# Arcserve® Unified Data Protection Appliance User Guide

**Version 6.0**

arcserve®

# Legal Notice

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

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

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

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

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

The manufacturer of this Documentation is Arcserve.

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

# Contact Arcserve Support

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

Contact Support

With Arcserve Support:

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

# Arcserve UDP Appliance Return Policy

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

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

Information needed for the RMA request:

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

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

# Contents

# Chapter 1: About Appliance Documentation

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

This section contains the following topics:

# Language Support

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

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

This release is available in the following languages:

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

# Product Documentation

For all Arcserve UDP related documentation, click this link for the Arcserve Documentation.

The Arcserve UDP Knowledge Center consists of the following documentation:

- **Arcserve UDP Solutions Guide**

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

- **Arcserve UDP Release Notes**

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

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

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

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

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

# Chapter 2: Introducing the Arcserve UDP Appliance

This section contains the following topics:

# Introduction

The Arcserve UDP appliance is the first complete and most cost-effective data protection appliance, featuring Assured Recovery™. Each Arcserve UDP 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 UDP appliance delivers unmatched operational agility and efficiency, and truly simplifies disaster recovery activities.

The Arcserve UDP 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 preinstalled in the Arcserve UDP appliance:

- Arcserve UDP
- Arcserve UDP Agent (Linux)
- Arcserve Backup
- Arcserve Replication and High Availability (RHA)

Each Arcserve UDP appliance comes with a 3-year hardware warranty. Please visit arcserve.com/udp-appliance-warranty for detailed information about this warranty.

# Arcserve Unified Data Protection

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

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.

# Arcserve UDP Agent (Linux)

Arcserve UDP Agent (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 UDP Agent (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 UDP Agent (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 UDP Agent (Linux) is preinstalled in a virtual machine within the appliance. This virtual machine becomes the Linux Backup Server. Arcserve UDP Agent (Linux) is installed at the default installation path in the UDP 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 UDP Appliance.

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

The Linux Backup Server uses the following default login information:

- Username – root
- Password - Arcserve

**Note:** We recommend to change the default password.

# Arcserve Replication and High Availability (Arcserve RHA)

Arcserve RHA is a solution based on asynchronous real-time replication and automated application switchover and switchback to provide cost-effective business continuity for virtual environments on Windows Servers.

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

You can download the full installation package of Arcserve RHA from Arcserve website to install all components. For details, refer to Arcserve RHA online documents.

# Arcserve Backup

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

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

UDP 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 UDP Appliance lets you back up the destination of Arcserve UDP to a tape.

You can download the full installation package of Arcserve Backup from Arcserve website to install other components. For details, refer to Arcserve Backup online r17.5 online documents.

Arcserve Backup Server uses the following default login information:

- Username -- caroot
- Password -- Arcserve

# Safety Precautions

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

For more information about the safety precautions, see the Safety Precautions Appendix.

# What is Included in the Box

The following items are contained in the box:

- Arcserve UDP Appliance (serial number label is located on rear of appliance)
- Power cable: 1
- Network Cables: 1 red, 1 blue (3-feet long each)
- IPMI port cable: 1 (7-feet long)
- Rail/Rack Mounting Kit - consisting of 2 quick-install outer rails, 2 inner rail extensions, 3 rail adapters (standard rail mounting only), and attaching hardware (as needed)
- 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, please retain all packaging materials and contact Arcserve Support immediately at: https://www.arcserve.com/support.

# What is Not Included in the Box

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

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

# Available Models

The Arcserve UDP 7000 series and 8000 series appliances are available in a variety of different models designed to meet your specific needs:

- Models 7100 - 7300v
- Models 7400 - 7600v
- Models 8100 - 8400

# Models 7100-7300v

Arcserve UDP Appliance Models 7100 - 7300v

| Arcserve UDP 7000 Series Appliance Specifications | | | | | |
|---|---|---|---|---|---|
| **Appliance Model** | **7100** | **7200** | **7200V** | **7300** | **7300V** |
| **Backup Storage Capacity** | | | | | |
| Raw Storage capacity* | 3 TB | 6 TB | 6 TB | 9 TB | 9 TB |
| Usable backup capacity** | 2.8 TB | 5.8 TB | 5.8 TB | 8.8 TB | 8.8 TB |
| Protected (source data) capacity*** | Up to 8 TB | Up to 17 TB | Up to 17 TB | Up to 26 TB | Up to 26 TB |
| **Standard Features** | | | | | |
| Unified management console, global deduplication, block level infinite incremental backups, compression, encryption, WAN optimized replication, advanced virtualization support, agentless backup, remote virtual standby, tape support, application consistent backups, granular restore, unified reporting and dashboard. | | | | | |
| On-Appliance Virtual Standby | N/A | N/A | Up to 3 VMs | N/A | Up to 3 VMs |
| **Warranty and Technical Specifications** | | | | | |
| Full System Depot Warranty | 3 Years | | | | |
| Physical Dimensions (H x W x D in Inches) | 1.7" x 17.2" x 25.6" (1U - 19" Rack Mount rails provided) | | | | |
| Remote management and network interface ports | 1 x IPMI & 2 x 1 GbE (RJ45) | | | | |
| Hard Disk type and RAID configuration | 4 x 1 TB SAS (RAID 5) | 4 x 2 TB SAS (RAID 5) | 4 x 2 TB SAS (RAID 5) | 4 x 3 TB SAS (RAID 5) | 4 x 3 TB SAS (RAID 5) |
| External Tape Backup Connectivity (SAS, SATA, FC) | 1 x PASS | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Total system RAM | 16 GB | 16 GB | 32 GB | 32 GB | 48 GB |
| SSD drive (For deduplication hash tables) | 120 GB SSD | 120 GB SSD | 120 GB SSD | 240 GB SSD | 240 GB SSD |
| Maximum weight (lbs) | 41 lbs | | | | |
| Power Supplies (Single or redundant) | 1 x 600W | | | | |
| Power consumption (Watts @ idle/-load/startup) | 93/116/143 | 122/164/143 | 125/167/145 | 125/167/145 | 129/188/152 |
| AC voltage & frequency range | 100 - 240v | | | | |
| Ampere rating | 7.5 Amp Max | | | | |

*1 TB = 1,000,000,000,000 bytes.

** On "V" models, space available for backup is reduced by the size of virtual standby VMs.

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

# Models 7400-7600v

Arcserve UDP Appliance Models 7400 - 7600v

| Arcserve UDP 7000 Series Appliance Specifications | | | | | | |
|---|---|---|---|---|---|---|
| **Appliance Model** | **7400** | **7400V** | **7500** | **7500V** | **7600** | **7600V** |
| **Backup Storage Capacity** | | | | | | |
| Raw Storage capacity* | 16 TB | 16 TB | 20 TB | 20 TB | 30 TB | 30 TB |
| Usable backup capacity** | 15.8 TB | 15.8 TB | 19.8 TB | 19.8 TB | 29.8 TB | 29.8 TB |
| Protected (source data) capacity*** | Up to 46 TB | Up to 46 TB | Up to 58 TB | Up to 58 TB | Up to 90 TB | Up to 90 TB |
| **Standard Features** | | | | | | |
| Unified management console, global deduplication, block level infinite incremental backups, compression, encryption, WAN optimized replication, advanced virtualization support, agentless backup, remote virtual standby, tape support, application consistent backups, granular restore, unified reporting and dashboard. | | | | | | |
| On-Appliance Virtual Standby | N/A | Up to 6 VMs | N/A | Up to 9 VMs | N/A | Up to 12 VMs |
| **Warranty and Technical Specifications** | | | | | | |
| Full System Depot Warranty | 3 Years | | | | | |
| Physical Dimensions (H x W x D in Inches) | 3.5" x 17.2" x 25.6" (2U - 19" Rack Mount rails provided) | | | | | |
| Remote management and network interface ports | 1 x IPMI & 2 x 1 GbE (RJ45) and 4 x 1GbE (RJ45). Optional 2 x 10Gb | | | | | |
| Hard Disk type and RAID configuration | 10 x 2 TB SAS (RAID 6) | 10 x 2 TB SAS (RAID 6) | 12 x 2 TB SAS (RAID 6) | 12 x 2 TB SAS (RAID 6) | 12 x 3 TB SAS (RAID 6) | 12 x 3 TB SAS (RAID 6) |
| External Tape Backup Connectivity (SAS, SATA, FC) | 1 x PASS | | | | | |
| Total system RAM | 64 GB | 96 GB | 64 GB | 96 GB | 128 GB | 192 GB |
| SSD drive | 240 GB | 240 GB SSD | 480 GB | 480 GB | 480 GB | 480 GB |

| | | | | | | |
|---|---|---|---|---|---|---|
| (For deduplication hash tables) | SSD | | SSD | SSD | SSD | SSD |
| Maximum weight (lbs) | 52 lbs | | | | | |
| Power Supplies (Single or redundant) | 2 x 920w | | | | | |
| Power consumption (Watts @ idle/-load/startup) | 208/257/358 | 208/257/358 | 208/257/358 | 208/257/358 | 240/296/369 | 240/296/369 |
| AC voltage & frequency range | 100 - 240v | | | | | |
| Ampere rating | 11 Amp Max | | | | | |

*1 TB = 1,000,000,000,000 bytes.

** On "V" models, space available for backup is reduced by the size of virtual standby VMs.

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

# Models 8100-8400

Arcserve UDP Appliance Models 8100 - 8400

| Arcserve UDP 8000 Series Appliance 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/96GB/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 | 9361-4i | | 9361-8i | |
| RAID Con-figuration | RAID-5 with BBU | | RAID-6 with BBU | |
| Drive Bays | 4 | | 12 | |
| Drives | 3x 2TB SAS 12G<br>4x 2TB SAS 12G | 3x 4TB SAS 12G<br>4x 4TB SAS 12G | 6x 4TB SAS 12G<br>7x 4TB SAS 12G<br>8x 4TB SAS 12G<br>9x 4TB SAS 12G<br>10x 4TB SAS 12G<br>11x 4TB SAS 12G<br>12x 4TB SAS 12G | 6x 8TB SAS 12G<br>7x 8TB SAS 12G<br>8x 8TB SAS 12G<br>9x 8TB SAS 12G<br>10x 8TB SAS 12G<br>11x 8TB SAS 12G<br>12x 8TB SAS 12G |
| DIMMs / Max DIMMs | 4x 8GB DDR4-2400/ 8 | | 4x 16GB DDR4-2400/ 8 | 4x 32GB DDR4-2400/ 8 |
| Cards | LSI SAS9200-8E | | | |
| Power Sup-plies | 2x hot swap redundant 500W AC 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 Appliances have 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.

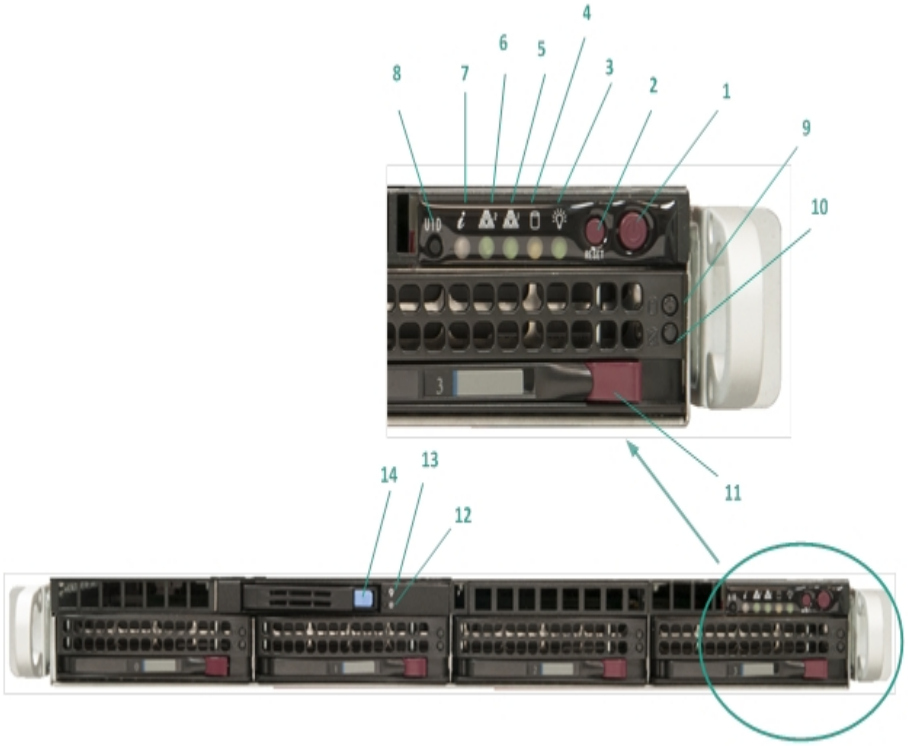
# Controls and Indicators

The Arcserve UDP 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
- Rear Panel 7100-7300v
- Rear Panel 7400-7600v
- Rear Panel 8100-8200
- Rear Panel 8300-8400

# Front Panel 7100-7300v

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



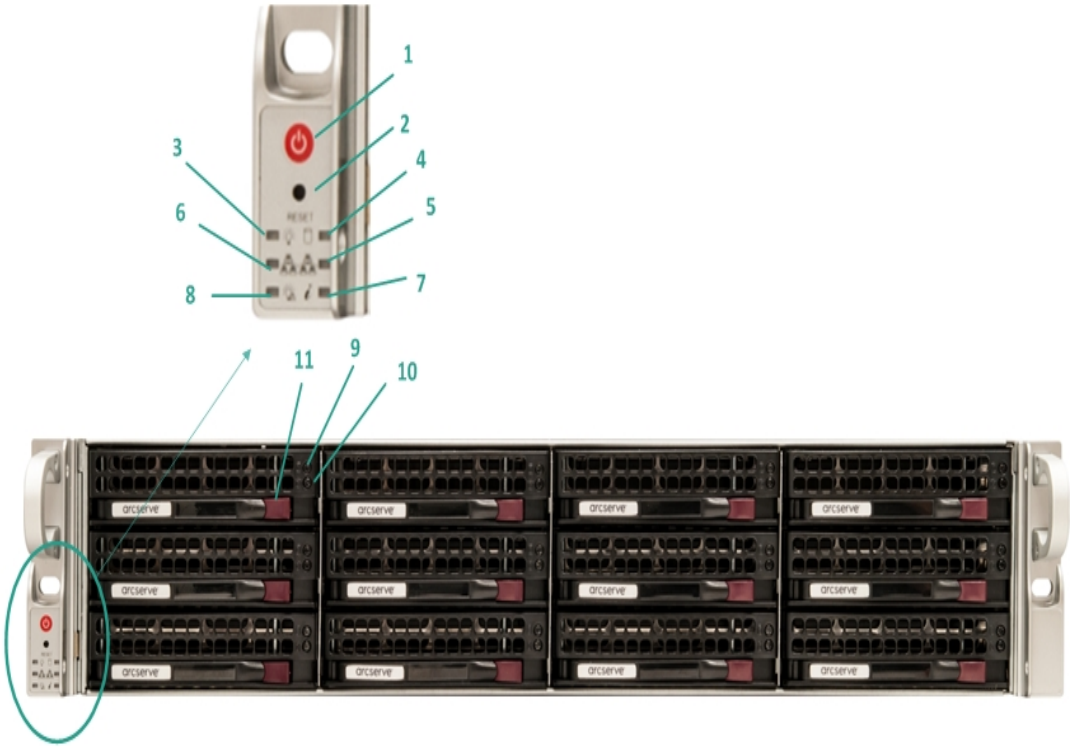

| Number | Control/Indicator | Description |
|---|---|---|
| 1 | Power button | Used to turn on and off power from the power supply to the appliance components. When turning off the power, the main power is turned off but standby power is still supplied. Therefore, to ensure power is completely removed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

| | | |
|---|---|---|
| 7 | Information LED | **Continuously on and Red:** An overheat condition has occurred. (This can be caused due to cable congestion.)<br>***Blinking Red - Fast (1 second):** Fan Failure. Check for an inoperative fan.<br>***Blinking Red - Slow (4 seconds):** Power Failure. Check for an inoperative power supply.<br>**Solid Blue:** Local UID has been activated. Use this function to locate the Server in a rack environment.<br>**Blinking Blue:** Remote UID has been activated. Use this function to locate the Server from a remote location. |
| 8 | Unit Identifier (UID) button | Used to turn on or off the Universal Information LED (blue) on both the front and rear appliance panels.<br>When the blue LED is on, the appliance can be easily located in a rack (from either the front or the back). |
| 9 | Hard Drive (HDD) LED | **Blinking Green**: Indicates activity on the corresponding drive. |
| 10 | Hard Drive (HDD) LED | ***Solid Red**: Indicates failure of the corresponding hard drive.<br>With the Arcserve UDP appliance, if one hard drive fails, the rest of the drives will kick in immediately to ensure no data is lost and the appliance continues to work normally. Therefore, to guard against any problems associated with multiple hard drive failures, it is important to replace a hard drive as soon as possible to minimize potential loss of data. |
| 11 | Hard Drive (HDD) Latch | Used to unlock and remove the hard drive. |
| 12 | Solid State Drive (SSD) LED | ***Solid Red**: Indicates drive failure. |
| 13 | Solid State Drive (SSD) LED | **Solid Green**: Indicates drive activity.<br>**Blinking Green**: Indicates the drive is being accessed. |
| 14 | Solid State Drive (SSD) Latch | Used to unlock and remove the SSD drive. |

*Any Solid or Blinking Red light indicates some kind of failure. To quickly resolve this issue, contact our support site at arcserve.com/support.

# Front Panel 7400-7600v

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



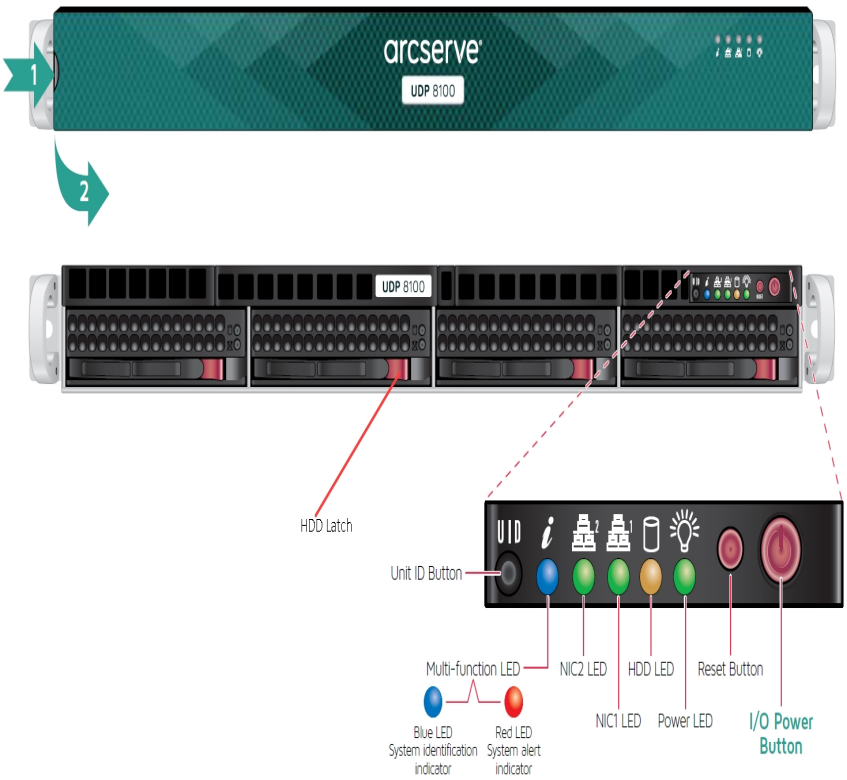

| Number | Control/Indicator | Description |
|---|---|---|
| 1 | Power button | Used to turn on and off power from the power supply to the appliance components. When turning off the power, the main power is turned off but standby power is still supplied. Therefore, to ensure power is completely removed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

| | | |
|---|---|---|
| 7 | Information LED | **Continuously on and Red:** An overheat condition has occurred. (This can be caused due to cable congestion.)<br>***Blinking Red - Fast (1 second):** Fan Failure. Check for an inoperative fan.<br>***Blinking Red - Slow (4 seconds):** Power Failure. Check for an inoperative power supply.<br>**Solid Blue:** Local UID has been activated. Use this function to locate the Server in a rack environment.<br>**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 drive. |
| 10 | Hard Drive (HDD) LED | ***Solid Red**: Indicates failure of the corresponding hard drive.<br>With the Arcserve UDP appliance, if one hard drive fails, the rest of the drives will kick in immediately to ensure no data is lost and the appliance continues to work normally. Therefore, to guard against any problems associated with multiple hard drive failures, it is important to replace a hard drive as soon as possible to minimize potential loss of data. |
| 11 | Hard Drive (HDD) Latch | Used to unlock and remove the hard drive. |

*Any Solid or Blinking Red light indicates some kind of failure. To quickly resolve this issue, contact our support site at arcserve.com/support.

# Front Panel 8100-8200

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



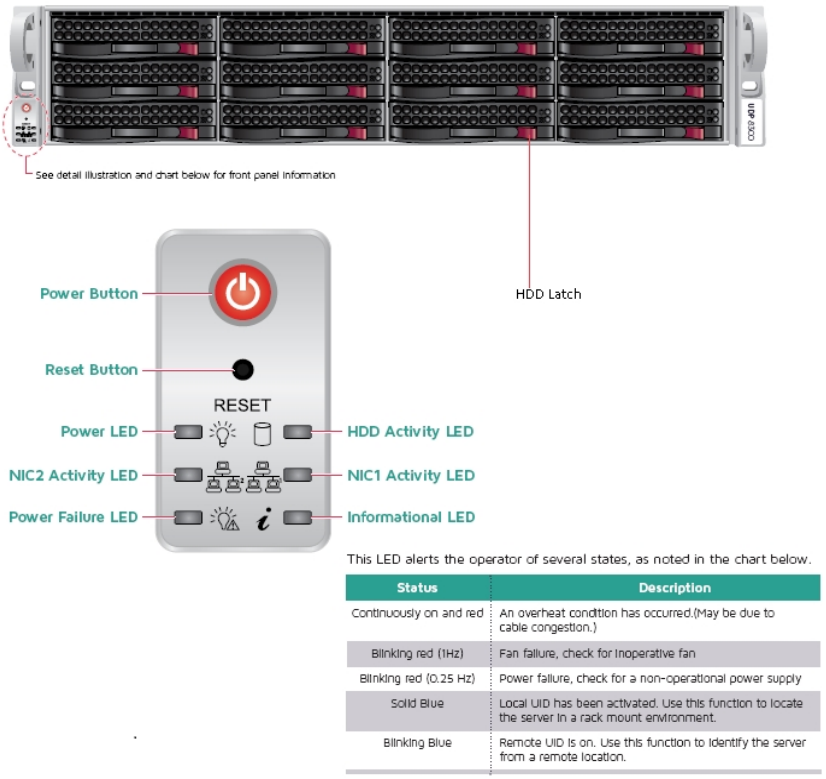

| Control/Indicator | Description |
|---|---|
| I/O Power button | Used to turn on and off power from the power supply to the appliance components. When turning off the power, the main power is turned off but standby power is still supplied. Therefore, to ensure that power is completely removed from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

| | |
|---|---|
| Information LED | **Continuously on and Red:** An overheat condition has occurred.<br>**Note:** A cable congestion may cause this situation.<br>***Blinking Red - Fast (1 second):** Fan Failure. Check for an inoperative fan.<br>***Blinking Red - Slow (4 seconds):** Power Failure. Check for an inoperative power supply.<br>**Solid Blue:** Local UID is activated. Use this function to locate the Server in a rack environment.<br>**Blinking Blue:** Remote UID is activated. Use this function to locate the Server from a remote location. |
| Unit Identifier (UID) button | Used to turn on or off the Universal Information LED (blue) on both the front and rear appliance panels.<br>When the blue LED is on, the appliance can be easily located in a rack (from either the front or the back). |
| Hard Drive (HDD) LED | **Blinking Green**: Indicates activity on the corresponding drive. |
| Hard Drive (HDD) LED | ***Solid Red**: Indicates failure of the corresponding hard drive.<br>With the Arcserve UDP appliance, if one hard drive fails, the rest of the drives will kick in immediately to ensure no data is lost and the appliance continues to work normally. Therefore, to guard against any problems associated with multiple hard drive failures, it is important to replace a hard drive as soon as possible to minimize potential loss of data. |
| Hard Drive (HDD) Latch | Used to unlock and remove the hard drive. |
| Solid State Drive (SSD) LED | ***Solid Red**: Indicates drive failure. |
| Solid State Drive (SSD) LED | **Solid Green**: Indicates drive activity.<br>**Blinking Green**: Indicates the drive is being accessed. |
| Solid State Drive (SSD) Latch | Used to unlock and remove the SSD drive. |

*Any Solid or Blinking Red light indicates some kind of failure. To quickly resolve this issue, contact our support site at arcserve.com/support.

# Front Panel 8300-8400

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



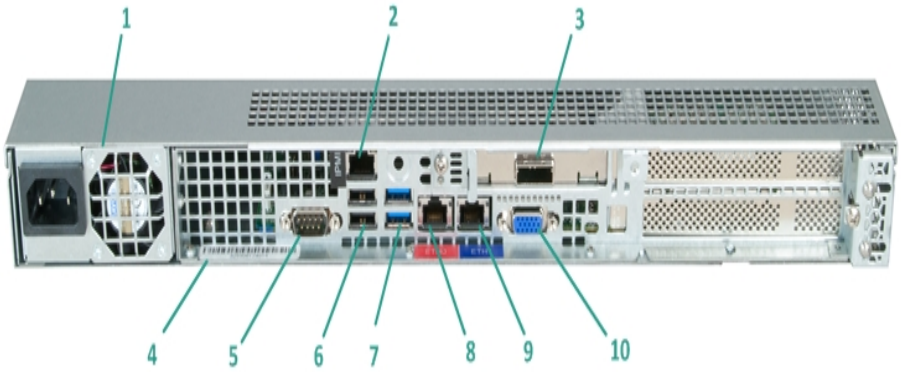

| Control/Indicator | Description |
|---|---|
| Power button | Used to turn on and off power from the power supply to the appliance components. When turning off the power, the main power is turned off but standby power is still supplied. Therefore, to ensure power is completely removed from the appliance, unplug the power supply cable before performing maintenance. |
| Reset button | Used to reboot the appliance. |
| Power LED | **Solid Green:** Indicates that the power is being supplied to the power supply of the appliance.<br>This LED should normally be on when the appliance is operating. |
| Network Interface Card (NIC1) LED | **Blinking Amber**: Indicates network activity on Network 1 (ETH0 Port). |
| Network Interface Card (NIC2) LED | **Blinking Amber:** Indicates network activity on Network 2 (ETH1 Port). |
| Information LED | **Continuously on and Red:** An overheat condition has occurred. (This can be caused due to cable congestion.) |

| | |
|---|---|
| | ***Blinking Red - Fast (1 second):** Fan Failure. Check for an inoperative fan.<br>***Blinking Red - Slow (4 seconds):** Power Failure. Check for an inoperative power supply.<br>**Solid Blue:** Local UID has been activated. Use this function to locate the Server in a rack environment.<br>**Blinking Blue:** Remote UID has been activated. Use this function to locate the Server from a remote location. |
| Power Failure LED | Indicates a power supply module has failed. |
| Hard Drive (HDD) LED | **Blinking Green**: Indicates activity on the corresponding drive. |
| Hard Drive (HDD) LED | ***Solid Red**: Indicates failure of the corresponding hard drive.<br>With the Arcserve UDP appliance, if one hard drive fails, the rest of the drives will kick in immediately to ensure no data is lost and the appliance continues to work normally. Therefore, to guard against any problems associated with multiple hard drive failures, it is important to replace a hard drive as soon as possible to minimize potential loss of data. |
| Hard Drive (HDD) Latch | Used to unlock and remove the hard drive. |

*Any Solid or Blinking Red light indicates some kind of failure. To quickly resolve this issue, contact our support site at arcserve.com/support.

