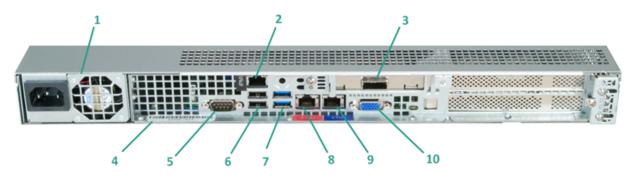
4

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

## **Front Panel of X Series**

For more information about the Front Panel, see <u>Appliance Installation of X Series</u> - <u>Compute Node</u> and <u>Appliance Installation of X Series - Storage Node</u>.

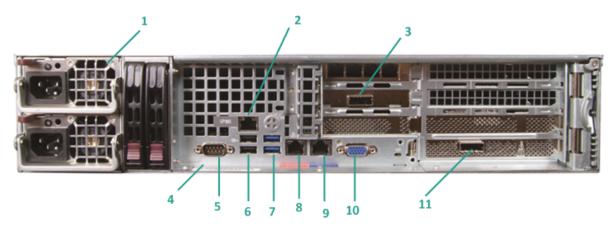
### Rear Panel of 7100-7300v



Number	Name of Con- trol/Indicator	Description	
1	Power Supply	Provides high-efficiency power supply to the appliance. <b>Note:</b> 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 main- tenance.	
2	IPMI Port (Remote Management)	The IPMI (Intelligent Platform Management Interface) por is used to monitor the physical health of Servers, such as temperature, voltage, fans, power supplies, and the appli- ance. <b>Note</b> : 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 <u>How to</u> 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	Used to transfer network data to and from the appliance.	

	Port 1	((ETH0 for Network 1)	
0	Network Data I/O	Used to transfer network data to and from the appliance.	
9	Port 2	(ETH1 for Network 2)	
10	VGA Connector	Used to connect a monitor to the appliance (if needed).	

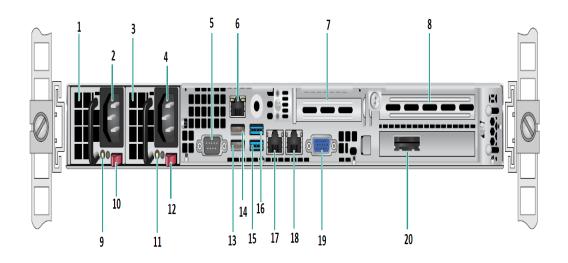
## Rear Panel of 7400-7600v



Number	Name of Con- trol/Indicator	Description	
	Dual Power Supply	Provides high-efficiency power supply to the appliance.	
1		<b>Note:</b> The main power switch is used to apply or remove power from the power supply to the appliance. The bene- fit of having a dual power supply is if one fails then the other is available for use.	
Ţ		Turning off the appliance power with this button removes the main power but standby power is still supplied. There- fore, to ensure power is completely removed from the appliance, unplug the power supply cable before per- forming 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 appli- ance.	
		<b>Note</b> : 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 <u>How to</u> <u>Change the IPMI Password</u> .	
	External Storage Device Port	Used to connect an external storage device (hard drive, tape drive, etc.) to the appliance. These portable external	
3	(SAS port for tape drive)	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).
11	External Storage Device Port (Tap Auto- loader/Library) LSI SAS 9212 - 4i4e	Used to connect an external storage device (Tape Auto- loader/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. <b>Note</b> : This port is present in the operating system as LSI Adapter SAS2 2008 Falcon.

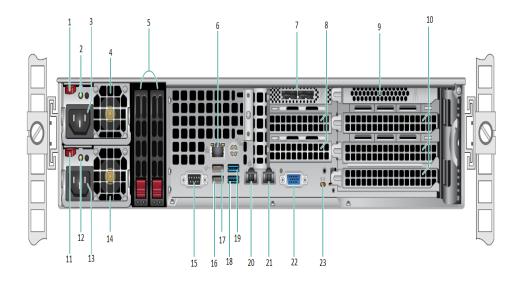
### Rear Panel of 8100-8200



Number	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	IPMI 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 of 8300-8400

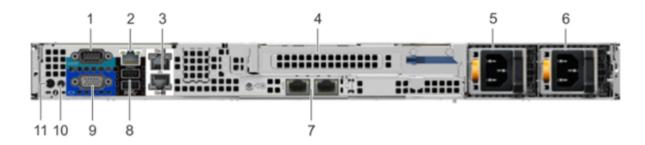


Number	Name of Control/Indicator
1	Power Supply Module #1 Lock
2	Power Supply Module #1 Power Good LED
3	Power Supply Module #1 AC Receptacle
4	Power Supply Module #1 Fan
5	Rear SSDs (optional)
6	IPMI Port (Remote Management)
7	External SAS HBA Ports
8	Half-length PCI Expansion Slots
9	Internal RAID 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 of 9012-9048**

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

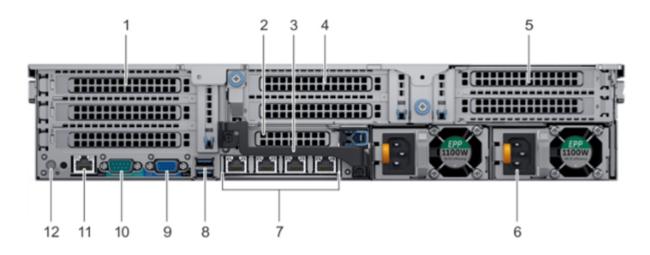


Number	Control / Indicator	lcon	Description
1	Serial port	10101	Use the serial port to connect a serial device to the system. For more information, see <u>link</u> .
2	iDRAC9 dedicated net- work port		Use the iDRAC9 dedicated network port to securely access the embedded iDRAC on a separate management network. For more information, see <u>link</u> .
3	Ethernet ports (2)	물급	Use the Ethernet ports to connect Local Area Networks (LANs) to the system. For more information, see <u>link</u> .
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 con- figurations, see link.
6	Power supply unit (PSU)		For more information about the PSU con- figurations, see <u>link</u> .
7	LOM riser ports (2)	문	For more information about the PSU con- figurations, see <u>link</u> .
8	USB 3.0 port (2)	ss~:-	Use the USB 3.0 port to connect USB devices to the system. These ports are 4-pin, USB 3.0-compliant.
9	VGA port		Use the VGA port to connect a display to the system. For more information, see <u>link</u> .
10	CMA power port		The Cable Management Arm (CMA) power port enables you to connect to the CMA.

11	System identification button	٢	<ul> <li>Press the system ID button:</li> <li>To locate a particular system within a rack.</li> <li>To turn the system ID on or off.</li> <li>To reset iDRAC, press and hold the button for 15 seconds.</li> <li>Notes:</li> <li>To reset iDRAC using system ID, ensure that the system ID button is enabled in the iDRAC setup.</li> </ul>
			<ul> <li>If the system stops responding during POST, press and hold the system ID but- ton (for more than five seconds) to</li> </ul>
			enter the BIOS progress mode.

# Rear Panel of 9072DR-9504DR

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



Number	Control / Indicator	lcon	Description
1	Full-height PCIe expan- sion card slot (3)	NA	The PCIe expansion card slot (riser 1) con- nects up to three full-height PCIe expansion cards to the system. For more information, see <u>link</u> .
2	Half-height PCIe expansion card slot	NA	The PCIe expansion card slot (riser 2) con- nects one half-height PCIe expansion cards to the system. For more information, see <u>link</u> .
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 expan- sion card slot (2)	NA	The PCIe expansion card slot (riser 2) con- nects up to two full-height PCIe expansion cards to the system. For more information, see <u>link</u> .
5	Full-height PCIe expan- sion card slot (2)	NA	The PCIe expansion card slot (riser 3) con- nects up to two full-height PCIe expansion cards to the system. For more information, see <u>link</u> .
6	Power supply unit (2)	NA	For more information, see <u>link</u> .
7	NIC ports	ठैठ	The NIC ports that are integrated on the net- work daughter card (NDC) provide network connectivity. For more information about the supported configurations, see <u>link</u> .

8	USB port (2)	\$\$ <del>~.</del>	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 <u>link</u> .
10	Serial port	10101	Enables you to connect a serial device to the system. For more information, see <u>link</u> .
11	iDRAC9 dedicated port	عراد	Enables you to remotely access iDRAC. For more information, see link.
12	System identification button	٤	The System Identification (ID) button is avail- able on the front and back of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step through mode.

### **Rear Panel of X Series**

For more information about the Rear Panel, see <u>Appliance Installation of X Series</u> - <u>Compute Node</u> and <u>Appliance Installation of X Series</u> - <u>Storage Node</u>.

# 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:

escription
ecifies the
fault com-
unication
ort between
e Arcserve
OP console
d Microsoft
L Server
tabases
nen they
side on dif-
rent com-
iters.
ote: You can
odify the
fault com-
unication
ort when
stalling SQL
rver.
ansfers data
r Virtual
andby tasks
the proxy
ode.
served for
cserve UDP
S Global
eduplication
ata Store Se
ce (GDD).
ne Arcserve
DP GDD data
ore will use
free ports
at start
DP GE ore w free p

				fram 5000 H		
				from 5000. It		
				is needed		
				when the data		
				store with		
				GDD is		
				enabled for		
				backup or the		
				restore task is		
				used.		
				Com-		
				munication		
				that lets the		
				Arcserve UDP		
		Arcserve		Console and		
6052	ТСР	lBackun	CA.ARCserve.CommunicationFoundation.	the Arcserve		
		GDB	WindowsService.exe	Backup Global		
				Dashboard		
				Primary		
				Server syn-		
				chronize data.		
				Com-		
			e CA.ARCserve.Com- municationFoundation.WindowsService.exe	munication		
				that lets the		
				Arcserve UDP		
				Console and		
6054	ТСР			the Arcserve		
				Backup		
				Primary		
				Server syn-		
				chronize data.		
				To shut down		
				Tomcat that is		
8006				used by the		
8000				Arcserve UDP		
				console.		
				Specifies the		
				default		
				HTTP/HTTPS		
		Arcserve		com-		
8014	ТСР		Tomcat7.exe	munication		
		sole		port between		
			sole			remote man-
				agement con-		
				soles and the		
				Arcserve UDP		

	1		1
			Server.
			Specifies the
			default
			HTTP/HTTPS
			com-
			munication
			port between
			remote man-
			agement con-
			soles and the
			Arcserve UDP
			Agent.
			Note: You can
			modify the
			default com-
			munication
			port when
			you install the
			Arcserve UDP
			components.
			Specifies the
			default
			HTTP/HTTPS
			com-
			munication
			port between
			the Arcserve
			UDP Server
			and Arcserve
			UDP consoles.
			*Specifies the
	Arcserve		default shared
8014			port and the
0014		httpd.exe	
	Server		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 dedu-
				plication
				enabled.
				<b>Note</b> : You can
				modify the
				default com-
				munication
				port when
				you install the
				Arcserve UDP
				components.
				Specifies the
				default
				HTTP/HTTPS
				com-
				munication
				port between
				remote man-
				agement con-
				soles and the
				Arcserve UDP
		Arcserve UDP Con		Server.
				Specifies the
				default
				HTTP/HTTPS
0045				com-
8015	ТСР		Iomcat7.exe	munication
		sole		port between
				remote man-
				agement con-
				soles and the
				Arcserve UDP
				Agent.
				Note: You can
				modify the
				default com-
				munication
				port when
				you install the
				Arcserve UDP
				components.
		Arcserve		
8016	тср	UDP	Tomcat7.exe	Reserved for
		Server		Arcserve UDP

		Server Web
		Services to
		communicate
		with the Arc-
		serve UDP RPS
		Port Sharing
		Service on the
		same Server.
		Note: The
		port cannot
		be customized
		and can be
		ignored for
		the firewall
		setting.
		To shutdown
		Tomcat that is
1800-	CA.ARCserve.CommunicationFoundation.	used by the
5	WindowsService.exe	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	ТСР	SSH ser- vice		Arcserve UDP Linux third party dependency. Spe- cifies the default for SSH service, however, you can change this port. This port is required for both incoming and out- going 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 com- munications. <b>Note</b> : 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 com- munications. <b>Note</b> : The port number cannot be customized.
8014	ТСР	Arcserve UDP Linux	Java	Specifies the default HTTP/HTTPS com- munication ports between the remote con- soles and the Arcserve UDP agent for Linux. This port is required for both incoming and outgoing communications.
18005	ТСР	Arcserve UDP Linux	Java	Used by Tomcat, can be ignored for firewall set-

		tings

## Node protected by UDP Linux remotely

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

Port	Port	Initiated	Listening	Description
#	Type	by	Process	
22		SSH ser- vice		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 incom- ing 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	ТСР			Microsoft Port Mapper
445	тср		MSRPC over the Named Pipes	
6050	TCP/UDP	CASUniver- salAgent	Univagent.exe	Arcserve Universal Agent
6502	тср	Arcserve Com- munication Found- ation	CA.ARCserve.Com- municationFoundation. WindowsService.exe	Arcserve Com- munication Foundation
6502	ТСР	CASTapeEngine	Tapeng.exe	Arcserve Tape Engine
6503	ТСР	CASJobEngine	Jobengine.exe	Arcserve Job Engine
6504	ТСР	CASDBEngine	DBEng.exe	Arcserve Data- base Engine
7854	ТСР	CASportmapper	Catirpc.exe	Arcserve PortMapper
41523	ТСР	CASDiscovery	casdscsvc.exe	Arcserve Dis- covery Service
41524	UDP	CASDiscovery	casdscsvc.exe	Arcserve Dis- covery Service
9000- 9500	ТСР		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:

			Description	
Type	y	1100033	NAT port redirection, redirects 8017 on appliance	
тср			to the Linux backup server in order to backup	
ICP			other Linux node to Amazon S3.	
ТСР			NAT port redirection, redirects 8018 on appliance	
			to the Linux Backup Server Agent port 8014.	
ТСР			NAT port redirection, redirects 8019 on appliance	
			to the Linux Backup Server SSH port 22.	
			NAT port redirection, redirects 8021 on appliance	
тср			to Linux backup server to backup other Linux node	
			using 8021 port.	
тср			NAT port redirection, redirects 8036 on appliance	
ICP			to the Linux Backup Server port 8036.	
			NAT port redirection, redirects 50000 on appliance	
ТСР			to Linux backup server in order to backup other	
			Linux node to cloud using 50000 port.	
			NAT port redirection, redirects 50001 on appliance	
ТСР			to Linux backup server in order to backup other	
			Linux node to cloud using 50001 port.	
			NAT port redirection, redirects 50002 on appliance	
ТСР			to Linux backup server in order to backup other	
			Linux node to cloud using 50002 port.	
			NAT port redirection, redirects 50003 on appliance	
ТСР			to Linux backup server in order to backup other	
			Linux node to cloud using 50003 port.	
			NAT port redirection, redirects 50004 on appliance	
ТСР			to Linux backup server in order to backup other	
			Linux node to cloud using 50004 port.	
	Туре ТСР ТСР ТСР ТСР ТСР ТСР ТСР ТСР	Type         by           TCP	TCP       Image: Constraint of the second seco	

## 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.
- 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 18.0	65
How to Install 8100-8200 Series Appliance	67
How to Install 8300-8400 Series Appliance	68
How to Install 9012-9048 Series Appliance	
How to Install 9072-9504DR Series Appliance	
How to Install X Series Appliance	68

### How to Install Arcserve Backup 18.0

Arcserve Backup 18.0 is not pre-installed on the appliance. You can install Arcserve Backup 18.0 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 18.0, otherwise go to step 2.

```
Checking Arcserve Backup installation environment ...
Select language for Arcserve Backup Installation:
1. Japanese (default)
2. English
Your choice [1]:
You select "Japanese". Are you sure? [y/n]:y
```

2. Enter the Administrator password and start the installation of Arcserve Backup 18.0.

Checking Arcserve Backup installation environment ... Enter Password for Administrator: \*\*\*\*\*\*\*\*\* Starting to install Arcserve Backup r18 (English). This may take up to 25 minutes. Please do not close this window or shutdown the appliance. Installing Arcserve Backup... Completed. Updating configurations of the Arcserve Backup server... Arcserve Backup r18 is installed successfully. UserName: caroot Password: Arcserve Press any key to continue ....

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 <u>Appliance Installation of 8100-8200</u>.

## 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 <u>Appliance Installation of 8300-8400</u>.

## 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 <u>Appliance Installation of 9012-9048</u>.

## 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 <u>Appliance Installation of 9072-9504DR</u>.

## How to Install X Series Appliance

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

For the complete installation process, see <u>Appliance Installation of X Series - Com-</u> <u>pute Node</u> and <u>Appliance Installation of X Series - Storage Node</u>.

# **Chapter 4: Upgrading Arcserve UDP on the Appliance**

This section contains the following topics:

How to Apply a License After Upgrading Arcserve Software	.70
Upgrade Sequence on Arcserve Appliance	71
Upgrade Sequence for UDP Console, RPS, and Agent	77

# How to Apply a License After Upgrading Arcserve Software

After upgrading Arcserve UDP to 8.0 or upgrading Arcserve Backup to 18.0, the original license key on the Arcserve Appliance will not work. To obtain the new license keys for Arcserve UDP 8.0 and Arcserve Backup 18.0, contact your account representative.

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

## **Upgrade Sequence on Arcserve Appliance**

The upgrade from Arcserve Appliance v5.0 to Arcserve UDP 8.0 could involve one of the following sequences:

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

# Upgrade the Arcserve Appliance Used as Arcserve UDP Console and RPS

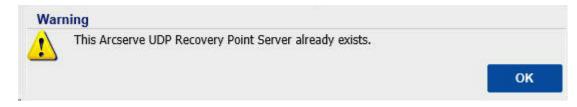
Upgrade this Arcserve Appliance, then follow up the <u>upgrade sequence</u> described to upgrade the environment.

# Upgrade the Arcserve Appliance Used as Arcserve UDP RPS

Upgrade the complete productive environment. For details, refer to the <u>upgrade</u> <u>sequence</u>.

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

- Upgrade the whole product environment. For details, refer to <u>upgrade</u> <u>sequence</u>.
- If you see warning as displayed below when you add an Appliance as RPS from Arcserve UDP Console after upgrade, refer to the <u>Backing Up Arcserve Appli-</u> <u>ance from Another Appliance Reports Duplicated Nodes</u> 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 <u>Arcserve Unified Data Protection Agent for Linux Online</u> <u>Help</u>.

# Upgrade the Arcserve Backup on the Arcserve Appliance

Refer to the <u>Arcserve Backup Implementation Guide</u> 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).
- 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	.79
How to Set Up the Arcserve Appliance	83
Configure Arcserve Appliance as Gateway	92

# 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.

Welcome to the A	Arcserve® Appliance Configuration Tool
	to connect your Arcserve Appliance to the LAN so that further configuration the web-based console UI.
	o the Appliance. This will be used to identify the Appliance on your local ou may add the Appliance to a Domain.
	me will require a reboot to take effect. You may configure the other settings uration screen before rebooting the Appliance.
Hostname	appliance ×
Add this Arcs	erve Appliance to a domain
Add this Arcs	serve Appliance to a domain
Add this Arcs	serve Appliance to a domain

**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.

erve Appliance			-	X
arcserve	Appliance Configuration	<b>e</b> 4	bout the Appliance	
Your Arcserve Appliance m Reboot Appliance	nust be rebooted for the Hostname a	nd Domain settings to take effect.		
Hostname/ Domain	appliance (not assigned)	Edit		
UDP Console URL	https://appliance:8015			
Date and Time	1/24/2019 11:53:51 PM	Edit		
Network Connections				
Connection Name	IP Address	Description		
SLOT 3 Port 1 S Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	Edit	^
SLOT 3 Port 2 3 Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #2	Edit	
SLOT 3 Port 3 ONt Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #3	Edit	
SLOT 3 Port 4 3 Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #4	Edit	
NIC1 ⊘ Connected	<b>10.57.25.39</b> Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #5	Edit	~

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

The Network Connection dialog opens.

NIC1					
Status	Connected				
Description	Broadcom NetXtreme Giga	bit Ether	met #5		
Connection	Use DHCP to obtain I	P addres	ss automa	atically.	
	IP Address	10	. 57	. 25	. 39
	Subnet Mask	255	. 255	255	. 0
	Default Gateway	10	. 57	. 25	. 1
	<ul> <li>Obtain DNS server ad</li> </ul>	dress au	utomatica	lly.	
	Preferred DNS Server	10	. 57	. 1	. 11
	Alternate DNS Server	10	. 64	. 1	. 11
		1	Sav	e	Cancel

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

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

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

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

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

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

The Arcserve Appliance Configuration screen appears.

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

		-	×
Appliance Configuration	<b>6</b> A	bout the Appliance	
ntinue configuring your appliance with	h the Arcserve UDP Plan Configuration Wizard.		
appliance (not assigned)			
https://appliance:8015			
1/25/2019 12:04:48 AM	Edit		
IP Address	Description		
None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	Edit	
None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #2	Edit	
None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #3	Edit	
None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #4	Edit	
10.57.25.39 Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet #5	Edit	
	appliance (not assigned) https://appliance:8015 1/25/2019 12:04:48 AM IP Address None Assigned Automatic via DHCP None Assigned Automatic via DHCP None Assigned Automatic via DHCP None Assigned Automatic via DHCP	appliance (not assigned)       appliance:8015         1/25/2019 12:04:48 AM       Edit         IP Address       Description         None Assigned Automatic via DHCP       Broadcom NetXtreme Gigabit Ethernet #2         None Assigned Automatic via DHCP       Broadcom NetXtreme Gigabit Ethernet #2         None Assigned Automatic via DHCP       Broadcom NetXtreme Gigabit Ethernet #2         None Assigned Automatic via DHCP       Broadcom NetXtreme Gigabit Ethernet #2         None Assigned Automatic via DHCP       Broadcom NetXtreme Gigabit Ethernet #3         None Assigned Automatic via DHCP       Broadcom NetXtreme Gigabit Ethernet #3	Antinue configuring your appliance with the Arcserve UDP Plan Configuration Wizard.

## How to Set Up the Arcserve Appliance

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

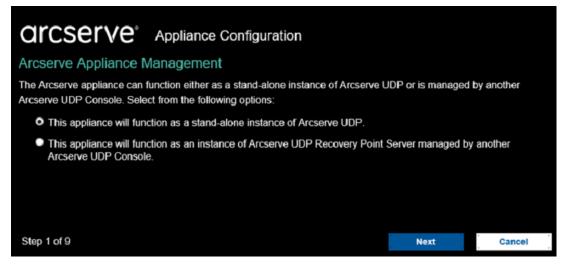
**Note:** If Appliance is configured in Domain, complete the Appliance wizard configuration using the Administrator login as a domain user cannot configure the appliance wizard.

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

#### Follow these steps:

1. Log into the Arcserve UDP console.

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



- 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 <u>Data Deduplication</u> in Arcserve UDP Solutions Guide.

Data Stores	e Appliance Con uration is shown below. More			the Arcserve UDP	<sup>2</sup> Console.
	Compression Deduplication	Standard Enabled			
	Encryption	Enabled			
Total Capacity 14.33 TB	Password				
	Confirm Password				
Step 2 of 9			Previous	Next	Cancel

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.

# **CICSEIVE**<sup>®</sup> Appliance Configuration

## Email and Alert

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

Enable email notifications.					
Service	Other	w			^
Email Server					
Port	25				
Email service requires a	uthentication.				
Subject	Arcserve Unified Data Protection Alert				
From					
Recipients	Separate email addresses with ;				
Options	■ Use SSL ■ Send STARTTLS ■ Use HTML format				
■ Connect using a proxy s	erver				
Send a Test Email					ľ
Send Alerts For	✓ Successful Jobs				V
Step 3 of 9		Previous	Next	Cancel	

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.

arcserve	Appliance Configuration			
Replication to Remote	e RPS			
Configure the settings below	if you want to replicate to a remotel	y-managed Recov	very Point Server de	stination.
<ul> <li>This appliance will replic Arcserve UDP Console URL</li> </ul>	ate to a remotely-managed RPS.			
Username				
Password				
Connect using a prox	y server.			
This appliance will not re	eplicate to a remotely-managed RPS	5.		
Step 4 of 9		Previous	Next	Cancel

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.

arcserve	Appliance Configuration			
Create a Plan			•••	bout Creating a Plan
	a protection plan for your data. In th one protection plan can be created.		you will add nodes	and configure a
Skip Plan Creation				
Plan Name	Protection Plan 1			
Session Password				
Confirm Password Output: Confirm Password	ssword. You will need it to restore th	he data.		
How do you want to add no	odes to the plan?			
	Hostname/IP Address (for Windows machi	ines only)	*	
Step 5 of 9		Previous	Next	Cancel

**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.

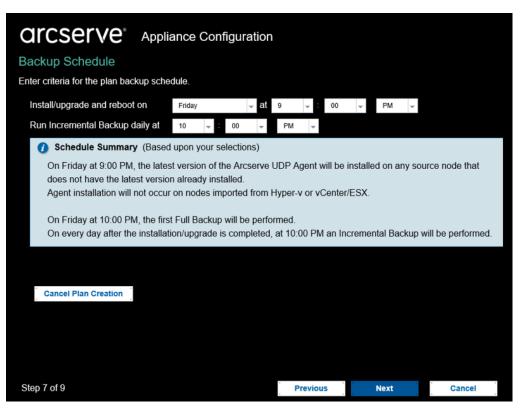
Importing from a Hyper-V Server

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.

arcserve <sup>®</sup> Ap	pliance Configuration		
Plan Confirmation			
This is a confirmation of the plan the	nat you created. You can edit pla	ns or create a new plan.	
Protection Plan 1	Plan Name	Protection Plan 1	
⊕ Add a Plan	Nodes Protected Destination	1 app7600	
	Install/Upgrade	Friday, 9:00 PM	
	Backup Schedule	Daily Incremental, 10:0	0 PM
	Edit Nodes Edit	Schedule Delete Plan	
Step 8 of 9		Previous Next	Cancel

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.