# Rear Panel 7100-7300v

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

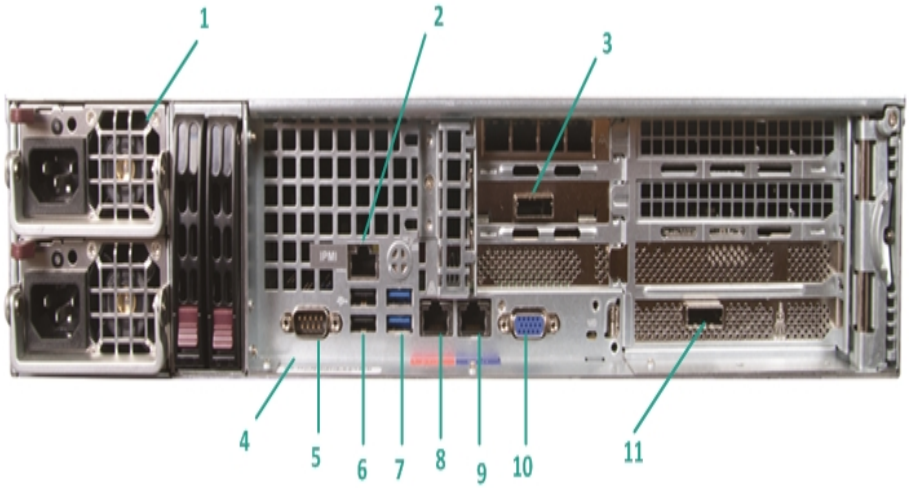



| Number | Name of Control/Indicator | Description |
|---|---|---|
| 1 | Power Supply | Provides high-efficiency power supply to the appliance.<br>**Note:** The main power switch is used to apply or remove power from the power supply to the appliance. Turning off the appliance power with this button removes the main power but standby power is still supplied. Therefore, to ensure power is completely removed from the appliance, unplug the power supply cable before performing maintenance. |
| 2 | IPMI Port (Remote Management) | The IPMI (Intelligent Platform Management Interface) port is used to monitor the physical health of Servers, such as temperature, voltage, fans, power supplies, and the appliance.<br>**Note**: The default user name/password for IPMI access is ADMIN/ARCADMIN (case-sensitive). We recommend that you change the password as soon as possible. For details about how to change the IPMI password, see How to Change the IPMI Password. |
| 3 | External Storage Device Port<br>(SAS port for tape drive) | Used to connect an external storage device (hard drive, tape drive, etc.) to the appliance. These portable external storage devices can be used to store backed-up data for easy transporting from one location to another. |
| 4 | Serial Number Label | A unique serial number that is assigned to the appliance. |
| 5 | COM1 Serial Port | Communication port that is used to connect a serial device, such as a mouse to the appliance (if needed). |
| 6 | USB 2.0 (black) | Used to connect USB 2.0 type devices to the appliance. |

| | | |
|---|---|---|
| 7 | USB 3.0 (blue) | Used to connect USB 3.0 type devices to the appliance. |
| 8 | Network Data I/O Port 1 | Used to transfer network data to and from the appliance. ((ETH0 for Network 1) |
| 9 | Network Data I/O Port 2 | Used to transfer network data to and from the appliance. (ETH1 for Network 2) |
| 10 | VGA Connector | Used to connect a monitor to the appliance (if needed). |

# Rear Panel 7400-7600v

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

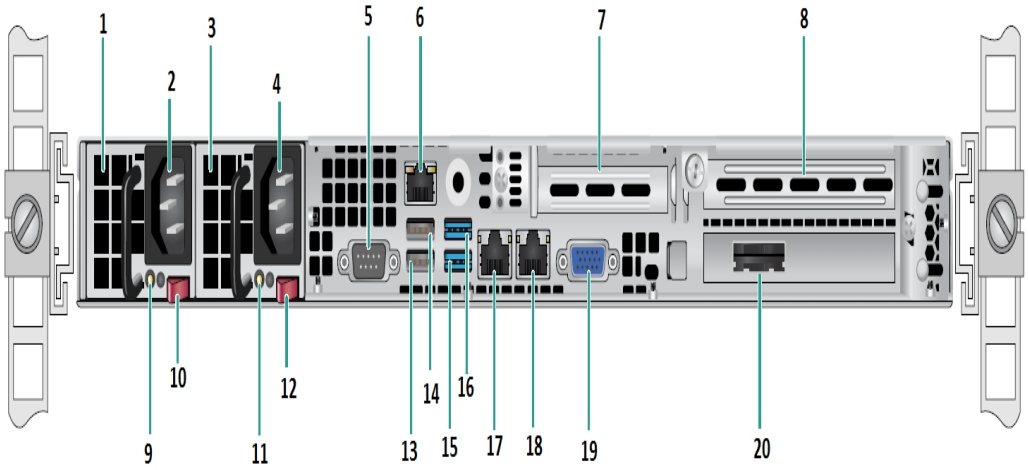



| Number | Name of Control/Indicator | Description |
|---|---|---|
| 1 | Dual Power Supply | Provides high-efficiency power supply to the appliance.<br>**Note:** The main power switch is used to apply or remove power from the power supply to the appliance. The benefit of having a dual power supply is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

| | | |
|---|---|---|
| | drive) | |
| 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<br>(Tap Auto-loader/Library)<br>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.<br>**Note**: This port is present in the operating system as LSI Adapter SAS2 2008 Falcon. |

# Rear Panel 8100-8200

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

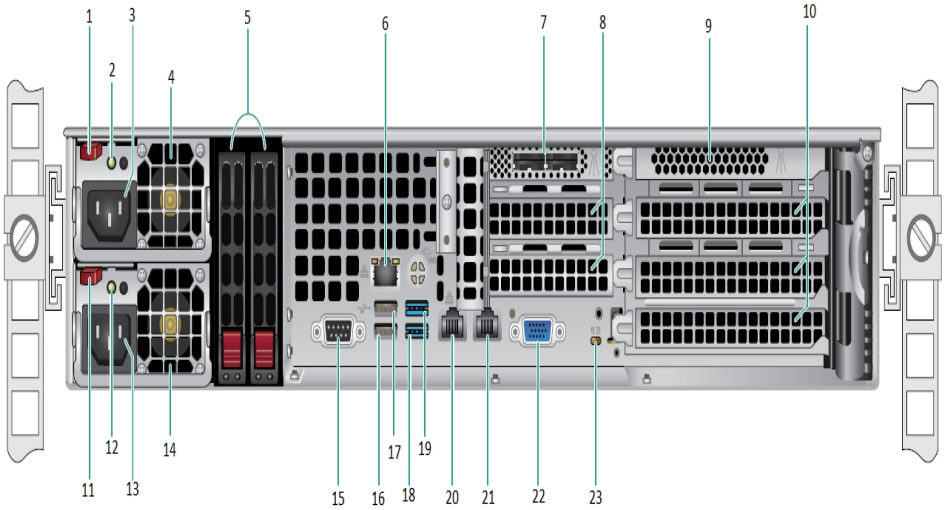



| Num-ber | Name of Control/Indicator |
|---|---|
| 1 | Power Supply Module #1 |
| 2 | AC Power Inlet #1 |
| 3 | Power Supply #2 |
| 4 | AC Power Inlet #2 |
| 5 | COM Port |
| 6 | IPMI Port (Remote Management) |
| 7 | Low Profile PCI Expansion Slot |
| 8 | PCI Expansion Slot |
| 9 | Power Good LED #1 |
| 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<br>(SAS port for tape drive option) |

# Rear Panel 8300-8400

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




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

| | |
|---|---|
| 19 | USB Port 4 (generation 3) |
| 20 | ETH0 (Network 1) |
| 21 | ETH1 (Network 2) |
| 22 | VGA Port (Monitor) |
| 23 | UID LED |

# Ports Used by the Appliance

The following list of tables provide information about ports that are used by Arcserve UDP, Arcserve Backup, and the appliance for Linux support:

- Arcserve UDP
- Arcserve Backup
- Appliance for Linux Support

# Arcserve UDP

This section contains the following topics:

- Components installed on Microsoft Windows
- Components installed on Linux
- Production node protected by UDP Linux remotely

# Components installed on Microsoft Windows

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

| Port # | Port Type | Initiated by | Listening Process | Description |
|---|---|---|---|---|
| 1433 | TCP | Remote Java | sqlsrvr.exe | Specifies the default communication port between the Arcserve UDP console and Microsoft SQL Server databases when they reside on different computers.<br>**Note**: You can modify the default communication port when installing SQL Server. |
| 4090 | TCP | Arcserve UDP Agent | HATransServer.exe | Transfers data for Virtual Standby tasks in the proxy mode. |
| 5000-5060 | TCP | Arcserve UDP Server | GDDServer.exe | Reserved for Arcserve UDP RPS Global Deduplication Data Store Service (GDD). One Arcserve UDP GDD data store will use 3 free ports that start from 5000. It is needed when the data store with GDD is enabled for backup or the restore task is used. |
| 6052 | TCP | Arcserve Backup GDB | CA.ARCserve.CommunicationFoundation.WindowsService.exe | CA.ARCserve.CommunicationFoundation.WindowsService.exe<br>Communication that lets the Arcserve UDP Console and the Arcserve Backup Global Dashboard Primary Server synchronize data. |
| 6054 | TCP | Arcserve Backup | | CA.ARCserve.CommunicationFoundation.WindowsService.exe<br>Communication that lets the Arcserve UDP Console and the Arcserve Backup Primary Server synchronize data. |
| 8006 | | | | To shut down Tomcat that is used by the Arcserve UDP console. |
| 8014 | TCP | Arcserve UDP Console | Tomcat7.exe | Specifies the default HTTP/HTTPS communication port between remote management consoles and the Arcserve UDP Server.<br>Specifies the default HTTP/HTTPS com- |

| | | | | |
|---|---|---|---|---|
| | | | | munication port between remote management consoles and the Arcserve UDP Agent.<br>**Note**: You can modify the default communication port when you install the Arcserve UDP components. |
| 8014 | TCP | Arcserve UDP Server | httpd.exe | Specifies the default HTTP/HTTPS communication port between the Arcserve UDP Server and Arcserve UDP consoles.<br>*Specifies the default shared port and the only port you must open when you use the Arcserve UDP Server as the replication destination. Do not open ports 5000-5060 which are used by data stores that have global deduplication enabled.<br>**Note**: You can modify the default communication port when you install the Arcserve UDP components. |
| 8015 | TCP | Arcserve UDP Console | Tomcat7.exe | Specifies the default HTTP/HTTPS communication port between remote management consoles and the Arcserve UDP Server.<br>Specifies the default HTTP/HTTPS communication port between remote management consoles and the Arcserve UDP Agent.<br>**Note**: You can modify the default communication port when you install the Arcserve UDP components. |
| 8016 | TCP | Arcserve UDP Server | Tomcat7.exe | Reserved for Arcserve UDP Server Web Services to communicate with the Arcserve UDP RPS Port Sharing Service on the same Server.<br>**Note**: The port cannot be customized and can be ignored for the firewall setting. |
| 18005 | | | CA.ARCserve.CommunicationFoundation.WindowsService.exe | To shutdown Tomcat that is used by the Arcserve UDP Server or Agent. |

# Components installed on Linux

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

| Port # | Port Type | Initiated by | Listening Process | Description |
|---|---|---|---|---|
| 22 | TCP | SSH service | | Arcserve UDP Linux 3rd party dependency. Specifies the default for SSH service, however, you can change this port. This port is required for both incoming and outgoing communications. |
| 67 | UDP | Arcserve UDP Linux | bootpd | Used for the PXE boot Server. Only required if the user wants to use the PXE boot feature. This port is required for incoming communications.<br>**Note**: The port number cannot be customized. |
| 69 | UDP | Arcserve UDP Linux | tffpd | Used for the PXE boot Server. Only required if the user wants to use the PXE boot feature. This port is required for incoming communications.<br>**Note**: The port number cannot be customized. |
| 8014 | TCP | Arcserve UDP Linux | Java | Specifies the default HTTP/HTTPS communication ports between the remote consoles and the Arcserve UDP agent for Linux. This port is required for both incoming and outgoing communications. |
| 18005 | TCP | Arcserve UDP Linux | Java | Used by Tomcat. Can be ignored for firewall settings. |

# Production node protected by UDP Linux remotely

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

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

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

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

# Arcserve Backup

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

| Port # | Port Type | Initiated by | Listening Process | Description |
|---|---|---|---|---|
| 135 | TCP | | | Microsoft Port Mapper |
| 445 | TCP | | MSRPC over the Named Pipes | |
| 6050 | TCP/UDP | CASUniversalAgent | Univagent.exe | Arcserve Universal Agent |
| 6502 | TCP | Arcserve Communication Foundation | CA.ARCserve.CommunicationFoundation.WindowsService.exe | Arcserve Communication Foundation |
| 6502 | TCP | CASTapeEngine | Tapeng.exe | Arcserve Tape Engine |
| 6503 | TCP | CASJobEngine | Jobengine.exe | Arcserve Job Engine |
| 6504 | TCP | CASDBEngine | DBEng.exe | Arcserve Database Engine |
| 7854 | TCP | CASportmapper | Catirpc.exe | Arcserve PortMapper |
| 4152-3 | TCP | CASDiscovery | casdscsvc.exe | Arcserve Discovery Service |
| 4152-4 | UDP | CASDiscovery | casdscsvc.exe | Arcserve Discovery Service |
| 9000-9500 | TCP | | For other Arcserve MS RPC services that use dynamic ports | |

# Appliance for Linux Support

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

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

# Chapter 3: Installing the Arcserve UDP Appliance

This section contains the following topics:

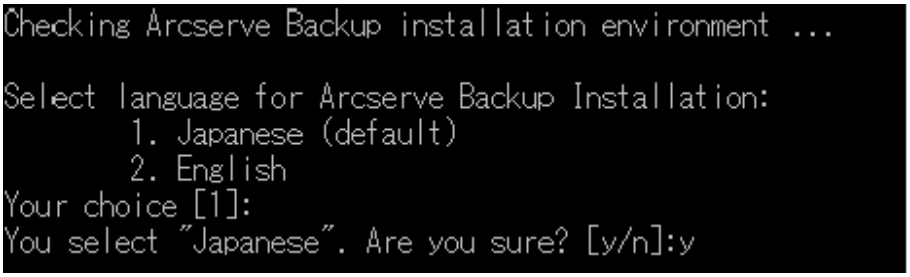
# How to Install Arcserve Backup r17.5

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

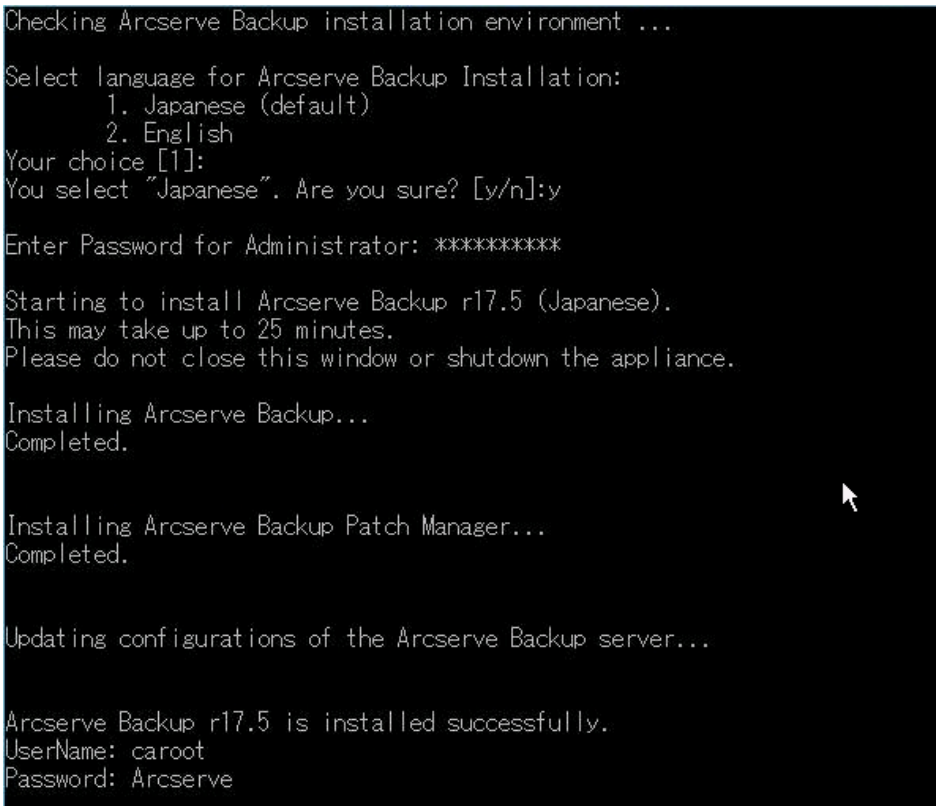
**Follow these steps:**

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

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




2. Enter the Administrator password and the script is generated to help install Arcserve Backup r17.5.



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. Initial setup and maintenance should be performed by qualified personnel.

For the complete installation process, see Appliance Installation of 8100-8200.

# How to Install 8300-8400 Series Appliance

The appliance is intended for installation in restricted areas only. Initial setup and maintenance should be performed by qualified personnel.

For the complete installation process, see Appliance Installation of 8300-8400.

# Chapter 4: Understanding Network Configuration

This section contains the following topics:

# How to Configure the NIC Teaming Process

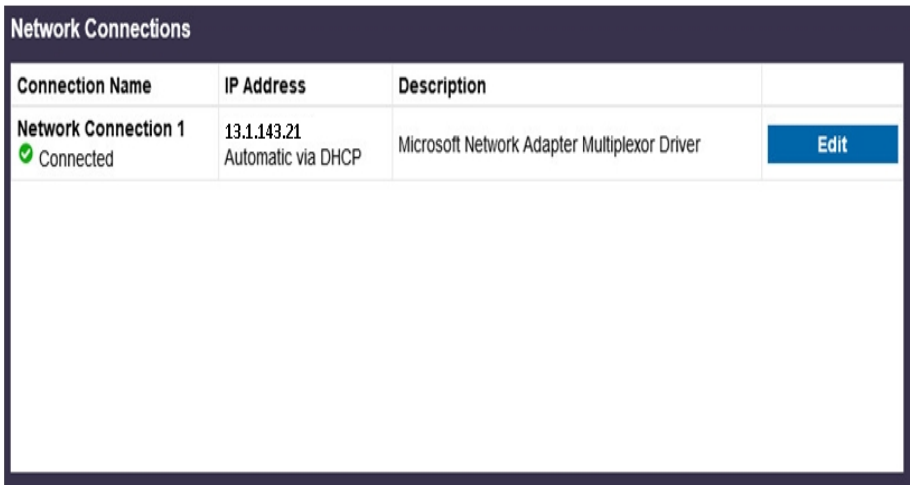
The Arcserve UDP Appliance contains built-in Ethernet ports. To use these ports, an Ethernet NIC teaming needs to be configured. NIC Teaming allows multiple network adapters placed into a team for bandwidth aggregation and traffic failover to maintain connectivity in the event of a network component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

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




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

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

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

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

   The Routing and Remote Access Server Setup Wizard opens.

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

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

   The configuration completes and the following message appears.


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

# How to Disable DHCP Server

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

To disable DHCP Server, follow these steps:

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

   *DHCP_ENABLE=false*

   *AdapterName=LinuxBkpSvr*

   *Appliance_IPAddress=192.168.10.1*

   *Linux_IPAddress=192.168.10.2*
3. Save the file.
4. Delete the file *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\dhcpdone.flag*.
5. Run *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\resetdhcp.ps1* to disable the DHCP Server service as below from dos command line:

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

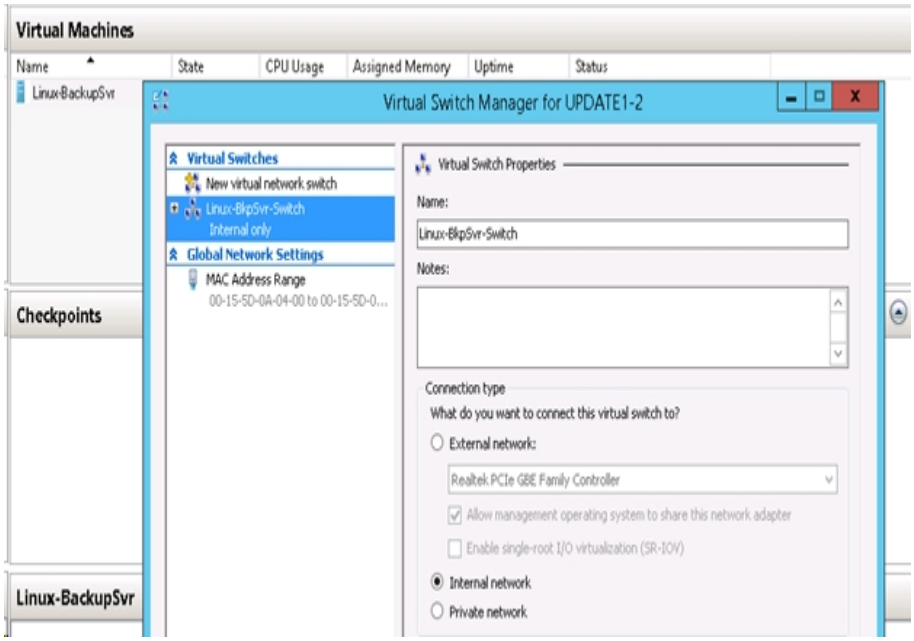
# How to Understand the Network Configuration on the UDP Appliance

The purpose of network configuration on the Appliance ensures the build-in Linux Backup Server (virtual name in Hyper-V Manager: Linux-BackupSvr) can work behind NAT. So that:

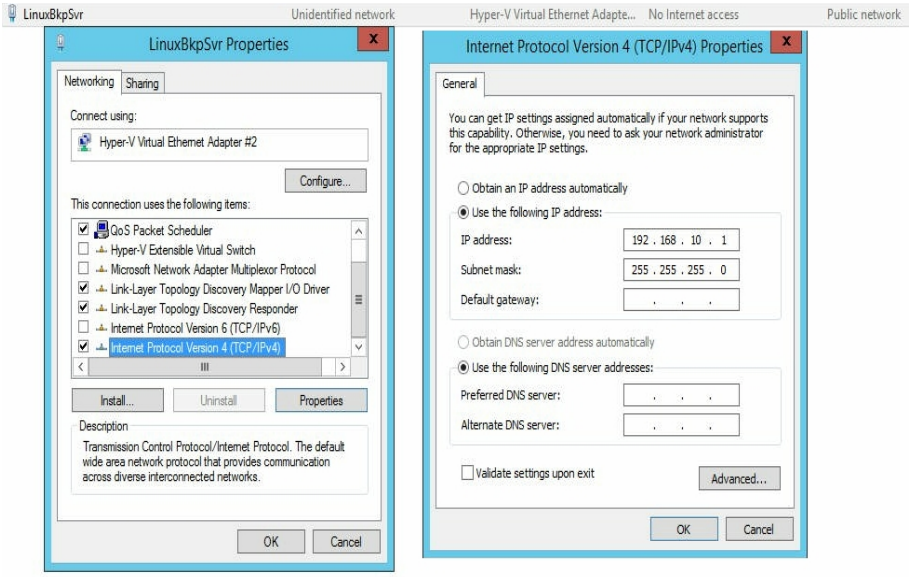
- User does not need to change the hostname of the build-in Linux.
- User saves an IP on the network for the Linux Backup Server.
- The Linux Backup Server can connect to any machine on the public network.
- Any machine on the public network can only connect to the Linux Backup Server through the Appliance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

**Network Configuration Detail:**

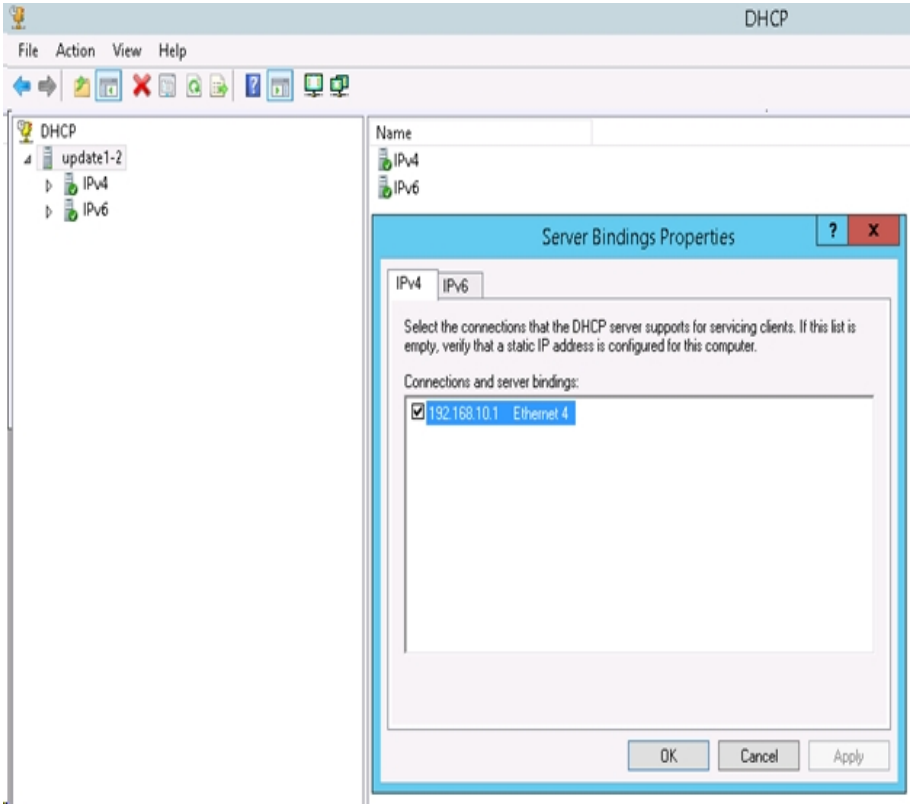
- On the Hyper-V Manager, an internal only virtual switch – *Linux-BkpSvr-Switch* is available that is used only by Linux-BackupSvr.