**Note:** To log into the UDP console using domain credentials, see <u>Assigning Admin</u> <u>Privileges and Roles to a Domain User</u>.

## **Configure Arcserve Appliance as Gateway**

You can configure Arcserve Appliance as Gateway.

#### Follow these steps:

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

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

# **Chapter 6: Working with Arcserve Appliance**

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

This section contains the following topics:

Activate Arcserve Product on the Appliance	94
Create a Plan Using Arcserve Appliance Wizard	
Add Nodes to a Plan	96
Create a Backup Plan for Linux Nodes	
Create a Backup Plan to a Tape Device	
Create an On-Appliance Virtual Standby Plan	108
Create Plan to Backup the Linux Backup Server	
Setting-up to Perform Linux Instant VM Job to Local Appliance Hyper-V	
Migrate Arcserve UDP Console Using ConsoleMigration.exe	
Migrate Pre-installed Linux Backup Server to CentOS 7.4	
Perform Migration between Arcserve Appliances	118
Modify the Input Source of Pre-installed Linux Backup Server	

## **Activate Arcserve Product on the Appliance**

For activating Arcserve product on the Appliance, see <u>Arcserve Product Licensing</u> <u>Online Help</u>.

### **Create a Plan Using Arcserve Appliance Wizard**

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

1. Add the nodes you want to protect.

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

- 2. Define the backup schedule.
- 3. Review and confirm the plan.



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

## Add Nodes to a Plan

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

Manually entering the node IP Address or hostname

(Add Nodes by Hostname/IP Address)

Discovering nodes from an active directory

(Add Nodes by Active Directory)

Importing virtual machine nodes from VMware ESX/vCenter Servers (Add vCenter/ESX Nodes)

Importing virtual machine nodes from Microsoft Hyper-V Servers (Add Hyper-V Nodes)

# Add Nodes by Hostname/IP Address

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

#### Follow these steps:

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

arcserve	Appliance Configuration			
Add Nodes by Hostn	ame/IP address		?	About Adding Node
Enter the hostname/IP addre	ess information for the selected Wind	ows nodes, to ad	d to the plan.	
Hostname/IP Address		Nod	es Protected by Pl	an
Username			Node Name	
Password		Use	the fields on the left to add r	nodes to the plan.
Description				
				Remove
Cancel Plan Creation				
Step 6 of 9		Previous	Next	Cancel

#### 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.

arcserve	Appliance Configuration			
Add Nodes by Active	Directory		e	About Adding Node
Enter the Active Directory info	prmation to add nodes to the plan.			
Username	domain\username	Noc	les Protected by P	lan
Password			Node Name	
Computer Name Filter	ż		the fields on the left to vali dentials and add the nodes t	
			_	
				Remove
Cancel Plan Creation				
Step 6 of 9		Previous	Next	Cancel

2. Click Browse.

The discovered nodes are displayed.

Add N	CSERVE® lodes by Active e Active Directory inf	Dire	ctory				About Adding Nod
Activ	ve Directory Results		Type node filter t	ext		×	Nodes Protected by Plan
	Name		Domain	Username	Verify		Node Name
	applia8400.ARCSERVE.0	сом	ARCSERVE.CO			~	Use the fields on the left to validate the node credentials and add the nodes to the plan.
	appliance1.ARCSERVE.0	COM	ARCSERVE.CO				creaendais and add the nodes to the plan.
	appliance2511.ARCSERV	/E.COM	ARCSERVE.CO			~	
<					>		-
M	Page 3 of 61	$\blacktriangleright = [M]$	2				
User	rname	administ	trator				
Pass	sword	•••••	••••  4	•	Apply		
1	Return			Add	l to List		Remove
Car	ncel Plan Creation						
	1						
Step 6 c	of 9						Previous Next Cancel

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:

 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.

arcserve	Appliance Configuration				
Add Nodes by vCent	er/ESX				About Adding Node
Enter the vCenter/ESX inform	nation to add nodes to the plan.				
Hostname/IP Address	1		Nodes	Protected by P	lan
Port	443		n N	ode Name	
Protocol	HTTPS		Use the	e fields on the left to add	nodes to the plan.
Username	root				
Password					
					Remove
Cancel Plan Creation					
Step 6 of 9		Previous		Next	Cancel

2. Click Connect.

The discovered hostnames are displayed.

3. Expand a hostname to see the nodes.

Add Nodes by vCenter/	ESX	n			About Adding Node:
vCenter/ESX Results	Type node filter text	×	Noc	es Protected by	Plan
Name	Object Type			Node Name	
a 🔲 📋 10.57.25	Host System	- 1		VM(agent node)	
▷ □	Resource Pool	^			
LinuxAgent	Resource Pool		_		
⊳ 🔲 🥱 restore	Resource Pool		_		
Virtual Lab 1	Resource Pool		_		
a 🔲 🦳 windows	Resource Pool		_		
📃 🧽 LicenseTesting	Resource Pool		_		
🔽 🔂 agent node	Virtual Machine	×	_		
Return	Add to	List			Remove
Cancel Plan Creation					
Step 6 of 9		P	revious	Next	Cancel

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.

Add Hyper-v Nodes Enter Hyper-v information to	Appliance Configuration		0	About Adding Node
Hostname/IP Address				
Username			Node Name	an
Password		Us	e the fields on the left to add r	nodes to the plan.
				Remove
Cancel Plan Creation				
Step 6 of 9		Previous	Next	Cancel

### 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.

Add Hyper-v Nodes	pliance Configuration odes to the plan.			,	3 About Adding Nod
Hyper-v Results	Type node filter text	×	Nod	es Protected by F	Plan
Name	Object Type			Node Name	
a 🔲 📑 🛔 10.57.25.	Hyper-v Host			app-hyv-02	
Backup-agent	Virtual Machine				
Backup-hbbu	Virtual Machine				
DPIVM_10.57.11	Virtual Machine				
UDPIVM_10.57.11.44725	Virtual Machine				
🔲 🚪 app-hyv-01	Virtual Machine				
V 🗃 app-hyv-02	Virtual Machine				
m 🚆 appliance-test3	Virtual Machine	$\sim$			
Return	Add to L	ist		1	Remove
Cancel Plan Creation					
Step 6 of 9		Pr	evious	Next	Cancel

- 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 <u>How to</u> <u>Create a Linux Backup Plan</u> 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 <u>Managing Devices and Media</u> 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 <u>Backing</u> <u>Up and Recovering D2D/UDP Data</u> 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 <u>How to Create a Virtual Standby Plan</u> 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.

Add nodes by Add Linux Node     Mode Name/IP Address     Inux-BackupSvr   SSH Key Authentication   User Name   Non-root Username   Password   Non-root Username   Password   Add Description     Add to List     Charlen Linux-BackupSvr	Add Nodes to	Arcserve UDP Console						
Node Name/IP Address Linux-BackupSvr   SSH Key Authentication   User Name rool   Password   Non-root Username   Password   Add Description	Add nodes by	Add Linux Node	•					
Node Name/IP AddressLinux-BackupSvrSSH Key AuthenticationUser NamerootPasswordNon-root CredentialNon-root UsernamePasswordAdd Description					Node Name	VM Name	Hypervisor	
SSH Key AuthenticationUser NamerootPassword••••••Non-root CredentialNon-root Username□Password□Add Description					You have not added any node to the list.			
User NamerootPassword•••••••Non-root CredentialNon-root UsernamePasswordAdd Description	1	Node Name/IP Address	Linux-BackupSvr					
Password   Non-root Credential   Non-root Username   Password   Add Description	6	SSH Key Authentication						
Non-root Credential   Non-root Username   Password   Add Description	L. L.	User Name	root					
Non-root Username       Password       Add Description	F	Password	•••••					
Password       Add Description	6	Non-root Credential						
Add Description	P							
		Password						
Add to List Remove	,	Add Description						
Add to List Remove								
Add to List Remove			_					
			Ad	d to List			Remove	
Help Save Can	Help						Save Can	cel

6. Click Save.

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

resources								
41	Nodes:	All Node	s					≫
Nodes	Actions	- A	dd Nodes	Filter ×	(No filter applied)	-		Configuration Wizard
All Nodes								
Nodes without a Plan		Status	Node Name	VM N	lame	Plan		Select a node to view the related details.
Plan Groups			linux-backupsvr					a crane.
Linux Backup Server Groups	-							
Linux Nodes								
Plans								
All Plans								
Destinations								
Recovery Point Servers								
Arcserve Backup Servers								
Shared Folders	1							
Cloud Accounts								
Remote Consoles								
Arcserve Cloud								
<ul> <li>Infrastructure</li> </ul>								
Storage Arrays								
Instant Virtual Machines								
Sites								
SLA Profiles								
	4						•	
	4 4 1	Page 1	of 1   🕨 🕅   ಿ			Displaying 1	- 1 of 1	

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

The **Source** tab appears.

resources					
Add a Plan	Agent-Based I	.inux Backup Plan	Pause this plan	Save	Cancel Help
Task1: Backup: Agent-Based Linux	Task Type	Backup: Agent-Based Linux	Y		Obelete Task
Add a Task	Sourc	e Destination Schedule	Advanced		
	Linux Backup	Server appliance	▼ Add		
	€Add	Remove			
	Node Na	ime VM Name Pi	an	Site	
	Filter volumes				

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

resources					
Add a Plan	Agent-Based Linux Backup Plan		Pause this plan	Save	Cancel Help
Task1: Backup: Agent-Based Linux	Task Type	Backup: Agent-Based Linux	•		ODelete Task
Add a Task	Sour	ce Destination Schedule	Advanced		
		Remove Nodes to Protect in Accenve UDP	v Add	Site	
	Filter volume	s for backup Exclude v			

The Select Nodes to Protect dialog opens.

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

Select	Nodes to Protect										
Ava	ilable Nodes	;			-	Sele	ected Nodes				
Group	s All Nodes (Def	ault Groups)	Ŧ								
	Node Name	VM Name	Plan	Site			Node Name	VM Name	Plan	Site	
	linux-backupsvr			Local Site			linux-backupsvr			Local Site	
					» > < «						
Hel		] of 1   🕨 🎽	🛛 🦑 Dis	playing 1 - 1 of 1						OK Can	

### 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.

resources							
Add a Plan	Agent-Based	Linux Backup Plan		Pause this plan		Save	Cancel Help
Task1: Backup: Agent-Based Linux	Task Type	Backup: Agent-Ba	sed Linux	¥			Delete Task
<ul> <li>Add a Task</li> </ul>	Sourc	e Destination	Schedule	Advanced			
	Destination Type	e	O Local disk or s	hared folder	e UDP Recovery Point Server		
	Recovery Point:	Ŝerver	appliance		¥		
	Data Store		appliance_data	_store ~			
	Password Prote	ction	<b>I</b>				
	Session Passwo	ord					
	Confirm Session	Password					

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

resources								
4	Plans: A	II Plans						≫
Nodes     All Nodes	Actions	- Add a Plan						Configuration Wizard
Nodes without a Plan		Plan Name		Nodes P	rotected		Status	Select a plan to view the related details.
vCenter/ESX Groups			Total	0	0	0		dound.
<ul> <li>Hyper-V Groups</li> <li>Linux Nodes</li> </ul>		Agent-Based Linux Backup Plan	1	0	1	0	Deployment: Successful (1)	
Linux Backup Server Groups	_							
Plan Groups								
⊿ Plans								
All Plans								
⊿ Destinations								
Recovery Point Servers								
Arcserve Backup Servers								
Shared Folders								
Cloud Accounts	4							
Remote Consoles								
Arcserve Cloud								

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

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

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

# Follow these steps:

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

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

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

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

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

# Migrate Arcserve UDP Console Using ConsoleMigration.exe

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

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



To complete the migration process, follow these steps:

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

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe -backupdb
Start Backup...
Backed up D8 and version files completed.
D8 and version files were created at: "C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\D8_Migration".
```

The DB\_Migration folder is created successfully.

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

<UDP\_Home> \Management\BIN\Appliance\

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

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

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

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



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

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

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

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

- 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.
- 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.

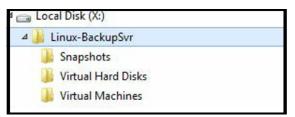
# Migrate Pre-installed Linux Backup Server to CentOS 7.4

**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. Also, upgrade Linux Agent on Linux Backup Server to the version similar to the version of Arcserve UDP console
- 3. Download the *Linux-BackupSvr.zip* from the <u>link</u> (the MD5 for this download is *OA51C1020CB8EA569B9DCEAF7BF226E0*) 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 <u>How to Migrate Arc</u>serve 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.

Intel         12/08/2016, 12.14.7.0         x64         C:\WINDOWS\INF\oem43.inf           Intel         07/30/2013, 9.4.2.10         x64         C:\WINDOWS\INF\oem43.inf           MS_HDC, INTEL_HDC         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\oem8.inf           ISI         03/06/2015, 6.707.0         x64         C:\WINDOWS\INF\oem8.inf           INTEL         08/19/2016, 10.1.2.80         x64         C:\WINDOWS\INF\oem45.inf           MD.Section, ACER.S         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\oem45.inf           INTEL         08/19/2016, 10.0.14         x64         C:\WINDOWS\INF\oem45.inf           MD.Section, ACER.S         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\oem45.inf           GENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\oem47.inf	ocess is launched.	[u ·		1.5.4
Intel         07/30/2013, 9.4.2.10         x64         C:\WIND0WS\INF\oem9.inf           MS_HDC, INTEL_HDC         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\oem9.inf           ISI         03/06/2015, 6.707.0         x64         C:\WIND0WS\INF\oem8.inf           NTEL         08/19/2016, 10.1.2.80         x64         C:\WIND0WS\INF\oem45.inf           MD.Section, ACER.S         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\oem45.inf           INTEL         07/30/2013, 9.4.2.10         x64         C:\WIND0WS\INF\oem45.inf           SENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\oem45.inf	Manufacturer	Version	Platform	Path
MS_HDC, INTEL_HDC         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\mshdc.inf           LSI         03/06/2015, 6.707.0         x64         C:\WIND0WS\INF\oem8.inf           NTEL         08/19/2016, 10.12.80         x64         C:\WIND0WS\INF\oem8.inf           AMD.Section, ACER.S         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\oem45.inf           NTEL         08/19/2013, 94.2.10         x64         C:\WIND0WS\INF\ousbpct.inf           NTEL         07/30/2013, 94.2.10         x64         C:\WIND0WS\INF\ousbpct.inf           GENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\machine.inf				
LST 03/06/2015, 6.707.0 x64 C:\WINDOWS\INF\oem8.inf INTEL 08/19/2016, 10.1.2.80 x64 C:\WINDOWS\INF\oem45.inf AMD.Section, ACER.S 06/21/2006, 10.0.14 x64 C:\WINDOWS\INF\oem47.inf INTEL 07/30/2013, 9.4.2.10 x64 C:\WINDOWS\INF\oem47.inf GENDEV_SYS, ACC 06/21/2006, 10.0.14 x64 C:\WINDOWS\INF\ome47.inf				
NTEL         08/19/2016, 10.1.2.80         x64         C:\WIND0WS\INF\oem45.inf           MD.Section, ACER.S         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\oem45.inf           NTEL         07/30/2013, 9.4.2.10         x64         C:\WIND0WS\INF\oem45.inf           BENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\oem45.inf				
AMD.Section, ACER.S         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\usbport.inf           INTEL         07/30/2013, 9.4.2.10         x64         C:\WIND0WS\INF\osem47.inf           GENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\machine.inf				
INTEL         07/30/2013, 9.4.2.10         x64         C:\WIND0\WS\INF\oem47.inf           GENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WIND0\WS\INF\machine.inf				
GENDEV_SYS, ACC 06/21/2006, 10.0.14 x64 C:\WINDOWS\INF\machine.inf	INTEL			
	Generic			

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

cserve Appliance			
arcserve	Appliance Configuration		3 About the Appliance
Click Launch Wizard to con Launch Wizard	tinue configuring your appliance wit	h the Arcserve UDP Plan Configuration V	Vizard.
Hostname/ Domain	appliance Microsoft Windows	×	
UDP Console URL	You must restart your co		
Date and Time	changes	Edit	
Network Connections	Before restarting, save any open	files and close all programs.	
Connection Name	IP Ad	t Now Restart Later	
SLOT 3 Port 1 S Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	Edit
SLOT 3 Port 2 3 Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	#2 Edit
SLOT 3 Port 3 3 Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	#3 Edit
SLOT 3 Port 4 3 Not Connected	None Assigned Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	#4 Edit
NIC1 Connected	10.57.25.39 Automatic via DHCP	Broadcom NetXtreme Gigabit Ethernet	#5 Edit

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

Run the following command with PowerShell:

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

			•
Name	Date modified	Туре	Size
setnat.ps1.log	5/10/2017 5:18 AM	Text Document	2 KB
inat.log	5/10/2017 5:18 AM	Text Document	6 KB
🚳 nat2.bat	5/10/2017 5:18 AM	Windows Batch File	2 KB
dhcpdone.flag	5/10/2017 5:17 AM	FLAG File	0 KB
resetdhcp.ps1.log	5/10/2017 5:17 AM	Text Document	2 KB
linuxdone.flag	5/10/2017 4:52 AM	FLAG File	0 KB
vmstarted.flag	5/10/2017 4:52 AM	FLAG File	0 KB
adapterNameChanged.flag	5/10/2017 4:52 AM	FLAG File	0 KB
language.txt	5/10/2017 1:19 AM	Text Document	1 KB
initstorage.ps1.log	5/9/2017 4:26 AM	Text Document	1 KB
setos.flag	5/9/2017 1:42 AM	FLAG File	0 KB
configuration_change.status	5/9/2017 1:39 AM	STATUS File	1 KB
configuration_change.flag	5/9/2017 1:39 AM	FLAG File	0 KB
ARCDiskCheck-Finish.tag	5/9/2017 1:39 AM	TAG File	0 KB
Rebuild-VMSwitch.ps1	Open	Windows PowerS	3 KB
resetdhcp.ps1	Run with PowerShell	Windows PowerS	23 KB
ApplianceInformation.ex	Edit	Application	30 KB
configuration_change.ps		Windows PowerS	19 KB
🚳 arcrun.bat	Open with	Windows Batch File	1 KB
initstorage.ps1	Restore previous versions	Windows PowerS	15 KB
E ARCDiskCheck.exe	Send to >	Application	130 KB
e setnat.ps1	Cut	Windows PowerS	4 KB
	Сору		

- 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.

resources			
Import a Data Store			
Recovery Point Server Data Store Folder Encryption Password	appliance X:\Arcserve\data_store\common •  Next		Browse
		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 <u>How to Migrate Arcserve UDP Console</u> <u>Using ConsoleMigration.exe</u>.

# 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