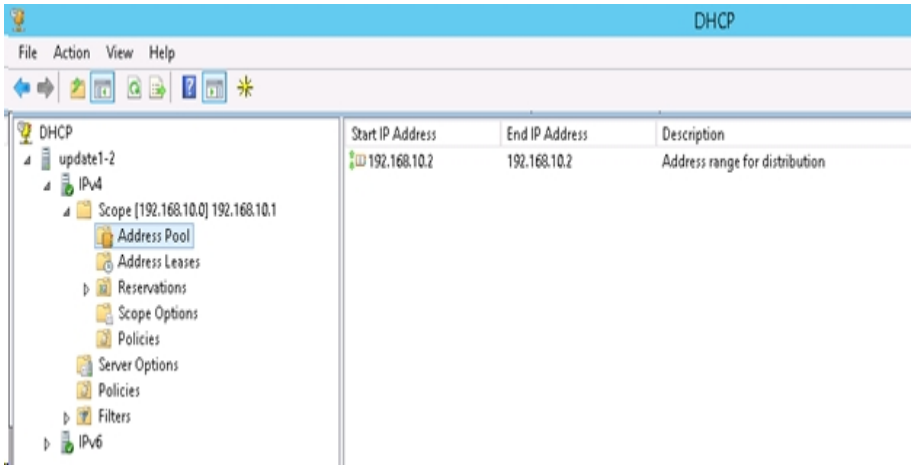

- In the *Control Panel\Network and Internet\Network Connections*, you can see "Hyper-V Virtual Ethernet Adapter" named as "LinuxBkpSvr". You have configured the IPv4 for this switch as "192.168.10.1" by default as below.



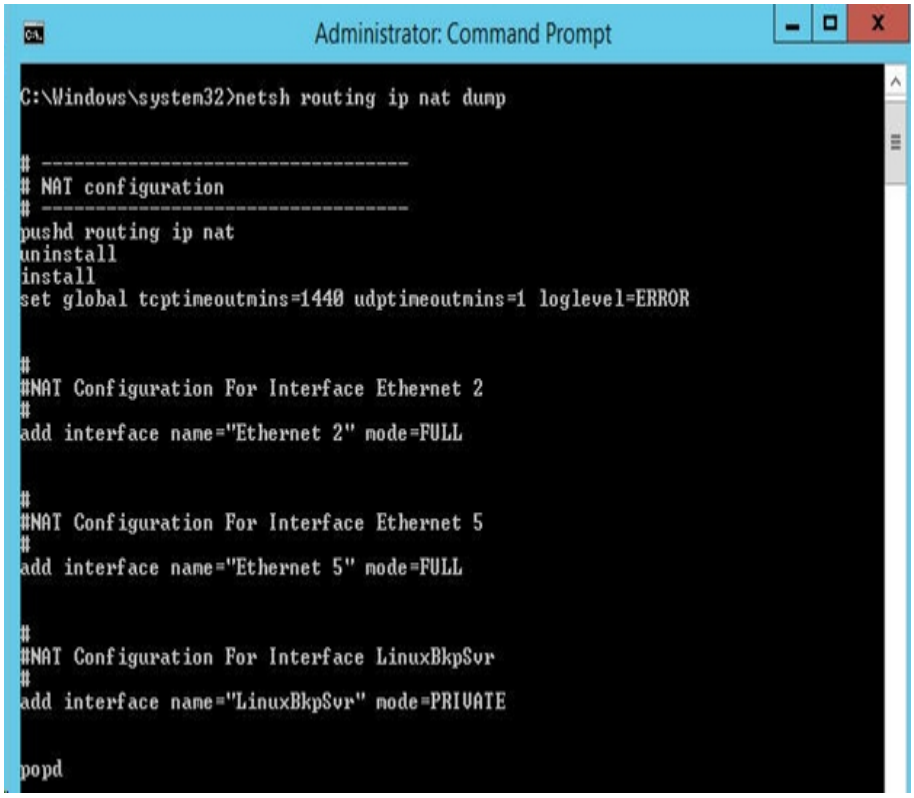

- You have configured DHCP Server on the appliance machine by default, the DHCP Server only works on the Hyper-V virtual adapter.




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




- We have configured NAT on the Appliance machine.


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

```
C:\Windows\system32>netsh interface portproxy show all

Listen on ipv4:             Connect to ipv4:

Address         Port        Address         Port
--------------- ----------  --------------- ----------
*               8018        192.168.10.2    8014
*               8019        192.168.10.2    22
*               8035        192.168.10.2    8035
```

- 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
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=dhcp
DEFROUTE=yes
NAME="eth0"
[root@Linux-BackupSvr network-scripts]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5D:0A:04:00
          inet6 addr: fe80::215:5dff:fe0a:400/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:481943 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100859 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36784482 (35.0 MiB)  TX bytes:21795976 (20.7 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

# 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. Please refer to the network configuration introduction for preinstalled Linux Backup Server as for how preinstalled Linux Backup Server communicate with Appliance Server.

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

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

   **Note:**

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

     Here is the file after modified:

     *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.

Run the command prompt and enter the following command:

*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.

For more details, refer to Microsoft KB 168321.

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.

# Chapter 5: Upgrading Arcserve UDP on the Appliance

This section contains the following topics:

# How to Apply a License After Upgrading Arcserve Software

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

For more details about adding a license key for Arcserve UDP, see **Arcserve Product Activation** topic from the *Arcserve Unified Data Protection Solutions Guide*.

For more details about adding a license key for Arcserve UDP, see *Apply Arcserve Backup Component Licenses* from the *Arcserve Backup Administration Guide*.

# Upgrade Sequence on the Arcserve UDP Appliance

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

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

# Upgrade the Arcserve UDP Appliance that performs as Arcserve UDP Console and RPS

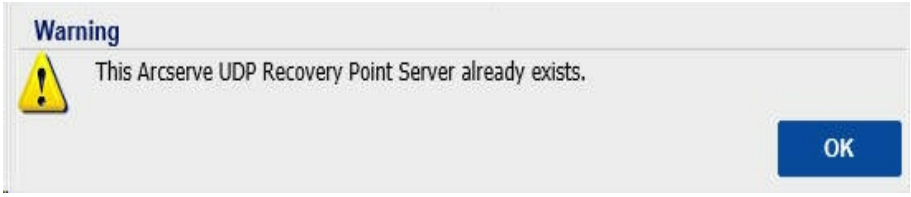
Upgrade this Arcserve UDP Appliance, then follow up the upgrade sequence described to upgrade the environment.

# Upgrade the Arcserve UDP Appliance that performs as Arcserve UDP RPS only

Upgrade the complete productive environment. For details, refer to the upgrade sequence.

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

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



# Upgrade the Arcserve UDP Linux Agent on the Arcserve UDP Appliance

- First, upgrade the Arcserve UDP Console which manages the Linux Backup Server environment;
- Then, upgrade the Linux Backup Server on the Arcserve UDP Appliance. For details, refer to the *Arcserve Unified Data Protection Agent for Linux Online Help*.

# Upgrade the Arcserve Backup on the Arcserve UDP Appliance

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

# Upgrade Sequence for UDP Console, RPS, and Agent

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

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

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

**Note:** Per the replication backward support policy, always upgrade the target RPS before the source RPS.

# Chapter 6: Configuring the Arcserve UDP Appliance

This section contains the following topics:

# How to Configure Network Settings for a UDP Appliance

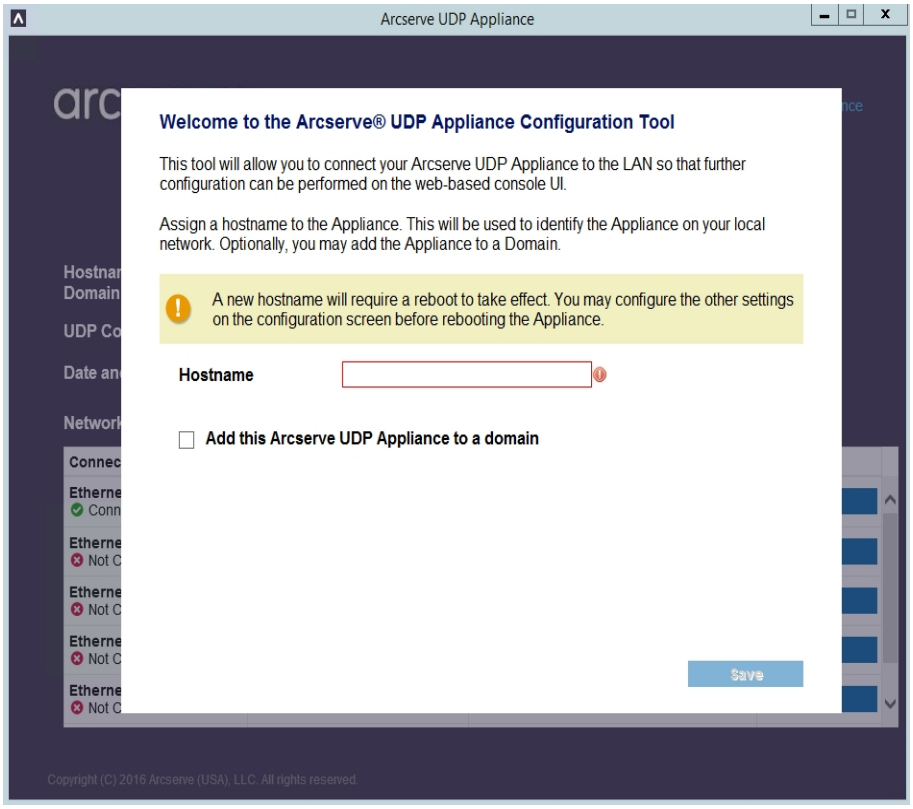
To manage the Arcserve UDP appliance, the first step is to have the appliance in your network. For that, you need to assign a hostname to the appliance and then configure network ports.

**Follow these steps:**

1. After you power on the appliance, the Settings screen for the Microsoft License terms opens. Read and accept the terms.
2. The UDP **End User License Agreement** dialog opens. Read and accept the license agreement and click **Next**.
3. Enter a hostname for the appliance. Assigning a name helps identify the appliance on your network.

   To make your appliance a member of a domain in your network, click the **Add this Arcserve UDP Appliance to a domain** option and specify the domain, user name, and password.

   **Note**: The Domain, Username, and Password fields is displayed when the option is selected.



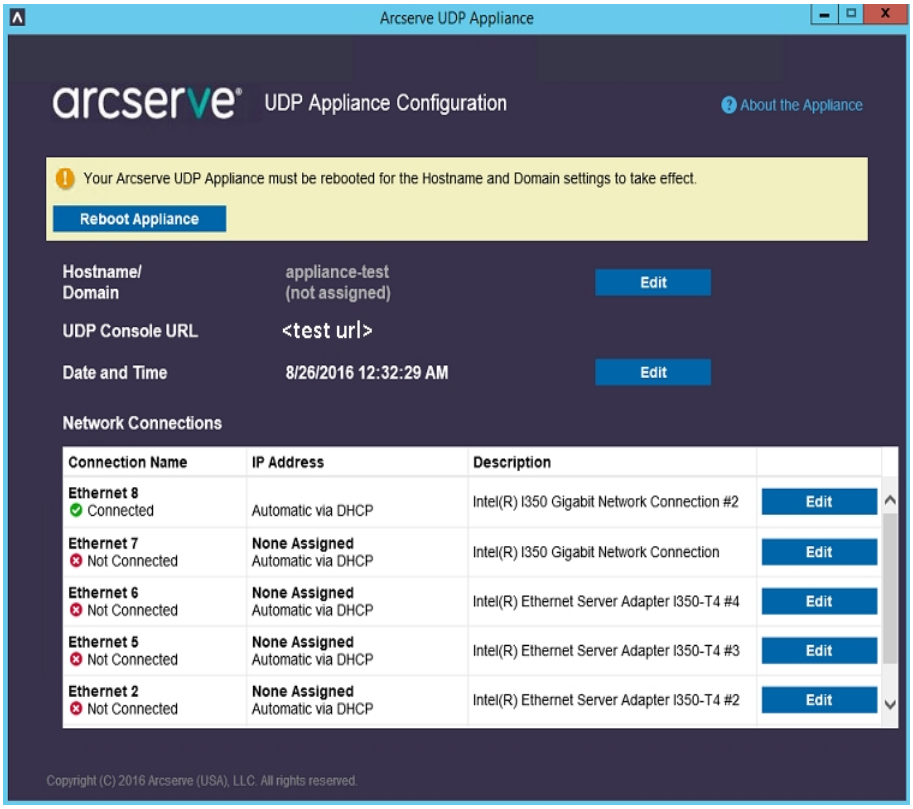

**Note:** To apply a new hostname, you need to restart the appliance. You can choose to reboot the appliance now or after you configure the network settings.

After you reboot the appliance, you can access the appliance from any other machine using the following URL:

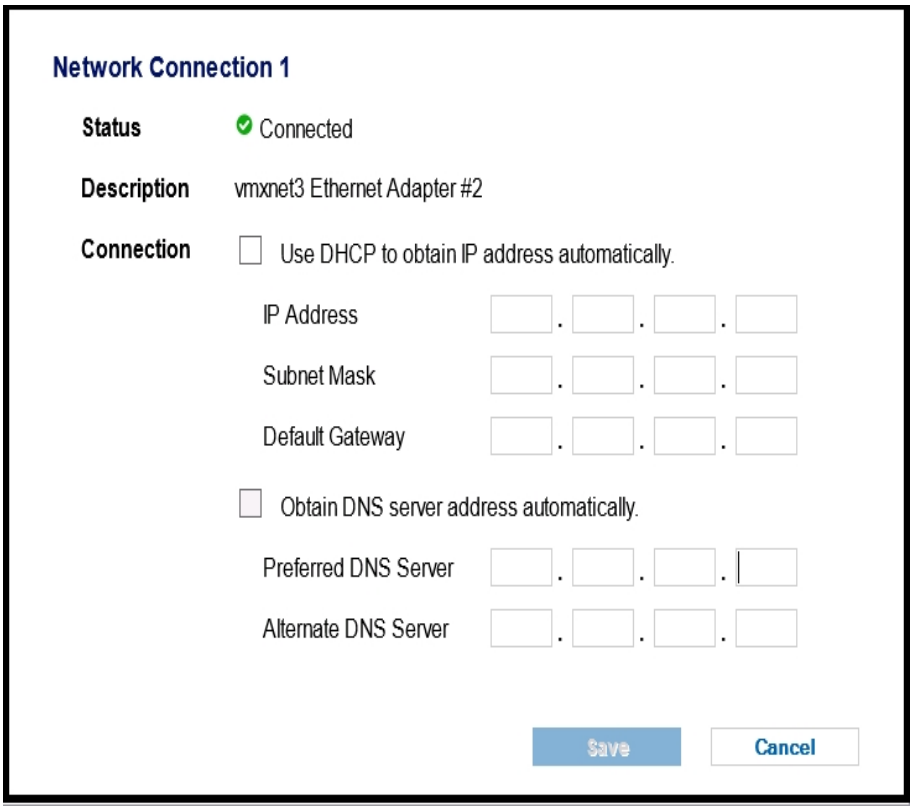
`https://<hostname>:8015`

4. Click **Save**.
5. 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.




6. To edit a network connection, click **Edit** from the **Network Connections** box.
7. The **Network Connection** dialog opens.



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

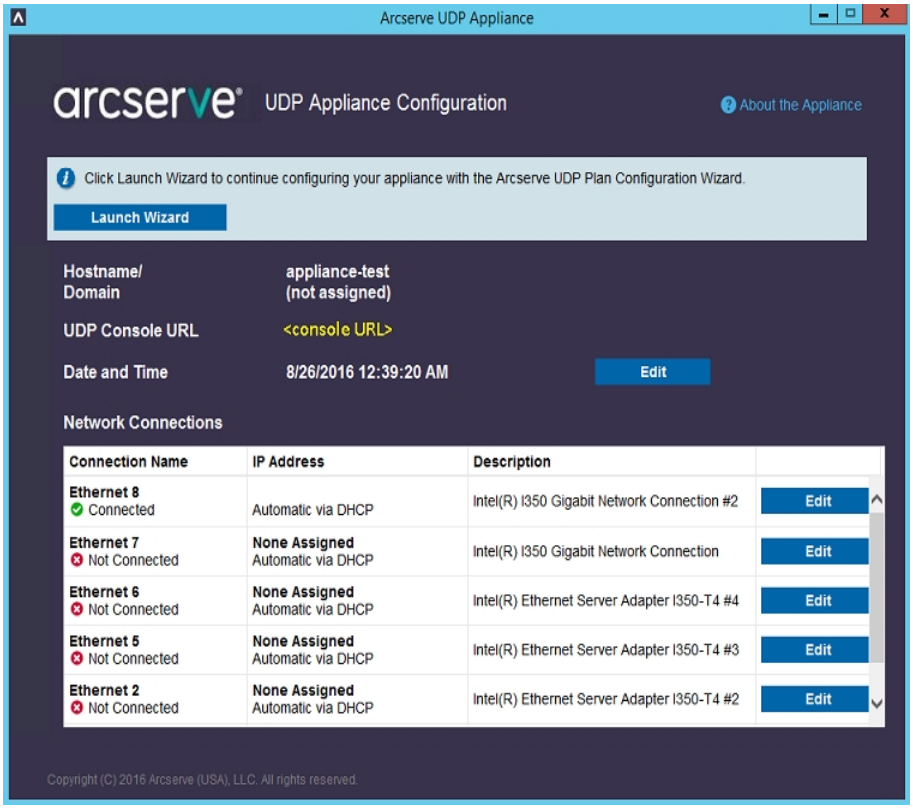
   **Note:** Optionally, you can also modify the hostname, domain, date, and time.

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

   The appliance restarts with a new hostname.

10. The Login screen opens again. Enter the user name and password and click **Enter**.

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



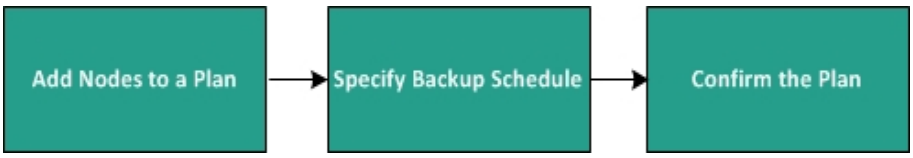
# Overview of Creating a Plan Using the UDP Appliance Wizard

A plan is a collection of steps that define what nodes to back up and when to back up. The Arcserve UDP appliance lets you create basic plans. Creating a plan using the UDP Appliance 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*.

# How to Set up the Arcserve UDP Appliance and Create Plans

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 you want to protect and when to create backups. The backup destination is the appliance Server.

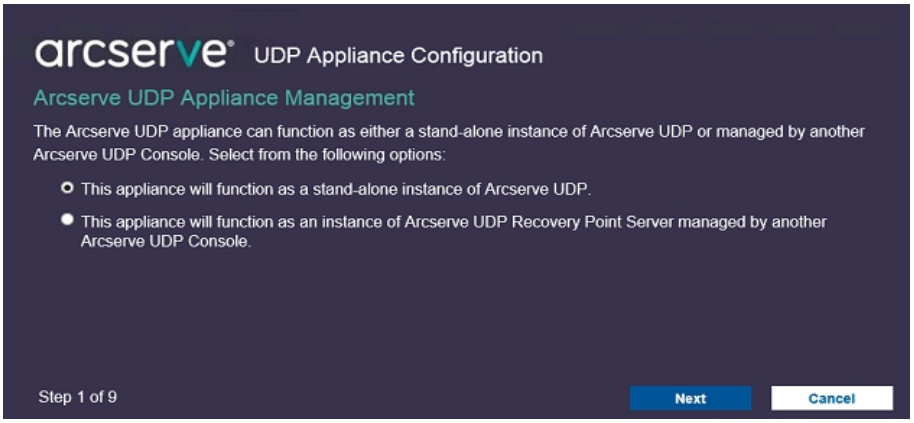
**Note:** All the steps on the wizard are optional, you can skip these and directly open the UDP console and create plans.

Video

How to Run the Arcserve UDP Appliance Wizard

**Follow these steps:**

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




3. 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.

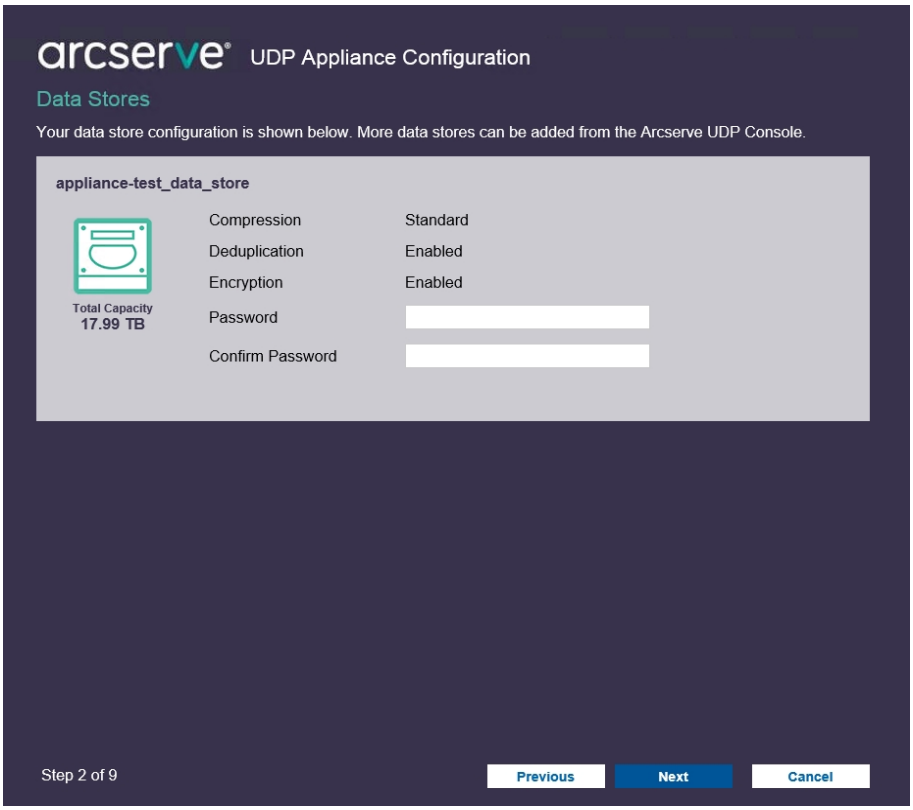
4. Click **Next**.

   **Note:** To cancel the wizard and open the Arcserve UDP Console, click **Cancel.**

5. The **Data Stores** dialog opens.

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

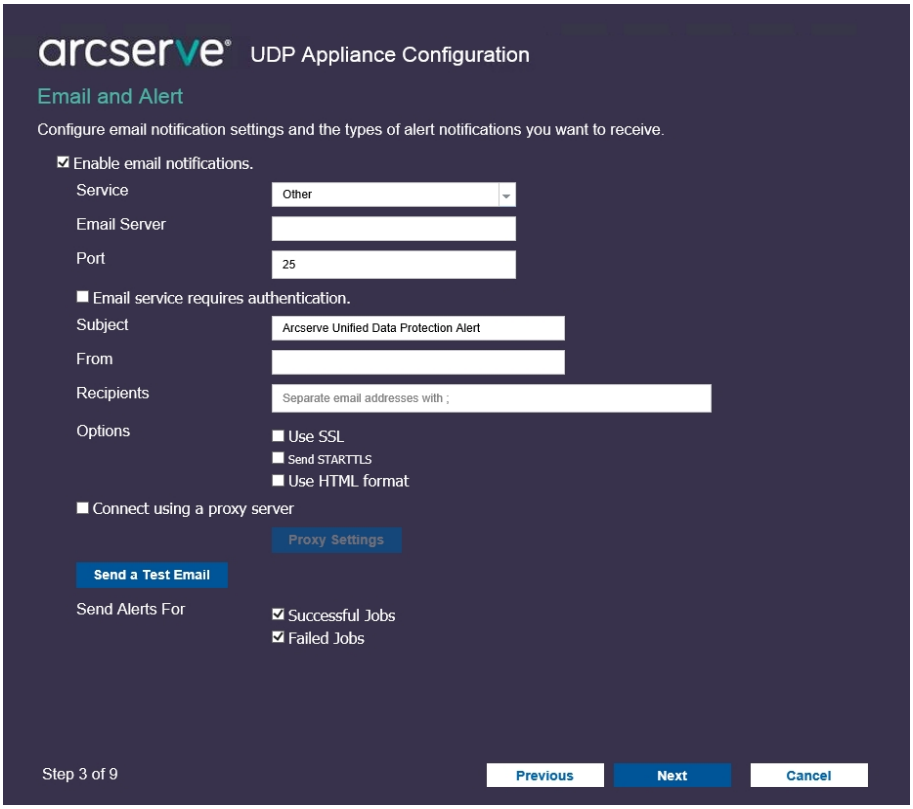
   By default, Arcserve UDP creates a data store called <hostname>_data_store. This data store is deduplication and encryption enabled. For more information about deduplication and encryption, see *Data Deduplication* topic in Arcserve UDP Solutions Guide.




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

6. Enter and confirm the encryption password for this data store.
7. Click **Next**.
8. The **Email and Alerts** dialog opens.

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




9. 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 semi-colons ";" to separate multiple recipients).

**Options**

Specifies the encryption method to use for the communication channel.

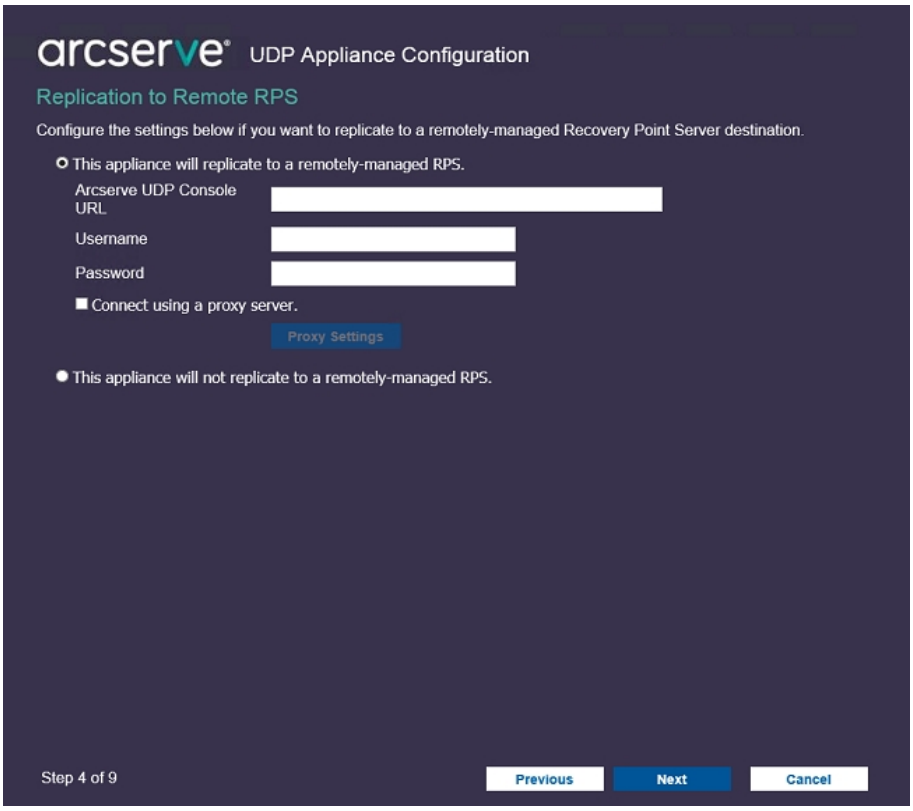
**Connect using a proxy Server**

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.