```
- 0
C: 9.
                  Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>cmdut
il.exe /stopall
Start to kill process explorer.exe
Killing process explorer.exe
Process killed.
 tart to kill process D2DVDgc.exe
Stopping service 'Arcserve UDP Agent Service'...
Service Stopped.
 topping service 'Arcserve UDP RPS Data Store Service'...
ervice Stopped.
Stopping service 'Arcserve UDP RPS Port Sharing Service'...
Service Stopped.
Stopping service 'Arcserve UDP Identity Service'...
Service Stopped.
Stopping service 'Arcserve UDP Management Service'...
Service Stopped.
Stopping service 'Arcserve UDP Management Port Sharing Service'...
Service Stopped.
Stopping service 'Arcserve UDP Agent Explorer Extension Service'...
Service Stopped.
Stopping service 'Arcserve UDP Update Service'...
Service Stopped.
Stopping Arcserve UDP agent monitor...
Arcserve UDP agent monitor stopped.
Start to kill Arcserve UDP processes
Killing process sync_utl_d.exe
Process killed.
Killing process AFD2DMonitor.exe
Process killed.
Killing process GDDServer.exe
Process killed.
Killing process GDDServer.exe
Process killed.
Killing process GDDServer.exe
Process killed.
Killing process AStartup.exe
Process killed.
Killing process explorer.exe
Process killed.
Stopping mounting driver...
Mounting driver stopped.
Start Windows Explorer.
```

- 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.

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

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

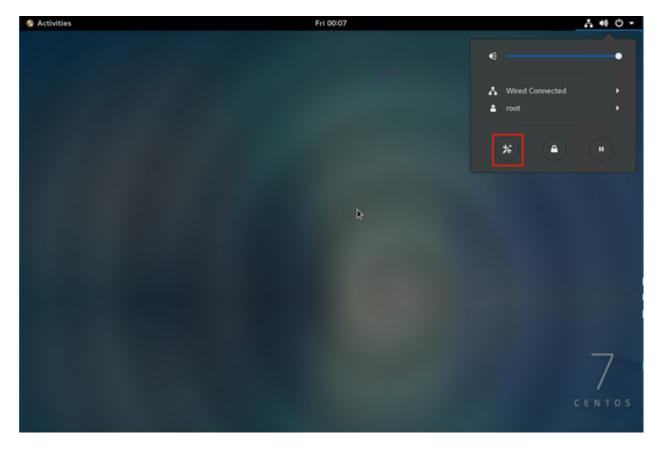
You have migrated the existing Arcserve Appliance to another fresh Arcserve Appliance successfully.

# Modify the Input Source of Pre-installed Linux Backup Server

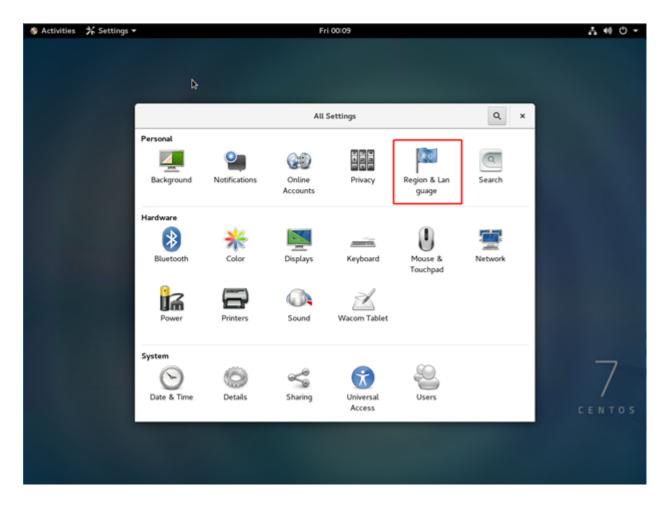
You can change the Keyboard of pre-installed Linux Backup Server.

# 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.

🔮 Activities	$\%$ Settings $ extsf{-}$	Fri 00:14	.t •0 ♥ ▼
		< Region & Language ×	
		Language     English (United States)       Formats     United States (English)	
		Input Sources English (US)	₽
			_
			CENTOS

5. Select the language and keyboard layout.

🚸 Activities 🤸 Settings 🕶			Fri 00:20			.t 40 € -
				_		
		Cancel	Add an Input Source	Add		
	<	<	English (United States)		×	
		English (US)			h.	
	La	Cameroon M	fultilingual (Dvorak)	25)		
	Fo		fultilingual (qwerty)	ih)		
	Input	English (Aus		_		
		English (Can				
	En	English (Can English (Cole				
	+		orak alternativernational no de	rad keys)		
	_	English (Dvo				
alle a start and						
						7
						/
						CENTOS

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	32
Working with Integrated Dell Remote Access Controller (iDRAC)	37

# 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.

BMC Network Configuration		BIOS will set below setting to IPMI in next BOOT
IPMI LAN Selection IPMI Network Link Status:	[Failover] Shared LAN	
Update IPMI LAN Configuration Configuration Address Source Station IP Address Subnet Mask Station MAC Address Gateway IP Address	[No] [DHCP] 172.31.8.192 255.255.0.0 00-25-90-9c-46-eb 172.31.0.1	<pre>++: Select Screen f1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>

- 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.

PI	ease Login
Username	
Password	
	login

7. Enter your user name in the Username field.

Default: ADMIN

8. Enter your password in the Password field.

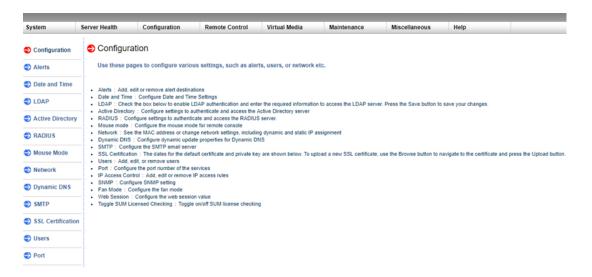
Default: ARCADMIN

The home page (IPMI main screen) is displayed.

System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	Help
🔿 System	1	\ominus Summa	ary				
🔿 FRU Re	eading	Firmware Revis			010.057.025.011		
Hardwa	are Information	BIOS Version : BIOS Build Tim Redfish Versior	e : 12/17/2015	System LAN	address : 00:25:90:1 I1 MAC address : 0 I2 MAC address : 0	0:25:90:fc:70:48	
			Carcserve Garcserve Garcserve	un fied fails groups on conside 	Windon gran martinezari		
				wer Down Rese			

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.

System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	Help
Configu	uration	🚭 Modify l	Jser				
Alerts							
⋺ Date an	id Time	Enter the r	new information for the	user below and pres	s Modify. Press Ca	ncel to return to the user	list.
LDAP		User Name	e:				
Active	Directory	Change Pa					
RADIU:	s	Password: Confirm Pa					
Mouse	Mode	Network P	rivileges:	Ŧ			
Networ	k	Modify	Cancel				
⋺ Dynam	ic DNS						
SMTP							
🔿 SSL Ce	rtification						
Users							

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)

This section contains the following topics:

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

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

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

### Follow these steps:

### Log into iDRAC:

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

iDRAC login page displays.

2. Enter the following information:

User Name: root

Password: ARCADMIN

3. Click Login.

### Monitor System Status and Manage System Information:

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

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

### Launch Virtual Console:

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

The Virtual Console page displays.

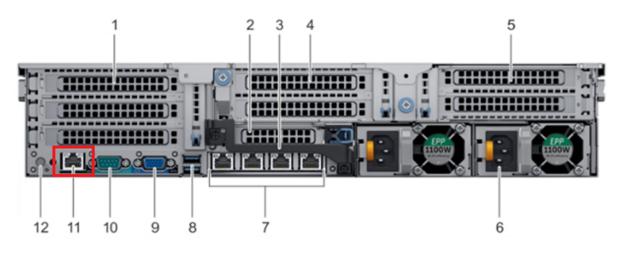
The Virtual Console Viewer displays the remote system desktop. You can take the control of remote system and run the operations using keyboard and mouse.

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

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

#### 

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



### View Rear Panel of 9072DR-9504DR for iDRAC9

View Rear Panel of 9012-9048 for iDRAC9

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

You can find the IP address of iDRAC from appliance.

Follow these steps:

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

F2 = System Setup F10 = Lifecycle Controller (Config IDRAC, Update FW, Install OS) F11 = Boot Manager F12 = PXE Boot	BIOS Version: 1.4.9 IDRAC IP: 10.57.25	
Initializing Firmware In	terfaces	Activate Windows

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

$\leftrightarrow$ $\rightarrow$ G	A Not secure https://10.57.25/restgui/start.html?login		☆ ⊖
		Access Controller 9	
	iDRAC-5Q6MH	Q2   Enterprise	
	Type the User Name an	d Password and click Log In.	
	Username:	Password:	
	root		
	Domain:		
	This iDRAC •		
	Security Notice: By accessing this computer, you confirm	that such access complies with your organization's security policy.	
		Log In	
	<u>Online Help</u>	Support About	

iDRAC login page is displayed.

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

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

### **View Rear Panel of X Series**

You can find the IP address of iDRAC from appliance.

### Follow these steps:

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

Controller (Config ate FW, Install OS)	ersion: 1.4.9 IP: 10.57.25.	
 itializing Firmware Interfaces		Activate Windows to to Action Center to activate Win

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

$\leftrightarrow$ $\rightarrow$ G	A Not secure https://10.57.25/restgui/start.html?login	☆	9
	Integrated Remote Access Controller 9		
	iDRAC-5Q6MHQ2   Enterprise		
	Type the User Name and Password and click Log In.		
	Username: Password:		
	root		
	Domain:		
	This IDRAC •		
	Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.		
	Log In		
	Online Liele   Quenet   Mout		

iDRAC login page is displayed.

### **Configure DHCP or Static IP address of iDRAC**

You can set DHCP network mode for iDRAC.

#### Follow these steps:

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



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

System Setup	Help   About   Exit
System Setup	
System Setup Main Menu	
System BIOS	
IDRAC Settings	
Device Settings	
iDRAC Settings allows you to configure iDRAC.	
	Activate Windows Go to Action Center to a <b>Finish</b> Windo
Service Tag: 5QI	Go to Action Center to a <b>Finish</b> Windo

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

The Network Settings fields are displayed.

System Setup		Help   About   Exit
iDRAC Settings		
iDRAC Settings		
iDRAC Settings Version iDRAC Firmware Version	3.00.00.32 3.21.21.21 (Build 30)	•
System Summary System Event Log		
Alerts		-
Front Panel Security Media and USB Port Settings		
Lifecycle Controller Power Configuration		
Use this page to configure the network properties, c properties, IPMI settings, and VLAN settings.	ommon iDRAC settings, IPv4 and IPv6	
Service Tag : 5Q6	The second se	Activate Windows Go to Action Center to a <b>Finish</b> Windo

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

System Setup		Help   About   Exit
iDRAC Settings		
iDRAC Settings • Network		
NETWORK SETTINGS		-
Enable NIC	○ Disabled	
NIC Selection	Dedicated	•
Failover Network	None	
MAC Address	54:48	
Auto Negotiation	⊖ Off	
Auto Dedicated NIC	Disabled     O Enabled	
Network Speed	O 10 Mbps O 100 Mbps ● 1000 Mbps	
Active NIC Interface	Dedicated	
Duplex Mode	O Half Duplex	
COMMON SETTINGS		
Register DRAC on DNS	Disabled     O Enabled	
		-
Select Enabled to enable NIC. When NIC is enabled, i this group. When a NIC is disabled, all communication	•	
Service Tag:5QI	Go to Action	

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

Static DNS Domain Name         V4 SETTINGS         Enable IPv4       O Disabled @ Enabled         Enable DHCP       O Disabled @ Enabled         IP Address       10.57.25         Gateway       10.57.25         Subnet Mask       255.255.25         Use DHCP to obtain DNS server addresses       @ Disabled O Enabled
Enable IPv4       O Disabled       Imable Enabled         Enable DHCP       O Disabled       Imable Enabled         IP Address       10.57.25         Gateway       10.57.25         Subnet Mask       255.255.250         Use DHCP to obtain DNS server addresses       Imabled         Imable DHCP       Imable DHCP
Enable DHCP       O Disabled       Image: Enabled         IP Address       10.57.25         Gateway       10.57.25         Subnet Mask       255.255.250         Use DHCP to obtain DNS server addresses       Image: Image
IP Address       10.57.25         Gateway       10.57.25         Subnet Mask       255.255.25         Use DHCP to obtain DNS server addresses       Image: Constraint of the server addresses
Gateway       10.57.25         Subnet Mask       255.255.255         Use DHCP to obtain DNS server addresses
Subnet Mask     255.255.25       Use DHCP to obtain DNS server addresses
Use DHCP to obtain DNS server addresses
D. (
Preferred DNS Server 0.0.0.0
Alternate DNS Server 0.0.0.0
V6 SETTINGS

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

DRAC Settings			
DRAC Settings • Network			
Auto Config Domain Name Static DNS Domain Name	Oisabled	⊖ Enabled	
PV4 SETTINGS			
Enable IPv4 Enable DHCP		⊛ Enabled ⊖ Enabled	
IP Address	10.57.25	d	
Gateway	10.57.25		ī.
Subnet Mask	255.255.255.	v	ī.
Use DHCP to obtain DNS server addresses	<ul> <li>Disabled</li> </ul>	⊖ Enabled	
Preferred DNS Server	0.0.0.0		
Alternate DNS Server	0.0.0.0		ī.
PV6 SETTINGS			

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

The network information is saved.

System Setup		Help   About   Exit
iDRAC Settings		
iDRAC Settings		
iDRAC Settings Version iDRAC Firmware Version System Summary	3.21.21.21 (Build 30)	-
System Event Log Network Alerts Front Panel Security Media and USB Port Settings Lifecycle Controller Power Configuration	Warning Saving Changes Settings have changed. Do you want to save the changes? Yes No	-
Service Tag: 5C		Go to Action Center <mark>to a <b>Finish</b> Win</mark> do

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

System Setup		Help   About   Exit
iDRAC Settings		
iDRAC Settings		
iDRAC Settings Version iDRAC Firmware Version System Summary		
System Event Log Network Alerts Front Panel Security Media and USB Port Settings Lifecycle Controller Power Configuration	Saving Changes The settings were saved successfully.	
Service Tag : 5Q		Go to Action Center to a Finish Windows

You have completed configuration of iDRAC DHCP.

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

System Setup		Help   About   Exit
System Setup		
System Setup Main Menu		
System BIOS		
iDRAC Settings		
Device Settings	Warning	
	Confirm Exit Are you sure you want to exit? Yes No	
		Activate Windows
Service Tag : 50		Go to Action Center to a Finish Wind

The DHCP network mode for iDRAC is configured.

# **Chapter 8: Restoring or Repairing the Arcserve Appli**ance

This section contains the following topics:

\_\_\_\_\_

Debug Factory Reset	52
Apply Arcserve UDP Factory Reset Using Boot Option in 7000-8000 Series Appliance 15	54
Apply Arcserve UDP Factory Reset Using Boot Option in 9012-9504DR Series Appli- ance 15	57
Apply Arcserve UDP Factory Reset Using Boot Option in X Series Appliance	59
Clear Configuration and Apply Appliance Factory Reset	52
Replace Factory Reset Image Using Set Appliance Image Utility	54
Remove and Replace a Hard Drive	57
Perform Bare Metal Recovery (BMR) without Preserving Data	59
Perform Bare Metal Recovery (BMR) and Preserving Data	34

### **Debug Factory Reset**

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

Error			
8	Execute post_factoryreset.ps1 failed[Error C investigation. Contact Arcserve Support in		e the logs for further
Trouble	eshoot   🗸	Restart	Shut Down

To resolve the issue, perform the following steps:

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

The following options are displayed:

### **Command Prompt**

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

### **View Logs**

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

### **Restart Factory Reset**

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

### Help

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

2. From the options displayed, click Help.

The screen displays multiple Error Code with details.

	Factory Reset Help	
ategory:		
Help Error Error code 1001 Error code 1002 Error code 1003 Error code 1004 Error code 1005 Error code 1005 Error code 1007 Error code 1008 Error code 1010 Error code 1010 Error code 1011 Error code 1011 Error code 1013 Error code 1013 Error code 1014 Error code 1015 Error code 1015 Error code 1016 Error code 1018 Error code 1020 Error code 1021 Error code 1021 Error code 1021 Error code 1022 Error code 1023 Error code 1031 Error code 1031 Error code 1032 Error code 1032 Error code 1034	<ul> <li>Cause: Program cannot find "post_factoryreset.ps1".</li> <li>Debug: Check if "post_factoryreset.ps1" exist at the path "xc\wine existing, check the content, otherwise please collect the logs and Steps:         <ol> <li>Open Command Prompt (cmd) from "Troubleshoot"</li> <li>Type "cd xc\windows\system32\appliance\" and press</li> <li>Type "dir" and press Enter. All the files and folders in the folder are displayed. Che "post_factoryreset.ps1" is exist.</li> <li>Also refer to ["Tip"&gt;"How to save the logs?"] for inf save the logs for further analysis.</li> </ol> </li> </ul>	> "Command Prompt". s Enter.

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

		Factory Res	et Help					
ategory:								
Error code 1019 Error code 1020 Error code 1022 Error code 1023 Error code 1031 Error code 1032 Error code 1032 Error code 1033 Error code 1034	∧ Steps:	<ol> <li>Type "diskpar Version of disl</li> <li>Type DISKPAI The disk list approximation</li> </ol>	rt" and pre kpart is dis RT> "list di ppears as s	ss Enter. played. sk" and p hown be	ress Ente low. The	er.	ize disk is usu	mand Prompt". Jally our system disk.
Error code 1035 Error code 1036 Error code 1037 Error code 1038 Error code 1039 Error code 1051		Disk ### Disk 0 Disk 1 Here, the Disk 1	Status Online Online is the data	447G 3725G	Free OB OB e Disk 0 i	Dyn s the SSD	Gpt disk.	
Error code 1052 Fror code 1053 Fror code 1054 Fror Code 1054 Fror Code 1054 How to get the diskla How to get the conte		<ol> <li>Type "select of It will respond</li> <li>Type DISKPAI The disk layou</li> </ol>	l with "Disk RT> "list pa	<disk ni<br="">rtition" a</disk>	umber g ind press	ot above Enter.		selected disk."
How to save the logs How to get IP address		Partition ### Partition 1 Partition 2	Type Recover System	у	Size 300MB 99MB	1	Offset 1024KB 301MB	

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

# Apply Arcserve UDP Factory Reset Using Boot Option in 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 nonconfigured status.

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

### Follow these steps:

- CICCSERVE® Assured recovery Press <TAB> to display BIOS POST message. Press <DEL> to run Setup. Press <F11> to invoke Boot Menu. Press <F12> to boot from PXE/LAN. XE--Onboard AHCI Device Detection...
- 1. Press F11 to invoke Boot Menu.

2. Select the boot option UDP Factory Reset.



A page about factory reset is displayed.

Factory Reset
Performing a Factory Reset on your Arcserve Appliance will return all settings to their factory defaults. All resources, job history, reports and log entries will be deleted. The Arcserve UDP software will revert from its current version to the version originally installed on the Appliance.
Reverting to Arcserve UDP Version 7.0.4399.
Preserve existing backup data.
Reset Cancel

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.
- 1. Click Reset.

### A confirmation dialog appears.

	Are you sure you want to perform a factory reset on your Arcserve Appliance? Sel	lecting Reset will
:	result in returning all settings to their factory defaults.	2.78%
	All of your backup data will be preserved during the reset.	
	Reset	Cancel

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

- 2. 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	Appliance
	settings on the Arcserve Appliance to their factory defaults. All resources, job history, reports, and logs are being e is reverting to the version originally installed on the Appliance.
Reverting to Arcserve UDP V	fersion 7.0.4404.
Existing backup data is being	g preserved.
Factor	y Reset Is Complete
<b>S</b>	Your Arcserve Appliance has been returned to its factory defaults.
	Click Restart to restart the appliance and launch the Configuration Wizard or click Shut Down to shut down the appliance.
	Restart Shut Down
Factory reset is complete.	

## 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.

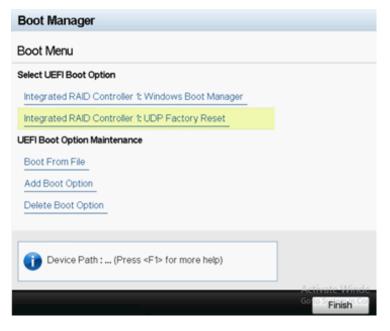
**Note:** You can also select the Preserve the backup data option while running UDP factory reset.

### Follow these steps:

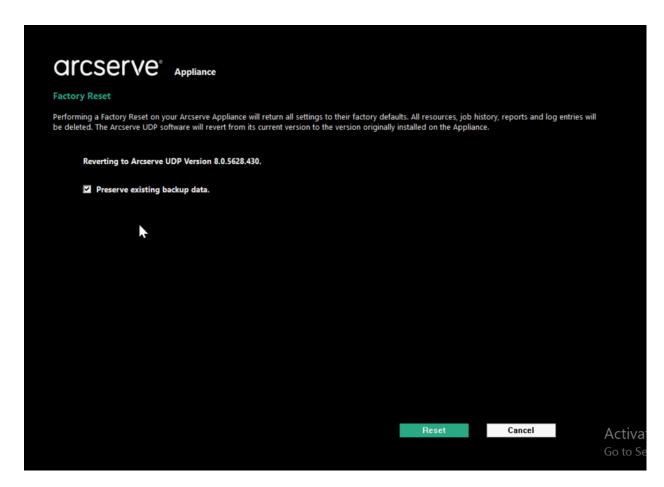
1. Press F11 on the keyboard to invoke Boot Menu.

Initializing Firmware In	terfaces	Activate Windo Go to System in Cont
Entering Boot Manager F12 = PXE Boot	10404 P. 10372310	
F2 = System Setup F10 = Lifecycle Controller (Config iDRAC, Update FW, Install OS)	BIOS Version: 1.4.9 iDRAC IP: 10.57.25.18	

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.

Confir	m Factory Reset	
1	Are you sure you want to perform a factory reset on your Arcserve Appliant result in returning all settings to their factory defaults.	ce? Selecting Reset will
	All of your backup data will be preserved during the reset.	
	Reset	Cancel

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	Appliance
Factory Reset	
	settings on the Arcserve Appliance to their factory defaults. All resources, job history, reports, and logs are b is reverting to the version originally installed on the Appliance.
Reverting to Arcserve UDP Ve	ersion 8.0.5628.430.
Existing backup data is being	preserved.
Factory	Reset Is Complete
	Your Arcserve Appliance has been returned to its factory defaults.
	Click Restart to restart the appliance and launch the Configuration Wizard or click Shut Down to shut down the appliance.
	Restart Shut Down
Factory reset is complete.	

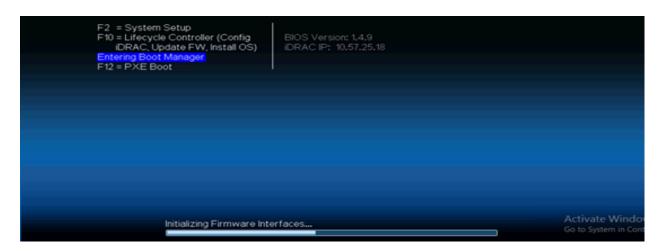
# Apply Arcserve UDP Factory Reset Using Boot Option in X Series Appliance

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

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

Follow these steps:

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



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

Boot Manager	Help   About   Exit
Boot Manager	
Boot Menu	
Virtual Floppy Drive	•
Virtual Optical Drive	
Embedded RAID Controller 1: windows Boot Manager	
windows Boot Manager	
Windows Boot Manager	
Embedded RAID Controller 1: Windows Boot Manager	
Embedded RAID Controller 1: UDP Factory Reset	
UEFI Boot Option Maintenance	
Boot From File	
Add Boot Option	

A page about factory reset is displayed.

Factory	Reset								
Performin be delete	ng a Factory Reset on y id. The Arcserve UDP si	our Arcserve App oftware will revert	liance will retu from its curre	rn all settings nt version to t	to their factory he version orig	defaults. All re- ginally installed of	ources, job hi on the Applian	istory, reports and log entries v ice.	vill
•	Reverting to Arcserve	UDP Version 8.0.	5628.						
E	Preserve existing t	backup data.							
						*			
							set	Activate Windows Go Cancel as to a tivate Win	

Notes:

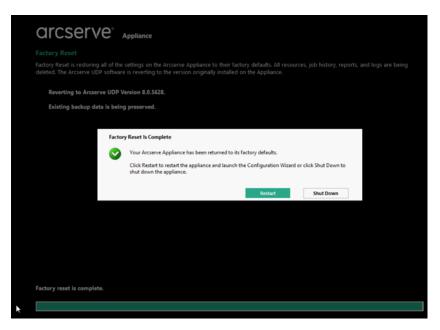
- The Preserve existing backup data option is selected by default. Only
   C:\ volume in the original operating system is rebuilt. Data at X:\
   volume and Y:\ volume remain unchanged.
- If you clear the selection of the Preserve existing backup data option, all the data on the respective volumes of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

A confirmation dialog appears.



You can click Cancel to reboot the Arcserve Appliance unit.

- 4. After factory reset finishes, you can perform either of the following actions:
  - \* Click **Restart** to reboot the appliance.
  - \* Click **Shut Down** to close the appliance.

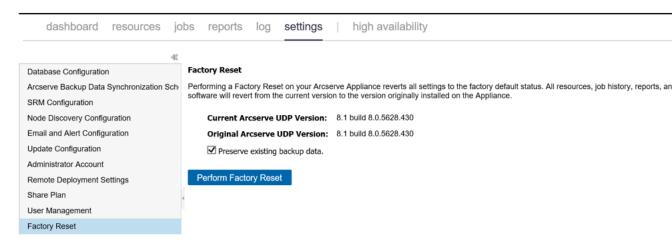


# **Clear Configuration and Apply Appliance Factory Reset**

Using Factory Reset, you can return your Arcserve Appliance back to clean and nonconfigured 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.



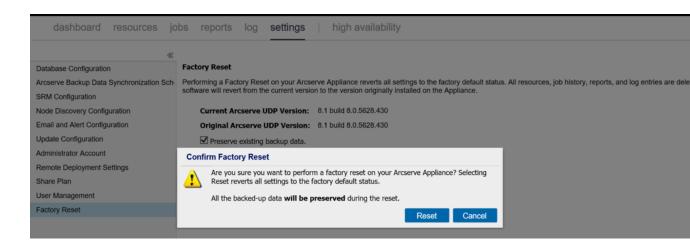
All the backed up data is preserved by default.

### 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:

Factory Reset	
Factory Reset is restoring all of the settings on the Arcserve Appliance to their deleted. The Arcserve UDP software is reverting to the version originally instal	
Reverting to Arcserve UDP Version 8.0.5628.430.	
Existing backup data is being preserved.	
Reinstalling Arcserve UDP: 52% Complete	

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.

Factory Reset	Appliance
	settings on the Arcserve Appliance to their factory defaults. All resources, job history, reports, and logs are is reverting to the version originally installed on the Appliance.
Reverting to Arcserve UDP V	ersion 8.0.5628.430.
Existing backup data is being	) preserved.
Factor	y Reset Is Complete
	Your Arcserve Appliance has been returned to its factory defaults.
	Click Restart to restart the appliance and launch the Configuration Wizard or click Shut Down to shut down the appliance.
	Restart Shut Down

# Replace Factory Reset Image Using Set Appliance Image Utility

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

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

**Note:** The Appliance image used for replacement should have higher version than the *Original Arcserve UDP version* installed on the Arcserve Appliance. Replacing

the Arcserve Appliance image with a different Windows operating system version is not supported.

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

Factory Reset	
	erve UDP Appliance will return all settings to their factory defaults. All resources, job history, the Arcserve UDP software will revert from its current version to the version originally installed on
Current Arcserve UDP Version:	6.5.4175 update 4 build 1223
Original Arcserve UDP Version:	6.5.4175 update 4 build 1223
☑ Preserve existing backup data.	
Perform Factory Reset	

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

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

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

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

#### Follow these steps:

- 1. Download the Appliance factory reset image of Arcserve Appliance 9000 series, and execute the Set Appliance Image Utility. Perform the following steps to use set Appliance Image Utility:
  - a. To download the 7.0 factory reset image, contact Arcserve Support.
  - b. Open the Windows command line and run the following command:

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

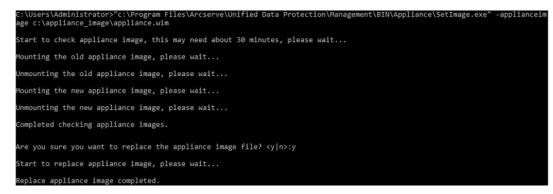
After *checking appliance images finished* step is complete, you can view the following query:

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

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

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

Replace appliance image completed.



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

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

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

Factory Reset

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

```
      Current Arcserve UDP Version:
      6.5.4175 update 4 build 1223

      Original Arcserve UDP Version:
      7.0.4455

      ✓ Preserve existing backup data.
```

Perform Factory Reset

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

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

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

For more information about Factory Reset, refer the link.

### **Remove and Replace a Hard Drive**

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

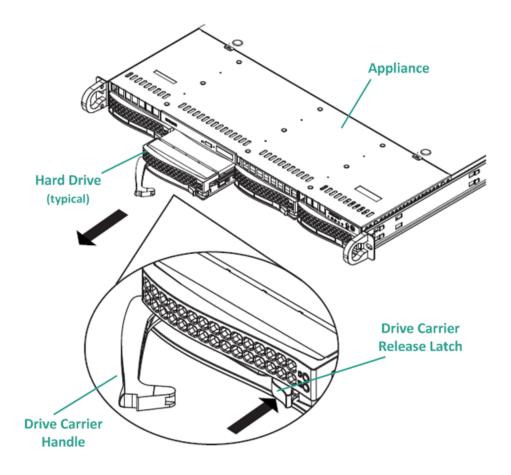
The Arcserve Appliance contains four hard drive carriers which are labeled 0, 1, 2 and 3 from left to right. If you replace more than one hard drive at a time, you should label the replacement hard drives so that you know which drive is placed into each drive carrier. You should also label the hard drives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

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

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

### Follow these steps:

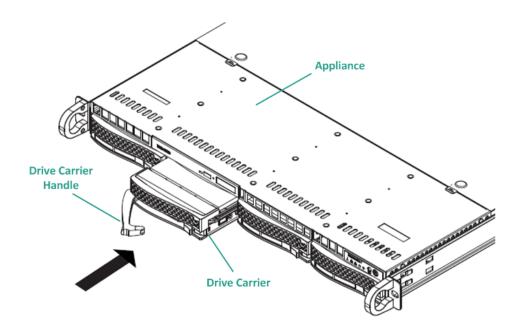
- 1. To gain access to the drive holders, you first need to remove the faceplate:
  - a. Unlock the faceplate lock.
  - b. Press the release knob to retract the faceplate pins.
  - c. Carefully remove the faceplate (using two hands).
- 2. Press the release latch on the drive carrier. This extends the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



 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 airflow for the drive bays.

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

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



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

## Perform Bare Metal Recovery (BMR) without Preserving Data

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

#### Follow these steps:

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

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

Manufacturer         Version         Platform         Path           Intel         12/08/2016, 12.14.7.0         x64         C:\WINDDWS\INF\oem43.inf           Intel         07/30/2013, 9.4.2.10.         x64         C:\WINDDWS\INF\oem43.inf           Intel         07/30/2013, 9.4.2.10.         x64         C:\WINDDWS\INF\oem3.inf           Intel         03/06/2015, 6.707.0         x64         C:\WINDDWS\INF\oem45.inf           INTEL         03/06/2015, 6.707.0         x64         C:\WINDDWS\INF\oem45.inf           INTEL         08/19/2016, 10.0.14         x64         C:\WINDDWS\INF\oem45.inf           AMD.Section, ACER.S         06/21/2006, 10.0.14         x64         C:\WINDDWS\INF\oem45.inf           INTEL         07/30/2013, 9.4.2.10         x64         C:\WINDDWS\INF\oem45.inf           GENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WINDDWS\INF\oem47.inf           Generic         10/08/2017, 10.0.14         x64         C:\WINDOWS\INF\usbp\theta.inf	ocess is launched.	14		
Intel         07/30/2013, 9.4.2.10         x64         C:\WINDOWS\INF\oem3.inf           MS_HDC, INTEL_HDC         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\oem3.inf           LSI         03/06/2015, 6.707.0         x64         C:\WINDOWS\INF\oem8.inf           INTEL         08/19/2016, 10.1.2.80         x64         C:\WINDOWS\INF\oem8.inf           AMD.Section, ACER.S         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\oem45.inf           INTEL         07/30/2013, 9.4.2.10         x64         C:\WINDOWS\INF\oem45.inf           GENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\ome45.inf	Manufacturer	Version	Platform	Path
MS_HDC, INTEL_HDC         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\mshdc.inf           LSI         03/06/2015, 6.707.0         x64         C:\WINDOWS\INF\noem8.inf           INTEL         08/19/2016, 10.1.2.80         x64         C:\WINDOWS\INF\noem8.inf           AMD.Section, ACER.s         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\noem8.inf           INTEL         08/19/2013, 9.4.2.10         x64         C:\WINDOWS\INF\noem45.inf           INTEL         07/30/2013, 9.4.2.10         x64         C:\WINDOWS\INF\noem47.inf           GENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\machine.inf				
LSI         03/06/2015, 6.707.0         x64         C:\WIND0WS\INF\oem8.inf           INTEL         08/19/2016, 10.1.2.80         x64         C:\WIND0WS\INF\oem45.inf           AMD.Section, ACER.S         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\oem45.inf           INTEL         07/30/2013, 9.4.2.10         x64         C:\WIND0WS\INF\oem45.inf           GENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\omen47.inf				
INTEL         08/19/2016         10.1.2.80         x64         C:\WINDOWS\INF\oem45.inf           AMD.Section, ACER.S         06/21/2006         10.0.14         x64         C:\WINDOWS\INF\oem45.inf           INTEL         07/30/2013         9.4.2.10         x64         C:\WINDOWS\INF\oem47.inf           GENDEV_SYS, ACC         06/21/2006         10.0.14         x64         C:\WINDOWS\INF\omem47.inf				
AMD.Section, ACER.S         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\usbport.inf           INTEL         07/30/2013, 9.4.2.10         x64         C:\WINDOWS\INF\oem47.inf           GENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WINDOWS\INF\machine.inf				
INTEL         07/30/2013, 9.4.2.10         x64         C:\WIND0WS\INF\oem47.inf           GENDEV_SYS, ACC         06/21/2006, 10.0.14         x64         C:\WIND0WS\INF\machine.inf				
Generic 10/08/2017, 10.0.14 x64 C:\W/INDOWS\INF\usbxhci.inf	GENDEV_SYS, ACC	06/21/2006, 10.0.14	x64	C:\WINDOWS\INF\machine.inf
	Generic	10/08/2017, 10.0.14	x64	C:\WINDOWS\INF\usbxhci.inf

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.

arcse	rve	bare met	al recovery
	nglish		
Ke	yboard Layout:		
U	IS	~	
		Next	

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

arc	Serve <sup>®</sup> bare metal recovery
Bare Metal Re - <i>Select the</i>	 covery(BMR) <i>type of backup for BMR</i>
	Select type of restore source:
	Restore from a Arcserve Unified Data Protection backup Use this option to perform a restore from either a backup destination folder or a data store.
	O Recover from a virtual machine
	Use this option to perform a virtual-to-physical (V2P) restore from a virtual machine created by Virtual Standby or Instant VM
	O Source is on a VMware machine
	O Source is on a Hyper-v machine

The Select a Recovery Point wizard window appears.

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

Bare Metal Recovery(BMR) - Select a Recovery Point	The following backed up machines are detected:		
The top pane displays all backed up machines and	Backed up Informati	on	
heir backup destinations. If you click on a machine, you can then see the associated recovery points on the bottom pane. Select a recovery point to continue.	Host Name:		
lote: By default, only the backed up machines hat are detected from local volumes are listed	Operating System:		
ere. After a new removable disk is attached or letached, you can dick "Refresh" the mitopine list. iou can also dick "Browse" to add any baked up achines from the remote shared folder or the	DNS Suffix:		
achines from the remote shared folder or the sata store. If you fail to browse the remote shared folder, it	Source:		
nay be because the NIC driver is not installed or the IP address is incorrect. If necessary, you can		Refresh	Bro <u>w</u> se 🔻
perform the following: <u>Click here</u> to launch the load driver utility <u>Click here</u> to launch the network configuration		Browse from	network/local path
5 Network Adapter(s) Detected			
ntel(R) 1350 Gigabit Network Connection - IP Address: 10.10.255.255 - Status: Connected			
Intel(R) 1350 Gigabit Network Connection #2 - IP Address: 0.0.0.0 - Status: Disconnected			
▲ Utilities		Back	Next Abort

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**.

Name:	appliance7501	~	Port:	8014
lser Name:	administrator		Protocol:	
assword:	•••••			Connect
		Node ID	095	1fd5c-3dd2-4968-be64-5eaef
		DNS Suffix Node ID	arcs	iance7205 erve.com 1fd5c-3dd2-4968-be64-

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

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

Backed up Information Host Name: Operating System:	applance7205 Windows Server 2016 X64
Host Name:	
Operating System:	Windows Server 2016 X64
DNS Suffix:	arcserve.com
Source:	Recovery Point Server
	<u>R</u> efresh Bro <u>w</u> se <b>v</b>
AR Status: - Backup Type: - Incremental Backup Backup Destination (Dete - Recovery Point Server: appl - Recovery Point Server data	<pre>cted from current system): iance7501 store: appliance7501_data_store</pre>
Boot Firmware: - UEFI Backed up Volumes (Used <	l Size/Total Size/Minimum Size Required):
	ified machine. Select a recovery point at AR Status: - Backup Type: - Incremental Backup Backup Destination (Dete - Recovery Point Server: appl - Recovery Point Server: appl - Recovery Point Server: appl - Recovery Point Server data - Node ID: 0951fd5c-3dd2-49 Backup Description: - Boot Firmware: - UEFI

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

ter Session Password	
•	ок
Current password length: 1 characters Maximum password length: 23 characters	Cancel

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

11. Select Advanced Mode and click Next.

Which recovery mode do you wan	t to use?		
O Express Mode			
The express mode will recov machine default settings.	er the system automatically with minimal user interaction by using the		
Advanced Mode	1		
able to:	st you in customizing the restore process. Using this mode you will be a on basic volumes or dynamic disks.		

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**.

Bare Metal Recovery(BMR) - Adjust Disk Partitions	Current Destination D	Disk/Volume Layouts	Qperations 🗸
You can adjust the disk/volume configuration on this screen. You can also select data to restore from the original source disk/volume to the current destination disk/volume, After selecting a disk/volume, you can then night-click the mouse button, and display the corresponding operation options. Note: If there is no mouse attached in your environment, you can select a disk/volume with TAB and Arrow keys, then press the Menu key to display the menu. The disk/volume changes you make will not take get into effect until you select "Commit" from the Operations menu or click "Next" to commit all changes.	<ul> <li>Bisk 1 (6574)</li> <li>Disk 1 (M</li> <li>447.13</li> <li>Disk 2 (0</li> <li>447.13</li> </ul>	Reset Commit Map Disk From Clean Disk Convert to MBR Convert to GPT	vstem Partiti C:\ (155.73 GB) \\\7\Volume(4dd 1 (18394.96 GB) (447.13 GB) (447.13 GB)
commit ai changes.		Convert to Basic Convert to Dynamic	
	Original Source	Online Disk	
	onginal source	Disk Properties	
	<ul> <li>Disk 0 (MBR) 111.79 GB</li> </ul>		Y:\ (111.79 G8)
	<ul> <li>Disk 1 (GPT) 7451.00 GB</li> </ul>	\\7\Volume(791b 👔 EF	Fl System Partiti 👔 C:\ (155.73 GB) 👔 \\?\Volume[4dd 1 👔 X:\ (7218.46 GB) 👔

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

Bare Metal Recovery(BMR) - Adjust Disk Partitions	Current Destination Di	isk/Volume Layouts	<b>O</b> perations
You can adjust the disk/volume configuration on this screen. You can also select data to restore from the original source disk/volume to the current destination disk/volume.	+//5/6/6/15/15/1/// //79597/59/5	Reset	(18627.37 GB)
After selecting a disk/volume, you can then right-click the mouse button, and display the corresponding operation options.	<ul> <li>Disk 1 (ME 447.13 G</li> </ul>	Commit	(447. 13 GB)
Note: If there is no mouse attached in your environment, you can select a disk/volume with TAB and Arrow keys, then press the Menu	<ul> <li>Disk 2 (MB 447.13 GE</li> </ul>	Map Disk From" Clean Disk	(447.13 GB)
key to display the menu. The disk/volume changes you make will not take get into effect until you select "Commit" from the Operations menu or click "Next" to		Convert to MBR Convert to GPT	
commit all changes.		Convert to Basic Convert to Dynamic	
	Original Source De	Online Disk	
	Disk 0 (MBk) 111.79 GB	Disk Properties	Y:\ (111.79 GB)
	Disk 1 (GPT) 7451.00 GB	\\?\Volume(791b 👔 EFI Syste	rm Partiti

The Submit Disk Changes window appears.

14. Click Submit.

Details
Volume Path[\\?\Volume{791b0915-1396-4e8d-8dfb-1fa02793003f}\
Volume Path[\\?\Volume{821d05a8-3ecd-436f-a497-cc04fb3e4708}\
Volume Path[C:\]
Volume Path[F:\]
Volume Path[D:\]
Clean Disk [0]
N

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

Operation	Details
Delete Volume	Volume Path[\\?\Volume{791b0915-1396-4e8d-8dfb-1fa02793003f}\
Delete Volume	Volume Path[\\?\Volume{821d05a8-3ecd-436f-a497-cc04fb3e4708}\
Delete Volume	Volume Path[C:\]
Delete Volume	Volume Path[F:\]
Delete Volume	Volume Path[D:\]

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

Bare Metal Recovery(BMR) - Adjust Disk Partitions	Current Destinat	tion Disk/Volume Layouts	Operations 🔻
You can adjust the disk/volume configuration on this screen. You can also select data to restore from the original source disk/volume to the current destination disk/volume.		(18627.37 GB)	
After selecting a disk/volume, you can then right-click the mouse button, and display the corresponding operation options.	<ul> <li>Disk 1 (ME 447.13 G</li> </ul>		
Note: If there is no mouse attached in your environment, you can select a disk/volume with TAB and Arrow keys, then press the Menx Key to display the menu. The disk/volume changes you make will not take get into effect until you select "Commit" from the Operations menu or click "Next" to commit all changes.	Disk 2 (ML 447.13 G		
	Original Source D Disk 0 (ME 111.79 G		(1)
	Disk 1 (GF 7451.00 C		218.46 GB) 🕕
	Unollocated	ed 🗖 Primary	
▲ <u>U</u> tilities		Back	Abort

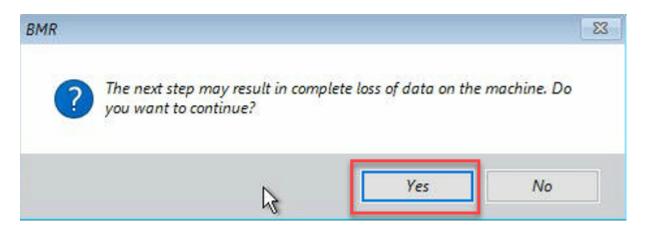
The Bare Metal Recovery(BMR)- Choose a Recovery Mode dialog appears.

17. Select Express Mode and click Next.

Which recovery mode do you want to use?	
Express Mode	
The express mode will recover the system automatically with minimal user interaction by using the machine default settings.	
O Advanced Mode	
The advanced mode will assist you in customizing the restore process. Using this mode you will be able to: Select where to restore data on basic volumes or dynamic disks. Insert device driver before reboot.	
Note: After clicking Next, the BMR Wizard will create new partitions on the destination	

The **BMR** dialog appears.

18. Click Yes.



The Summary of Restore Settings dialog appears.

19. Click Cancel.

ummary of Volume Restore Settings: Source Volume Destination Volume	
U\/2\Volume{791b0915-1396-4e8d-8dfb-1fa02793003f}\(300 MB) \\?c06aa5e0-adb9-4849-8b1	5-20
EFI System Partition (99 MB)	
C:\ (155.73 GB) \\?257b3c2a-9cf1-44a0-a8b3	
\\?\Volume{4dd1123f-0464-4cd6-9df0-1ab9b95c8901}\ (76.29 GB) \\?98fb5326-630f-4842-82fa	-48b
	3

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.

Bare Metal Recovery(BMR) - Adjust Disk Partitions	Current Destination Disk/Volume Layouts
You can adjust the disk/volume configuration on this screen. You can also select data to restore from the original source disk/volume to the current destination disk/volume.	Disk 0 (GPT)     18627.50 GB     117:Volume(791b     EFI System Partiti     C:\ (155.73 GB)     1\17:Volume(4dd 1     (18394.96 GB)
After selecting a disk/volume, you can then right-dick the mouse button, and display the corresponding operation options.	Disk 1 (MBR)     Destination Volume: \\7\Volume(03331745-9734-4066-bd25-693087d5826b)\     File System Type : RAW
Note: If there is no mouse attached in your environment, you can select a disk/volume with TAB and Arrow keys, then press the Menu key to display the menu. The disk/volume changes you make will not	Disk 2 (MBR)     Data on this volume will be restored from original volume "\\?\Volume(791b0915-1396-4e8d-     8dfb-1fa02793003f)\.
take get into effect until you select "Commit" from the Operations menu or click "Next" to commit all changes.	Original Source Disk/Volume Layouts
	- Disk 0 (MBR) 111.79 GB Y:\ (111.79 GB) (1
	Disk 1 (GPT)     7451.00 GB     11?\Volume(791b)     EFI System Partiti     C:\ (155.73 GB)     ()     \\?\Volume(4dd 1)     X:\ (7218.46 GB)     ()
	Unallocated Primary
	Back Next Abort

The Summary of Restore Settings dialog appears.

21. Click **OK**.

Source Disk Destinat	ion Disk
ummary of Volume Restore Settings: Source Volume	Destination Volume
Volume {791b0915-1396-4e8d-8dfb-1fa02793003f} (300 MB)	
EFI System Partition (99 MB)	\\?b9994f56-8c58-4bbf-bd7a-85a.
()C:\(155.73 GB)	\\?496da605-7066-442c-8ea2-c3
()\?\Volume{4dd1123f-0464-4cd6-9df0-1ab9b95c8901}\ (76.29 G	B) \\?59eaea46-103c-45e3-b0ed-55
< .	
<	adjust restore settings manually, click Cancel.

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

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

Bare Metal Recovery(BMR) - Start Restore Process	Summary of Restore Settings			
	Restore Item  Restore source volume '\/?\Volume{791b0915-1396-4e8d-8dfb-1fa02793003f}\'  Restore source volume 'EFI System Partition' to current destination disk 0  Restore source volume 'Ci\' to current destination disk 0  Restore source volume '\/?\Volume{4dd1123f-0464-4cd6-9df0-1ab9b95c8901}\'	Completed Restoring	Progress 100.0% 100.0% 0.8%	Throughput 367.44 MB/Minute 967.90 MB/Minute 2705.50 MB/Minute
BMR. For example, press F8 and boot into Active Directory Service Restore mode to perform Active Directory authoritative restore.	Automatically reboot your system after recovery.  Oo not start Agent service automatically after reboot.  Boot the system to Advanced Boot Options (F8) Menu on the next boot for Windows	s 8 / Windows Sen	ver 2012 and late	· 05.
	Elapsed Time: 00 : 00 : 24			
	Estimated Time Remaining: 01:30:50			
	[0.8%] [576MB/76631MB] Restoring basic source volume 'C:\' to current destination dis	k 0		
▲ Utilities		Back	N	of Abort

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

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

Eare Metal Recovery(BMR)	Provide drivers for following devices:	
An incompatibility problem has been detected and BMR is unable to find suitable driver for some device(s). The operating system of the host being recovered may be different than the operating system that was created on the BMR ISO image. Please select an appropriate driver for the device(s) or add a new driver by dicking "Add Driver" button.	applance7205     a	Property         Description           Vendor         LSI Logic / Symbios Logic           Manufacturer         AvagoTech           Class         SCSIAdapter           Driver Description         AVAGO MegaRAID SAS Adapter           Hardware ID         PCI\VEN_10008DEV_005D8SUBSY
	Available Driver(s):  Driver megasas2.inf megasas2.inf(1)  megasas3.inf	Property         Description           Version         03/02/2015, 6.706.06.00           Manufacturer         LSI, DELL           Class         SCSIAdapter           Service         megasas           INF Path         C:\WINDOWS\System32\driverStore\FileRepository\megasas.inf_a
	Insert Driver	< >>
▲ <u>U</u> tilities		Back Next Abort

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

Click Report to automatically reboot your system at this time. If you want to collect all BMR log files you can use the Activity log utility. <u>Click here</u> to launch the Activity Log utility.

1	Reboot	Cancel	
	Troope	guneer	
		3. <del></del>	

The BMR process is completed successfully.

# Perform Bare Metal Recovery (BMR) and Preserving Data

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

#### Follow these steps:

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

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

rocess is launched.		1	
Manufacturer	Version	Platform	Path
Intel	12/08/2016, 12.14.7.0	x64	C:\WINDOWS\INF\oem43.inf
Intel	07/30/2013, 9.4.2.10	x64	C:\WINDOWS\INF\oem9.inf
MS_HDC, INTEL_HDC.		x64	C:\WINDOWS\INF\mshdc.inf
LSI	03/06/2015, 6.707.0	x64	C:\WINDOWS\INF\oem8.inf
INTEL AMD.Section.ACER.S	08/19/2016, 10.1.2.80	x64 x64	C:\WINDOWS\INF\oem45.inf
AMD. Section, ALER.S	06/21/2006, 10.0.14	x64	C:\WINDOWS\INF\usbport.inf C:\WINDOWS\INF\oem47.inf
GENDEV_SYS, ACC		x64 x64	C:\WINDOWS\INF\oem47.inr
Generic	10/08/2017, 10.0.14	x64	C:\WINDOWS\INF\usbxhci.inf

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.

arcse	erve	bare metal recovery
	English	
	Keyboard Layout:	
	03	Next

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

arcs	Serve® bare metal recovery
Bare Metal Rec - <i>Select the t</i>	Covery(BMR) type of backup for BMR
	Select type of restore source:
	Restore from a Arcserve Unified Data Protection backup Use this option to perform a restore from either a backup destination folder or a data store.
	○ Recover from a virtual machine
	Use this option to perform a virtual-to-physical (V2P) restore from a virtual machine created by Virtual Standby or Instant VM
	O Source is on a VMware machine
	◯ Source is on a Hyper-v machine

The Select a Recovery Point wizard window appears.

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

Bare Metal Recovery(BMR) - Select a Recovery Point	The following backed up machines are detected:	
The top pane displays all backed up machines and	Backed up Information	
heir backup destinations. If you dick on a achine, you can then see the associated ecovery points on the bottom pane. Select a ecovery point to continue.	Host Name:	
ote: By default, only the backed up machines nat are detected from local volumes are listed	Operating System:	
ere. After a new removable disk is attached or etached, you can dick "Refresh" the mixpine list. ou can also dick "Browse" to add any basked up achines from the remote shared folder or the	DNS Suffix:	
ata store.	Source:	
f you fail to browse the remote shared folder, it hay be because the NIC driver is not installed or he IP address is incorrect. If necessary, you can	<u>R</u> efresh	Bro <u>w</u> se 🔻
erform the following: lick here to launch the load driver utility	Browse from network	/local path
Network Adapter(s) Detected		
ntel(R) 1350 Gigabit Network Connection - IP Address: 10, 10, 255, 255 - Status: Connected		
ntel(R) I350 Gigabit Network Connection #2 - IP Address: 0.0.0.0 - Status: Disconnected		
Status: Disconnected	Back Next	Abort

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**.

Host Name:	appliance7501 V		Port:	8014	8014	
Jser Name:	administrator		Protocol:		● HTTPS	
assword:	•••••			Conr	nect	
		DNS Suffix Node ID		erve.com 1fd5c-3dd2-4968	3-be64-5eaef	

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

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

Bare Metal Recovery(BMR) - Select a Recovery Point	The following backed up machines are deter	cted:	
he top pane displays all backed up machines and		Backed up Information	
heir backup destinations. If you click on a nachine, you can then see the associated ecovery points on the bottom pane. Select a ecovery point to continue.	appliance7205	Host Name:	appliance7205
lote: By default, only the backed up machines		Operating System:	Windows Server 2016 X64
hat are detected from local volumes are listed ere. After a new removable disk is attached or letached, you can click "Refresh" the machine list. ou can also click "Browse" to add any backed up		DNS Suffix:	arcserve.com
nachines from the remote shared folder or the lata store.		Source:	Recovery Point Server
If you fail to browse the remote shared folder, it may be because the NIC driver is not installed or the IP address is incorrect. If necessary, you can perform the following: <u>Click here</u> to launch the load driver utility <u>Click here</u> to launch the network configuration utility			
			<u>R</u> efresh Bro <u>w</u> se 🔻
	The following recovery points are detected 5/28/2018 2:41:41 AM 5/27/2018 5/26/2018 5/26/2018 5/26/2018 5/25/2018 11:39:14 AM	- Recovery Point Server: appl	cted from current system): iance7501 store: applance7501_data_store
6 Network Adapter(s) Detected	<ul> <li>⇒ \$/28/2018</li> <li>⊕ 10:00:15 PM</li> <li>⊕ 2:41:41 AM</li> <li>⊕ \$/27/2018</li> <li>⊕ \$/26/2018</li> <li>⊕ \$/25/2018</li> <li>⊕ \$/25/2018</li> </ul>	AR Status: Backup Type: - Incremental Backup Backup Destination (Dete - Recovery Point Server: appl - Recovery Point Server data - Node ID: 0951fdSc-3dd2-49	cted from current system): iance7501 store: applance7501_data_store
6 Network Adapter(s) Detected	<ul> <li>⇒ \$/28/2018</li> <li>⊕ 10:00:15 PM</li> <li>⊕ 2:41:41 AM</li> <li>⊕ \$/27/2018</li> <li>⊕ \$/26/2018</li> <li>⊕ \$/25/2018</li> <li>⊕ \$/25/2018</li> </ul>	AR Status: - Backup Type: - Incremental Backup Backup Destination (Dete - Recovery Point Server: appl - Recovery Point Server: appl - Recovery Point Server data - Node ID: 0951fdSc-3dd2-49 Backup Description: - Boot Firmware: - UEFI	cted from current system): iance7501 store: applance7501_data_store

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

•	ок
urrent password length: 1 characters	Cancel

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

11. Select Advanced Mode and click Next.

Which recovery mode do you want to use?		
○ Express Mode		
The express mode will recover the system automatically with minimal user interaction by using the machine default settings.		
Advanced Mode		
The advanced mode will assist you in customizing the restore process. Using this mode you will be able to: Select where to restore data on basic volumes or dynamic disks. Insert device driver before reboot.		

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

You can adjust the disk/volume configuration on this screen. You can also select data to restore from the original source disk/volume to the current destination disk/volume. After selecting a disk/volume, you can then right- click the mouse button, and display the	<ul> <li>Disk 0 (GPT) 18616.32 GB</li> <li>Disk 1 (MBR) 223.57 GB</li> </ul>	EFI System Partiti		me(4dd 1 (18383.77 GB)
corresponding operation options. Note: If there is no mouse attached in your environment, you can select a disk/volume with TAB and Arrow keys, then press the Menu key to display the menu. The disk/volume changes you make will not take get not effect until you select "Commit" from the Operations menu or click "Next" to commit all changes.	22357 00			
	Original Source Disk/Vo	olume Layouts		2
	<ul> <li>Disk 0 (MBR) 223.57 GB</li> </ul>		Y:\ (223.57 GB)	() ()
	<ul> <li>Disk 1 (GPT) 18616.32 GB</li> </ul>	\\?791b) EFI System Partiti)	C:\ (155.73 GB) 👔 \\?\Volu	me[4dd1() X:\ (18383.77 GB) 🕕
	Primary			
▲ <u>U</u> tilities			Back	<u>N</u> ext <u>A</u> bort

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

Source Disk	Destination Disk	
mmary of Volume Restore Settings:		
Source Volume	Destination Volume	On Disk
C:\(155.73 GB)	C:\(155.73 GB) \/?791b0915-1396-4e8d-8dfb-1fa	Disk 0 Disk 0
\(?4dd1123f-0464-4cd6-9df0-1	(1) The provide state of the second state o	Disk 0
EFI System Partition (99 MB)	\\?821d05a8-3ecd-436f-a497-cc0	Disk 0

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

Bare Metal Recovery(BMR) - Start Restore Process	Summary of Restore Settings				
This page displays a summary of the disk/volume	Restore Item		Status	Progress	Throughput
restore settings that you have made.	Restore source volume 'C: \' to current de	estination disk 0	Restoring	1.8%	3115.69 MB/Minute
Note: After the BMR process is complete and server has been rebooted, you may not want to perform backup jobs from this server. If you are just testing the BMR functionality, we recommend that you select the 'Do not start Agent service automatically after reboot' option. When you select this option, you can manually start the Agent service (and the Recovery Point Server service, if installed) after reboot if you want to perform backup jobs. Enable Windows F8 boot option helps user perform further recovery or troubleshooting after BMR. For example, press F8 and boot into Active Directory Service Restore mode to perform Active Directory.	Restore source volume '\/2\Volume(791b     Restore source volume '\/2\Volume(4d1     Restore source volume 'EFI System Parti	123f-0464-4cd6-9df0-1ab9b95c8901}\'			
	Automatically reboot your system after re Do not start Agent service automatically a Boot the system to Advanced Boot Option	after reboot.	8 / Windows Serv	er 2012 and late	- 05.
	-				
	Elapsed Time:	00:00:33			
	Estimated Time Remaining:	00:52:55			
	[1.8%] [1632MB/90738MB] Restoring basic s	ource volume 'C: \' to current destination di	sk 0		
▲ <u>U</u> tilities			Back	Ne	ext <u>A</u> bort

The BMR process is completed successfully.

## **Chapter 9: Performing Appliance Capacity Expansion**

This section contains the following topics:

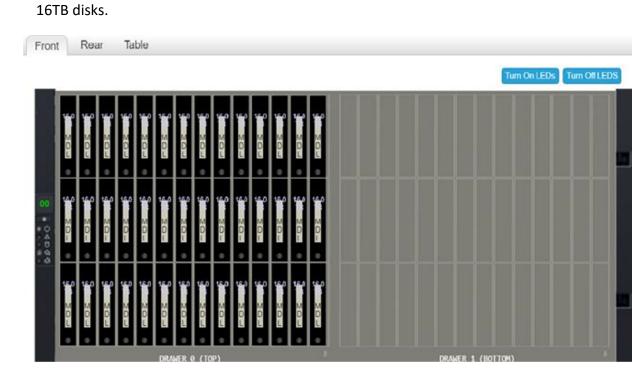
Working with Arcserve Appliance Expansion Kit - X Series Models	192
Working with SSD Flash Expansion Kit in Arcserve X Series Appliance	196
Working with Expansion Kit in Arcserve Appliance 9072-9504 DR Models	206
Working with SSD Flash Expansion Kit in Arcserve Appliance 9072-9504 DR Models .	.211
Connecting Appliance Expansion Shelf to the Appliance Server (8000)	217

## Working with Arcserve Appliance Expansion Kit - X Series Models

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

#### Follow these steps:

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



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

	VA084 Value Array Storage Manager	System: <b>Unini</b> Version: GT28
Home	Action Clear Filters Export	to CSV Show All V S
ADDRESS OF THE OWNER.	Name A V Health	Size
System	Arc01 🤣 OK	5 Storage Setup Add Disk Group
	Related Disk Groups	Modify Disk Group Remove Disk Group
Hosts	Clear Filters Export	Manage Spares
	Name V Health V Pool V RAID	
	Arc01 🤗 OK Arc01 ADA	PT Change Pool Setting Disk Group Utilities Dequarantine Disk C
Pools	Related Disks	
	Clear Filters Export t	to CSV Show All 🗸 S
	Location A V Health V Des	scription 🕎 Siz
Volumes	0.0 🧭 OK SA	S MDL 16.
5		S MDL 16.
		S MDL 16.
Mapping	0.3 🔗 OK SA	S MDL 16.

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

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

Expand Disk Group				
Name:	Arc01	Type:		Linea
Owner:	A	Data Protection	n:	ADAI
Disk Selection Sets, C	omplete: Yes			
Туре	Disk Description	Selected	Maximum	Size
ADAPT	SAS MDL	0	128	672.0TB
Add disks to the disk g	roup by entering a ran	ge of disks or by sele	cting disks from the tab	
Enter Range of Disks:		6		
🔲 Select All 🚺				
Clear Filters Sh	owing 1 to 0 of 0 entries			
Description	Enclosure ID	· •	🍸 Slot 🔺	────────────────────────────────────
No data available in th	e table			

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

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

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

📅 Disk	Management						
File /	Action View Hel	р					
<b>(n</b> m	Refresh						
Volur	Rescan Disks	6	Туре	File System	Status	Capacity	Free Spa
🛲 (C	Create VHD		Basic	NTFS	Healthy (B	155.73 GB	80.56 GB
💻 (Di	Attach VHD		Basic		Healthy (R	499 MB	499 MB
💳 (Di			Basic		Healthy (E	100 MB	100 MB
💻 (Di	All Tasks	>	Basic		Healthy (R	76.29 GB	76.29 GB
	Help						
*O Dis	k0						

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

<b>⊨ →   </b>										
/olume	Layout	Туре	File System	Status		Free Spa	% Free			
= (C:)	Simple	Basic	NTFS	Healthy (B		80.50 GB	52 %			
(Disk 1 partition)		Basic Basic		Healthy (R		499 MB 100 MB	100 % 100 %		6	
<ul> <li>(Disk 1 partition</li> <li>(Disk 1 partition</li> </ul>		Basic		Healthy (E Healthy (R		76.29 GB	100 %		- 0	
*O Disk 0	-									
Unknown 223.57 GB Not Initialized	223.57 GB Unallocated									
Disk 1 Basic			(C-)			-		_		
1489.85 GB Online	499 MB Healthy (Rec		155.73 GB NTFS Healthy (Boot, Page	File, Ci Heal	9 GB thy (Recovery Partit	ii Unalloc				
ODisk 2				1						
18627.45 GB Not Initialized	18627.45 GB Unallocated									
Disk 3 Removable (E:)										
No Media										
*O Disk 4										

## Working with SSD Flash Expansion Kit in Arcserve X Series Appliance

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

#### Follow these steps:

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

b. Insert SSDs in the empty disk slot.



- 2. Perform the following steps to configure Raid-5 from the BIOS Boot Manager option:
  - a. To launch the Virtual Console dashboard, log in to iDRAC, and then click **Start the Virtual Console**.
  - b. In the Virtual Console page, click Boot, and then select the BIOS Boot Manager option.

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

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

The appliance boots and relaunches the Boot Manager setup page.

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

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

DELL EMC PERC S140 Configuratio	n Utility
Configuration Options • Virtual Disk Ma	nagement • Create Virtual Disk
Create Virtual Disk	
Select RAID Level:	Volume
Select Physical Disks From:	Volume KAID 0
Select Physical Disks	RAID 1
Configure Virtual Disk Parameters:	RAID 5 RAID 10
Virtual Disk Size:	0
Virtual Disk Size Unit:	O MB (MegaBytes)
Read Cache Policy:	No Read Ahead
Write Cache Policy:	Write Through
Physical Disk Write Cache:	Default      Default      Disable
	iguration utility supports RAID levels 0, 1, 5 and 10.
(Press <f1> for more help)</f1>	

f. Select the Select Physical Disks option.

Select RAID Level:		
Delect INAID Level.	RAID 5	•
Select Physical Disks From:	Unconfigured Capacity	
elect Physical Disks		
nfigure Virtual Disk Parameters:		
Virtual Disk Size:	0	
Virtual Disk Size Unit:	O MB (MegaBytes)	
Read Cache Policy:	No Read Ahead	•
Write Cache Policy:	Write Through	•
Physical Disk Write Cache:	Oefault      Enable      Disable	
nysical Disk witte Cacile.		