10. Click **Next**.
11. The **Replication to Remote RPS** dialog opens.



12. 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 the Arcserve UDP Solutions Guide*.

    **Arcserve UDP Console URL**

    Specifies the URL of the remote Arcserve UDP console.

    **Username and Password**

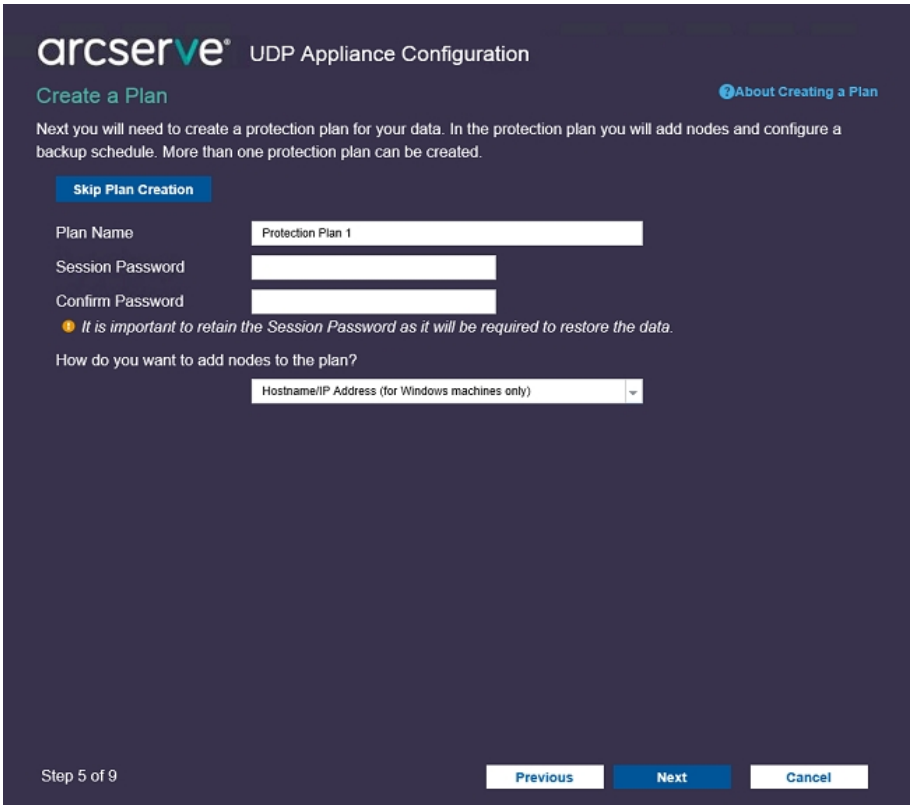
    Specifies the username and password to connect to the remote console.

    **Connect using a proxy Server**

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

13. 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.
14. Click **Next**.
15. The **Create a Plan** dialog opens.

    Using this dialog, you can create a basic plan where you specify the nodes that you want to protect and the backup schedule.



**Note:** If you do not want to create basic plans using the wizard, click **Skip Plan Creation**. This will open the last dialog, the **Next Steps** dialog. Click **Finish** to open the UDP console and create plans.

16. 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 as it is required when you restore data. Make sure that you do not lose the password.

**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

  Use this method to manually add the nodes by specifying the node hostname or IP address. You can add as many nodes as you want.

- Discovering Nodes from Active Directory

  Use this method to add nodes that are in an active directory, you can first discover the nodes by providing the active directory details and then adding the nodes.

- Importing from a vCenter/ESX Server

  Use this method to import virtual machine nodes from ESX or vCenter Servers. This option lists all the virtual machines that are discovered on the hostname or IP address you specify here.

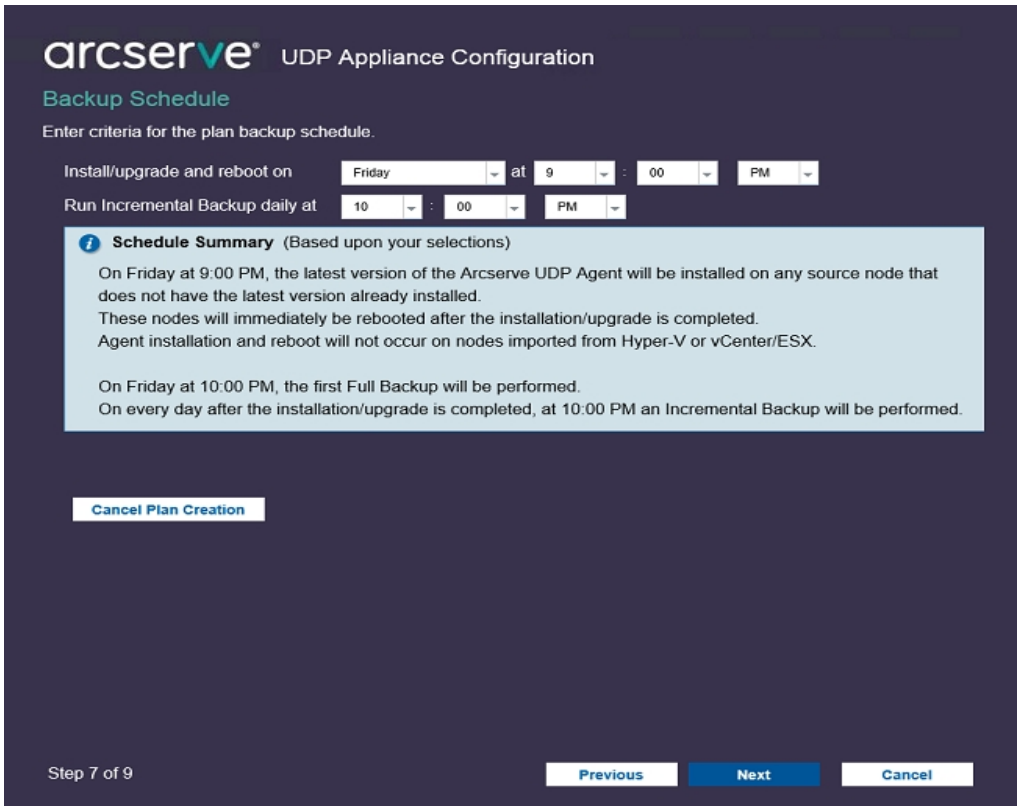
- Importing from a Hyper-V Server

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

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

17. After the nodes are added to your plan and click **Next**.

The **Backup Schedule** dialog opens.




18. Enter the following schedule:

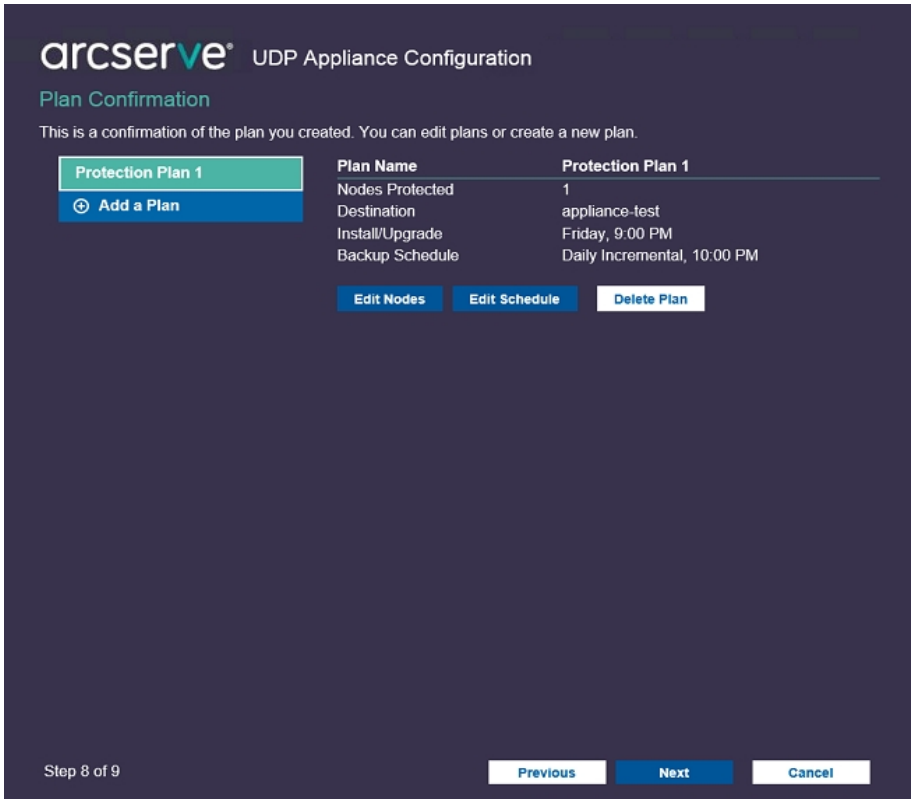
- **Arcserve UDP agent install or upgrade schedule:** The latest version of the Arcserve UDP agent is installed on source nodes that do not have the agent installed. Any previous agent installations is upgraded to the latest version.
- **Incremental backup schedule:** A full backup is performed for the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

  **Note:** If you specify the backup time earlier than the install/upgrade time, 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**.

19. Click **Next**.

    The **Plan Confirmation** dialog opens.




20. From here you can 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.

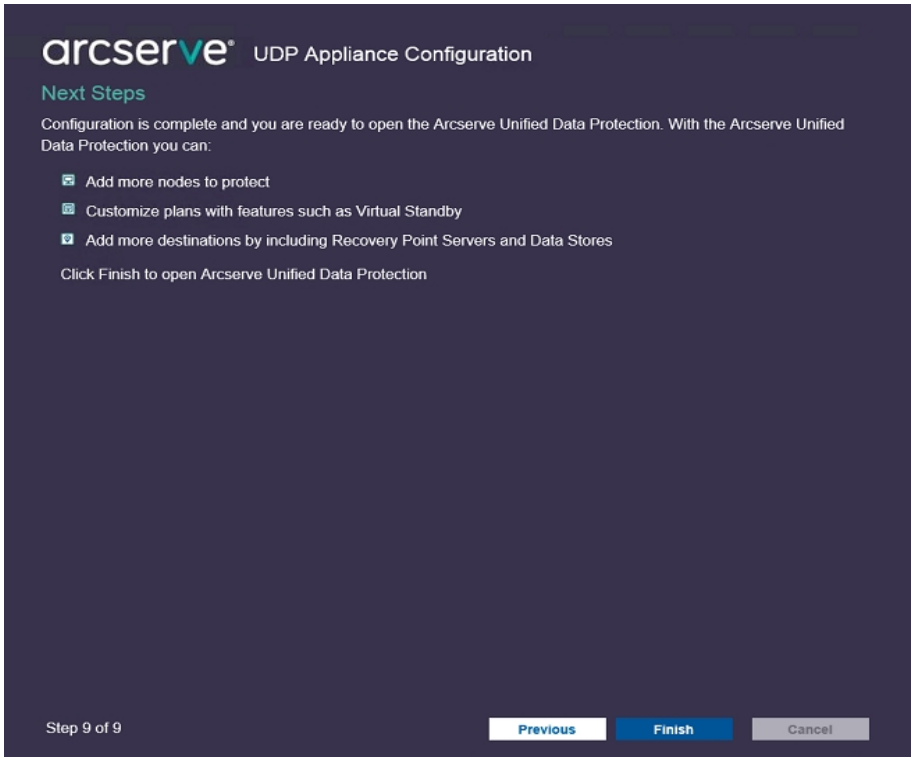
    **Edit Schedule**

    Modifies the backup schedule.

21. After you are satisfied that the plans are correct, 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.




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

# Additional Information on Adding 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 UDP Appliance wizard. The wizard lets you add nodes using the following methods:

- Manually entering the node IP Address or hostname

  (Add Nodes by Hostname/IP Address)
- Discovering nodes from an active directory

  (Add Nodes by Active Directory)
- Importing virtual machine nodes from VMware ESX/vCenter Servers

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

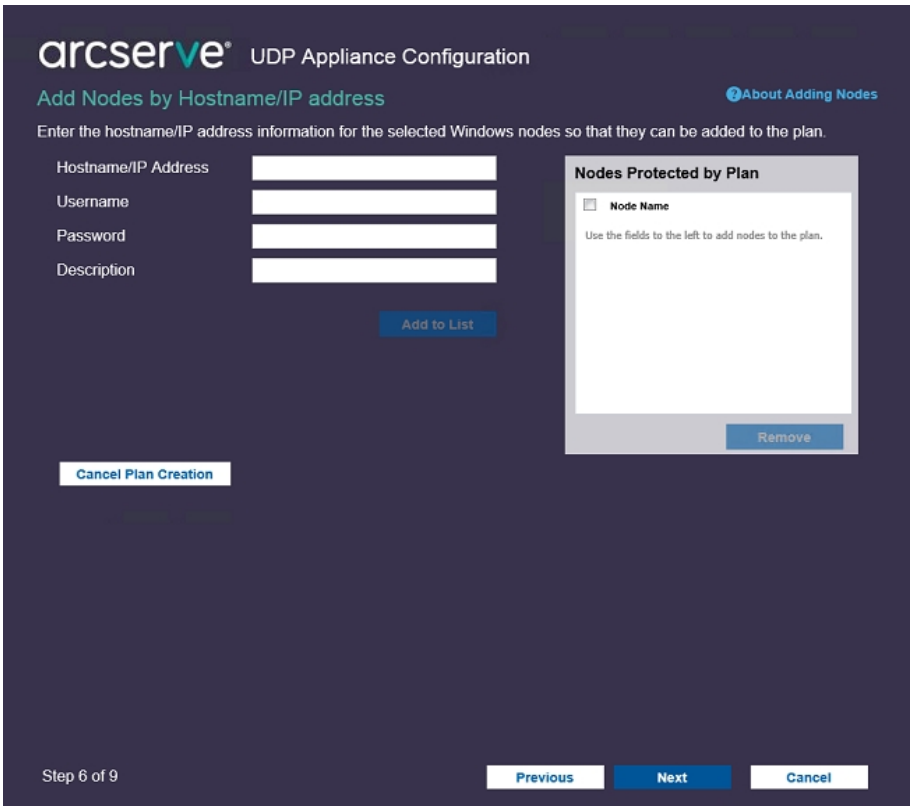
  (Add Hyper-V Nodes)

# Add Nodes by Hostname/IP Address

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

**Follow these steps:**

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




**Hostname/IP Address**

Specifies the hostname or IP address of the source node.

**User name**

Specifies the user name of the node having administrator privileges.

**Password**

Specifies the user password.

**Description**

Specifies any description to identify the node.

**Cancel Plan Creation**

Cancels the plan that you just created.

2. Click **Add to List**.

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

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

4. Click **Next**.

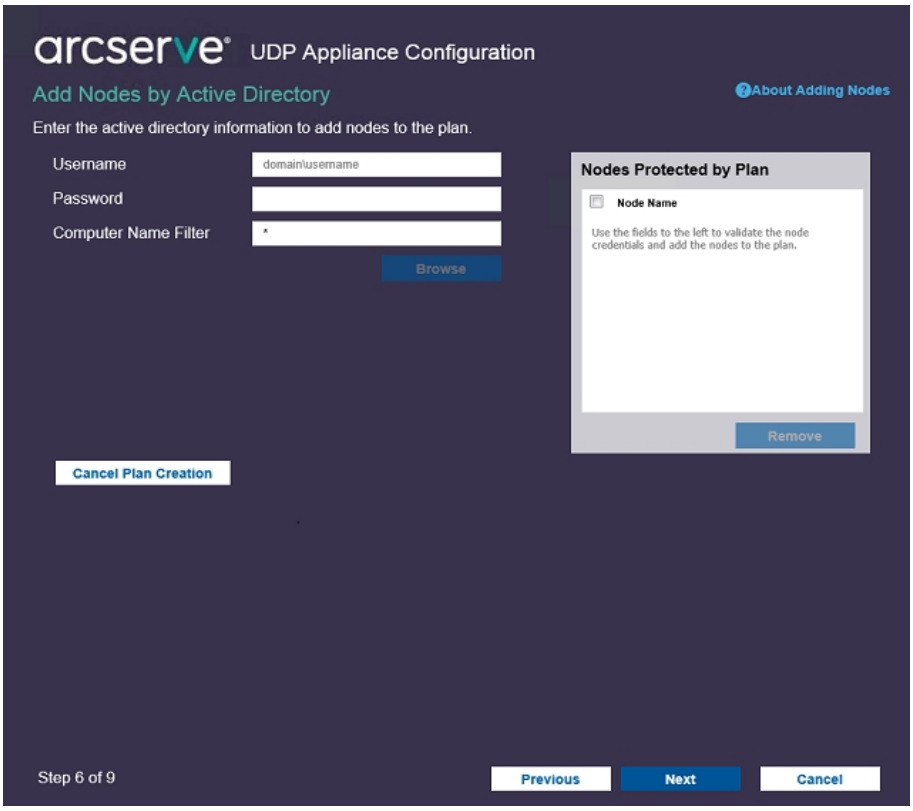
   The nodes are added to the plan.

# Add Nodes by Active Directory

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

**Follow these steps:**

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




**Username**

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

**Password**

Specifies the user password.

**Computer Name Filter**

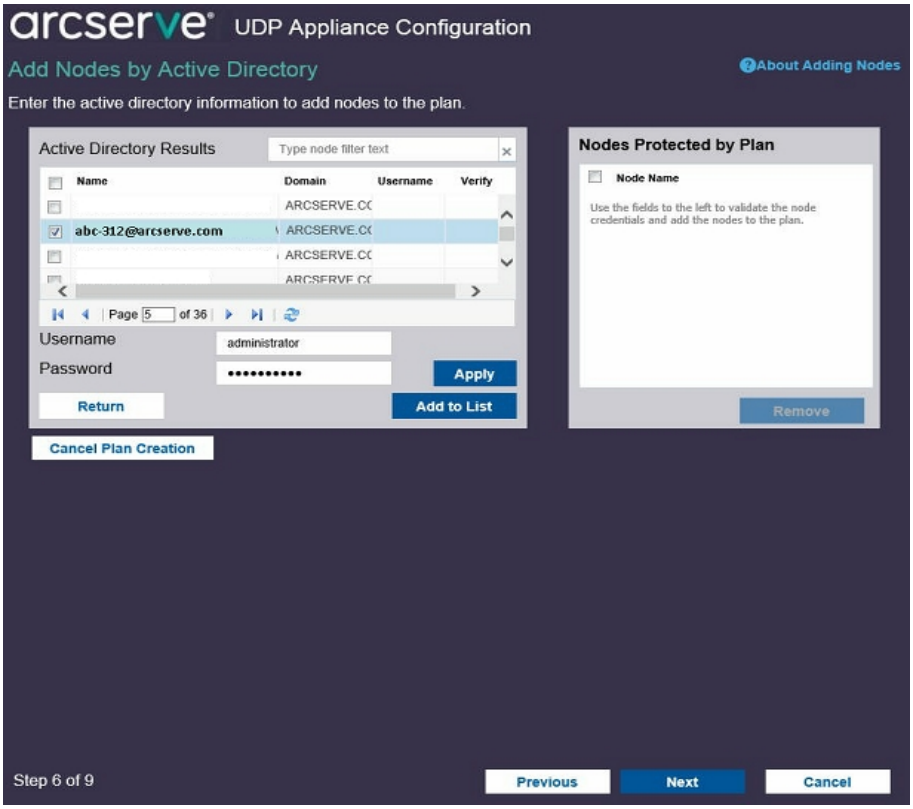
Specifies the filter to discover node names.

**Cancel Plan Creation**

Cancels the plan that you just created.

2. Click **Browse**.

The discovered nodes are displayed.




To add nodes, select the nodes and verify.

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

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

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

4. Click **Add to List**.

   The selected node is added to the right pane.

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

6. Click **Next**.

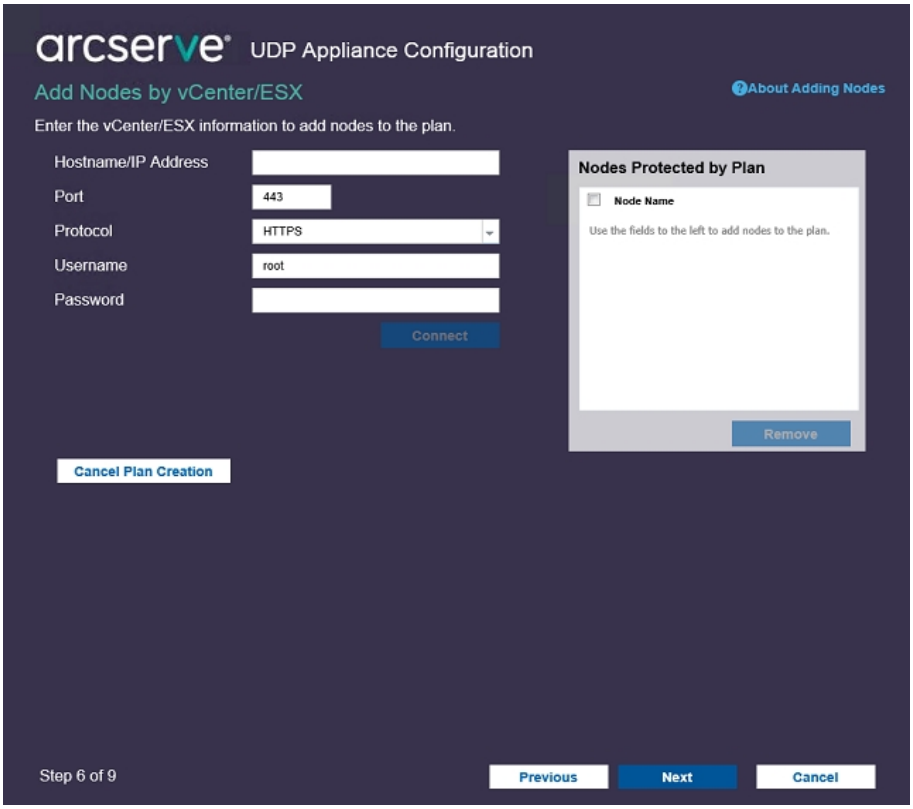
   The nodes are added to the plan.

# Add vCenter/ESX Nodes

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

**Follow these steps:**

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




**Hostname/IP Address**

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

**Port**

Specifies the port number to be used.

**Protocol**

Specifies the protocol to be used.

**Username**

Specifies a user name of the Server.

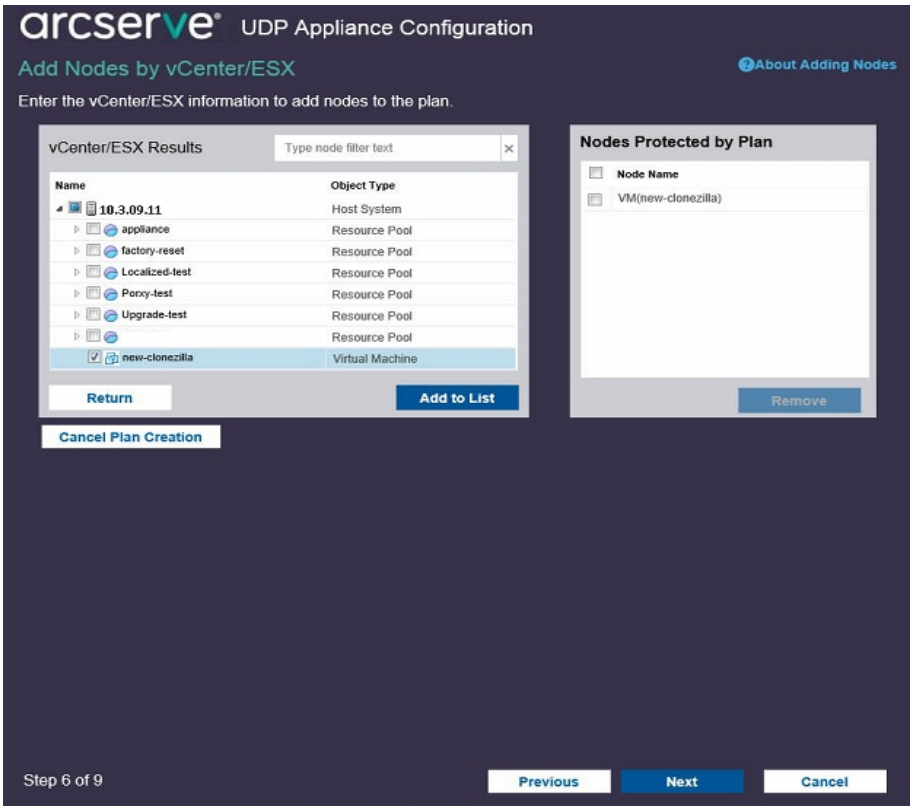
**Password**

Specifies the user password.

**Cancel Plan Creation**

Cancels the plan that you just created.

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




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

   The selected nodes are added to the right pane.

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

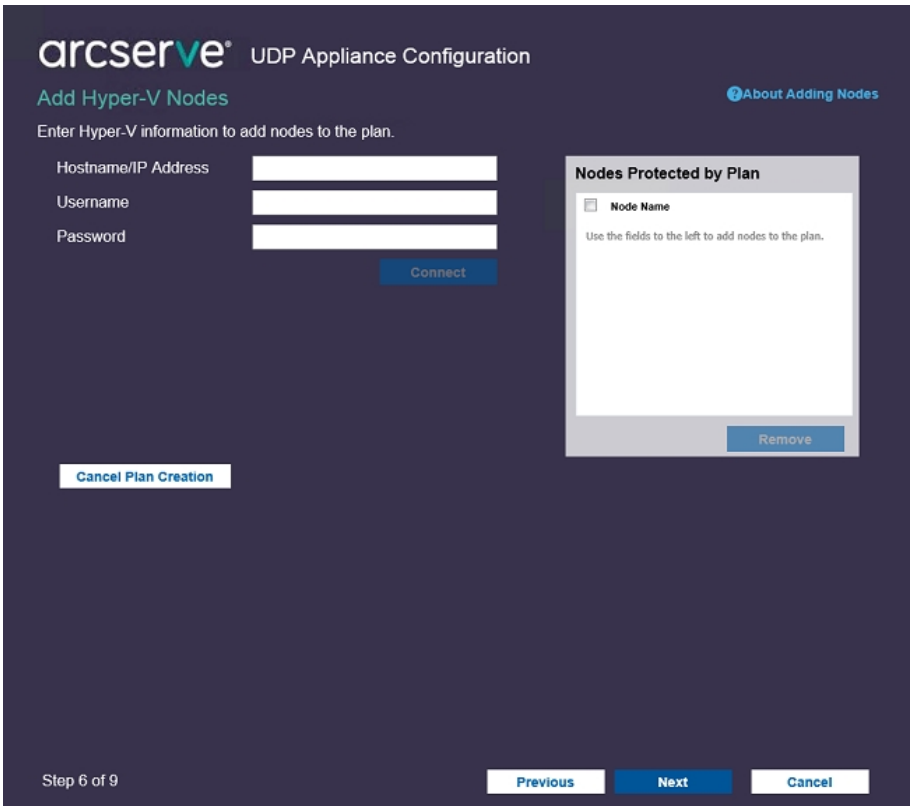
   The nodes are added to the plan.

# Add Hyper-V Nodes

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

**Follow these steps:**

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




**Hostname/IP Address**

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

**Username**

Specifies Hyper-V user name having the administrator rights.