The Select Physical Disk Operation window opens.

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

A list of physical disks is displayed.

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

System Setup		Help   About   Exit
DELL EMC PERC S140 Configuration Utility	,	
Configuration Options • Virtual Disk Manageme	ent • Create Virtual Disk	
Create Virtual Disk Select RAID Level:	m RAID 5	v
Select Physical Disks From: Physical Disk 0:1:8, NVMe, 3.63 TB, Ready Physical Disk 0:2:8, NVMe, 3.63 TB, Ready Physical Disk 0:1:9, NVMe, 3.63 TB, Ready Physical Disk 0:2:10, NVMe, 3.63 TB, Ready Physical Disk 0:2:10, NVMe, 3.63 TB, Ready Physical Disk 0:2:11, NVMe, 3.63 TB, Ready Check All Uncheck All Apply Changes	••• • • Unconfigured Capacity	
<b>(</b> ) Submits the changes made to the entire form.		
Service Tag: G19CR53		Back

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

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

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

Select Interface Type:	-		
Select Physical Disk:	Physical Disk 0:1:8, NVMe, 3.6:	3 TB, Online	•
Convert to Non-RAID Disk			
Convert to RAID Capable Disk			
Manage Physical Disk Properties			
Assign Global Hot Spare			
Jnassign Hot Spare		N	
Cryptographic Erase		2	
ryptographic Erase			

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

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

- 1. Verify that there are no OS-configured RAID arrays, and then click OK.
- 2. Click OK.
- 4. Navigate to **Configuration Options** > **Virtual Disk Management**, and then do the following:



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

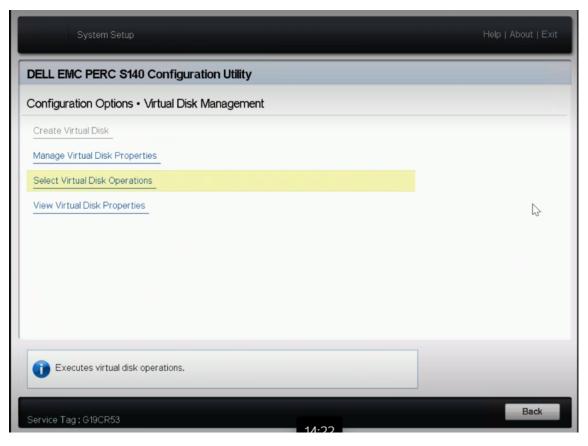
From the Select Virtual Disks drop-down list, select any RAID 5 disk, and then click **View Associated Physical Disks**.

System Setup		Help   About   Exit
DELL EMC PERC S140 Configuration Utility		
Configuration Options • Virtual Disk Managemen	t • Manage Virtual Disk Properties	
Select Virtual Disk:	Virtual Disk 2, RAID 5 , 7.27 TB, Ready	•
Virtual Disk Properties:		
Virtual Disk ID:	2	
RAID Level:	RAID 5	
Virtual Disk Status:	Ready	
Virtual Disk Capacity:	7.27 TB	
Sector Size:	512 bytes	
View Associated Physical Disks		
Manage Dedicated Hot Spares		
Displays the physical disks associated with the virtu	al disk.	
Service Tag: G19CR53		Back

## The associated disks are displayed.

System Setup	About   Exit
DELL EMC PERC S140 Configuration Utility	
Configuration Options • Virtual Disk Management • View Associated Physical Disks	
Selected Virtual Disk: Virtual Disk 2, RAID 5 , 7.27 TB, Ready Associated Physical Disks:	
Physical Disk 0:10, NVMe, 3.63 TB, Online     Physical Disk 0:1:9, NVMe, 3.63 TB, Online     View Physical Disk Properties	
Service Tag : G19CR53	Back

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



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

iDRAC9 Enterprise		
	🖾 Maintenance 🔨 🤹 iDRAC Setting	s ~
O Graceful Shutdown → LED On → More Actions →		
Health Information	System Information	
SYSTEM HAS CRITICAL ISSUES	Power State	ON
STSTENT HAS CRITICAL ISSUES	Model	
System Health Storage Health	Host Name	APPX-QA
8 Critical Details	Operating System	Windows Server 2019
Miscellaneous	Operating System Version	10.0
Power Supplies	Service Tag	G19CR53
	BIOS Version	2.12.2
	iDRAC Firmware Version	5.00.10.20

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

	iDRAC	C9   Enterpri							
ŵ	Dashb	board 📰	System ∨ 🛢 Storage ∨ †‡† Co	onfiguration $^{\checkmark}$	🖾 Maintenance 🗸	🍫 iDRAC Setting	js V		
St	ora	age							
0	verviev	w Tasks							
	Phys	Summary	Controllers	Physi	cal Disks	Virtual Disks		Enclosures	
2	i iiya	nour biono							
	i iiys				▼ Filter Driv	ves			
	link	Unblink	Create Virtual Disk		<b>Y</b> Filter Driv	ves			
			Create Virtual Disk Name	State	Filter Driv	ves Size	Bus Protocol	Media Type	Hot Spare
	link	Unblink		State Non-RAID			Bus Protocol SATA	Media Type SSD	Hot Spare No
В	link	Unblink Status	Name		Slot Number	Size			
8		Unblink Status	Name SSD 0	Non-RAID	Slot Number	<b>Size</b> 223.57 GB	SATA	SSD	No
8 + +		Unblink Status V	Name SSD 0 PCIe SSD in Slot 8 in Bay 1	Non-RAID Online	Slot Number 0 8	<b>Size</b> 223.57 GB 3726 GB	SATA NVMe	SSD	No

- 6. To initialize and format the newly added Virtual Disk, do the following:
  - a. Navigate to Computer Management and Disk Management.
  - b. Double click the new virtual disk that you added.

The Initialize Disk window appears.

- c. Select the GPT (GUID Partition Table) option and click OK.
- d. From the Disk Management window, select the virtual disk and apply the following properties:
  - \* Assign a Drive Letter
  - Specify NTFS as File System
  - Format the disk

<b>.</b>										-	
Computer Management									-		×
File Action View Help											
🗢 🔿 🙇 🔟 📓 📼 🗩 🤅	2 💷										
E Computer Management (Local					Status				Actions		
V 👫 System Tools	= (C:)	Simple					Crash Dump, Primary Partitio	n)	Disk Manageme	int	
> P Task Scheduler > III Event Viewer	(Disk 0 partition 2) = 2_6_7-28-AM (D:)					y (EFI System Parti y (Active, Primary )			More Actio	ns	•
Shared Folders	New Volume (E:)	Simple				y (Primary Partition					
> A Local Users and Groups	- Recovery	Simple				y (OEM Partition)	.,				
> N Performance	- UDPData1 (X:)	Simple	Basic	NTFS	Health	y (Primary Partition	n)				
A Device Manager	<ul> <li>UDPFactoryReset</li> </ul>					y (OEM Partition)					
✓ A Storage	- UDPHash (Y:)	Simple	Basic	NTFS	Health	y (Primary Partition	n)				
> 🚯 Windows Server Backup											
T Disk Management											
> 🔓 Services and Applications	<							>			
	- Disk 0										
		Recove		(C:) 155.73 GB NT		UDPFactoryRes	UDPData1 (X:)				
		499 MB Healthy	100 N Healt	Healthy (Boo		76.29 GB NTFS Healthy (OEM Pa	22121.87 GB NTFS Healthy (Primary Partition)				
		- Carlony		i nearring (and		Country (Country	reading of minary readering				
							1				
	- Disk 1										
		UDPHash									
		1787.87 G8 Healthy (P		Destition)							
	o mine	ricaluty (P	nmary	rancicioni							
	- Dak 2										
		New Volu 10729.11 G									
		Healthy (P									
	— Disk 3										
		2 6 7.28.		4	_			_			
		117.87 GB					1				
< >	Unallocated P	nimary par	ucon								

The virtual disk is created.

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

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

#### Follow these steps:

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



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

A dialog appears to display the following warning message:

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

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

c. Click OK.

The Convert to Raid status appears under Pending Actions.

Dashboard	i 🗏 System 🗸 🛢 Storage 🗸	Configurat	ion 🗸 🖂 Mainte	nance∨ ®₀ iD	RAC Settings 🗸		🖻 Open Group Manager 💌
	configuration						🕏 Edit SSD Wear Thresh
Status	Name	State	Hotspare Status	Capacity	Media Type	Action	Pending Actions
	Physical Disk 0:1:10	Non-RAID	Unassigned	10949.00 GB	HDD	Action •	Convert to RAID
	Physical Disk 0:1:11	Non-RAID	Unassigned	10949.00 GB	HDD	Action •	Convert to RAID
	Physical Disk 0:1:14	Non-RAID	Unassigned	10949.00 GB	HDD	Action •	Convert to RAID
	Physical Disk 0:1:15	Non-RAID	Unassigned	10949.00 GB	HDD	Action •	Convert to RAID
	Physical Disk 0:1:16	Non-RAID	Unassigned	10949.00 GB	HDD	Action •	Convert to RAID
	Physical Disk 0:1:17	Non-RAID	Unassigned	10949.00 GB	HDD	Action •	Convert to RAID
Virtual Disk	Configuration						
Enclosure (	Configuration						

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.

Create Virtual Disk	
Name	Enter or use auto-name
Layout	RAID-6 *
Media Type	HDD *
Stripe Element Size	64 KB 🔻
Capacity*	14.55 TB 🔻
Read Policy	Read Ahead
Write Policy	Write Back
Disk Cache Policy	Default 🔻
T10 PI Capability	Disabled •
Span Count	1.
	Cancel 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.

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

File       Action       View       Help         Image: Computer Management (Local System Tools Computer Management (Local System Tools Computer Management (Local System Tools Computer Management (Local System Tools Computer Management (Local Computer Management (Local) Computer Managemen
Computer Management (Local       Volume       Layout Type       File System       Status       Cape         System Tools       System Tools       Simple Basic       Healthy (Recovery Partition)       300 h         Event Viewer       Simple Basic       Healthy (Recovery Partition)       99 M         Shared Folders       Simple Basic       Healthy (Recovery Partition)       99 M         C(C)       Simple Basic       Healthy (Recovery Partition)       99 M         C(C)       Simple Basic       Healthy (Recovery Partition)       96 M         More Actions       UDPDate (X)       Simple Basic       NTFS       Healthy (Pinnary Partition)       1467         UDPHash (Y)       Simple Basic       NTFS       Healthy (Pinnary Partition)       1467       Nore Actions         UDPHash (Y)       Simple Basic       NTFS       Healthy (Pinnary Partition)       1787         UDPHash (Y)       Simple Basic       NTFS       Healthy (Pinnary Partition)       1787         Verific Storage       Vourmut intibilize Disk       Vourmut intibilize a dak before Logical Disk Manager can access it.       Select disks:         Volume       Use the following partition style for the selected disks:       More Actions of Memory       More Actions of Memory         MBR (Master Boot Record)       W SPT (GUID
V       System Tools       3001         O Task Scheduler       Simple Basic       Healthy (Recovery Partition)       3001         Mexent Viewer       Simple Basic       Healthy (Recovery Partition)       99 M         More Actions       Simple Basic       Healthy (Recovery Partition)       99 M         More Actions       Simple Basic       Healthy (Recovery Partition)       99 M         More Actions       Simple Basic       Healthy (Recovery Partition)       96 M         More Actions       UDPData (X)       Simple Basic       NTFS       Healthy (Primary Partition)       1467         More Actions       UDPData (X)       Simple Basic       NTFS       Healthy (Primary Partition)       1467         Windows Server Backup       Simple Basic       NTFS       Healthy (Primary Partition)       1787         More Actions       Vourmat Intialize Disk       X       You must Intialize a dak before Logical Disk Manager can access it.       Select disks:         Imitialize Disk       Use the following partition style for the selected disks:       More Actions of Meximum         Mind Mater Boot Record)       More Ref (P attion table)       Note: The GPT partition table is not recognized by all previous versions of Meximum
<ul> <li>Simple Basic Healthy (EFI System Partition)</li> <li>Simple Basic Healthy (EFI System Partition)</li> <li>Simple Basic NTFS Healthy (Recovery Partition)</li> <li>C(.) Simple Basic NTFS Healthy (Recovery Partition)</li> <li>DDData (X) Simple Basic NTFS Healthy (Recovery Partition)</li> <li>DDData (X) Simple Basic NTFS Healthy (Primary Partition)</li> <li>DDDAta (X) Simple Basic NTFS Healthy (Recovery Partition)</li> <li>DDDAta (X) Simple Basic NTFS Healthy (Recovery Partition)</li> <li>DDDAta (X) Simple Basic NTFS Healthy (Primary Partition)</li> <li>Total Recovery Simple Basic NTFS Healthy (Primary Partition)</li> <li>More Actions</li> <li>M</li></ul>
<ul> <li>Simple Basic Healthy (Ef system Partition) 99 M</li> <li>Simple Basic Healthy (Ef system Partition) 76.25</li> <li>Shared Folders</li> <li>Cos Berlor and Groups</li> <li>Cos Performance</li> <li>UDPData (X) Simple Basic NTFS Healthy (Primary Partition) 1467</li> <li>UDPHash (Y) Simple Basic NTFS Healthy (Primary Partition) 1787</li> <li>Windows Server Backup</li> <li>Storage</li> <li>Windows Server Backup</li> <li>Storage</li> <li>Services and Applications</li> <li>Gobisk 0</li> <li>Ude the following partition style for the selected disks:</li> <li>Obisk 0</li> <li>More Actions the selected disks:</li> <li>Services and Applications</li> </ul>
> Image: Strate Folders
Local Users and Groups     UDPData (X)     Simple Basic NTFS Healthy (Primary Partition) 1467     UDPTata (X)     Simple Basic NTFS Healthy (Primary Partition) 1467     UDPTata (X)     UDPTata (X)     Simple Basic NTFS     Healthy (Primary Partition) 1467     Initialize Disk     Vournaut Initialize a disk before Logical Disk Manager can access a     Secret cas and Applications     UDPTata (X)     UDPTata (X)     UDPTata (X)     UDPTata (X)     Simple Basic NTFS     Healthy (Primary Partition) 1467     Initialize Disk     Vournaut Initialize a disk before Logical Disk Manager can access a     UDPTata     Vournaut Initialize a disk before Logical Disk Manager can access a     Ues the following partition style for the selected disks:     OMBR (Master Boot Record)     @ GPT (GUID Partition Table)     Note: The GPT partition style is not recognized by all previous versions of
Constraints and Applications
> ● Performance       Initialize Disk       ×         > ● Storage       > ● Windows Server Backup       Initialize a disk before Logical Disk Manager can access #.         > ● Services and Applications        Select disks:         ♥ Disk Management           > ● Services and Applications           Image: Part of the selected disks:           ● Disk 0       Use the following pattion style for the selected disks:          ● SPT (GUID Pattion Table)       Note: The GPT pattion style is not recognized by all previous versions of Mercines
You must initiate a dak before Logical Dak Manager can access it.     You must initiate a dak before Logical Dak Manager can access it.     Secret cas and Applications     C     Construct a secret data:     Constr
> Windows Server Backup
Select disks:     Select disks:     Disk Management     Services and Applications     C     Use the following pattion style for the selected disks:     OMBR (Master Boot Record)     @ GPT (GUID Pattion Table)     Unknown     14903.00 GB     Note: The GPT pattion style is not recognized by all previous versions of     Note: The GPT pattion style is not recognized by all previous versions of
Services and Applications     C     Use the following pattion style for the selected disks:     OMBR (Master Boot Record)     @ GPT (GUID Pattion Table)     Unknown 1490300 GB     Note: The GPT pattion style is not recognized by all previous versions of
<      Use the following partition style for the selected disks:     OMBR (Master Boot Record)     @ GPT (GUID Partition Table)     Unknown 14903.00 GB Note: The GPT partition style is not recognized by all previous versions of
O MBR (Master Boot Record)     O MAR (Master Boot Record)
O MBR (Master Boot Record)     O MAR (Master Boot Record)
O MBR (Master Boot Record)     O MAR (Master Boot Record)
O MBR (Master Boot Record)     O GPT (GUID Pattion Table)     Unknown     Id903.00 GB     Note: The GPT pattion style is not recognized by all previous versions of     Note: The GPT pattion style is not recognized by all previous versions of
Obisk 0     @ GPT (GUID Patition Table) Unknown 14903.00 GB     Note: The GPT partition style is not recognized by all previous versions of     Note: The GPT partition style is not recognized by all previous versions of
Unknown 14903.00 GB Wordows
14903.00 GB Note: The GPT partition style is not recognized by all previous versions of Workness
Not Initialized Trinovis.
OK Cancel
Basic (C) (D) (D) (D) (D) (D) (D) (D) (D) (D) (D
Basic (C.) UDPData (XC) 14902.88 GB 300 ME 99 M 155.73 GB NTFS 76.29 GB 14670.46 GB NTFS
Online Health Healt Healthy (Boot, Pac Healthy (Recover Healthy (Primary Partition)
= Disk 5
Basic UDPHash (Y) 1787.87 GB 1787.87 GB 1
1787.87 GB 1787.87 GB NTFS Online Healthy (Primary Partition)
< >> Unallocated Primary antition

- 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**.

dashboard resources				ettings	high	availab	ility		and the second sec
	« Des	tina	ations: Recovery Po	int Server					appliatest75 > applia
Nodes All Nodes	Acti	ons	Add a Recove	ry Point Serv	er				Configuration Wizard
Nodes without a Plan			Name	Statu	s Plan	Count	Stored Data	D	Status
<ul> <li>Plan Groups</li> <li>Linux Backup Server Groups</li> </ul>	- 1	-	appliatest75						Running
Plans All Plans			appliatest75 data stor	m 👩	1		0 Byte	0	Backup Destination 18 TB free of.
Destinations Recovery Point Servers			De						Data 18.2 TB tree
Arcserve Backup Servers			-Sto						Destination 18 TB free et.
Shared Folders Cloud Accounts	4			wse Recovery I S Jumpstart	Points			-	Hash 223.5 GB tree.
Remote Consoles									Memory Allocation
Storage Arrays									✓ Settings
Instant Virtual Machines Sites									Compression Standard
SLA Profiles									Encryption AES-256

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 appliatest?5_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
                                     X:\Arcserve\data_store\data\
18384 GB 1 GB
Primary data path :
                                                                                                                 18383 GB
Expanded data path1:
                                     Y:\data
                                     224 GB
                                                                           1 GB
                                                                                                                 223 GB
                                                                           2 GB
Total
                                     18608 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.

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

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

#### Follow these steps:

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



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

A dialog appears to display the following warning message:

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

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

c. Click OK.

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

E	Integrated R	emote Access Controller 9 Enter							
1	Dashboard	I System∨ I Storage∨	Configuration	∼ ⊡ Mainter	ance∨ e, ibi	NAC Settings 🗸			B Open Group Manager
>	Controller Cont	figuration							
~	Physical Disk (	Configuration 😔 6 Pending							P Edit SSD Wear 1
	Status	Name	State	Hotspare Status	Capacity	Media Type	Action		Pending Actions
	8	Physical Disk 0.1.10	Non-RAID	Unassigned	10949.00 GB	HCO	Action		Convert to RAID
	2	Physical Oisk 0:1:11	Non-RAID	Unassigned	10949.00.08	ноо	Action	٠	Convert to RAID
	8	Physical Disk 0.1.14	Non-RAID	Unassigned	10949.00 GB	HCO	Action		Convert to RAID
	2	Physical Oisk 0:1:15	Non-RAID	Unassigned	10949.00.08	ноо	Action	٠	Convert to RAID
	8	Physical Disk 0.1.16	Non-RAID	Unassigned	10949.00 GB	HOD	Action		Convert to RAID
	2	Physical Oisk 0:1:17	Non-RAID	Unassigned	10949.00.08	HED	Action	*	Convert to RAID
	Virtual Disk Co								
>	Enclosure Con	Aguration							
I	Apply Now	At Next Reboot At Scheduled Tim	e Discard All Pero	ing					

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

#### **Apply Now**

Starts the convert to Raid action immediately.

#### At Next Reboot

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

#### **At Scheduled Time**

Starts the convert to Raid action at the scheduled time.

#### **Discard All Pending**

Discards the convert to Raid action for all the disks.

e. Navigate to Maintenance, Job Queue.

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

) ] <sup>  </sup>	-										
ñ (	ashb 23		System ∨ 😸 Storag	e∨ E	Configuration	V 🖂 Main	tenance V 🛛 🔍 🖗	iDRAC Settings ∨			Enable Gro
- 10		Status	Name	Chate	Slot Number	Size	Cartorino Chature	Bus Protocol	Marin Turn	List Cours	Demoising Dated White For
			rvarine	State	and number	0428	Security Status	DUS PTOLOCOI	Media Type	Hot Spare	Remaining Rated Write End
+		2	Physical Disk 0:1:0	Online	0	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable
+			Solid State Disk 0:1:1	Online	1	3576.38 GB	Not Capable	SAS	SSD	No	100%
+			Solid State Disk 0:1:2	Online	2	3576.38 GB	Not Capable	SAS	SSD	No	100%
+			Solid State Disk 0:1:3	Online	3	3576.38 GB	Not Capable	SAS	SSD	No	100%
+			Solid State Disk 0:1:4	Online	4	3576.38 GB	Not Capable	SAS	SSD	No	100%
+			Solid State Disk 0:1:12	Online	12	1787.88 GB	Not Capable	SATA	SSD	No	100%
+			Solid State Disk 0:1:13	Online	13	1787.88 GB	Not Capable	SATA	SSD	No	100%
+			Physical Disk 0:1:14	Online	14	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable
+			Physical Disk 0:1:15	Online	15	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable
+	0		Physical Disk 0:1:16	Online	16	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable

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

#### Create Virtual Disk

Name	UDPFlash
Layout	RAID-5 🗸
Media Type	SSD 🗸
Stripe Element Size	64 KB 🗸
Capacity*	10.48 TB 🗸
Read Policy	Read Ahead 🗸
Write Policy	Write Back 🗸
Disk Cache Policy	Default 🗸
T10 PI Capability	Disabled ~
Span Count	1 ~

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

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

]	Integrate	ed Rer	note	Access (	Controll	er 9   E	Enterpri	se			
ħ	Dashboa	rd		System 🗸	8	Stora	ge∨	114	Configuration	$\sim$	📼 Ma
С	onfig	gura	ati	on							
I	Power Mar	nageme	ent	Virtual	Console	e V	/irtual M	edia	Licenses	Sys	tem Set
		_	_	-	_	_	_		tings are confiri is created or th	-	
C	ontroller	PERC	H73(	0P Mini (En	nbeddeo	d) ~					
>	Controller	Config	gurat	ion							
>	Physical I	Disk Co	onfigu	uration							
~	Virtual Di	sk Con	figura	ation							
	Create V	'irtual D	)isk								
	Status			Name			R	AID L	evel		Ded
				UDPData	3		R	AID-6			Non
				UDPHas	h		R	AID-1			Non
				UDPFlas	h		R	AID-5			Non
>	Enclosure	e Config	gurat	ion							
l	Apply Nov	v A	t Nex	t Reboot	At Sc	hedule	d Time	Dis	card All Pending	g	

h. Navigate to Maintenance > Job Queue.

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

i. Navigate to Computer Management and Disk Management.

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

The Initialize Disk window appears.

- k. Select the GPT (GUID Partition Table) option and click OK.
- I. From the Disk Management window, select the virtual disk and apply the following properties:
  - \* Assign a Drive Letter
  - \* Specify NTFS as File System
  - \* Format the disk

Computer Management File Action View Help									×
🗢 🏟 🙍 📷 📓 🗩 🛛	2 🗉								
Computer Management (Local System Tools Carask Scheduler Carask	Volume (C:) (Disk 0 partition 2 2,6,7-28-AM (D:) New Volume (E:) Recovery UDPDta1 (X:) UDPTactoryReset UDPHash (Y:) C DBasic	Simple Simple Simple Simple Simple Simple Simple	Basic Basic Basic Basic Basic Basic Basic	NTFS FAT32 NTFS NTFS NTFS NTFS	Healthy (EFI System Parti Healthy (Active, Primary Healthy (Primary Partitio Healthy (OEM Partition) Healthy (OEM Partition) Healthy (Primary Partitio	Partition) n) n)		Actions Disk Manageme More Action	
	Online Disk 1 Basic 1787.87 GB		(Y:)	Healthy (Bool		22121.87 GB NTFS Healthy (Primary Partition)			
	10729.11 G8 Online — Disk 3	New Volu 10729.11 G Healthy (Pi	B NTFS rimary	Partition)		•	I		
()		2 6 7.28. 117.87 GB i	FAT32	4			•	_	

The virtual disk is created.

## **Connecting Appliance Expansion Shelf to the Appliance Server (8000)**

This section contains the following topics:

# Appliance Infield Expansion for all the Available Models

Mod- el	Current Capacities \TB	Expan- sion Shelf Capacity	Cur- rent SSD - GB	Ne- w SSD REQ -GB	Free Slot- s	Add-on Cards	DES	CRIPTION
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 Cop- per Infield Expansion - (MegaRAI- D SAS 9380-8e)	2. 3.	8100 model sup- ports only 8 TB Infield Expansion. 8100 - 8 TB Expansion Shelf comes with inbuilt and pre-con- figured SSD 240 GB. 8100 has 2 and 3 as optional slots . One free slot is mandatory for Appli- ance Infield Expansion / MegaRAID SAS 9380- 8e. If both the optional slots are filled with add-on Cards, then

			<b></b>	1	
					you need
					to free at
					least one
					slot , prefer
					ably slot 3
					in order to
					use Infield
					Expansion.
				5.	SAS con-
					nection is
					used
					between
					the Appli-
					ance and
					Expansion
					shelf.
				6	8100 -
				0.	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

							1.	Migrate HASH des- tination to new SSD instruc- tions given in the Expansion Guide. 8200
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 Cop- per Infield Expansion		model sup- ports either 8 TB or 16 TB Infield Expansion. Client can connect only one expansion shelf any time. 8200 - 16 TB Expan- sion Shelf comes with inbuilt and pre-con- figured SSD 480 GB. 8200 has 2 and 3 as
						(MegaRAI- D SAS 9380-8e)		and 3 as optional slots. One free slot is mandatory for Appli- ance Infield Expansion / MegaRAID

				SAS 9380-
				8e.
			1	If both the
			4.	optional
				slots are
				filled with
				add-on
				Cards, then
				you need
				to free at
				least one
				slot, prefer-
				ably 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.
			o	Follow Add
			0.	data path
				instruc-
				tions given
				in Expan-
				sion guide after con-
				necting the

								expansion shelf.
							9.	Wherever a new SSD is required follow the <b>Migrate</b> <b>HASH des-</b> <b>tination to</b> <b>new SSD</b> instruc- tions 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 Cop- per Infield Expansion (MegaRAI- D SAS 9380-8e)	2.	8300 model sup- ports either 8 TB or 16 TB OR 40 Infield Expansion. Client can connect only one expansion shelf any time. 8300 - 16 TB / 40 TB Expansion Shelf comes with inbuilt and pre- configured SSD 1.9 TB. 8300 has 2, 5, and 6 as

	I		1	
				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-
			5.	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 instruc- tions given in Expan- sion guide after con- necting the expansion shelf
			9.	shelf. Wherever a new SSD is required follow the <b>Migrate</b> <b>HASH des-</b> <b>tination to</b> <b>new SSD</b> instruc- tions given in Expan- sion Guide. (Only for Appliance 8300 con- nect with 40 TB Appli- ance expan- sion shelf, there is one unat-
				tached 2 TB SSD that you need to place in Base appli- ance and

8400 32		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 Cop- per Infield Expansion (MegaRAI- D SAS 9380-8e)	2.	not expan- sion shelf. Check expansion guide from details). 8400 model sup- ports either 8 TB or 16 TB OR 40 TB Infield Expansion . Client can connect only one expansion shelf any time. 8400 - Requires no addtional SSD. 8400 has 2, 5, and 6 as optional slots. One free slot is mandatory for Appli- ance Infield Expansion / MegaRAID SAS 9380- 8e. If both the optional slots are
---------	--	--	------	--	------------	--	----	---

filled v	
add-or	
Cards,	
you ne	eed
to free	e at 🛛
least c	one
slot, p	refer-
ably sl	lot 2
in orde	er to 🛛
use In	field
Expan	sion.
5. SAS cc	
nectio	
used	
betwee	
the Ap	
ance a	
Expan	sion
shelf.	
6. Expan	sion
shelf	
comes	s with
RAID-6	6.
7. Expan	sion
Shelf	
comes	s with
Dual P	
8. Follow	
Add d	ata
path	
instruc	
tions g	
in the	
Expan	
guide	after
conne	cting
the ex	pan-
	helf.

## 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 <u>Arcserve Support</u>.

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 40TB Appliance expansion and you have one unattached 2TB 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.

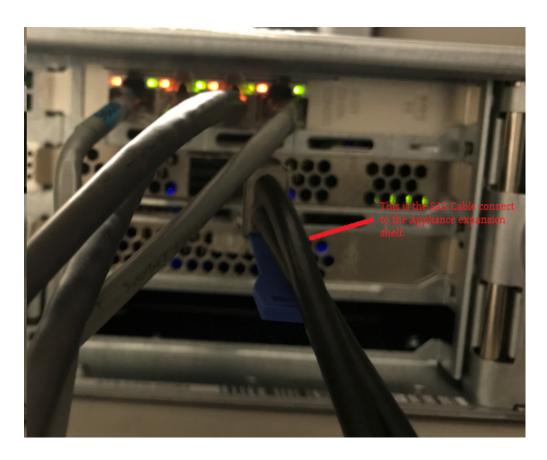
**Note:** Disconnect the computer from the power supply to avoid the risk of damaging the system or electric shock.

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.

3	MegaRAID	Storage Manager 15.05.01.00 - Host View	x
			Avago
Server Details This page displays all the servers th You will be prompted for entering he Use Configure Host to configure the	ost credentials while logging		
Use LDAP Login		Enter User Name & Password	×
IP Address 10.!		Avag	Configure Host
Remote servers:	Server :	10.1 Use your Operating System's login username and password to login the MSM server	
appliance-8400	User Name: Password:	administrator	
	Login Mode:	Full Access v	
		Login Cancel	

- 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**.

udpu2verify	
<ul> <li>Controller0: AVAGO MegaRAID SAS</li> <li>SC826P (16), Connector: Pc</li> <li>Slot: 0, SAS, 1.819 TB,</li> </ul>	5 9380-8e(Bus 1 Dev 0 Domain 0) Disable Alarm Silence Alarm
	Start Patrol Read Set Patrol Read Properties
<ul> <li>Slot: 4, SAS, 1.819 TB,</li> <li>Slot: 5, SAS, 1.819 TB,</li> </ul>	Disable SSD Guard
	Scan Foreign Configuration
Controller 1: AVAGO MegaRAID	Save Configuration
<ul> <li>Slot: 0, SAS, 3.639 TB,</li> <li>Slot: 1, SAS, 3.639 TB,</li> <li>Slot: 2, SAS, 3.639 TB,</li> </ul>	Set Consistency Check Properties Schedule Consistency Check
	Set Adjustable Task Rates
	Preserved Cache
	Manage Power Save Settings
	Update Controller Firmware Manage MegaRAID Advanced Software Options Manage Link Speed Save TTY Log

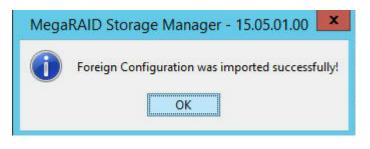
c. Select the **Import: Import logical configuration from all foreign drives** option and click **OK**.

Foreign Configuration Detected
7 Foreign drives were detected. You must import or clear these drives before they can be used.
Choose an option:

d. Click Yes to initiate the import process.

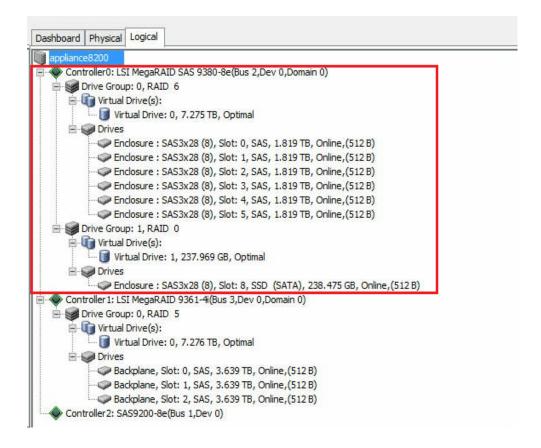


e. Click OK.



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:".

			Comp	outer Mai	nagement		
File Action View Help							
Þ 🔶 🙎 📰 📓							
Provide the terminal of the terminal sector of termin	Volume	Layout Type	File System	Status			Capa
⊿ 👔 System Tools	G	Simple Basi	-	Healthy (F	Recovery Partition)		300 N
D Task Scheduler		Simple Basi	-	Healthy (	EFI System Partition)		99 M
Event Viewer		Simple Basi	E	Healthy (F	Recovery Partition)		76.29
Shared Folders	🕞 (C:)	Simple Basi	C NTFS	Healthy (	Boot, Page File, Crash	Dump, Primary Partition)	155.7
Local Users and Groups	📼 (V:)	Simple Basi	c NTFS	Healthy (I	Primary Partition)		7449.
Performance	📾 (X:)	Simple Basi	c NTFS	Healthy (F	Primary Partition)		7218.
Device Manager	(Y:)	Simple Basi		100 C 100	Primary Partition)		223.5
4 🚝 Storage	Rew Volume (W:	) Simple Basi	C NTFS	Healthy (	Primary Partition)		237.8
							>
<ul> <li>Windows Server Backup</li> <li>Disk Management</li> <li>Services and Applications</li> </ul>	Carlosk 1 Basic	(V-)	Ш				
Disk Management	Disk 1 Basic 7449.88 GB	<b>(V:)</b> 7449.87 GB NTF Healthy (Primai	s				
Disk Management	Disk 1 Basic 7449.88 GB	7449.87 GB NTF	s				
Disk Management	Disk 1 Basic 7449.88 GB Online Basic 237.84 GB	7449.87 GB NTF	S y Partition) 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:

- 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	
How to Configure the NIC Teaming Process	250
How to Disable DHCP Server	
How to Configure IP Address for the Preinstalled Linux Backup Server	253
How to Enable Round Robin on the DNS Server to Balance Load	
How to Check Network Status on Appliance	

# **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.

Virtual Machin	nes					
Name	^		State	CPU Usage	Assigned Memory	Uptime
E Linux-Backu	Linux-BackupSvr		Running	0 %	4096 MB	00:07:26
<	*	Virtu X N	I Switch Manager fo al Switches lew virtual network sw inux-BkpSvr-Switch internal only	vitch	Name: Linux-BkpSvr-Switch	erties —
Checkpoint	~	Q M	al Network Setting IAC Address Range 00-15-5D-0A-01-00 to		Notes:	
					Connection type What do you want to C External network	
					0	reme Gigabit Etherne
Linux-Backı					Enable single	ment operating system of the s
2034					<ul> <li>Internal network</li> <li>Private network</li> </ul>	

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.

LinuxBkpSvr	Unidentified network	Hyper-V Virtual	Ethernet Adapter No network access
LinuxBkpSvr Properties Networking Sharing	X Internet General	Protocol Version 4 (TCP/IPv4	) Properties X
Connect using:	this can for the gure	ability. Otherwise, you need to appropriate IP settings. otain an IP address automatica	matically if your network supports ask your network administrator By
Clert for Microsoft Networks     Ges Packet Scheduler     Internet Protocol Version 4 (TCP/IPv4)     Microsoft Network Adapter Multiplexor Protocol     Microsoft LLDP Protocol Driver	A IP a Sub	e the following IP address: ddress: et mask: uit gateway: biain DNS server address autor	192.168.10.1         255.255.255.0            natically
Internet Protocol Version 6 (TCP/IPv6)     <	>	e the following DNS server add	
Install Uninstall Proper Description	Alte	erred DNS server: nate DNS server:	· · ·
Transmission Control Protocol/Internet Protocol. The del wide area network protocol that provides communication across diverse interconnected networks.		alidate settings upon exit	Advanced
ОК	Cancel		OK Cancel

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

👮 DHCP			—		$\times$
File Action View	Help				
🗢 🔿 🙍 🏹	🕻 🖾 🧟 📑 🛛 🖬 💭 💷				
DHCP	Name	Actions			
<ul> <li>appliance</li> <li>IPv4</li> </ul>	Server Bindings Properties			?	$\times$
> 🔒 IPv6	IPv4 IPv6				
	Select the connections that the DHCP server support empty, verify that a static IP address is configured for Connections and server bindings:	this computer		f this list is	

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.

望 DHCP File Action View Help ◆= ➡   〒   凾   図 〒   具			
<ul> <li>DHCP</li> <li>appliance</li> <li>IPv4</li> <li>Server Options</li> <li>Scope [192.168.10.0] nat</li> <li>Address Pool</li> <li>Address Leases</li> <li>Reservations</li> <li>Scope Options</li> <li>Policies</li> <li>Policies</li> <li>Filters</li> <li>IPv6</li> </ul>	Start IP Address	End IP Address 192.168.10.2	Description Address range for distribution

We have configured NAT on the Appliance machine.

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

Administrator: Command Prompt