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

**Password**

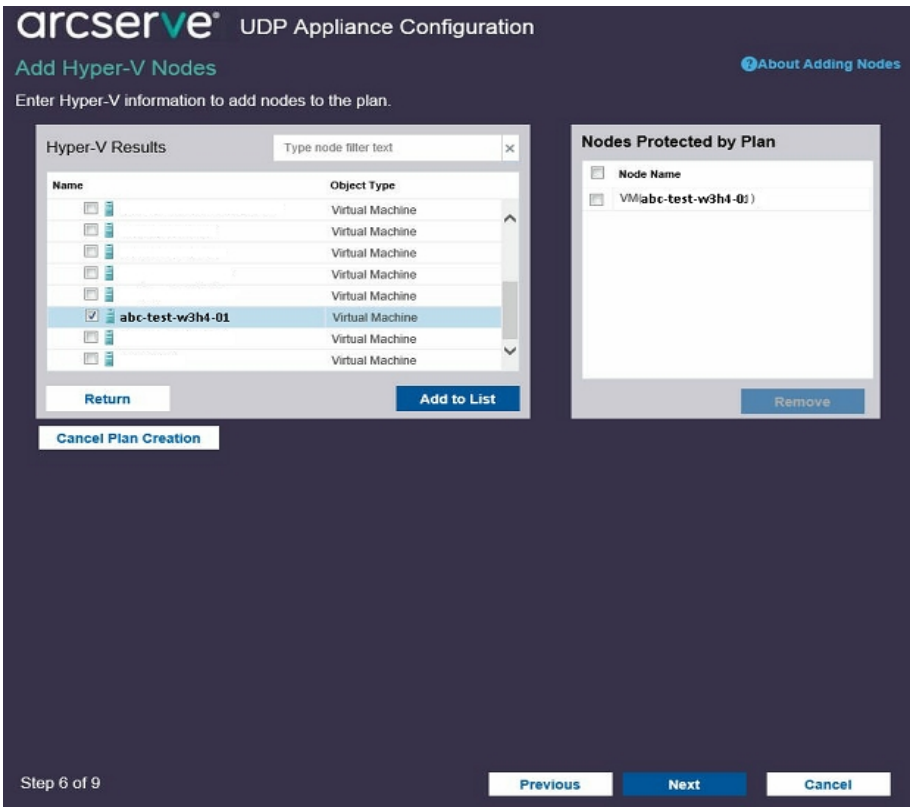
Specifies the password of user name.

**Cancel Plan Creation**

Cancels the plan that you just created.

2. Click **Connect**.

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




3. (Optional) You can type the node name in the filter field to locate the node in the tree.
4. Select the nodes, and then click **Add to List**.

   The selected nodes are added to the right pane.

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

   The nodes are added to the plan.

# Configure UDP Appliance as Gateway

You can configure the Arcserve UDP Appliance as Gateway.

**Follow these steps:**

1. Uninstall Arcserve UDP Console from the Arcserve UDP 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 UDP Appliance.

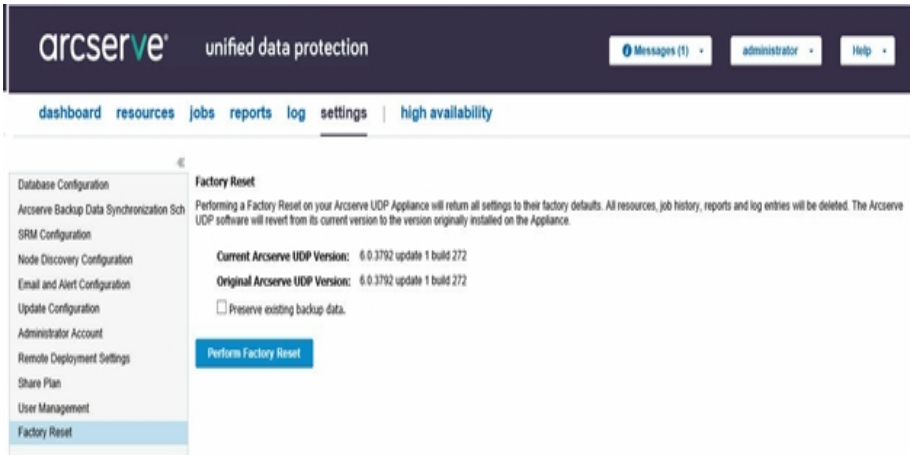
   **Note:** After installing Arcserve UDP Remote Management Gateway on the Arcserve UDP Appliance, click **Launch Wizard** on the Arcserve UDP Appliance wizard does not launch the Arcserve UDP Console. To access the Arcserve UDP Console, provide the URL of Arcserve UDP Console directly.

# Clear Configuration and Apply Appliance Factory Reset

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

**Follow these steps:**

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




   All the backed up data is preserved by default.

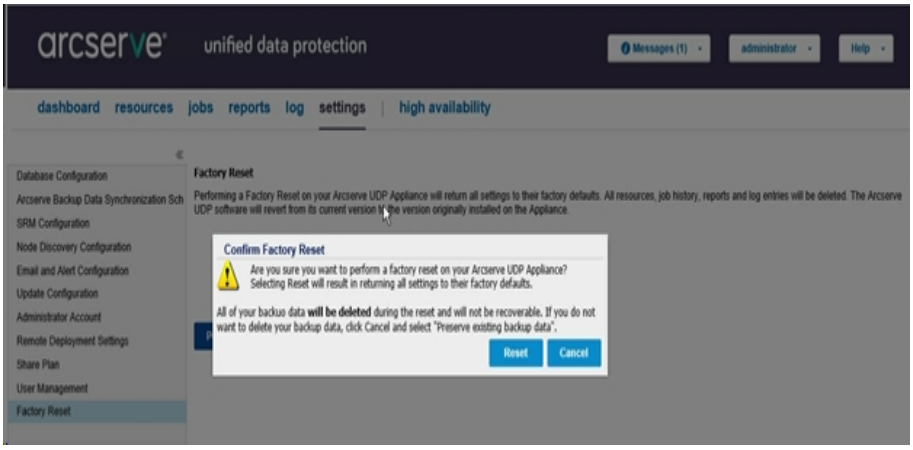
   **Notes:**

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

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

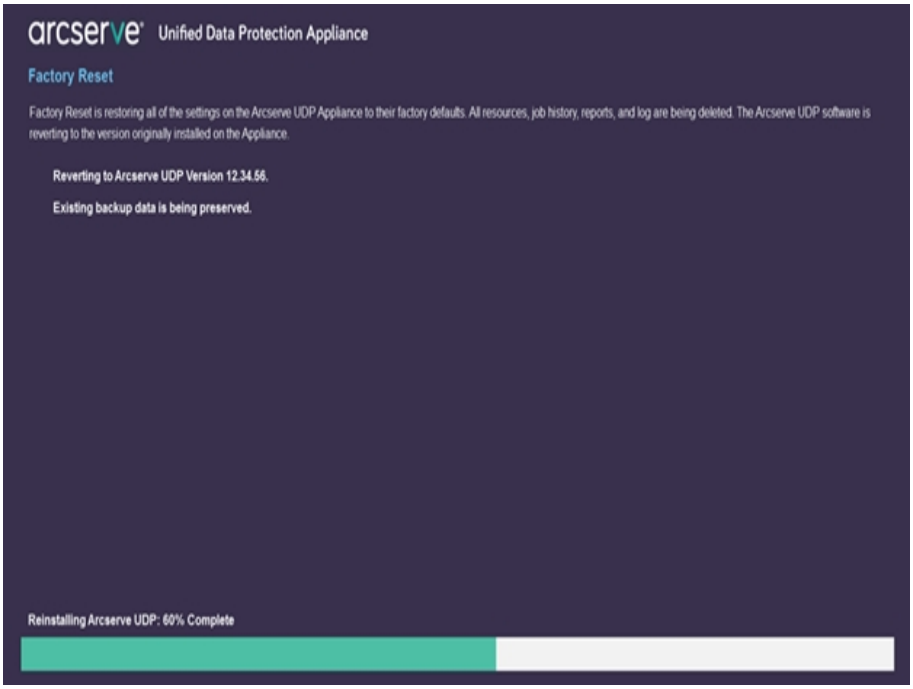
2. Click **Perform Factory Reset**.

   A confirmation dialog is displayed.



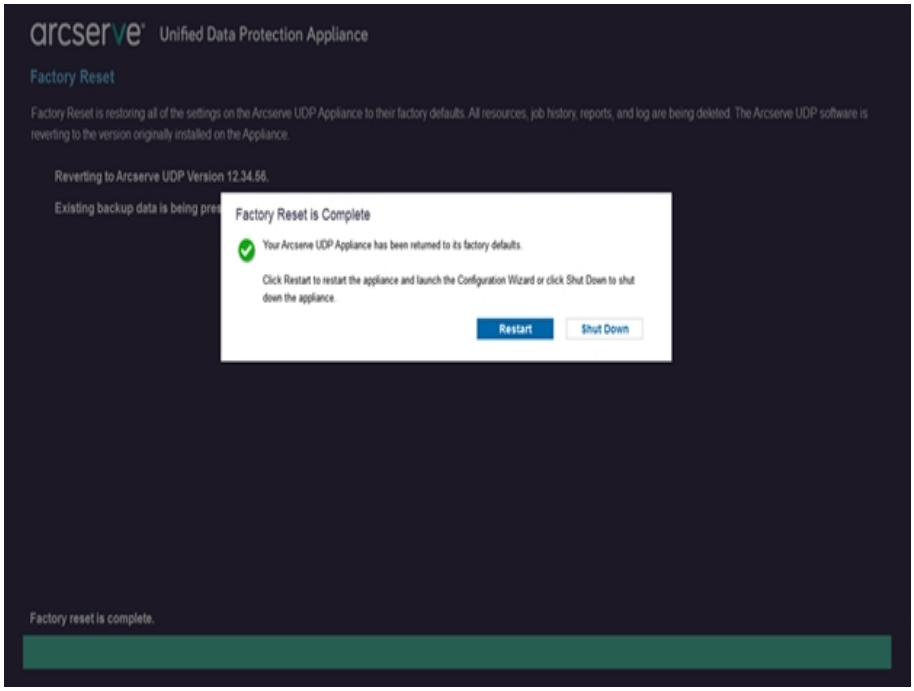

3. From the confirmation dialog, click **Reset** to launch the factory reset.

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




   Completion of factory reset displays a confirmation dialog.

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




# Apply Arcserve UDP Factory Reset Using Boot Option

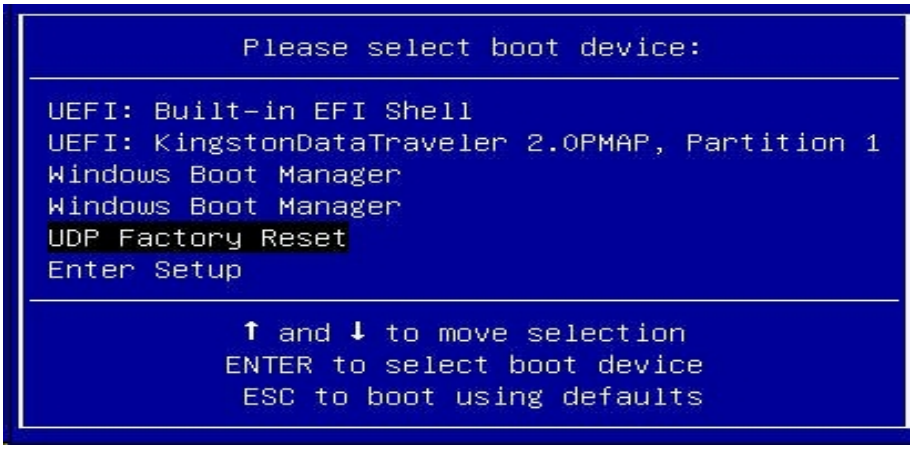
You can also apply UDP factory reset from the Boot Menu of the UDP Appliance. Using UDP factory reset, you can return your Arcserve UDP Appliance to clean and non-configured status.

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

**Follow these steps:**

1. Press F11 to invoke Boot Menu.


2. Select the boot option UDP Factory Reset.



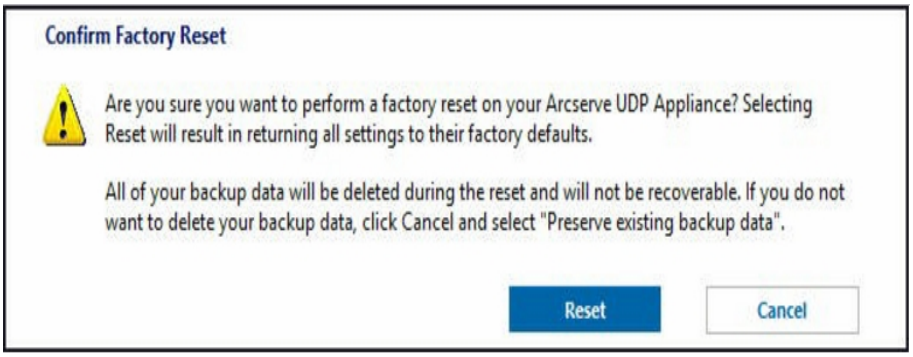

A page about factory reset is displayed.


**Notes:**

- The **Preserve existing backup data** option is selected by default. Only C:\ volume in the original operating system is rebuilt. Data at X:\ volume and Y:\ volume 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.

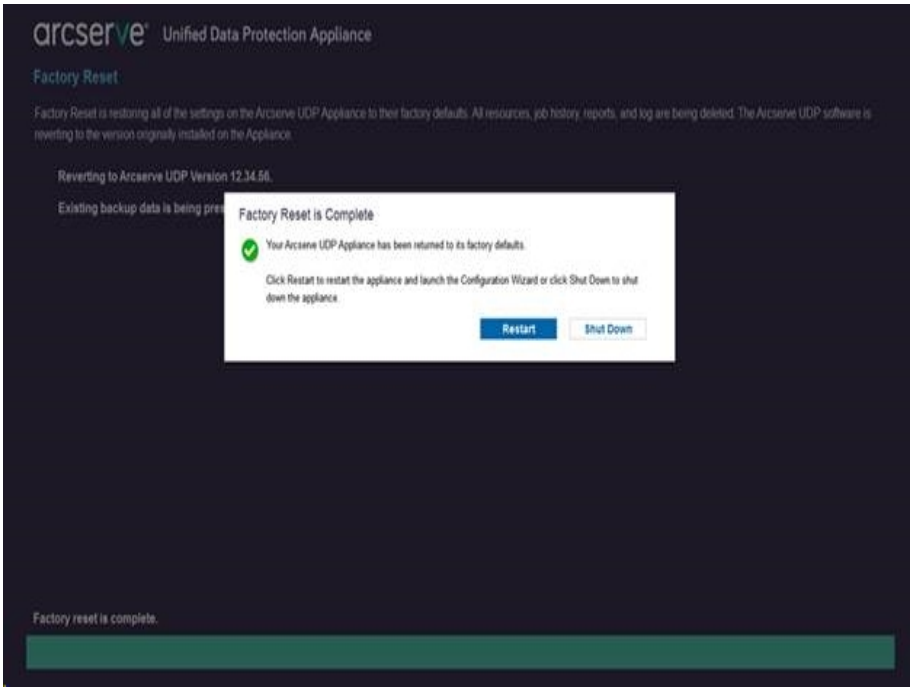
3. Click Reset.

A confirmation dialog appears.




You can click **Cancel** to reboot the 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.



# How to Activate Arcserve Product on the Appliance

For activating Arcserve product on the Appliance, refer to Activating Arcserve Product License Online topic in Solutions Guide.

# Chapter 7: Creating Backup Plans

Using UDP 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:

# Create a Backup Plan for Linux Nodes

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

**Follow these steps:**

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

   **Note:** For more information about each of the configurations, see How to Create a Linux Backup Plan in the Solutions Guide.
5. Run the backup plan.

# Create a Backup Plan to a Tape Device

UDP 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 UDP Appliance:

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

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

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

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

   **Note:** For more information on configuring and managing the device, see Managing Devices and Media in Arcserve Backup for Windows 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. Here the source data is the destination of UDP backup plan and the destination is the tape device.

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

# Create an On-Appliance Virtual Standby Plan

Appliance has the capability to serve as a virtual standby machine. This capability is present in the following Appliance series:

- Arcserve UDP Appliance 7200V
- Arcserve UDP Appliance 7300V
- Arcserve UDP Appliance 7400V
- Arcserve UDP Appliance 7500V
- Arcserve UDP Appliance 7600V
- Arcserve UDP Appliance 8100
- Arcserve UDP Appliance 8200
- Arcserve UDP Appliance 8300
- Arcserve UDP Appliance 8400

**Prerequisite:** You must have a successful backup plan.

**Follow these steps:**

1. Open the Appliance Console.
2. Navigate to the plans and modify the backup plan.
3. Add a Virtual Standby task.
4. Update the Source, Destination, Virtual Machine configurations.

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

5. Save and run the plan.

# Chapter 8: Repairing the Arcserve UDP Appliance

This section contains the following topics:

# Remove and Replace a Hard Drive

With the Arcserve UDP 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.

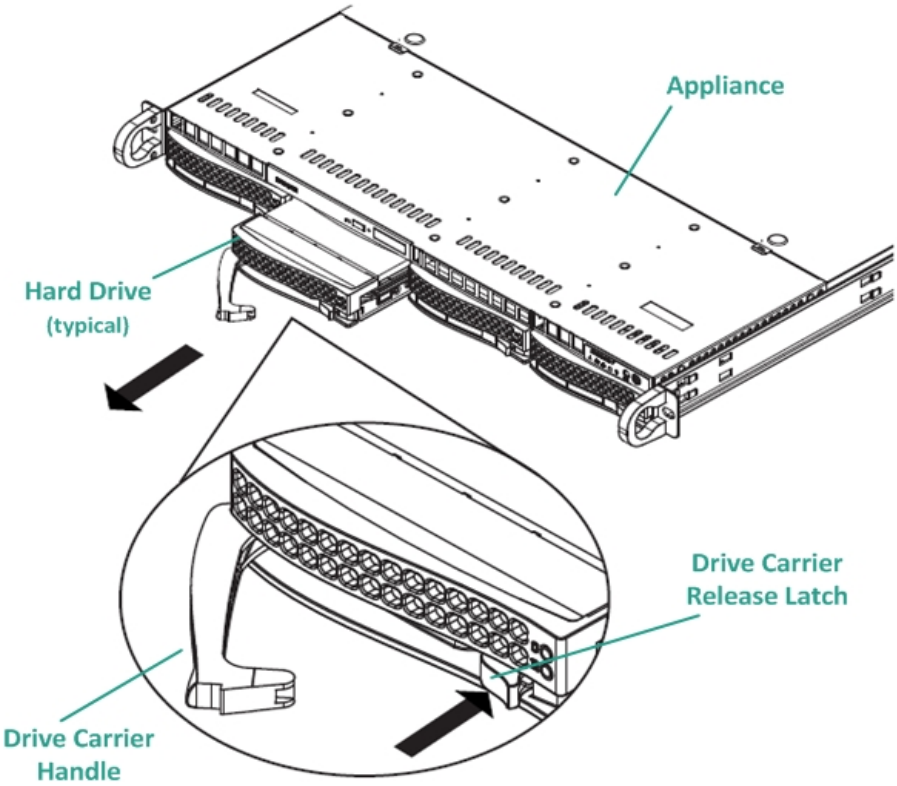
The Arcserve UDP appliance contains four hard drive carriers which are labeled 0, 1, 2 and 3 from left to right. If you replace more than one hard drive at a time, you should label the replacement hard drives so that you know which drive is placed into each drive carrier. You should also label the hard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

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

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

**Follow these steps:**

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

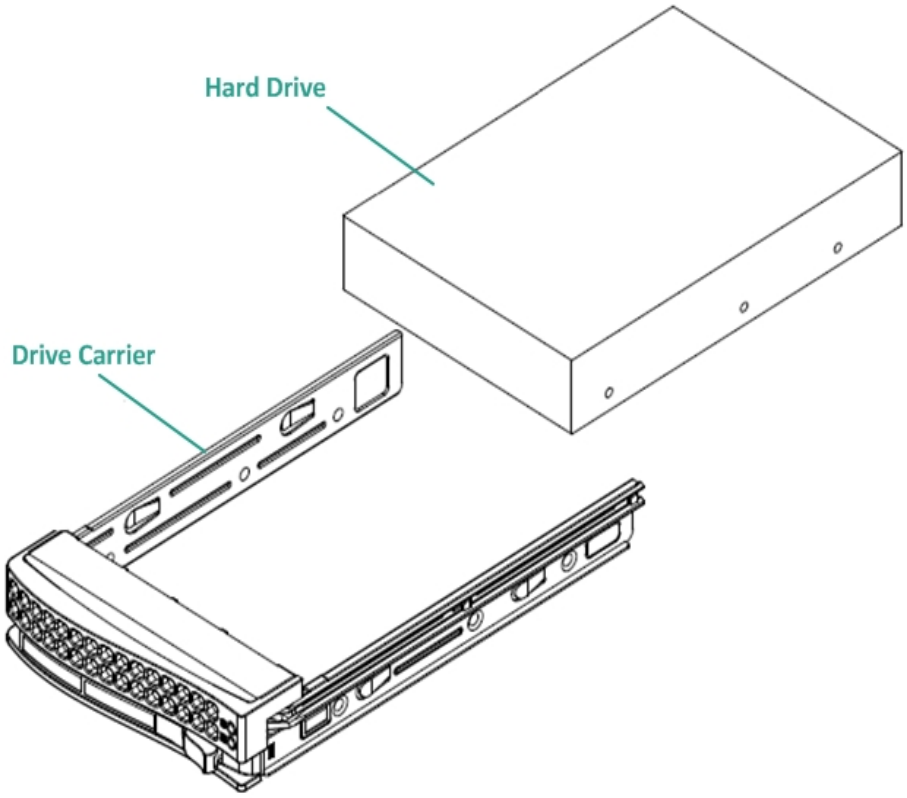



3. Using the handle, pull the drive carrier out from the front of the appliance. The hard drives are mounted in drive carriers to simplify their removal and replacement from the appliance. These carriers also help promote proper air-flow for the drive bays.

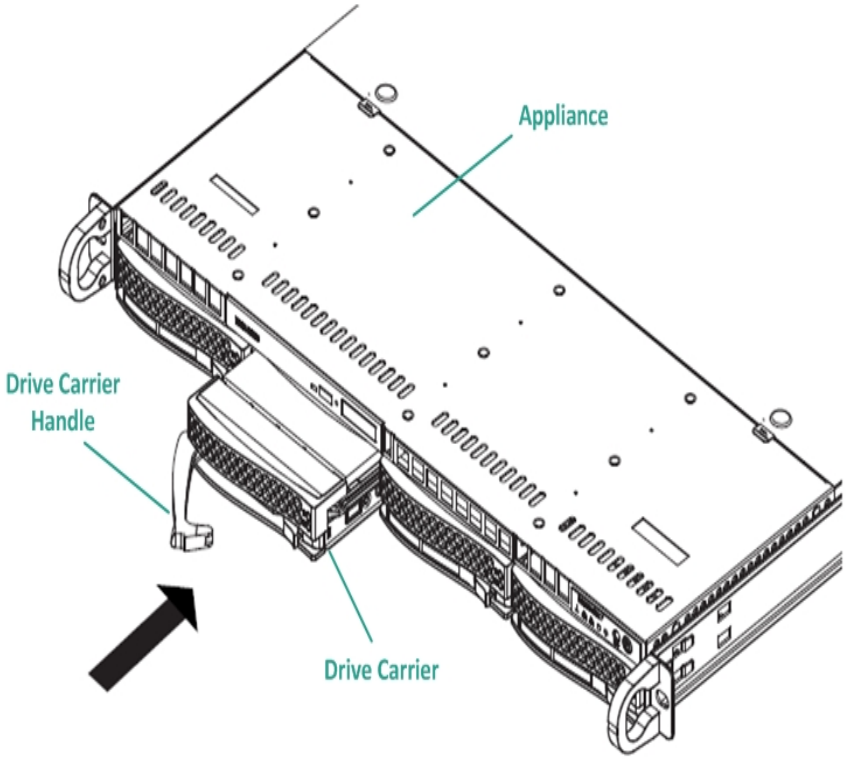
   **Important!** Except for short periods of time (swapping of the hard drives), do not operate the appliance without the drive carriers fully installed.

4. Remove the old hard drive from the drive carrier and install the new hard drive being careful to properly orient the replacement hard drive with the

label on top and the visible components on the bottom.




5. Slide the drive tray into the appliance until it is fully installed and secure by closing the drive carrier handle.




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

# Chapter 9: Safety Precautions

This section contains the following topics:

# General Safety Precautions

The following are general safety precautions you should adhere to in order to protect yourself from harm and to protect the appliance from damage or malfunction:

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

  A급기기(업무용방송통신기자재)

  이기기는업무용(A급)으로전자파적합기기로서판매자또는사용자는이점을주의하시기바라며,가정외의지역에서사용하는것을목적으로합니다

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

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

- 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

The following are electrical safety precautions you should adhere to in order to protect yourself from harm 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 10: Changing the IPMI Password

This section contains the following topics:

# How to Change the IPMI Password

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

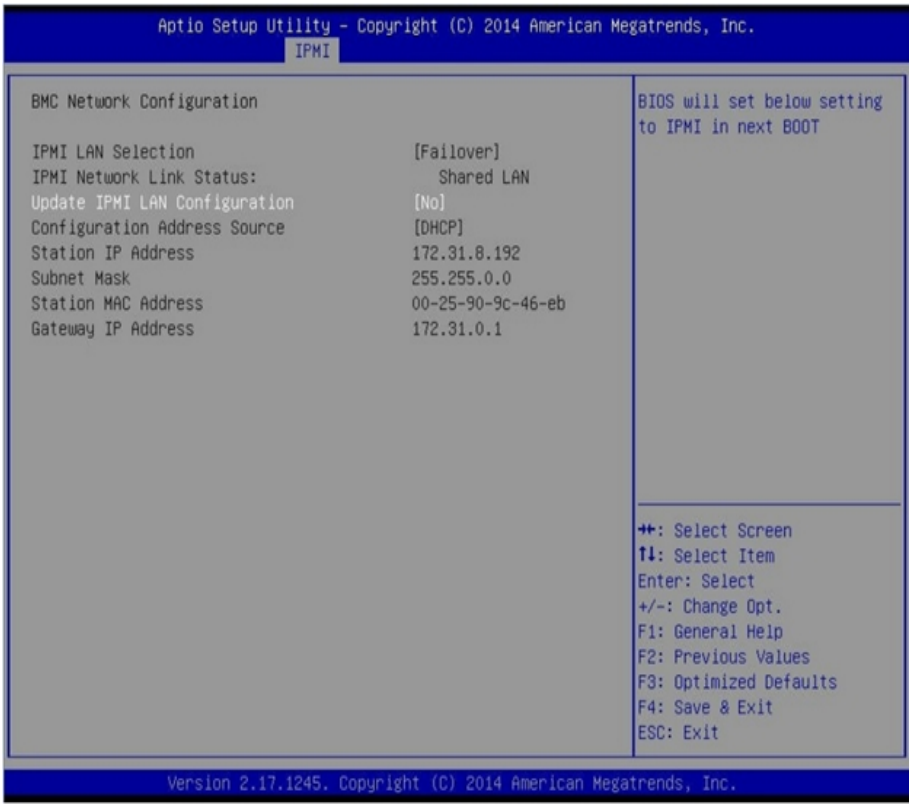
**Follow these steps:**

1. Boot up your system and a bootup screen appears. From this screen, 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.