```
c:\Windows\System32>netsh routing ip nat dump
# .....
# NAT configuration
# .....
pushd routing ip nat
uninstall
install
set global tcptimeoutmins=1440 udptimeoutmins=1 loglevel=ERROR
#
#NAT Configuration For Interface NIC4
# add interface name="NIC4" mode=FULL
#
#
#NAT Configuration For Interface LinuxBkpSvr
#
add interface name="LinuxBkpSvr" mode=PRIVATE
popd
```

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

:\Windows\	System32>netsh	n interface portp	roxy show all
Listen on i	pv4:	Connect to ip	/4:
Address	Port	Address	Port
*	8018	192.168.10.2	8014
*	8019	192.168.10.2	22
*	8035	192.168.10.2	8035
*	8017	192.168.10.2	8017
ŧ	8021	192.168.10.2	8021
8	50000	192.168.10.2	50000
	50001	192.168.10.2	50001
*	50002	192.168.10.2	50002
*	50003	192.168.10.2	50003
*	50004	192.168.10.2	50004

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

```
[root@Linux-BackupSvr network-scripts]# cat ifcfg-eth0
TYPE=Ethernet
B00TPR0T0=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.

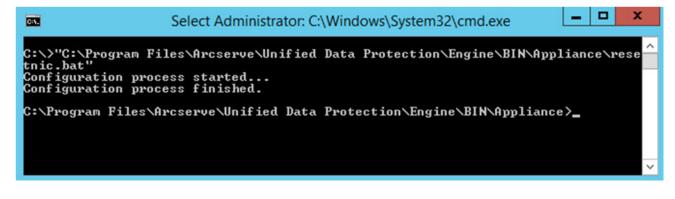
**Note**: If a DHCP or static IP address is used, you can configure the IP address for the NIC Team in the Network Connections screen. Ensure that a valid IP address is assigned to the NIC Team and is available on your network.

Network Connections	5		
Connection Name	IP Address	Description	
Ethernet 2 Connected	10.57.25 Automatic via DHCP	Intel(R) I350 Gigabit Network Connection #2	Edit
-			
		Activate	Windows

2. Run the following command:

```
C:\\Program Files\Arcserve\Unified Data Pro-
tection\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 pre-installed 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.
- 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 obtains IPAddress1 when sending a query for Altname1 and always obtains IPAddress2 when sending a query for Altname2.

### How to Check Network Status on Appliance

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

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

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

- 1. Log into the Arcserve Appliance Server as an administrator.
- 2. Open the command prompt and enter the folder location:

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

3. Run ApplianceNetworkStatusCheck.ps1 to generate report:

#Powershell .\ApplianceNetworkStatusCheck.ps1



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

# **Chapter 11: Understanding Safety Precautions**

This section contains the following topics:

General Safety Precautions	258
Electrical Safety Precautions	
FCC Compliance	
Electrostatic Discharge (ESD) Precautions	

### **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)으로전자파적합기기로서판매자또는사용자는 이점을주의하시기바라며,가정외의지역에서사용하는것을목적으로 합니다

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

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

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

### **Electrical Safety Precautions**

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

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

### **FCC Compliance**

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

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

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

### **Electrostatic Discharge (ESD) Precautions**

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

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

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

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

### Important!

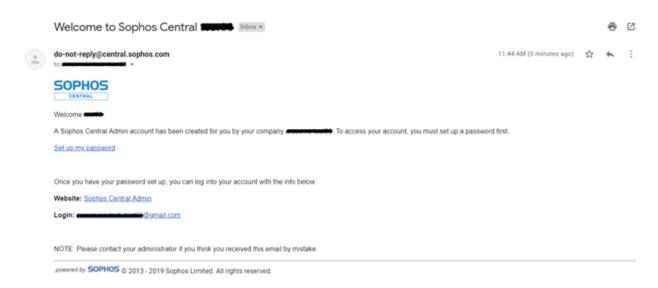
- If you are a new customer of Arcserve Appliances with Sophos Intercept X preinstalled as part of the delivery process, an email is sent with simple activation instructions. Please follow the given methods to complete the activation process. If you are an existing customer, the Arcserve Appliances have no Sophos Intercept X preinstalled. It is recommended to download and install Sophos Intercept X manually.
- Activation of Sophos using Method 1 or Method 2 is not applicable for Appliance X Series, and you need to install Sophos manually. For information about the complete installation process, see <u>Manually Installing Sophos Inter-</u> <u>cept X Advanced for Server on Arcserve Appliances</u>.

#### Follow these steps:

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

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

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



2. Two methods are provided to activate Sophos on the Arcserve Appliance.

**Note:** To activate more Arcserve Appliance Sophos, repeat steps from Method 1 or Method 2 as needed.

- Method 1: Activate Sophos on the Arcserve Appliance using the email from Arcserve.
- Method 2: Activate Sophos on the Arcserve Appliance using the script Customer\_Boot.ps1

### Method 1: Activate Sophos on the Arcserve Appliance using the email

Arcserve sends you a Zip file through email for activating Sophos. Unzip the file. The folder "Arcserve\_Appliance\_Sophos\_Activation\_YYYY-MM-DD-HH-MM-SS" contains the following files:

- **Config.xml:** The configuration file.
- **Registration.txt:** The registration file.
- Arcserve\_Appliance\_Sophos\_Activation.ps1: Powershell script to run to activate Sophos.

#### Follow these steps to activate Sophos:

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

#### 4. Run Arcserve\_Appliance\_Sophos\_Activation.ps1.

#powershell .\ Arcserve\_Appliance\_Sophos\_Activation.ps1

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

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

S	OPHOS CENTRAL Admin	Servers View and manage y					
C	Overview	Computers	Mobile Devices	Servers Servers			
🛃 Deshbo	ard	Search	Q Show	all servers	✓ All Health	Status	*
🛕 Alerts							
C Threat	Analysis Center 🕨	Name		IP		OS	
📄 🛯 Logs &	Reports						
📌 People	_						
Device:	5						

Sophos is activated on the Appliance.

### Method 2: Activate Sophos on the Arcserve Appliance using script

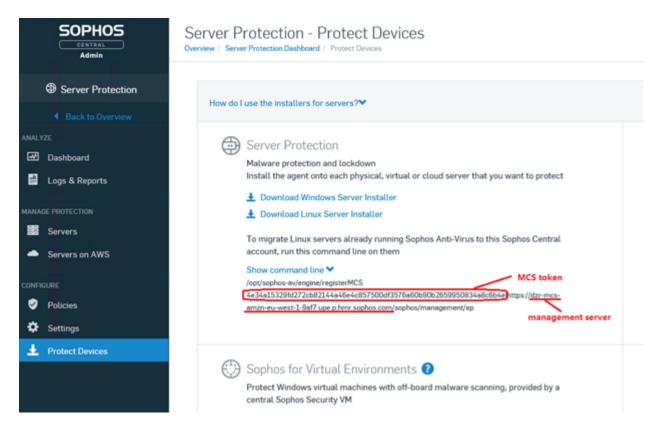
This section provides information about how to activate Sophos on the Arcserve Appliance using the script Customer\_Boot.ps1.

#### Follow these steps:

 To log into the Sophos Central page, go to <u>https://cloud.sophos.com</u> using your email address and password.

**Note:** If you have multiple email addresses associated with different Arcserve Appliance Sophos customer accounts, select a desired email address to use its corresponding account to activate Sophos.

2. Navigate to the Protection Devices page, under Server Protection, click the Show Command Line link.



- 3. Copy the mcstoken and management server information.
- 4. Log into the Arcserve Appliance system as an administrator.
- 5. Open the command prompt and enter the folder location "C:\Program Files\Arcserve\Appliance\Sophos\Customer\_Boot"

#cd "C:\Program Files\Arcserve\Appliance\Sophos\Customer\_Boot"

6. Run Customer\_Boot.ps1

#powershell .\Customer\_Boot.ps1

- 7. Enter the MCS token and management server values based on the command line prompt, and then wait for the command execution to complete.
- 8. To view the protected Arcserve Appliance, log into the Sophos Central page, and then navigate to Devices > Servers.

	SOPHOS CENTRAL Admin		anage your servers		1		
	Overview	Compu	ters Dobile Devices	Servers Servers			
	Dashboard	Search	Q Show	v all servers	✓ All Health	Status	*
▲	Alerts						
٨	Threat Analysis Center 🕨	O Nar	ne	IP		OS	
	Logs & Reports						
<u>,1</u>	People						
50	Devices						

Sophos is activated on the Appliance.

# Manually Installing Sophos Intercept X Advanced for Server on Arcserve UDP

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

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

#### Follow these steps:

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

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

- 3. To create a password for your new account on Sophos Central, follow the instructions in the email.
- 4. Log into Sophos Central.

5. Open the Product Setup dialog, then select Server Protection.

	Product Setup ×
	Choose a product below to get started.
Endpoint Protection	Mobile
Server Protection	Wireless
😣 Email Security	Ø Device Encryption
🕑 Web Gateway	Phish Threat
😔 Firewall Management	

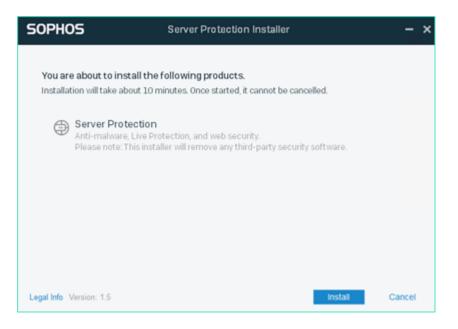
 From the Server Protection section, click Download Windows Server Installer, and then save SophosSetup.exe installer to a folder on UDP.

SOPHOS	Protect Devices	No. a
Derrent Constant Archa Constant	Not deliver the readjustice and waves IN	Bodd Calcinations     P     Advanced and strength     Bodd Calcinations     A Strength of the same diversion parameter to protocol.     A Strength of the same of the sam
Amerikansen Amerik	<ul> <li>Unified Endpoint Management and Mobile Security Rene management and Rents Trans Data Data in a security of the manage and product a factor in the model and its manage and product a factor</li> </ul>	General Protection     Hone with the set to below     Hone with the set to below     Hone with the set to below     Long the Long to below the set of s

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

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

8. Click Install.



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

SOPHO	S Server Protection Installer - ×
0	Installation successful
	Please restart your computer to complete the installation.  Restart my computer now
Legal Info V	ersion: 1.5

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

SOPHOS Status E	vents	Admin login – 🗙
Your com	nputer is protected	Scan
Mahware and PUAs O detections	Web Threats O requests blocked	Malicious Behavior     O     detections
(a) Controlled Items O user notifications	Malicious Traffic     O     connections detected	S Exploits O detections
		Help   About

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

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

#### Notes:

- It is mandatory to have Internet access in Arcserve UDP to install Sophos Intercept X Advanced and any related updates. Sophos Intercept X Advanced is cloud based and there are no offline installers available.
- If you have already purchased another UDP previously and have a Sophos account through Arcserve, use the same account for all your Arcserve UDP 8.0.
- If you already have a Sophos account through any other purchase, such as directly from Sophos, provide a different email address for a separate account on Sophos Central.
- If the Sophos installation fails for any reason, follow the on-screen or email instructions that are provided along with the error message.
- To receive the Sophos Intercept X Advanced for Server updates such as malware definition updates and version upgrades, you must have a valid and active maintenance or subscription for your Arcserve UDP.

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

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

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

# Manually Installing Sophos Intercept X Advanced for Server on Arcserve UDP

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

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

#### Follow these steps:

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

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

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

Product Setup		
	Choose a product below to get started.	
🕲 Endpoint Protection	Mobile	
Server Protection	Wireless	
😣 Email Security	O Device Encryption	
🕑 Web Gateway	(3) Phish Threat	
😂 Firewall Management		

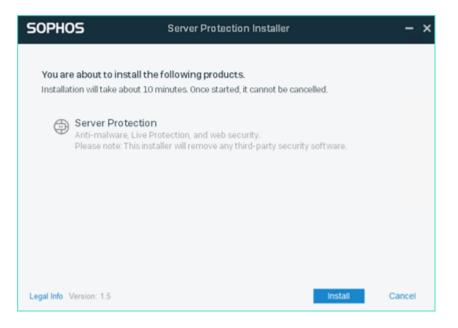
 From the Server Protection section, click Download Windows Server Installer, and then save SophosSetup.exe installer to a folder on UDP.

SOPHOS	Protect Devices	Nog a Bearing to be
Oversee	. First distance the installars for antipaths and servers $\Psi$	
A Anni Smart Andyn Camer I Lage S Angel Sange S Sange	<ul> <li>Enclosed Protection</li> <li>Rearry spatialised and event</li> <li>Bornerso Exception Protections to protect</li> <li>Constant Enclosed Protections and the Acceleration</li> <li>Constant Enclosed and events</li> <li>Constant Enclosed and events</li> <li>Constant Enclosed and events</li> <li>Constant Enclosed and events</li> <li>Interflated as is based</li> </ul>	Toth Contravery     Advanced one search     Advanced one search     Advanced one search     A. Instance: One one 10 is studies     A. Instance: One one 10 is studies     A. Instance: Instance
	(2) United Endpoint Management and Mubile Security Inter-imagement as them have been. (a) the the environment water's message and/or potent a datase	<ul> <li>Server Production</li> <li>Plane a priority and physical end of a prior of the physical end of the physical e</li></ul>

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

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

8. Click Install.



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

SOPHO	S Server Protection Installer - ×
0	Installation successful
	Please restart your computer to complete the installation.  Restart my computer now
Legal Info V	ersion; 1.5

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

SOPHOS Status E	vents	Admin login – 🗙
Your com	nputer is protected	Scan
Mahware and PUAs O detections	Web Threats O requests blocked	Malicious Behavior     O     detections
(a) Controlled Items O user notifications	Malicious Traffic     O     connections detected	S Exploits O detections
		Help   About

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

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

#### Notes:

- It is mandatory to have Internet access in Arcserve UDP to install Sophos Intercept X Advanced and any related updates. Sophos Intercept X Advanced is cloud based and there are no offline installers available.
- If you have already purchased another UDP previously and have a Sophos account through Arcserve, use the same account for all your Arcserve UDP 8.0.
- If you already have a Sophos account through any other purchase, such as directly from Sophos, provide a different email address for a separate account on Sophos Central.
- If the Sophos installation fails for any reason, follow the on-screen or email instructions that are provided along with the error message.
- To receive the Sophos Intercept X Advanced for Server updates such as malware definition updates and version upgrades, you must have a valid and active maintenance or subscription for your Arcserve UDP.

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

# Chapter 12: Upgrading Firmware for Arcserve Appliance 9000 Series

This section contains the following topics:

Upgrade BIOS Firmware for Arcserve Appliance 9000 Series	275
Upgrade iDRAC Firmware for Arcserve Appliance 9000 Series	279

# Upgrade BIOS Firmware for Arcserve Appliance 9000 Series

This section describes how to do the following:

### **Viewing BIOS Firmware Version**

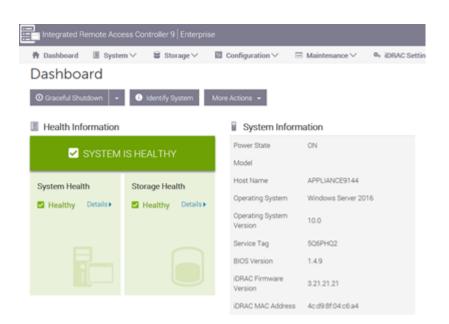
Use one of the following methods to view the BIOS firmware version:

- Method 1: View BIOS firmware version from iDRAC Web Interface
- Method 2: View BIOS firmware version from BIOS Arcserve Appliance 9000 Series

# Method 1: View BIOS firmware version from iDRAC Web Interface

#### Follow these steps:

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



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

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

#### Follow these steps:

- 1. When the system starts, press **F11** to enter Setup.
- To view the BIOS Version, navigate to System Setup > iDRAC Settings or System BIOS.

System Setup		Help   About   Ex
IDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.6.11	
IDRAC Firmware Version	3.21.23.22 (Build 7)	
iDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
IDRAC MAC Address	D0:94:66:7A:D7:B2	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	Yes	

The page displays the firmware version.

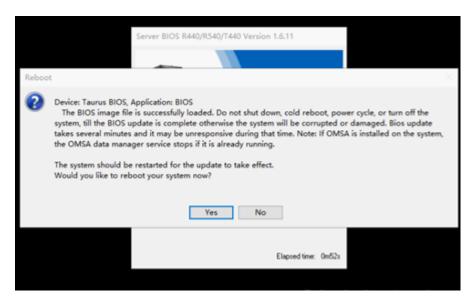
System Setup		Help   About   Exi
iDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.4.9	
iDRAC Firmware Version	3.21.21.21 (Build 30)	
iDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
IDRAC MAC Address	54:48:10:FB:C5:20	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	No	

### **Download the Updated Package for BIOS**

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

### **Upgrade BIOS**

- 1. Copy the upgrade package to local disk of Arcserve Appliance 9000 Series.
- 2. Start the upgrade package, and then follow the prompts to complete the upgrade.
- 3. To complete the update, restart the system.



**Note:** Make sure all applications are closed before starting the upgrade process.



### **Verify Updated BIOS**

Use one of the following methods:

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

### Verify Updated BIOS using System Logs

 Log into iDRAC, and then navigate to Maintenance >SupportAssist > Start a Collection.

cess.			
5CTNHQ2 > Hardv 2019-09-03 21:12:55 > Hardv	vare > Logs > Lifecyc	de Log	
	2019-08-29 15:40:34	USR0032	The session for root from 10.57.12.37 using GUI is logged off.
	2019-08-29 15:10:35	SRV088	The SupportAssist Save to Local operation is successfully completed.
	2019-08-29 15:10:34	SRV002	The SupportAssist Save to Local operation is started.
	2019-08-29 15:10:20	SRV108	The SupportAssist Job JID_670625874264 is completed.
	2019-08-29 15:10:20	SRV088	The SupportAssist Collection operation is successfully completed.
	2019-08-29 15:10:20	SRV096	The SupportAssist Collection TSR20190829021014_5CTNHQ2.zip is successfully created.
	2019-08-29 15:10:13	SRV007	The SupportAssist System information collection operation is successfully completed.
	2019-08-29 15:10:13	LOG009	The current Lifecycle Log is successfully created for the view or export operation.
	2019-08-29 15:10:07	LOG008	The complete Lifecycle Log was successfully created for an export operation.
	2019-08-29 15:09:47	SRV006	The SupportAssist System information collection operation is started.
	2019-08-29 15:09:47	SRV001	The SupportAssist Collection operation is started by IDRAC_GUL
	2019-08-29 15:09:47	SRV106	The Debug Logs are excluded from the SupportAssist collection because the Collection data is being filtered for personally identifiable Information.
	2019-08-29 15:09:47	SRV107	The Storage Logs are excluded from the SupportAssist collection because the Collection data is being filtered for personally identifiable Information.
	2019 00 29 15:09:17	SRV007	The Support/Posist Collection Job JID_070625074264 is successfully created.
	2019-08-29 15:09:25	RAC1195	User root via IP 10.57.12.37 requested state / configuration change to SupportAssist using GUI.
	2019-08-29 15:08:53	SEL9901	OEM software event.
	2019-08-29 15:08:53	OSE1002	C: boot completed.

Version change detected for BIOS firmware. Previous version: 1.6.11, Current version: 2.2.11

2. Review the log and verify that there are no errors during the updated pro-

# Verify Updated BIOS from iDRAC Web Interface or BIOS

2019-08-29 15:08:46 PR36

Log into the iDRAC web interface or enter system BIOS to see the updated BIOS firmware version.

## Upgrade iDRAC Firmware for Arcserve Appliance 9000 Series

This section describes how to do the following:

### Viewing iDRAC Firmware Version

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

- Method 1: View iDRAC firmware version from iDRAC Web Interface
- Method 2: View iDRAC firmware version from BIOS Arcserve Appliance 9000 Series

# View iDRAC firmware version from iDRAC Web Interface

#### Follow these steps:

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

▶ Dashboard            ■ Storage	etting
O Graceful Shutdown       •       ● Identify System       More Actions •         Image: Health Information       Image: System Information       Image: System Information         Image: System Health       Storage Health       Power State       ON         System Health       Storage Health       Host Name       APPLIANCE9144         Operating System       Undows Server 2016       Operating System       10.0	
Image: Health Information       Image: System Information         Image: System Health       Power State       ON         System Health       Storage Health       Model         Image: Healthy       Details>       Operating System       Windows Server 2016         Operating System       10.0       Operating System       10.0	
System Health         Storage Health         Power State         ON           Model         Model<	
System Health     Storage Health       Model       Model       Healthy     Details>       Healthy     Details>	ç
System Health         Storage Health         Host Name         APPLIANCE9144           Image: Healthy Details >         Image: Details >         Operating System         Windows Server 2016           Operating System         10.0         Image: Details >         Image: Details >         Image: Details >	
System Health         Storage Health           C Healthy         Details>           C Healthy         Details>           Operating System         10.0	
Healthy Details>     Details>     Coperating System     Windows Server 2016     Operating System     10.0	
Operating System 10.0	
Service Tag 5Q6PHQ2	
BIOS Version 1.4.9	
iDRAC Firmware 3.21.21.21	
IDRAC MAC Address 4c.d98f.04.c6.a4	
E Descriptions	

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

🕈 Dashboard 🛛 🗏 System	✓	figuration $\lor$ 🖂 Main	tenance $\lor = 0_{*}$ iDRAC Settings $\lor =$		
Dashboard					
O Graceful Shutdown → Identify System More Actions →					
Health Information		System Inform	ation		
	IS HEALTHY	Power State	ON		
STSTEM	IS REALINT	Model			
System Health	Storage Health	Host Name	appliance9012		
Healthy Details> Healthy Details>		Operating System	Microsoft Windows 2016 Server, Stan dard x64 Edition		
		Operating System Version	Version 10.0 (Build 14393) (x64)		
		Service Tag	SCTNHQ2		
		BIOS Version	1.6.11		
		IDRAC Firmware Version	3 21 23 22		
		IDRAC MAC Address	d0.94.66.7a.d7.b2		

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

#### Follow these steps:

- 1. When the system starts, press **F11** to enter Setup.
- To view the iDRAC Version, navigate to System Setup > iDRAC Settings or System BIOS.

System Setup		Help   About   Ex
iDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.6.11	
IDRAC Firmware Version	3.21.23.22 (Build 7)	
iDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
iDRAC MAC Address	D0:94:66:7A:D7:B2	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	Yes	

#### The page displays the firmware version.

System Setup		Help   About   Exi
iDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.4.9	
iDRAC Firmware Version	3.21.21.21 (Build 30)	
iDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
iDRAC MAC Address	54:48:10:FB:C5:20	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	No	

### **Download the Updated Package for iDRAC**

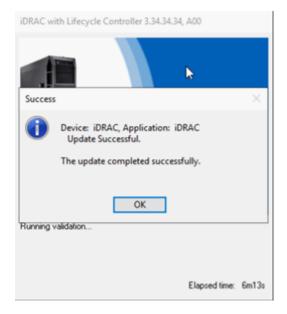
You can download the latest iDRAC firmware package of specific Arcserve Appliance 9000 Series model from the <u>Dell</u> website or contact Arcserve support.

### **Upgrade iDRAC**

#### Follow these steps:

- 1. Copy the upgrade package to local disk of Arcserve Appliance 9000 Series.
- 2. Start the upgrade package, and then follow the prompts to complete the upgrade.

**Note:** Make sure all applications are closed before starting the upgrade process.



3. During the upgrade process, iDRAC and virtual console gets disconnected for a few minutes. Log into iDRAC and restart the virtual console. The

Integrated Remote Access Controller 9 | Enterp 🕈 Dashboard 🔠 System 🗸 B Storage ∨ Configuration V Dashboard Graceful Shutdown
 e
 e
 identify System
 More Actions
 e Health Information ii System Information Power State ON SYSTEM IS HEALTHY Model Host Name WIN-SUQL6R8CBIC System Health Storage Health Operating System Microsoft Windows 2016 Server, Standard x64 Edition Healthy E Healthy Details+ Operating System Version Version 10.0 (Build 17763) (v64) Service Tag 506MH02 2211 BICS Version IDRAC Firmware Version 3.34.34.34 IDRAC MAC Address 54.4810 fb c 520

upgrade completes now.

### Verify Updated iDRAC

Use one of the following methods:

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

### Verify Updated iDRAC using System Logs

- Log into iDRAC, and then navigate to Maintenance >SupportAssist > Start a Collection.
- Review the log and verify that there are no errors during the updated process.

Hardware	> Logs > Lifecycl	eing	
	11-00-51 100-54	0000002	The second of non-international processing over a regime on.
	19-08-29 09:31:51	VM60007	Virtual Console session created.
	19-06-29 09:31:51	VM60005	Virtual Console session started.
20	19-08-29 09:31:51	USR0030	Successfully logged invaling root, from \$0.57.12.37 and Wrtual Console.
20	19-08-29 09:31-45	USR0000	Successfully logged in using root, from 10.57.12.37 and GUI.
20	19-08-29 09:28:22	RAC0721	Remote share mounted successfully //30.57.25.8/tool/clonec/lla
20	29-06-29 09:28:56	DI\$002	Auto Discovery feature disabled.
20	129-08-29 09:28:15	IPA0500	The IDRAC IP Address charged from 0.0.0.0 to 10.57.25.23.
20	19-08-29 09:28:54	PR36	Version change detected for Lifecycle Controller firmware. Previous version:3212322, Current version:3343434
20	19-08-29 09:28:12	RAC0182	The IDRAC firmware was rebooted with the following reasons user initiated.
20	19-08-29 09:27:22	PSU0800	Power Supply 2: Status = Gx5, IOUT = Gx0, VOUT = Gx0, TEMP= Gx0, FAN = Gx0, INPUT= Gx0,
20	19-06-29 09:27:22	PSU0800	Power Supply 1: Status = 0x1, IOUT = 0x0, VOUT = 0x0, TEMP= 0x0, FAN = 0x0, INPUT = 0x0.
20	19-06-29 09:25:58	5JP1906	Firmware update successful.
20	19-08-29 09:24:23	5UP1905	Firmware update programming flash.
20	19-08-29 09:24:22	SUP1903	Firmware update verify image headers.
20	19-08-29 09:24:55	SUP1904	Firmware update checksumming image.
20	29-08-29 09:24:55	SJP1911	Firmware update initialization complete.
20	19-08-29 09:24:55	SUP1901	Firmware update initializing.
20	19-06-29 09:02:59	LOG203	Lifecycle Log archived up to Log Sequence number 5491.
20	19-08-29 09:02:56	SEL9901	ODM software event.
20	19-08-29 09:02:55	OSE1002	C boot completed.
20	19-08-29 08-42-22	5Y51003	System CPU Resetting.
20	19-08-29 08:42:17	5Y51000	System is turning on.
20	29-06-29 08-42:07	SY51001	System's turning off.
20	19-08-29-08-42-07	SY51003	System CPU Resetting.
20	19-06-29 08:40:28	LOG009	The current Lifecycle Log is successfully created for the view or export operation.

# Verify Updated iDRAC from iDRAC Web Interface or BIOS

Log into the iDRAC web interface or enter system BIOS to see the updated BIOS firmware version.

### **Upgrade Firmware for Arcserve Appliance X Series**

This section describes how to do the following:

# Upgrade BIOS Firmware for Arcserve Appliance X Series

This section describes how to do the following:

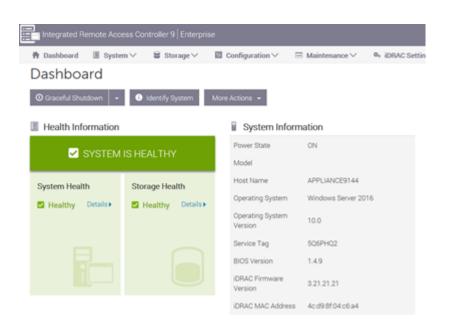
### **Viewing BIOS Firmware Version**

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

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

# Method 1: View BIOS firmware version from iDRAC Web Interface

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



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

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

- 1. When the system starts, press **F11** to enter Setup.
- To view the BIOS Version, navigate to System Setup > iDRAC Settings or System BIOS.

System Setup		Help   About   Ex
IDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.6.11	
IDRAC Firmware Version	3.21.23.22 (Build 7)	
IDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
IDRAC MAC Address	D0:94:66:7A:D7:B2	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	Yes	

The page displays the firmware version.

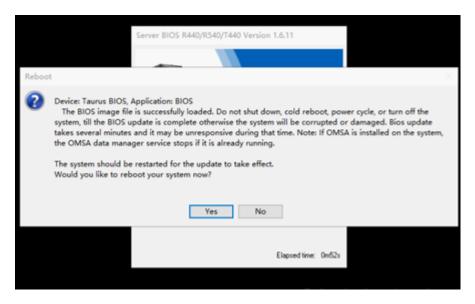
System Setup		Help   About   Exi
iDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.4.9	
IDRAC Firmware Version	3.21.21.(Build 30)	
iDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
IDRAC MAC Address	54:48:10:FB:C5:20	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	No	

### **Download the Updated Package for BIOS**

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

### **Upgrade BIOS**

- 1. Copy the upgrade package to local disk of Arcserve Appliance X Series.
- 2. Start the upgrade package, and then follow the prompts to complete the upgrade.
- 3. To complete the update, restart the system.



**Note:** Make sure all applications are closed before starting the upgrade process.



## **Verify Updated BIOS**

Use one of the following methods:

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

# Upgrade iDRAC Firmware for Arcserve Appliance X Series

This section describes how to do the following:

### **Viewing iDRAC Firmware Version**

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

- Method 1: View iDRAC firmware version from iDRAC Web Interface
- Method 2: View iDRAC firmware version from BIOS Arcserve Appliance 9000 Series