2. Select the IPMI tab at the top of the main BIOS screen.

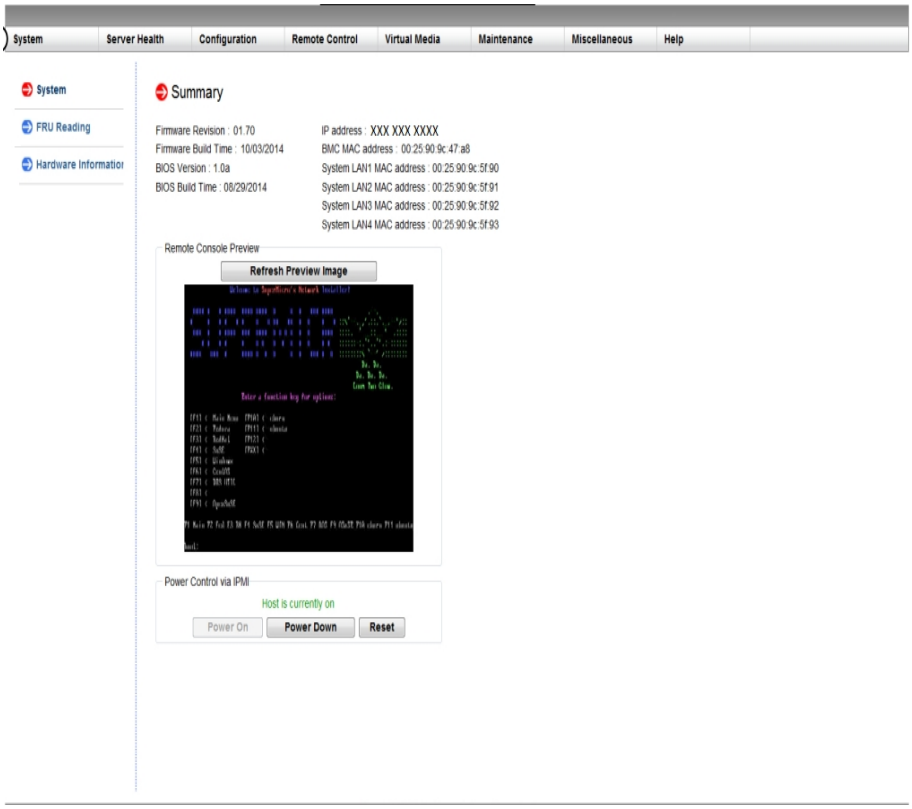
   **Note**: By default, the configuration address source is set to DHCP.



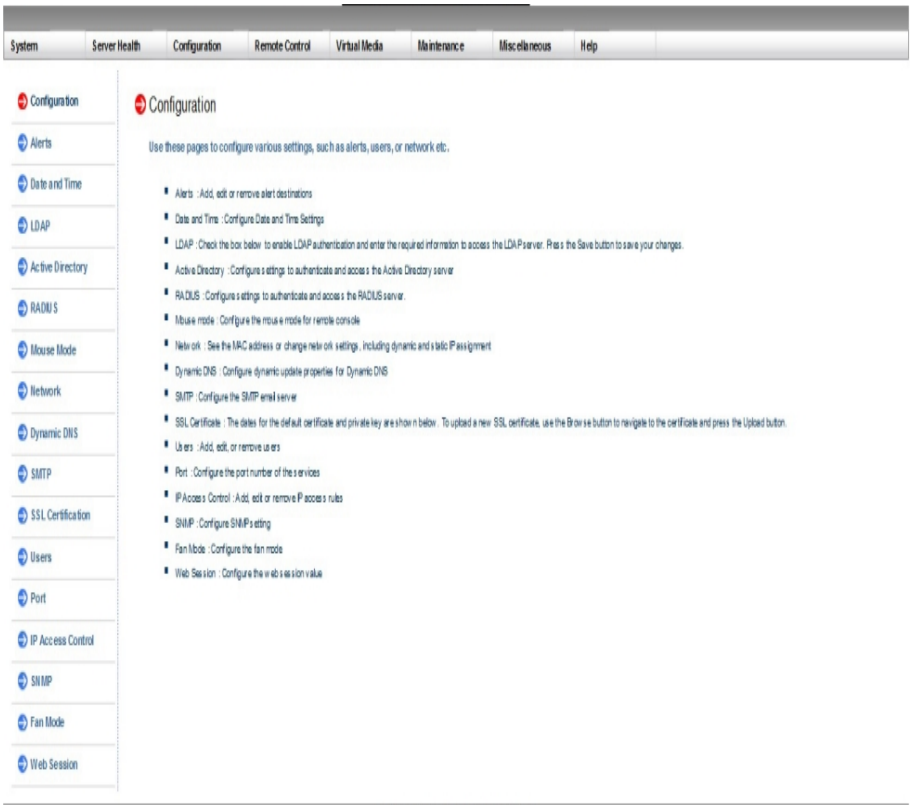

3. Verify that the IP address is correct. You can connect to the IPMI interface using your web browser only if your Server is on the same network.
4. Record the Station IP Address.
5. Enter the Station IP address on your web browser.

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


6. Enter your user name in the Username field. (ADMIN by default)
7. Enter your password in the Password field. (ARCADMIN by default)
8. The home page is displayed (IPMI main screen).

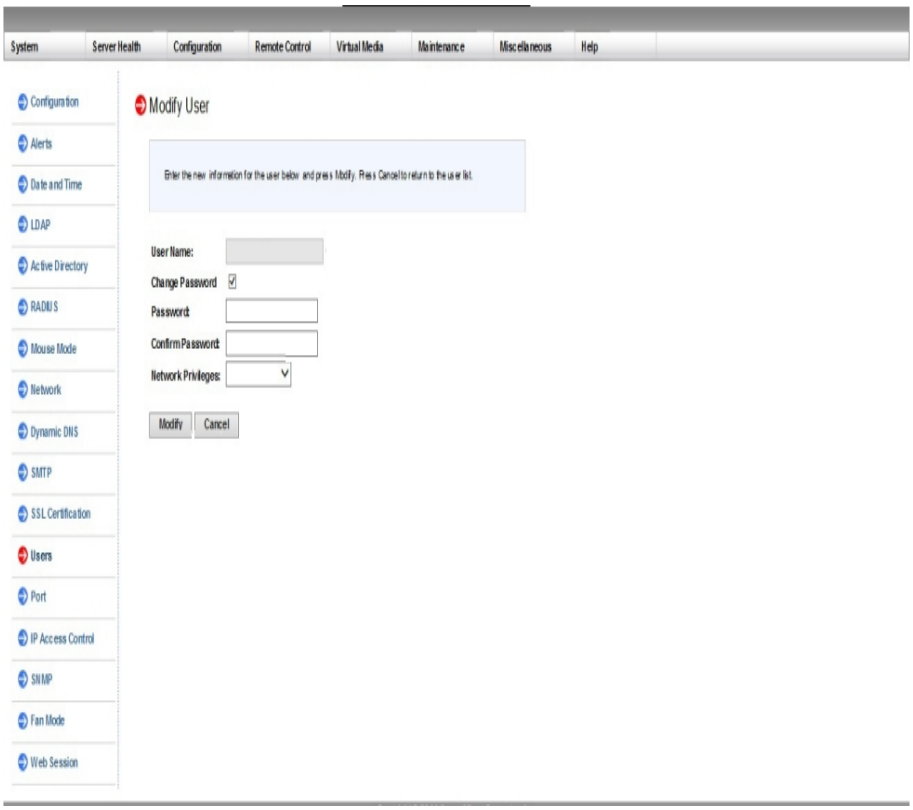



9. Click the Configuration option from the top bar. The Configuration screen is displayed.




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

12. Click Modify User and the Modify User screen is displayed.




13. Enter your user name. (ADMIN)
14. Select the Change Password check box to change the password. The password fields is enabled.
15. Enter the new password and confirm.
16. Click Modify to save the changes. Your IPMI password has been changed.

# Chapter 11: Connecting Appliance Expansion Shelf to the Appliance Server

This section contains the following topics:

# Appliance Infield Expansion for all the Available Models

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | slots are filled with add-on Cards, then you need to free at least one slot , preferrably slot 3 in order to use Infield Expansion.<br>5. SAS connection is used between the Appliance and Expansion shelf.<br>6. 8100 - Expansion shelf comes with RAID-6.<br>7. Expansion Shelf comes with Dual PSU.<br>8. Follow **Add data path instructions** given in Expansion guide after connecting the expansion |

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | mandatory for Appliance Infield Expansion / MegaRAID SAS 9380-8e.<br>4. If both the optional slots are filled with add-on Cards, then you need to free at least one slot, preferrably slot 3 in order to use Infield Expansion.<br>5. SAS connection is used between the Appliance and Expansion shelf.<br>6. Expansion shelf comes with RAID-6.<br>7. Expansion Shelf comes with Dual PSU |

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | D SAS 9380-8e) | comes with inbuilt and pre-configured SSD 1.9 TB.<br>3. 8300 has 2 , 5, and 6 as optional slots . One free slot is mandatory for Appli-ance Infield Expansion / MegaRAID SAS 9380-8e.<br>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.<br>5. SAS con-nection is used between the Appli-ance and Expansion |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | shelf.<br>6. Expansion shelf comes with RAID-6 (6x4 TB Disks).<br>7. Expansion Shelf comes with Dual PSU.<br>8. Follow **Add data path instructions** given in Expansion guide after connecting the expansion shelf.<br>9. Wherever a new SSD is required follow the **Migrate HASH destination to new SSD** instructions given in Expansion Guide. (Only for Appliance 8300 connect with 40 TB Appli- |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | ance expansion shelf, there is one unattached 2 TB SSD that you need to place in Base appliance and not expansion shelf. Check expansion guide from details). |
| 8400 | 32,40,48,56,64,72,80 | 8<br>( 6x2 TB Disks)<br>OR<br>16 ( 6x4 TB Disks)<br>OR<br>40 ( 12x4 TB Disks) | 1200 | 8 TB - NA<br>16 TB - NA<br>40 TB - NA | 2, 5, 6 | LSI SAS 9200 -8E HBA<br>Qlogic Dual port HBA<br>Quad-Port 1G NIC<br>Dual port 10G SPF+<br>Dual Port 10G Copper<br>Infield Expansion (MegaRAID SAS 9380-8e) | 1. 8400 model supports either 8 TB or 16 TB OR 40 TB Infield Expansion . Client can connect only one expansion shelf any time.<br>2. 8400 - Requires no addtional SSD.<br>3. 8400 has 2 , 5, and 6 as optional slots. One free slot is |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | mandatory for Appliance Infield Expansion / MegaRAID SAS 9380-8e.<br>4. If both the optional slots are filled with add-on Cards, then you need to free at least one slot, preferrably slot 2 in order to use Infield Expansion.<br>5. SAS connection is used between the Appliance and Expansion shelf.<br>6. Expansion shelf comes with RAID-6.<br>7. Expansion Shelf comes with Dual PSU. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | 8. Follow the **Add data path instruc-tions** given in the Expansion guide after connecting the expan-sion shelf. |

# What is included in the box

The following items are contained in the box:

**Note:** If you notice any damage in the items provided in the box, Contact Arcserve.

- 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.

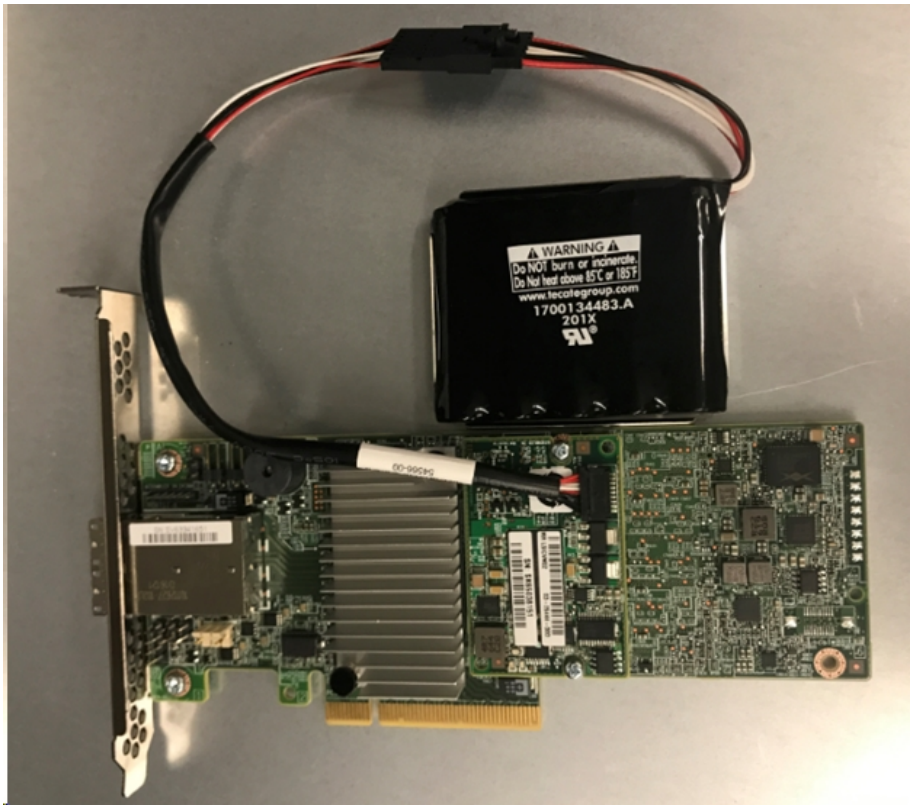

- SSD (optional)

  **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. Verify the Arcserve UDP Console to ensure that there are no running jobs on the Appliance Server and pause all the plans.
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 experiencing electrical shock.
5. Remove the cover of the Appliance Server chassis.

6. Insert the *MegaRAID Controller 9380-8e* into an available PCI-e slot of the Appliance Server.

**Follow these steps:**

a. Locate an empty PCI-e slot.

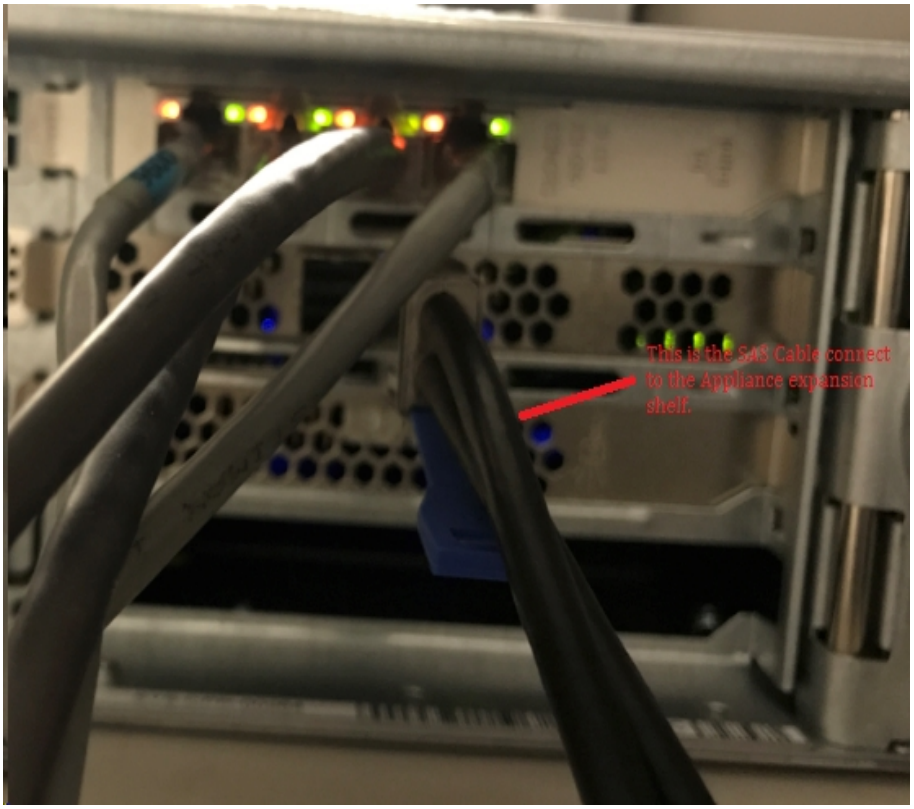
b. Remove the blank bracket panel on the backside of the computer that aligns with the empty PCIe slot.

c. Save this 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.

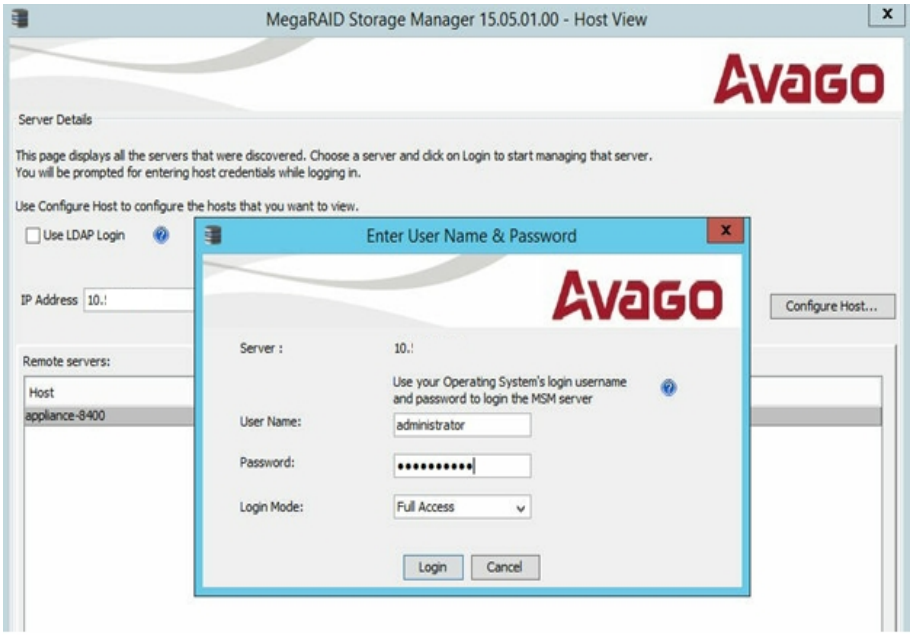
7. Secure the *MegaRAID Controller 9380-8e* bracket to the chassis of the system.
8. Replace the cover of the Appliance Server chassis.
9. Connect the SAS cable between the *MegaRAID Controller 9380-8e* which is in the Appliance Server and the MegaRAID Controller in the Appliance expansion shelf.




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

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

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



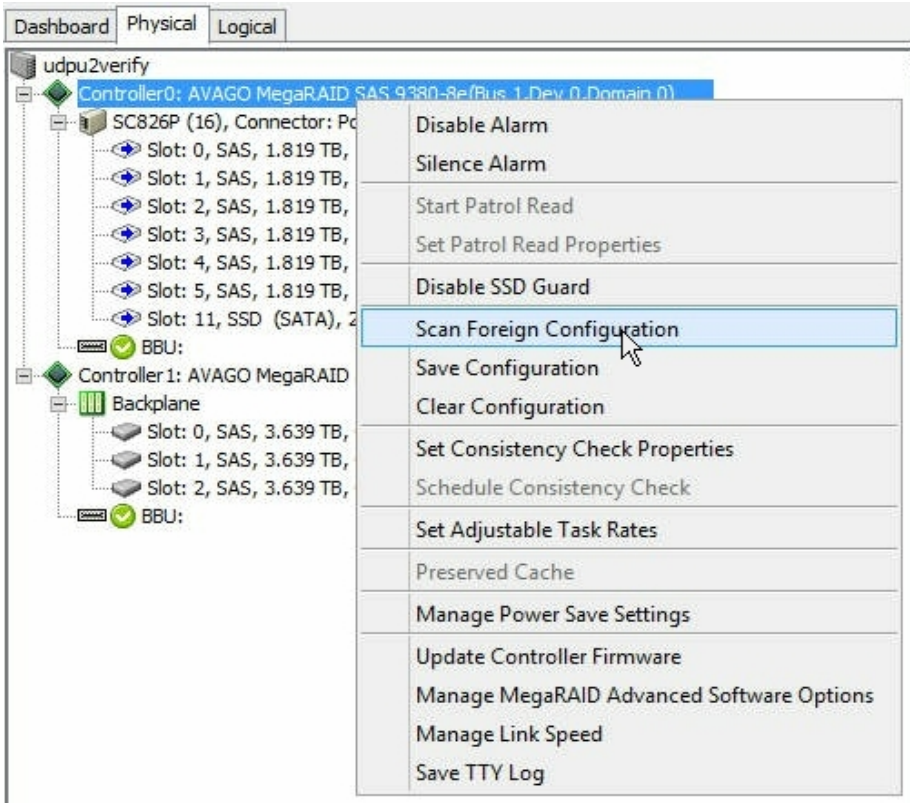

14. Verify the raid controller from MegaRAID Storage Manager.

**Follow these steps:**

a. Browse the Physical or Logical tab and there are two controllers listed there.

b. Select the controller 9380-8e, ensure that all the disks connected to the controller 9380-8e are online and available.

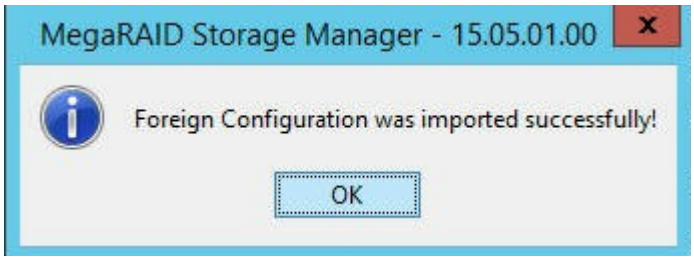
**Note:** If there are any disks that are not online, right click and select *Scan Foreign Configuration*.




Select Import the foreign drives and click OK.


Click Yes to initiate the import process.


Click OK.



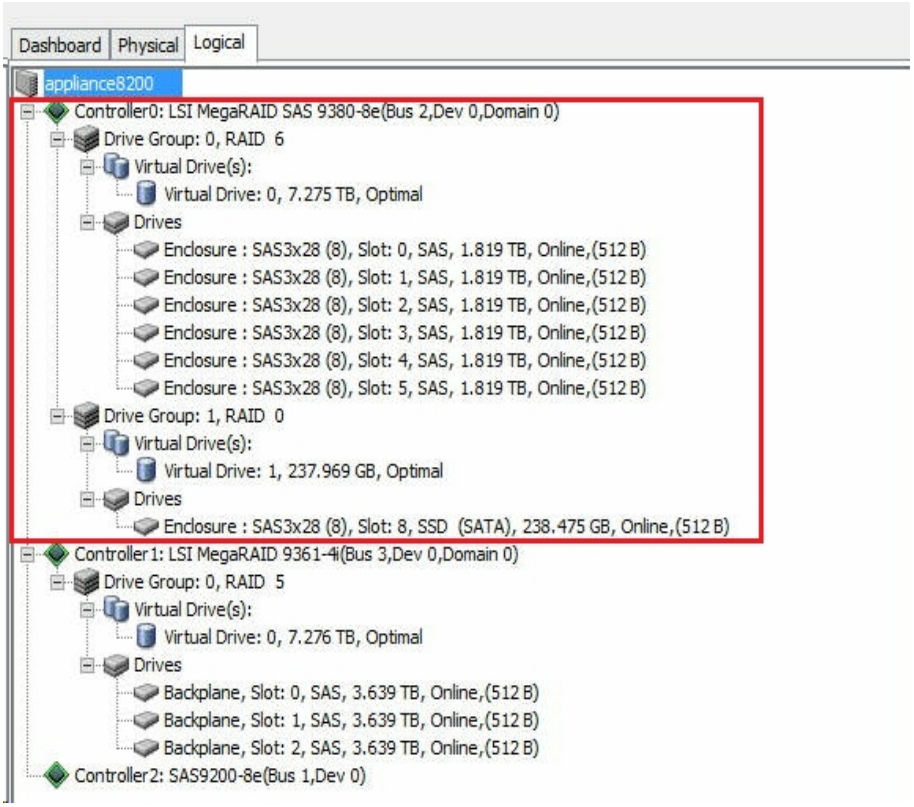

All the disk drives on the expansion shelf are online now.

On the Logical tab, we can see the disks have been configured with RAID-6, and for other modules of the expansion shelf, one SSD is set as RAID-0 and listed under *LSI MegaRAID SAS 9380-8e*.

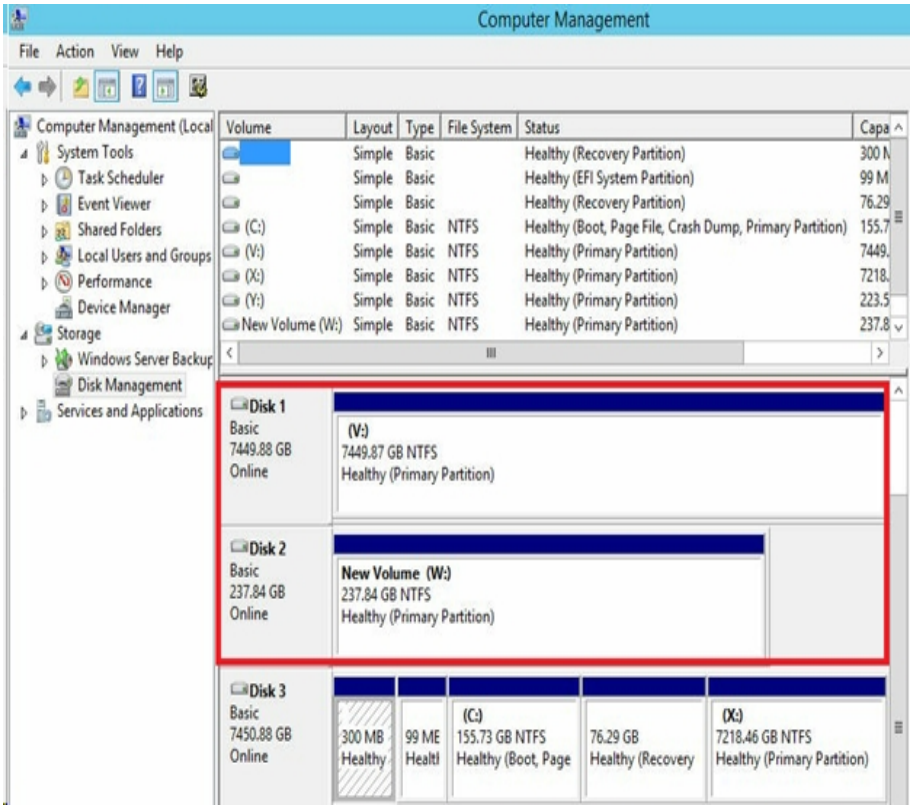
Appliance server 8100 + 8 TB expansion shelf;

Appliance server 8200 + 16 TB expansion shelf;

Appliance server 8300 + 16 TB expansion shelf;




15. Verify the disks from Disk Management. Open Disk Management, if the Appliance Expansion Shelf assembled disk is not formatted, then format it as NTFS and give it a drive letter such as “V:” and if the SSD is not formatted, then format it as NTFS also and give it a drive letter such as “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

**Follow these steps:**

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

*as_gddmgr.exe –DataPath Add <hostname_data_store> -NewDataPath <new data folder>*

*as_gddmgr.exe –DataPath Display <hostname_data_store>*

# Migrating Hash Destination to the new SSD

**Note:** This step is only required 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 *<hostname_data_store>* is stopped. If not, stop the data store *<hostname_data_store>* from the Arcserve UDP Console.
3. Modify the data store *<hostname_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 *<hostname_data_store>* from the Arcserve UDP Console.

# Checking the overall capacity of the <hostname_data_store> data store from the 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 12: Troubleshooting

This section contains the following topics:

# 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 a UDP Appliance from Another Appliance Reports Duplicated Nodes

**Symptom**

When I back up Appliance B from Appliance A, I see the following warning message in the activity log:

*"The following nodes are duplicated: Appliance_B, Appliance_A. As a result, they have the same agent identifier and may cause unexpected results. This duplicate node problem can be caused if the node was added using a different node name (such as the DNS name or IP address), or if some machines were set up by cloning from one to another."*

**Case 1: Appliance B is added as an RPS to the Appliance A UDP Console.**

For example: From Appliance B, you can configure the appliance using the UDP wizard and select "This appliance will function as an instance of Arcserve UDP Recovery Point Server managed by another Arcserve UDP console."

**Solution**

1. Stop the data store in the Appliance B node from the RPS pane of the UDP console.
2. Log into Appliance B and delete the registry key of the Node ID that is located under [HKEY_LOCAL_MACHINE\SOFTWARE\CA\ARCserve Unified Data Protection\Engine].
3. Restart the Arcserve UDP Agent Web Service from the Appliance B node.
4. Restart the Arcserve UDP RPS Data Store Service from the Appliance B node.
5. From the UDP console, go to the Nodes, All Nodes pane and update the Appliance B node.
6. Go to the Recovery Point Server pane and update the Appliance B node.
7. Import the existing data store to the Appliance B RPS by setting it with the original backup destination.

**Case 2: Appliance B is added only as an agent node to the Appliance A UDP Console.**

For example, a plan protects Appliance B through an agent-based backup task on the Appliance A UDP console.

1. Log into Appliance B and delete the registry key of the Node ID that is located under [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve Unified Data

Protection\Engine].

2. Restart the Arcserve UDP Agent service from Appliance B.
3. From the UDP console, go to the Nodes, All Nodes pane and update the node from Appliance B.

# Linux Backup Server Cannot 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 you set the static IP address to the appliance Server which 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**

To resolve this issue, go to the **Arcserve Backup Appliance Wizard** and click **Edit**, **Date and Time** to change the time zone.

# Licenses Error even when the licenses are available

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

# Chapter 13: Best Practices

This section contains the following topics:

# Best Practices for Network Configuration

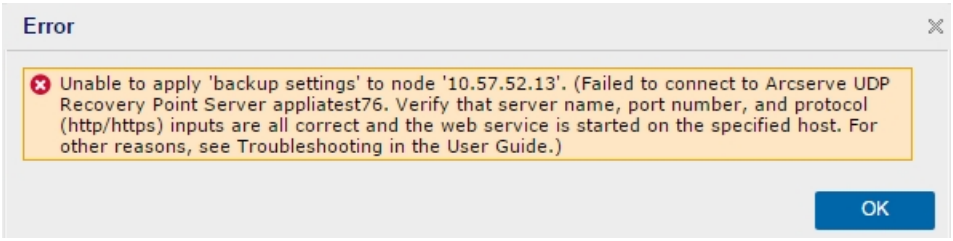
- If multiple network interfaces are connected in the production environment, ensure that each network adapter is connected to different sub network.
- If Linux node is not available in the production environment to protect, we recommend to stop the VM Linux-BackupSvr, DHCP Server service and RRAS on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

  For more information, refer How to Disable DHCP Server in Appliance User Guide.
- If you encounter a connection problem between the Appliance and an Agent node when both the Appliance and the Agent node are online on the network. The problem occurs if there are multiple network interfaces connected to the same sub network in the Appliance.

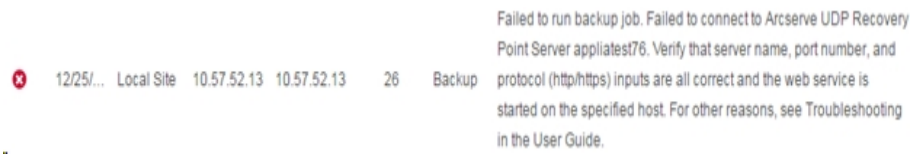
  **Symptom**

  If both the Appliance and Agent node are online on the same sub network. The following symptoms may occur:

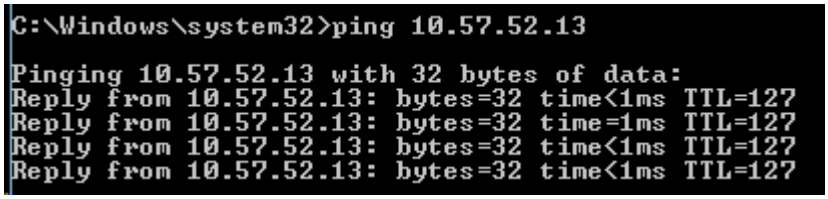
  - On the Arcserve UDP Console, when you deploy the plan to Agent node, the following error message is displayed:

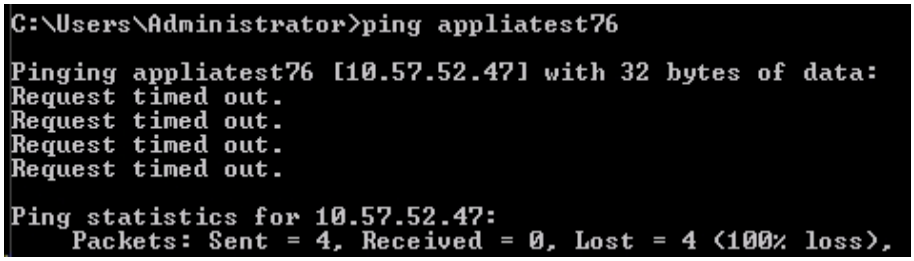
  - Backup job of the Agent node fails as below:

  - Ping the Agent node from the Appliance and verify whether the Agent node is connected or not as follows:




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




**Solution**

To resolve the connection problem between the Appliance and Agent node, perform one of the following steps:

- If Linux node is not available in the production environment, stop the DHCP Server service and RRAS service on the Appliance and verify whether the problem is resolved or not.

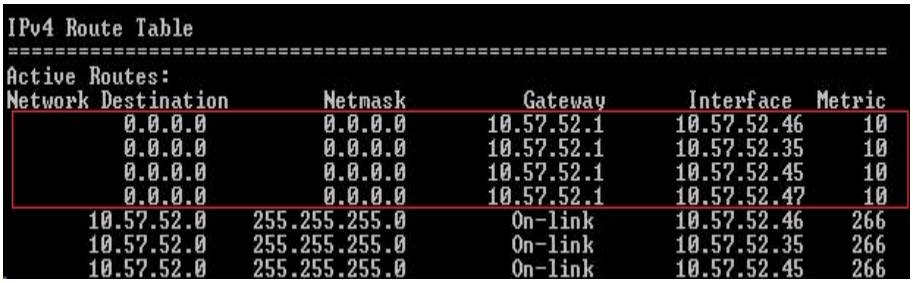
  For more information, refer How to Disable DHCP Server in Appliance User Guide.

- On the Appliance and Agent node, follow these steps:

  **Steps to be followed on Appliance:**

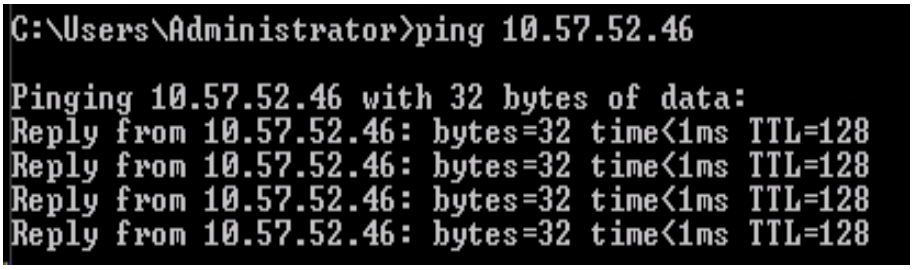
  1. Run *ipconfig /all* from DOS Command Prompt to get the available IPv4 address on the Appliance:
  2. Run *Route Print* from DOS Command Prompt to get the IPv4 Route Table, record the order list for all the available IPv4

address on the Appliance as below:




**Steps to be followed on Agent node:**

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




2. Modify the file *C:\Windows\System32\drivers\etc\hosts* to add a record for the pair *the_IPv4_got_above Appliance_hostname* and save the file.

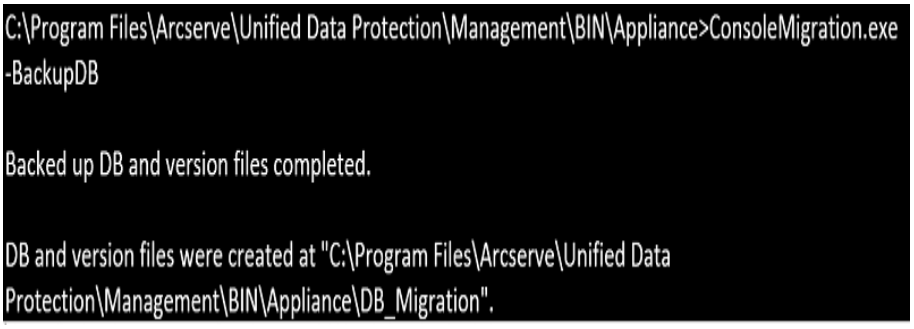
# Best Practices for Arcserve UDP Console Migration

On the Arcserve UDP Appliance, you can migrate the Arcserve UDP Console to another Appliance using *ConsoleMigration.exe*. In Arcserve UDP v6.5 Update 2, you can migrate the Arcserve UDP Console between any two Arcserve UDP consoles, no matter whether it is Appliance or not.

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


To complete the migration process, follow these steps:

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




   The *DB_Migration* folder is created successfully.

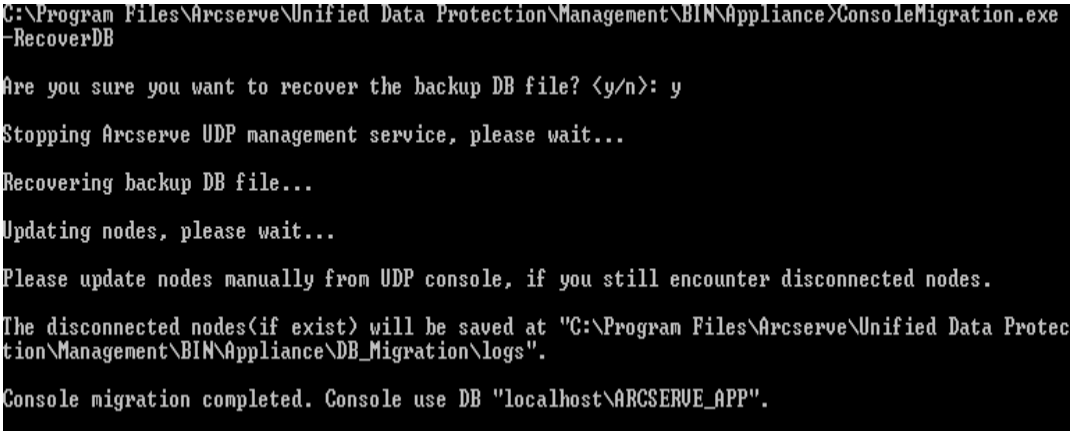
2. On the new Arcserve UDP Console, copy the *DB_Migration* folder to the following path:

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

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

   **Note:** If it is not an Arcserve UDP 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.




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

You have completed migration of Arcserve UDP 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:** When you use Console Migration tool to perform console migration between two Arcserve UDP Consoles then both the Arcserve UDP Console version and SQL database version should be consistent on the two Arcserve UDP Console systems. Otherwise, the console migration fails and an error message is displayed in the command line and log files in the following path:

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

# Best Practices for Set Appliance Image Utility Tool

Set Appliance Image Utility tool helps you to replace the original Appliance image in current system with desired Appliance image of Arcserve UDP Appliance available versions. You can download the Appliance image of Arcserve UDP v6.5 Update 2 from the URL.

**Note:** The md5 for Appliance image download is *1E9FB62D395EF1812B1DBE9EDB8F2C6E*.

After executing the utility, perform factory reset to revert Appliance to desired released version of Arcserve UDP Appliance using factory default setting available in the Arcserve UDP Console. Set Appliance Image utility is available for Arcserve UDP 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 UDP Appliance.

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


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

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

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

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

To upgrade, follow these steps:

1. Download the Appliance image of Arcserve UDP Appliance v6.5 Update 1, and execute the Set Appliance Image Utility. Perform the following steps to use set Appliance Image Utility:
    a. Download the Arcserve UDP v6.5 Update 1 Appliance image from the URL or contact suppport to get the download.

**Note:** The md5 for Appliance image download is *9F568A4BDC6B42972C5177284591B835*.

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>*

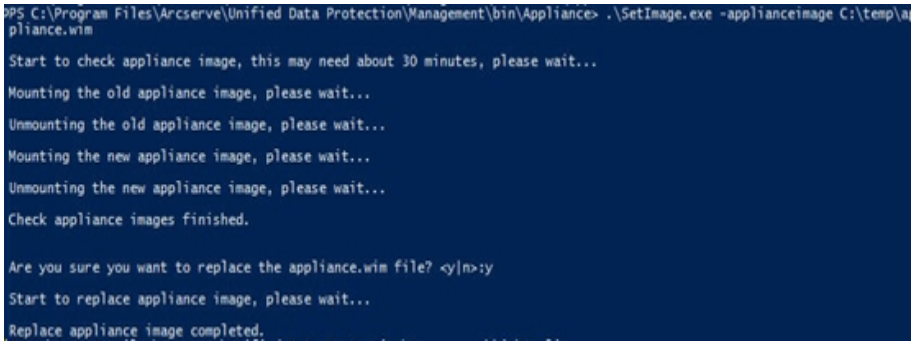
After *checking appliance images finished* step is complete, you can view the following query:

*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.

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

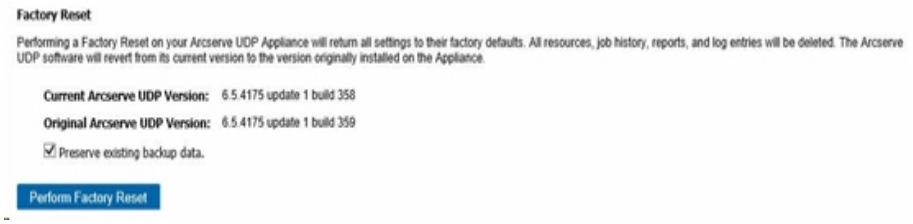
*Replace appliance image completed.*




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

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

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




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

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

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

For more information about Factory Reset, refer the link.

# Best Practices for pre-installed Linux Backup Server in the Arcserve UDP Appliance

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

**Follow these steps:**

1. Navigate to the following path:

   *vi /etc/sysconfig/iptables*

2. The iptables file must contain the following lines that are mentioned in bold, if not you need to add them maually:

   *# Firewall configuration written by system-config-firewall*

   *# Manual customization of this file is not recommended.*

   **filter*

   *:INPUT ACCEPT [0:0]*

   *:FORWARD ACCEPT [0:0]*

   *:OUTPUT ACCEPT [0:0]*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*-A INPUT -p icmp -j ACCEPT*

*-A INPUT -i lo -j ACCEPT*

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

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

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

*COMMIT*

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

   */etc/init.d/iptables restart*

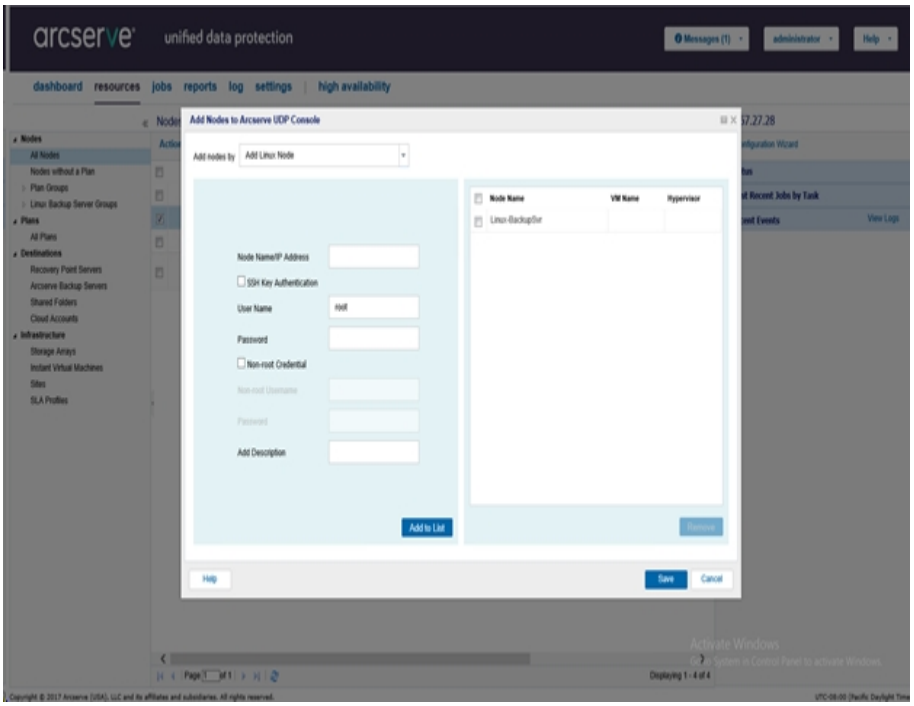
You have added the ports to CentOS 6.6 x64 firewall successfully.

# Best Practices for Arcserve UDP Appliance to backup the Linux Backup Server itself

In the Arcserve UDP Appliance, if you want the Linux Backup Server to backup itself, perform the following steps:

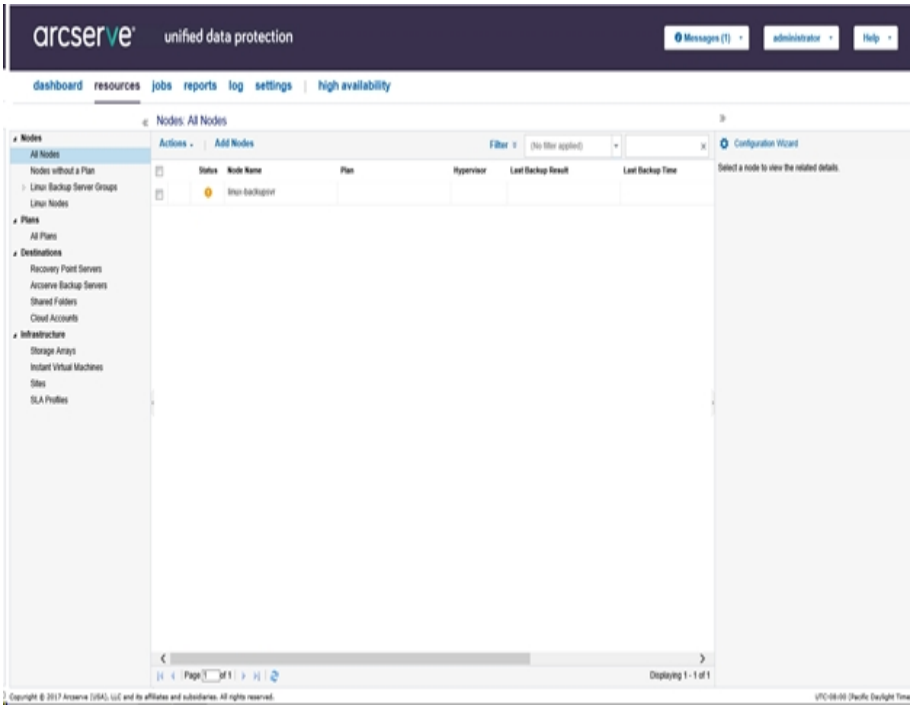
1. From Arcserve UDP Console, click the **resources** tab.
2. Click **All Nodes** in the right pane.
3. From the center pane, click **Add Nodes**.

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



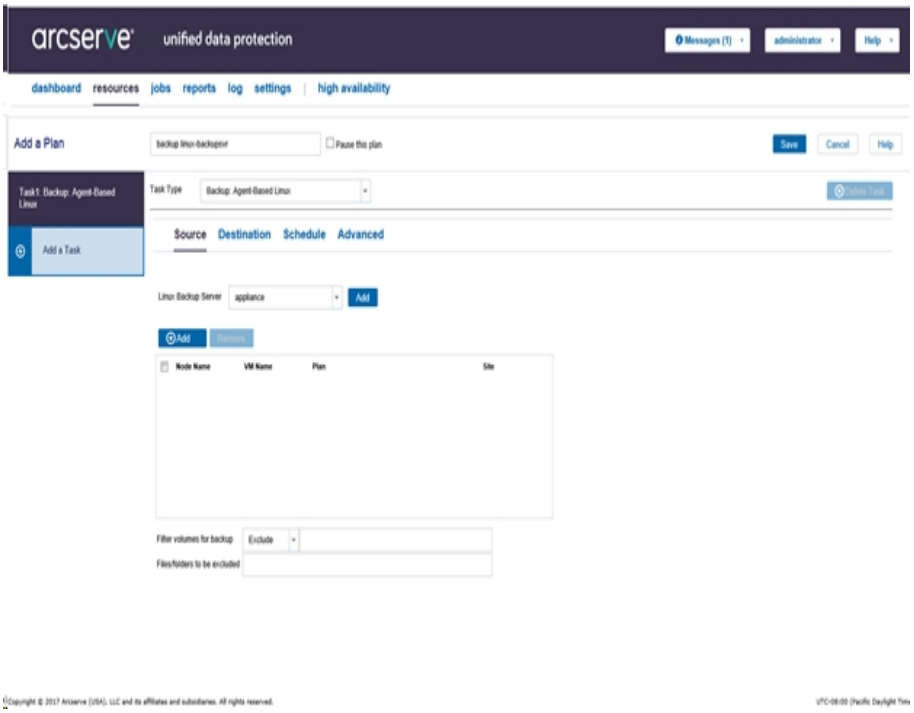

6. Click **Save**.

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

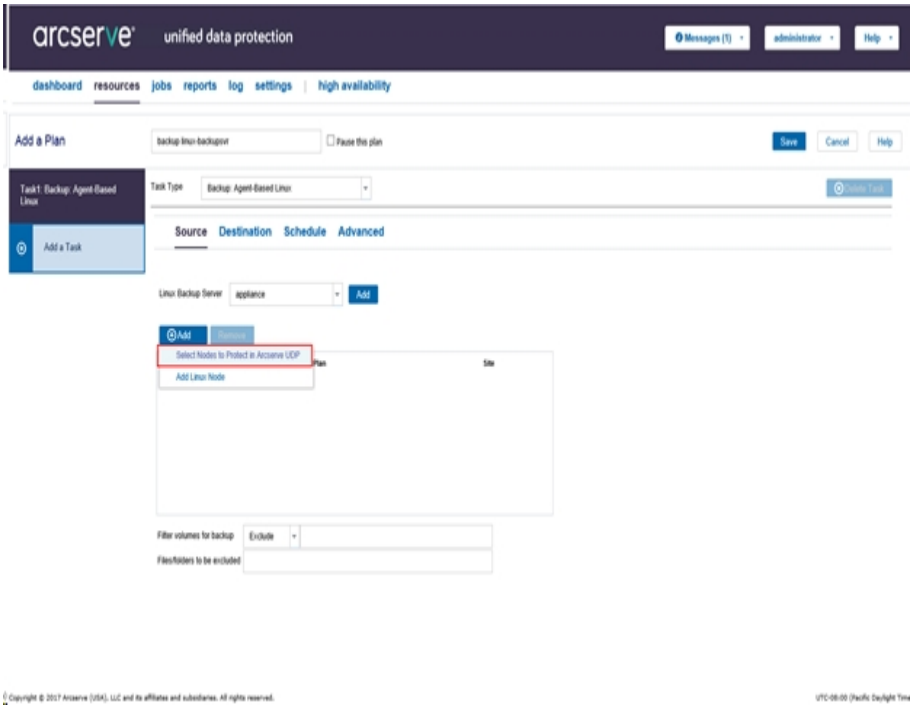



7. Navigate to **All Plans** and create an Agent-based Linux plan.

   The **Source** tab appears.

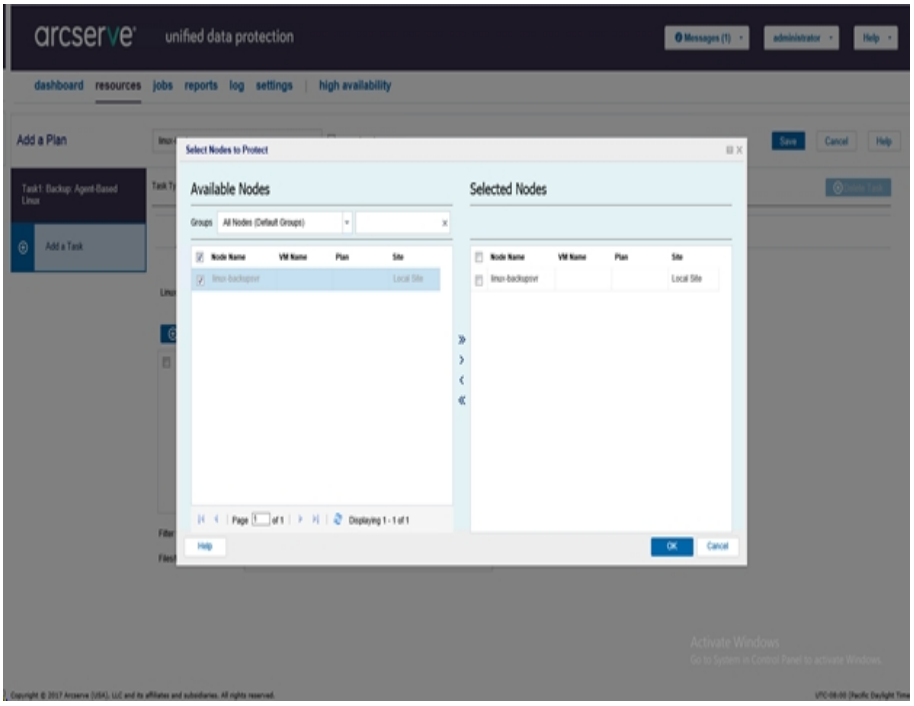



8. From the Add drop-down list, select *Select Nodes to Protect in Arcserve UDP*.



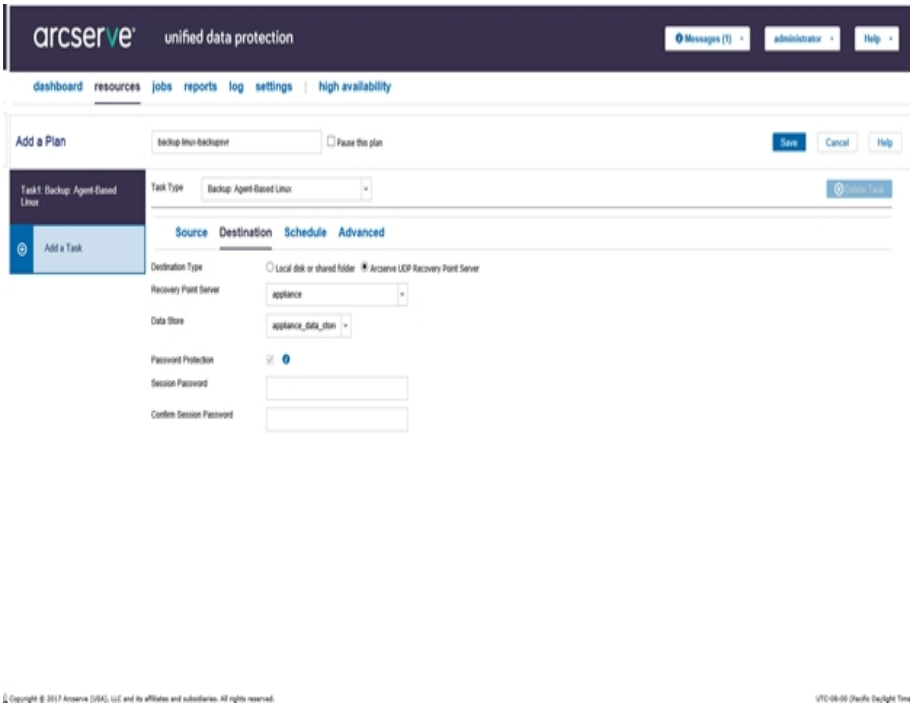

The **Select Nodes to Protect** dialog opens.