# Method 1: View iDRAC firmware version from iDRAC Web Interface

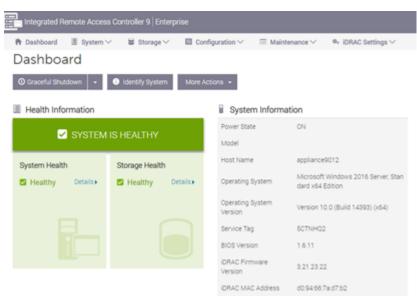
#### Follow these steps:

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

Integrated Remote	Access Co				
🕈 Dashboard 🛛 🗄 S	ystem 🗸	■ Storage ∨	$\blacksquare$ Configuration $\checkmark$	🖂 Maintenance 🗸	0. iDRAC Setting
Dashboard					
O Graceful Shutdown	• 0	Identify System	More Actions 👻		
Health Informat	ion		System Infor	rmation	
SA2			Power State	ON	
S151	EM IS HE	DALTHY	Model		
System Health	Sto	rage Health	Host Name	APPLIANCE9144	
Healthy Details			Operating System	Windows Server 2016	5
		including	Operating System Version	10.0	
			Service Tag	5Q6PHQ2	
			BIOS Version	1.4.9	
			iDRAC Firmware Version	3.21.21.21	
			IDRAC MAC Address	s 4c:d98f.04;c6:a4	

The iDRAC dashboard displays the system information, which contains iDRAC

#### firmware version.



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

- 1. When the system starts, press **F11** to enter Setup.
- To view the iDRAC Version, navigate to System Setup > iDRAC Settings or System BIOS.

System Setup		Help   About   Ex
IDRAC Settings		
IDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.6.11	
iDRAC Firmware Version	3.21.23.22 (Build 7)	
iDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
iDRAC MAC Address	D0:94:66:7A:D7:B2	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	Yes	

The page displays the firmware version.

System Setup		Help   About   Exi
iDRAC Settings		
iDRAC Settings • System Summary		
SERVER INFORMATION		
System Model		
BIOS Version	1.4.9	
iDRAC Firmware Version	3.21.21.21 (Build 30)	
iDRAC License	Enterprise	
IPMI Version	2.00	
CURRENT IDRAC NETWORK SETTINGS		
iDRAC MAC Address	54:48:10:FB:C5:20	
NIC Selection Mode	Dedicated	
Current IPv4 Settings		
IPv4 Enabled	Yes	
DHCP Enabled	No	

### **Download the Updated Package for iDRAC**

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

### **Upgrade iDRAC**

Follow these steps:

- 1. Copy the upgrade package to local disk of Arcserve Appliance X Series.
- 2. Start the upgrade package, and then follow the prompts to complete the upgrade.

**Note:** Make sure all applications are closed before starting the upgrade process.

iDRAC with Lifecycle Controller 3.34.34.34, A00	
Success	×
Device: iDRAC, Application: iDRAC Update Successful. The update completed successfully. OK	
Running validation	
Elapsed time: 6rr	n13s

3. During the upgrade process, iDRAC and virtual console gets disconnected for a few minutes. Log into iDRAC and restart the virtual console. The upgrade completes now.

integrated Remote	Integrated Remote Access Controller 9   Enterprise						
🕈 Deshboard 🗏 S	ystem∨ 🛛 🗃 Stori	ige∨ III Configuration	✓	noe 🗸 — 🗣 iDRAC Settings 🗸			
Dashboard							
O Graceful Shutdown	• Identify Sy	stem More Actions +	I				
III Health Informati	on			i System Information			
		IN LICALTUN		Power State	ON		
	STSTEM	IS HEALTHY		Model			
System Health		Storage Health		Host Name	WIN-SUQLERECEIC		
S Healthy	Detailsa	E Healthy	Details+	Operating System	Microsoft Windows 2016 Server, Standard x64 Edition		
				Operating System Version	Version 10.0 (Build 17763) (r64)		
				Service Tag	506A/H02		
Dashboard         Image: Construct Structure         Image: Constructure         Image: Construct Structure         Image: Constructure							
				IDRAC Firmware Version	3343434		
				IDRAC MAC Address	54.48.10.fb:c5.20		

### Verify Updated iDRAC

Use one of the following methods:

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

# **Chapter 13: Troubleshooting**

This section contains the following topics:

Linux Backup Server Fails to Connect from the Console	294
Backing Up Arcserve Appliance from Another Appliance Reports Duplicated Nodes	295
Linux Backup Server Cannot Communicate with Any Node in the Network	296
Linux Backup Server Cannot Get the Network DNS Suffix	298
Default Time Zone on the Appliance	299
Licenses Error even when the licenses are available	300
Arcserve UDP Console Shows Error while adding Remote Console in Replicate to a Remotely Managed RPS Task	301
Unable to Perform VSB Task Using Another Appliance as Monitor	303

### 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.
- 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 Pro-
tection\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. Delete the file *dhcpdone.flag* from the following location:

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

7. 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 UDP 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 Arcserve Appliance that has default version of Arcserve UDP v6.5 Update 3 or higher.

Error	message:	Please	select	a remote	console
-------	----------	--------	--------	----------	---------

resources			
Modify a Plan	Agent-Based Windows Backup Plan	Pause this plan	Save Cancel Help
Task1: Backup: Agent-Based 🥥 Windows	Task Type Replicate to a remote	ely-managed RPS 👻	S Delete Task
Task2: Replicate to a remotely- managed RPS	Source Destination	Schedule	
	Remote Console	10.10.255.255 (administrator) 👻 🌒	Add
Add a Task	Username	administrator	Please select a remote console.
Product Installation	Password		
	Port	8015	
	Protocol Enable Proxy:	○ HTTP ● HTTPS	
		Connect	

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 Catalog=\$database;Integrated Security=SSPI;" \$sqlconn.Open() \$sqlcmd = New-Object System.Data.SqlClient.SqlCommand \$sqlcmd.Connection = \$sqlconn \$sqlcmd.CommandText = "delete from as\_edge\_configuration where ParamKey='ConsoleUuid''' \$sqlcmd.ExecuteNonQuery() \$sqlconn.Close()

- 3. 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.

	arcser∨	- -	unified data p			O Mes	sages (1) 🔸	admin	strator	•	Help 🔹
da	shboard resou	irces jo	os reports log	settings ∣ hig -	gh availability						
Severity	All	- Node Name	10.10.255.255	× Job ID 3	× Job	Type Virtual S	Standby ~	Refresh	Reset	Export	Delete
Time	All	Generated	rom vsb2	× Message	×			Nellean	Reset	CAPOIL	Delete
Severity	Time	SiteNam	e Node Name	Generated From	Job ID	Job Type	Message				
0	7/18/2017 3:04:20 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	The Virtual Stan	dby job failed.			
0	7/18/2017 3:04:20 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	Synchronize sou	rce machine a	dapter info	rmation to	Virtual Standby s
0	7/18/2017 3:04:20 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	The Virtual Stan	dby job copied	l data totalii	ng 0 Bytes	, the elapsed time
0	7/18/2017 3:04:20 AM	Local Si	le	vsb2	3	Virtual Sta	Failed to convert	t session S000	0000001 te	the host	for VM [UDPVM_
0	7/18/2017 3:04:20 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta					to convert sessio oblem persists, c
0	7/18/2017 3:04:20 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	Failed to connect	t to remote se	rver [10.57.	21.10], po	rt = 4090.
0	7/18/2017 3:02:40 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	Failed to connect	t to remote se	rver [10.57.	21.10], po	rt = 4090.
0	7/18/2017 3:01:28 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	Try VDDK advar	nced transport	mode (SAM	N or HotAd	(d).
0	7/18/2017 3:01:12 AM	Local Si	0 10.10.255.255	vsb2	3	Virtual Sta	Upload meta dat	a to VM [UDP	VM_WIN-9	2KBNU8J	439].
0	7/18/2017 3:01:12 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	Begin to convert	session S000	0000001.		
0	7/18/2017 3:01:12 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	Virtual Standby j	ob will convert	session S	00000000	01.
0	7/18/2017 3:01:04 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	VM was created	VM name is (	UDPVM_V	/IN-92KBN	IU8J439].
0	7/18/2017 3:00:49 AM	Local Si	10.10.255.255	vsb2	3	Virtual Sta		-			stination is (X:\Ar nd the data store
0	7/18/2017 3:00:48 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	The monitor serv	ver is [10.57.2	1.10] and is	used as a	proxy for data tra
0	7/18/2017 3:00:48 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	Start a Virtual St	andby job with	destination	n type VM	ware ESX Server,
0	7/18/2017 3:00:48 AM	Local Si	e 10.10.255.255	vsb2	3	Virtual Sta	Virtual Standby j	ob started.			

**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.

# **Chapter 14: Applying Best Practices**

The section contains the following topics:

Best Practices for Network Configuration	306
Best Practices for Windows Defender with PowerShell cmdlets	
Configure Preinstalled Linux Backup Server to External Network	
Best Practices for replacing Factory Reset Image When Secured by Sophos	310
Best Practice for Creating Deduplication Data Store across Volumes	319

### **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 nodes are online on the same sub network, the following symptoms may occur:

 On the Arcserve UDP Console, when you deploy the plan to Agent node, the following error message is displayed:

Error	×
Unable to apply 'backup settings' to node '10.57.52.13'. (Failed to connect to Arcserve UDP Recovery Point Server appliatest76. Verify that server name, port number, and protocol (http/https) inputs are all correct and the web service is started on the specified host. For other reasons, see Troubleshooting in the User Guide.)	
ОК	

Backup job of the Agent node fails as below:

	0	12/25/ Local Site	10.57.52.13	10.57.52.13	26	Backup	Point Server appliatest76. Verify that server name, port number, and protocol (http:https) inputs are all correct and the web service is started on the specified host. For other reasons, see Troubleshooting in the User Guide.
--	---	-------------------	-------------	-------------	----	--------	--

Eailed to run backup job. Eailed to connect to Arcennia LIDD Decoupry

 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 ITL=1 Reply from 10.57.52.13: bytes=32 time=1ms ITL=1 Reply from 10.57.52.13: bytes=32 time<1ms ITL=1 Reply from 10.57.52.13: bytes=32 time<1ms ITL=1	27 27 27

 Ping Appliance host name from the Agent node and the Appliance is NOT connected as follows:

C:\Users	s∖Admin	istrate	or>ping	appliat	est76:				
Pinging Request Request Request Request	timed timed timed	out. out. out.	[10.57]	.52.47]	with	32 b	ytes ı	of d	lata:
Ping sta Pacl				2.47: ived = @	), Los	t =	4 (10	<b>0</b> % ]	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 <u>How to Disable DHCP Server</u>.

\* 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:

Active Routes:				
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0	0.0.0	10.57.52.1	10.57.52.46	10
0.0.0	0.0.0.0	10.57.52.1	10.57.52.35	10
0.0.0	0.0.0	10.57.52.1	10.57.52.45	10
0.0.0	0.0.0.0	10.57.52.1	10.57.52.47	10
10.57.52.0	255.255.255.0	On-link	10.57.52.46	266
10.57.52.0	255.255.255.0	On-link	10.57.52.35	266
10.57.52.0	255.255.255.0	On-link	10.57.52.45	266

Steps to be followed on Agent node:

 From the DOS Command Prompt, try to ping each available IPv4 address of Appliance one by one according to the order above to get the first IPv4 of the Appliance connected on the Agent node as follows:

C:\Users\Administrator>ping 10.57.52.46
Pinging 10.57.52.46 with 32 bytes of data: Reply from 10.57.52.46: bytes=32 time<1ms TTL=128 Reply from 10.57.52.46: bytes=32 time<1ms TTL=128
Reply from 10.57.52.46: bytes=32 time<1ms TTL=128 Reply from 10.57.52.46: bytes=32 time<1ms TTL=128

2. Modify the file C:\Windows\System32\drivers\etc\hosts to add a record for the pair the\_IPv4\_got\_above Appliance\_hostname and save the file.

# Best Practices for Windows Defender with PowerShell cmdlets

You can get the Defender cmdlets by using the following commands:

- PS C:\> (Get-MpPreference).ExclusionPath Gets exclusion path of Defender.
- PS C:\> (Get-MpPreference).ExclusionProcess
   Gets exclusion processes of Defender.
- PS C:\> Add-MpPreference -ExclusionPath "full\_path\_of\_the\_folder\_or\_file"
   Excludes a folder or file to the exclusion list.
- PS C:\> Add-MpPreference –ExclusionProcess "full\_path\_of\_executable\_programs"

Excludes files opened by the processes.

PS C:\> Remove-MpPreference -ExclusionPath "full\_path\_of\_the\_folder"
 Removes a folder from the exclusion list.

# **Configure Preinstalled Linux Backup Server to External** Network

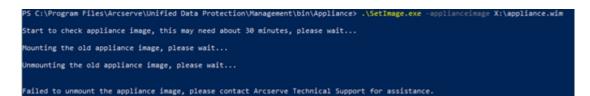
- 1. Disable DHCP server. For more information, see <u>How to Disable DHCP</u> <u>Server</u>.
- 2. To disable RRAS, open Routing and Remote Access, and then click **Disable Routing and Remote Access**.

	Routing an	d Remote Access	-		×
Fi	le Action	View Help			
4	• 🔿   💼	2 🖬			
9	Routing and	d Remote Access Routing and Remote Access tatus			-
~	APPLI ···	Configure and Enable Routing and Remote Access	mote Acce		^
	🔄 Re	Disable Routing and Remote Access	secure remote	access to	
	~ <u>e</u> p	Enable DirectAccess			
		All Tasks			
		Delete	eway.		
	> <u>a</u> 14	Refresh			
		Properties			
		Help	server, on the	Action mer	nu,
		click Add Server.	-		

- 3. To set Linux Backup Server network to external network, follow these steps:
  - a. Open the Hyper-V manager.
  - b. Create a new external virtual network switch.
  - c. Change the Linux Backup Server VM network adapter setting to use the newly created external virtual network switch.
  - d. Check network setting of Linux Backup Server, ensure it has got IP address and DNS through the external virtual network switch.
  - e. Remove the original Linux Backup server from UDP Console.
  - f. Add the Linux Backup Server to UDP Console again with the following information:
    - Hostname: Linux-BackupSvr
    - **Port:** 8014

# Best Practices for replacing Factory Reset Image When Secured by Sophos

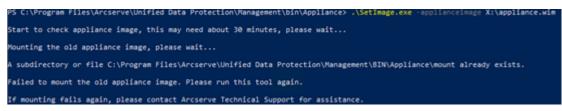
After Sophos has been activated and running on Arcserve Appliance, by default you cannot replace factory reset image using the Set Appliance Image Utility. Otherwise, the execution of SetImage.exe will fail as shown in the illustration below.



Before running the SetImage.exe command to replace factory reset image when Sophos is running on Arcserve Appliance, verify if the image has already been mounted.

As given in the illustration, the following prompt appears: A subdirectory or file C:\Program Files\Arcserve\Unified Data Pro-

tection\Management\BIN\Appliance\mount already exists.



#### To unmount the image, follow these steps:

 To locate the folder, open Windows Explorer, and go to C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\mount. Right-click the folder, and then click Properties > Security tab > Advanced.

Mount Properties		×
Previous Versions	Customize	NFS Sharing
General	Sharing	Security
Object name: C:\Pr	ogram Files\Arcserve\	Unified Data Protection
Group or user names:		
SCREATOR OWN	IER	
SYSTEM		
🞎 Administrators (🛲	Administrators)	
States (Millingia)	Users)	
To change permission	s, click Edit.	Edit
Permissions for CREA OWNER	TOR	Allow Deny
Full control		^
Modify		
Read & execute		
List folder contents		
Read		
Write		~
For special permission click Advanced.	s or advanced settings	3. Advanced
[	ОК С	ancel Apply

2. To change the owner of the mount folder to a local administrator, click the **Change** link.

In the Advanced Security Settings page, to take control of the subfolders inside of the folder and replace the subfolders permissions with the settings from the parent folder, select the check boxes for the following options:

- \* Replace ownership on subcontainers and object
- Replace all child object permission entries with inheritable permission entries from this object

lame:	C:\Program Files	Arcserve\Unified Data Protecti	on\Management\BIN\	Appliance\mount	
wner:	TrustedInstaller	Change			
Permissions	Auditing	Effective Access			
or additional	information doub	la aliab a accomission antos. To as	adife a norminai and		-and click Edit (if available).
ermission ent	select User	or Group		×	
Type	Princi Select this o	bject type:			lies to
& Allow	SYSTE User, Group	o, or Built-in security principal		Object Types	folder, subfolders and files
Allow .	Admi From this loc	ation:			folder, subfolders and files
Allow 2	Users difficient			Locations	folder, subfolders and files
	Users Enter the ob	ject name to select (examples):			folder and subfolders
	CREAT			Check Names	folders only folders and files only
Allow	Chea				loiders and nies only
Add	F Advance	d	ОК	Cancel	
Enable inhe	ritance				1

Apply all the changes. For mount folder, subfolders, and files, make sure the owner is changed to a local administrator.

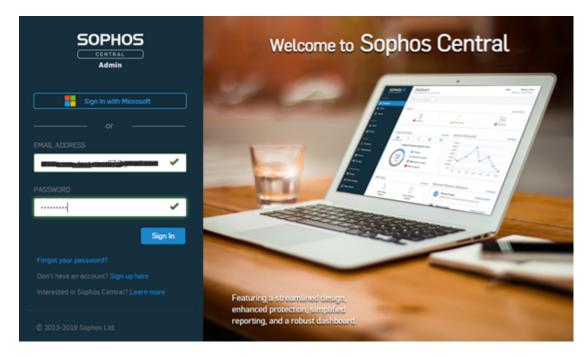
3. To unmount the image, execute the following command using command prompt:

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

> closed terms is an environment of a recent contrangement with output and a fundament lange fundament is a set of terms unit for and anagement to a deputation deputation deputation of a set of terms unit for and anagement to a deputation deputation deputation of a set of terms unit for and a fundament and a set of terms unit for and a fundament and a set of terms unit for an anagement to a deputation deputation of a set of terms unit for an anagement to a deputation deputation deputation of a set of terms unit for an anagement to a deputation deputation of a set of terms unit for an anagement to a deputation deputation of a set of terms unit for an anagement to a deputation of a set of terms unit for an anagement to a deputation deputation of a set of terms unit for an anagement to a deputation of a set of terms unit for a set of terms

To run SetImage.exe command to replace factory reset image when Sophos runs on Arcserve Appliance, follow these steps:

 Log into the Arcserve Appliance system as an administrator. Use your email address and password to access the Sophos Central Admin page <u>https://cloud.sophos.com/manage/</u>.



2. Navigate to Devices > Servers, and then click the server name of your Arcserve Appliance.

		Servers View and manage y	ur servers							
(	Overview	Computers	D Mobile Devices	Servers						
E Dashba	oard	Search	Q Show	al severs	All Health	Status 👻				
A Alerts										
@ Threat	Analysis Center	□ <b>①</b> NVME		p		05		LAST ACTIVE	Ŧ	GROUP
Logs &	Reports	• • •		10.57.25.29 🗢		Windows Server 20	16 Standard	Sep 23, 2019 1:30 AM		
1 People										
Device	-									

3. On the SUMMARY tab, for the Tamper Protection field, click **View details**.

#### Best Practices for replacing Factory Reset Image When Secured by Sophos

	C SUMMARY	EVENTS	🕲 STATUS	Ø EXCLUSIONS	## APPLICATIONS	O POLICIES
	Recent Events					View More
	🗉 🗇 Oct 8, 2019 6:27	PM Real time protec	tion re-enabled			
app82.4 Windows Server 2028 Standard	E Oct 8, 2019 6 26	PM Update succeed	nd			
Delete	E Oct 8, 2019 6-26	PM New server prote	ected: app814			
Scen Now	Oct 8, 2019 6:26	PM Real time protec	tion disabled			
Lock Down	A Oct 8, 2019 6 25	PM Application such	ost was blocked by an endp	oint firewall		
Degrese						
	Agent Summary					
	Last Sophos Central Activity	15 minutes ag	po (			
	Last Agent Update	an hour ago	Update Successful 🖌 🖌	Update Now		
	Agent Version	10.8.4 VE3.74	1 Rolease Notes 🗗			
			ment versions ¥			
	IPv4 Addresses	10.57.25.29				
		192.168.10.1				
	IPv6 Address		f7e:79e2:a021			
	Operating System		ver 2019 Standard			
	Lockdown Status	Not install				
	Group	No group Ch	ange group			
	Tamper Protection	On - Disable	Tamper Protection			
		Vew details 💙			Activate Windows Go to System in Control Pane	el to activate Windows.

4. For Show Password, select the check box. Make a note of the password that displays in the text field.

Tamper Protection

On - Disable Tamper Protection

Hide details ٨

Tamper Protection Password Details

Generate New Password

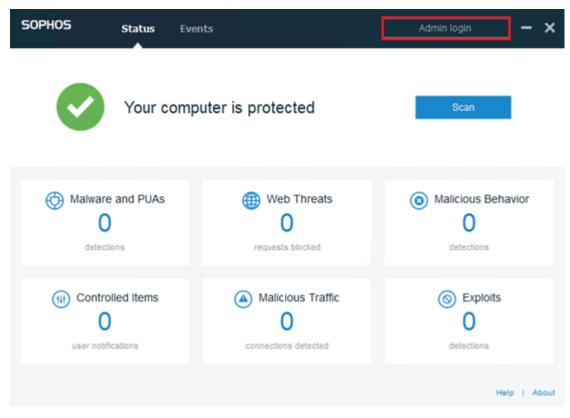
Show Password

5. Click Disable Tamper Protection.

Tamper Protection	On - Disable Tamper Protection
	Hide details 🛧
Tamper Protection Password Detai	ls
CURRENT PASSWORD	
2020000000	
Shaw Password	
Generate New Password	
Tenner Ductostics is turned off	
Tamper Protection is turned off.	

Tamper Protection	Off - Enable Tamper Protection
	Sophos recommends that you enable tamper protection.
	Tamper protection ensures that users with local administrator rights can't uninstall Sophos Central Endpoint software or change settings.

6. Launch Sophos Endpoint, and then click Admin Login.



7. Type the Tamper Protection password that was noted in Step 4.

SOPHOS	Status	Events		Admin login	-	×
	E	nter tamper protection password				
	•	•••••		)		
		Log in	Cancel			
				Hel	P   A	bout

8. On the Settings tab, select the **Override Sophos Central Policy for up to 4 hours to troubleshoot** check box, and disable the **Ransomware Detection** and **Malicious Behavior Detection (HIPS)** options.

SOPHOS	Status	Events	Settings	- ×
<ul> <li>Override Soph</li> </ul>	os Central Polic	y for up to 4 h	hours to troubleshoot	
Deep learnin C Enable deep Real Time So Files	learning		Runtime Protection Ransomware Detection Safe Browsing Exploit Mitigation Network Threat Protection	
Internet			Malicious Behavior Detection (HIPS)	
Controls on l Peripheral C Application C Web Control Data Loss Protection Tamper Protection	ontrol Control revention		Computer Controls  Windows Firewall	
			н	lelp   About

9. To replace factory reset image, run SetImage.exe. SetImage.exe gets executed successfully.

# To recover the default configuration of Sophos after the successful execution of SetImage.exe, follow these steps:

 To enable Tamper Protection in Sophos Central Admin, click Enable Tamper Protection.

Tamper Protection	Off Enable Tamper Protection
	▲ Sophos recommends that you enable tamper protection.
	Tamper protection ensures that users with local administrator rights can't uninstall Sophos Central Endpoint software or change settings.

2. Clear the **Override Sophos Central Policy for up to 4 hours to troubleshoot** checkbox.

SOPHOS	Status	Events	Settings	_	Admin logout	] –	×
Override Sopho	s Central Polic	y for up to 4 h	ours to troubleshoot				

3. To check the status of the Sophos Settings, wait for a few minutes, and then log into Sophos Endpoint with the tamper protection password.

SOPHOS	Status	Events		Admin login	] -	×
	E	nter tamper protection password				
		Log in	Cancel			
				н	elp   A	bout

SOPHOS Status Events Settings Override Sophos Central Policy for up to 4 hours to troubleshoot Deep learning Runtime Protection Enable deep learning Ransomware Detection Safe Browsing Real Time Scanning Exploit Mitigation Files Network Threat Protection Internet Malicious Behavior Detection (HIPS) Controls on Users Computer Controls Peripheral Control Windows Firewall Application Control Web Control Data Loss Prevention Tamper Protection Help | About

Now the Sophos Settings have been recovered to the default settings.

# Best Practice for Creating Deduplication Data Store across Volumes

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

#### To create deduplication data store across volumes, follow these steps:

- Log into the Arcserve UDP console user interface, and then create a deduplication data store without expanded data path. For more information, see <u>Add a Data Store</u>.
- 2. Stop the data store. For more information, see Stop a Data Store.
- 3. Open the command prompt, and then enter the following command to display the current path configuration of data store:

as\_gddmgr.exe -DataPath Display <data store name>

The following sample data store has one primary data path on X:\volume:

	<pre>"c:\Program Files\Ar a store configuration</pre>		rotection\Engine\bin\as_gddmgr.exe"	-DataPath Display	appliancetest_data_store
	Volume capacity	Used space	Free space		
Primary data path :	X:\Arcserve\data_stor 59605 GB	e\data\ 2 GB	59603 GB		

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

as\_gddmgr.exe -DataPath Add <data store name> -NewDataPath <new data folder>

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

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

Successfully load dat Successfully added ne	r>"c:\Program Files\Ar a store configuration w expanded data path f expanded data path(s)	information. or the data store.	otection\Engine\bin\as_gddmgr.exe* -OstaPath Add appliancetest_data_store -NewDataPath W:\Arcserve\data_store\data1
	Volume capacity	Used space	Free space
Primary data path :	X:\Arcserve\data_stor S9605 G8	e\data\ 2 GB	sees a
Expanded data path1:	W:\Ancserve\data_stor 14678 GB	e\data1 90 GB	14588 68
fotal	74283 68	92 68	74291 68

- 5. Repeat step 4 as needed.
- Return to the Arcserve UDP console user interface and start the data store.
   For more information, see <u>Start a Data Store</u>.

arcserve						ate server un		<b>O</b> Messag	pes (1) - Help -
All Nodes	٥١ ٣			ports log settings ations: Recovery Point S s .   Add a Recovery Po	Server	availabilit	y .		appliancetest > appliancetest_data_store Origonation Weard
All Nodes Nodes without a Plan Elinux Backup Server Groups			Aame		Status	Plan Count Stored Data	Deduplication	Status     Stopped	
All Plans  Destinations  Recovery Point Servers  Accerve Backup Servers  Shared Folders  Cloud Accounts  Remote Consoles  Accerve Cloud		ł		appliancetest_data_store Modify Delete Start Browse Recover RPS Jumpstart	o y Points	0	0 Byte	0%	Settings     Compression Type Standard     Encryption Algorithm AES-256     Backup Destination X:Varcserveridata_storel     mmon     Concurrent Active Nodes 20
<ul> <li>Intrastructure Storage Arrays</li> </ul>	~		_			_			Defuplication Data File Path X:\Arcserveridata_store

# **Chapter 15: Acknowledgements**

Portions of this product include software developed by third-party software providers. The following section provides information regarding this third-party software.

This section contains the following topic:

#### <u>PuTTY</u>

### PuTTY

This product includes the "PuTTY" component which entails the following details:

Component Name	PuTTY					
Component Vendor	Developed originally by Simon Tatham					
Component Version	0.64					
Legal Remark	http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html					
Project Name	Appliance Rhodium					
Component Type	Open Source					
Source Code URL	http://the.earth.li/~sgtatham/putty/0.64/					
Platform(s) Required	Windows 2012 R2, Windows 2016, Windows 2019					
Component URL	http://the.earth.li/~sgtatham/putty/0.64/x86/					
Component Version URL	http://the.earth.li/~sgtatham/putty/0.64/x86/					
Description	On the appliance machine, we use putty.exe to communicate with the Linux Backup Server to change the system locale and UDP Linux locale.					
Features	Appliance					
	http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html					
	PuTTY is copyright 1997-2019 Simon Tatham.					
License Text	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, Chris- topher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svyatoslav Kuzmich, Nico Williams, Viktor Dukhovni, and CORE SDI S.A.					
	Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:					
	The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.					
	THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,					

	EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
	http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html
	PuTTY is copyright 1997-2019 Simon Tatham.
	Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Chris- topher Staite, Lorenz Diener, Christian Brabandt, Jeff Smith, Pavel Kryukov, Maxim Kuznetsov, Svyatoslav Kuzmich, Nico Williams, Viktor Dukhovni, and CORE SDI S.A.
Copyright Text	Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
	The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
	THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Intended	On the appliance machine, we use putty.exe to communicate with the Linux
Usage	Backup Server to change the system locale and UDP Linux locale.
Modifications Required	No