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

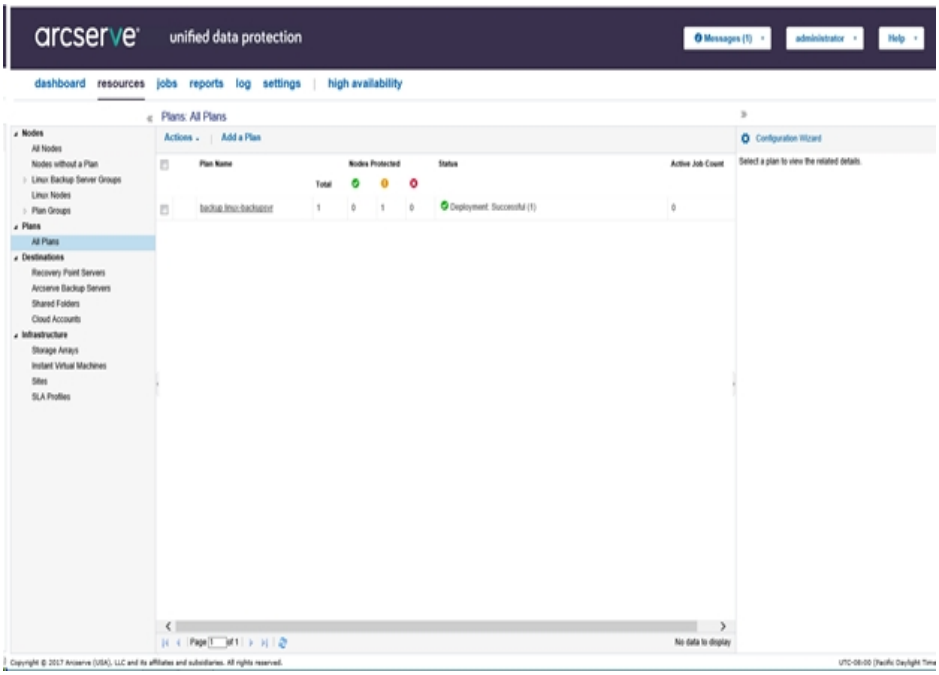



The **Destination** tab appears.

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




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




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

# Best Practices to Migrate from Arcserve UDP Appliance to Appliance

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

For example, let us migrate the Arcserve UDP Appliance 8200 to Arcserve UDP 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 UDP Appliance 8200, ensure that no job runs.

  For more information on Console migration, refer the Best Practices for Arcserve UDP Console Migration 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

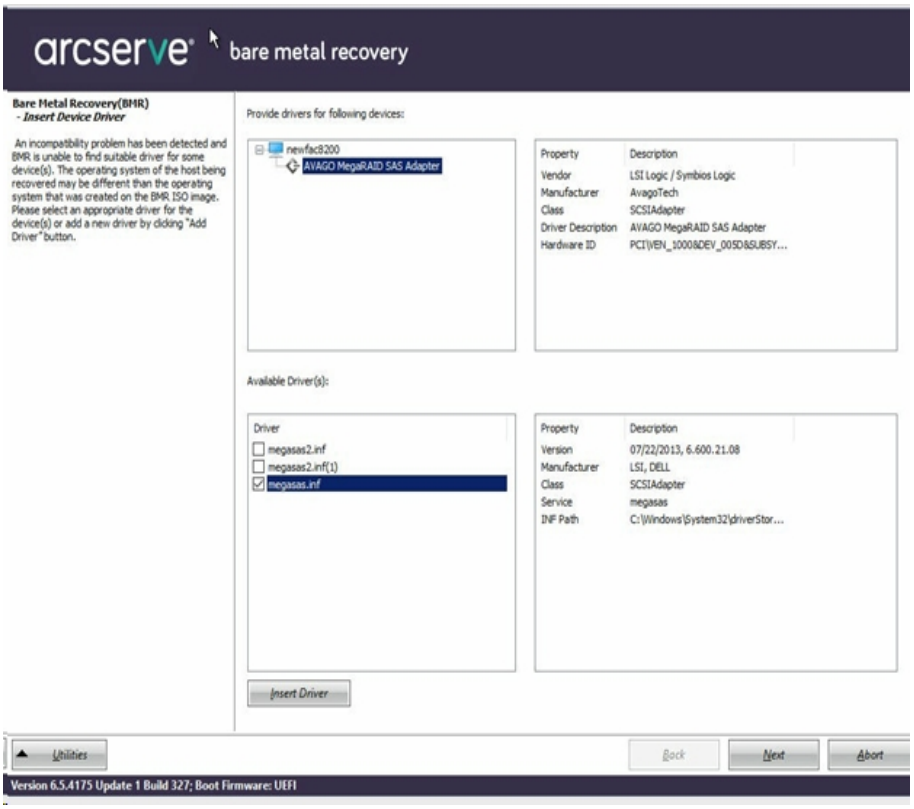
To perform BMR from existing UDP Appliance to another fresh UDP Appliance , follow these steps:

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

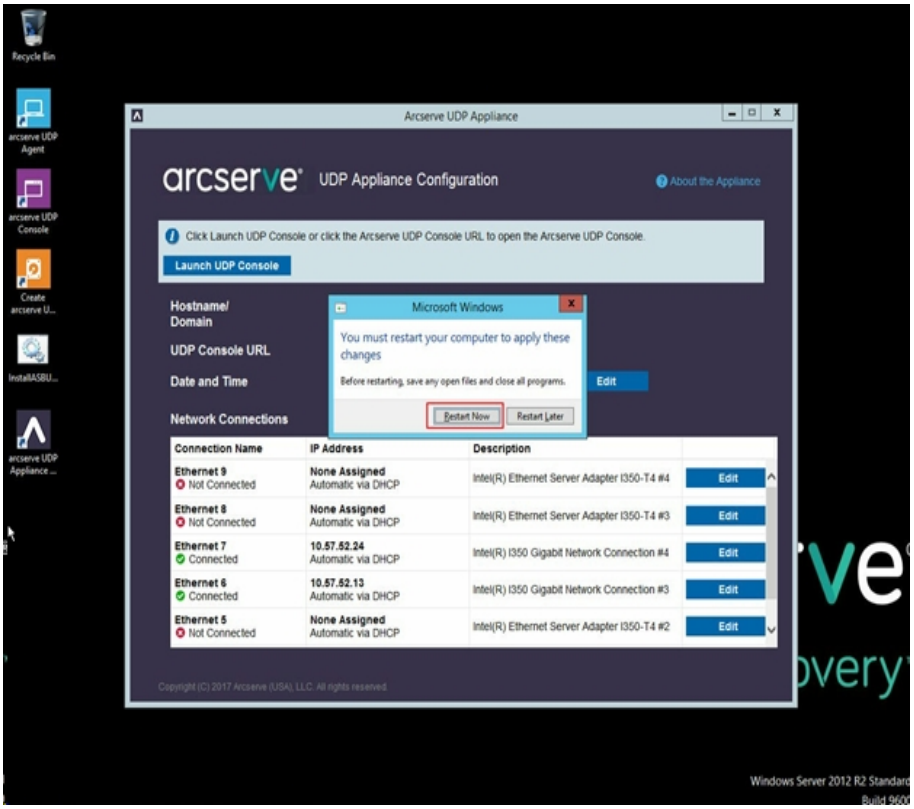
   **Note:** You can just ignore the following warning:

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

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



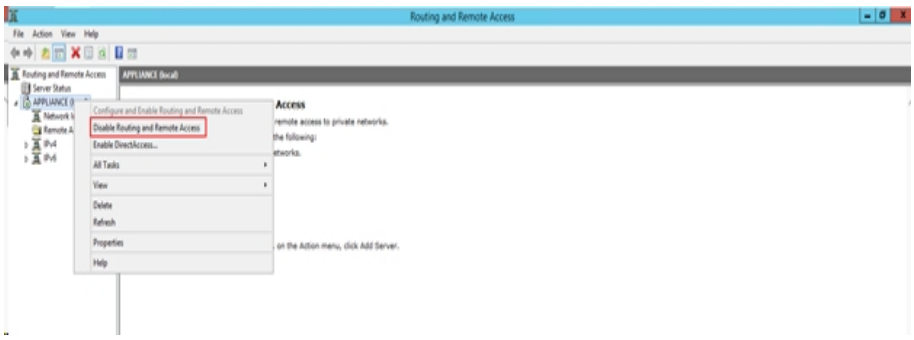

3. After the BMR, restart the Appliance 8400 according to the system prompt.




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

   Follow these steps:

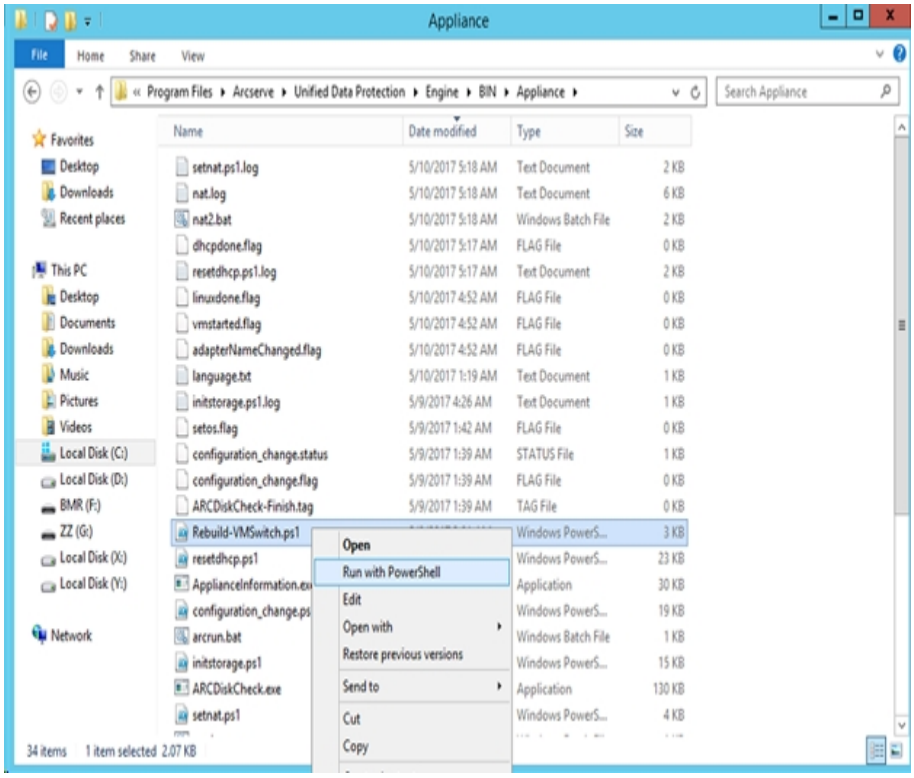
   a. Open Routing and Remote Access and click **Disable Routing and Remote Access**.




   b. Run the following command with PowerShell:

      *C:\Program Files\Arcserve\Unified Data Pro-*

*tection\Engine\BIN\Appliance\Rebuild-VMSwitch.ps1*

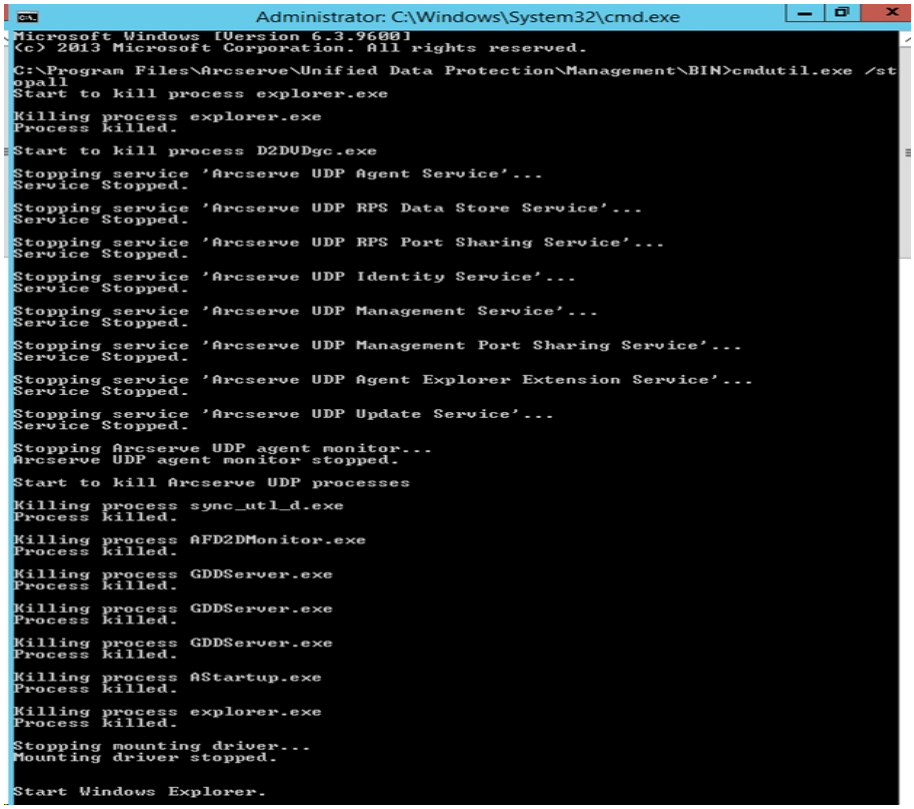



5. Now, follow these steps to copy the data on 8200 Appliance to 8400 Appliance and import the data on to 8400 Appliance:

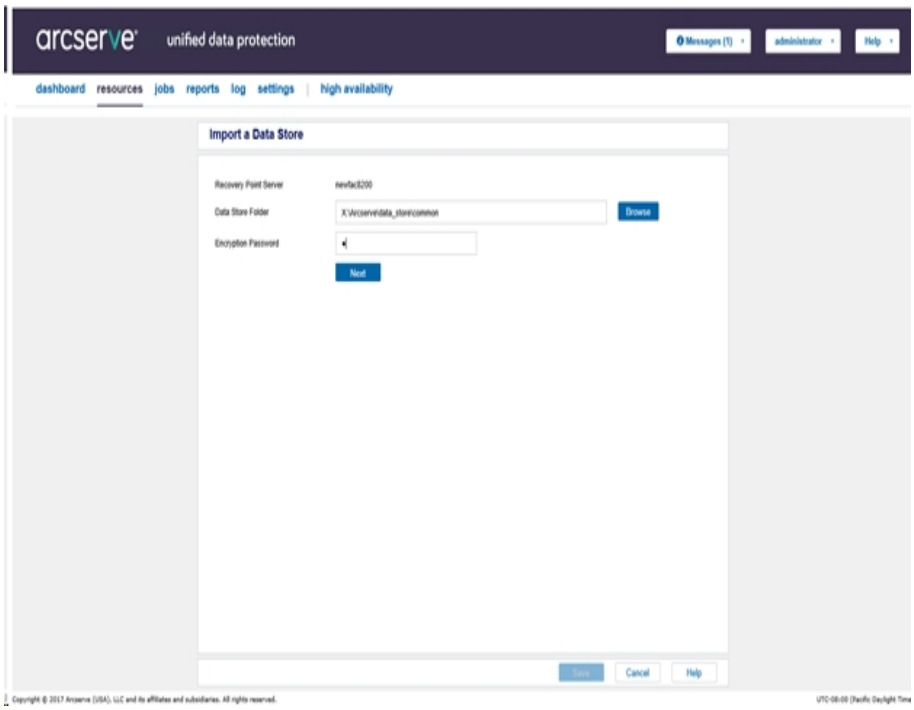
   a. Stop all the UDP services on UDP Appliance 8200 using the following command in the command line:

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

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




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



# Solution 2

**Migrate Arcserve UDP Appliance solution**

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

**Prerequisites:**

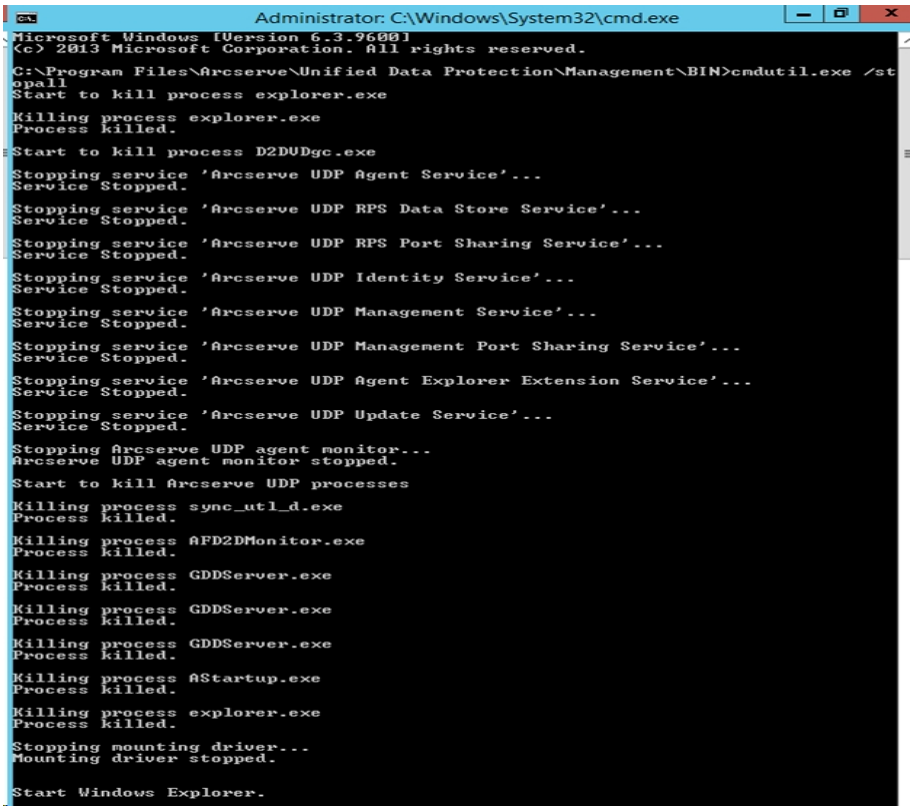
- On Arcserve UDP Appliance 8200, ensure that no job runs.
- You have migrated the Arcserve UDP Console from UDP Appliance 8200 to 8400.

  **Note:** For more information about how to migrate the Arcserve UDP Console from Appliance 8200 to 8400, refer Best Practices for Arcserve UDP Console Migration.

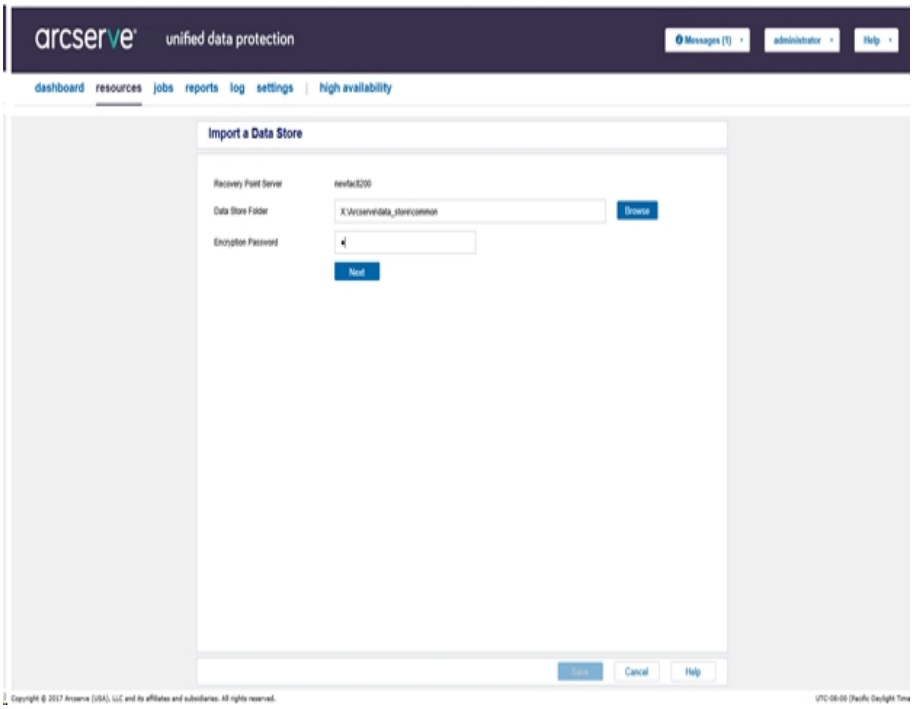
**Follow these steps:**

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

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



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




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

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

# Best Practices for Arcserve UDP Linux instant VM job to Local Appliance Hyper-V

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

**Follow these steps:**

1. Open Hyper-V manger.
2. Create a new external virtual network switch.
3. Open Routing and Remote Access and click **Disable Routing and Remote Access**.


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

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

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

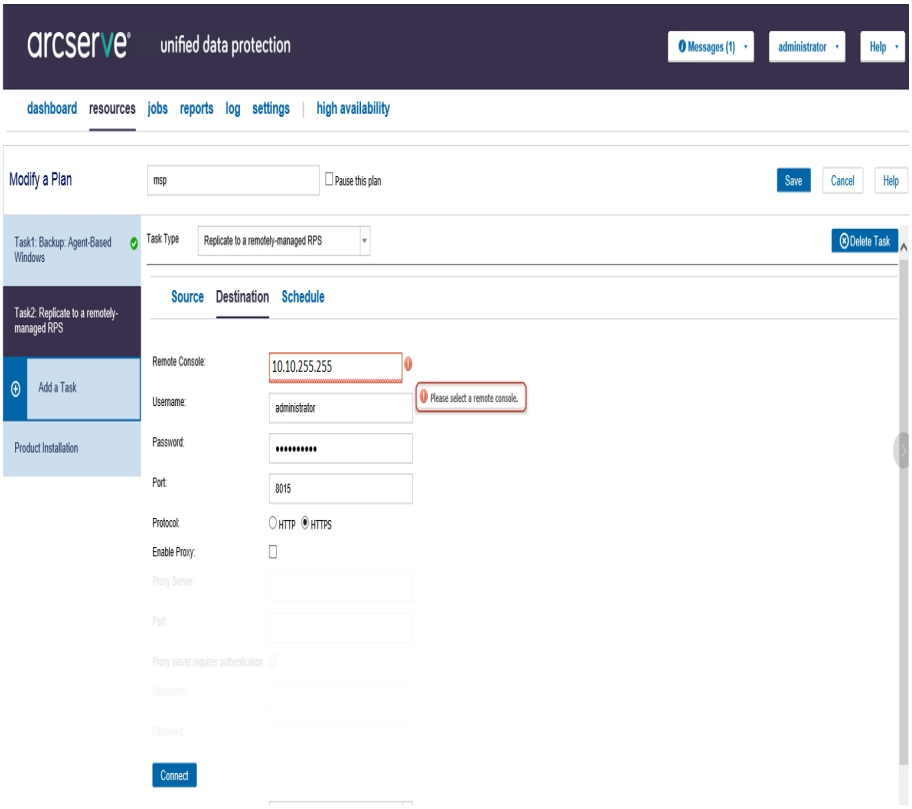
5. To perform Linux instant VM job to local Hyper-V, select the newly added virtual network switch created.

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

# Best Practices to add Replicate to a remotely managed RPS task to another Appliance

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 following error message is displayed in the Arcserve UDP Console:

*Please select a remote console*




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

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

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

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

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

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

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

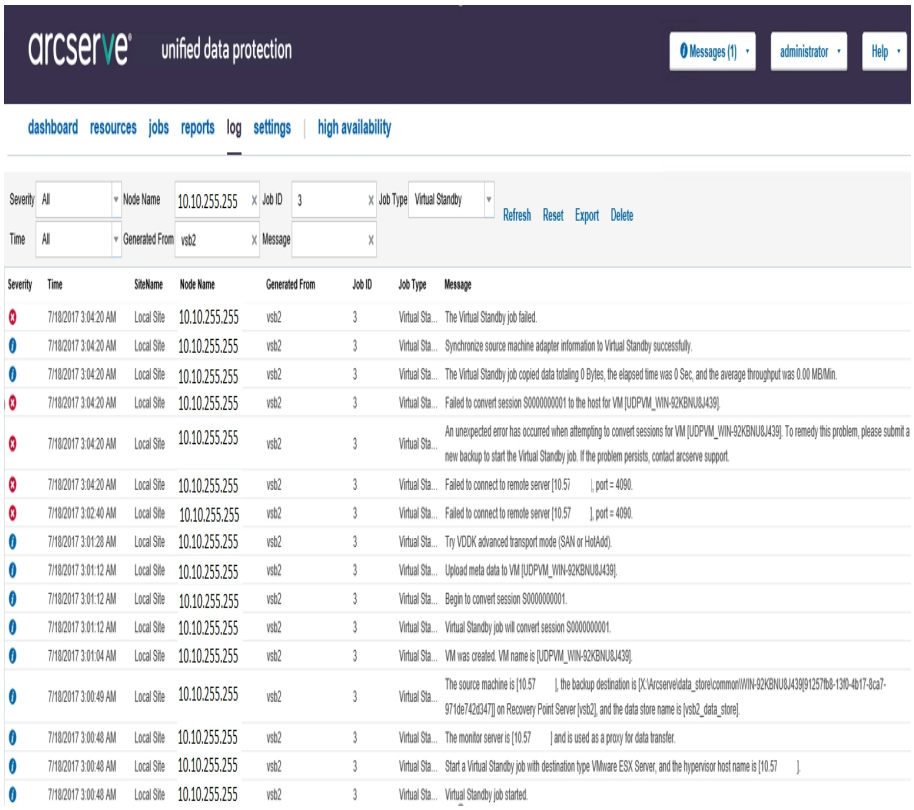
3. Restart UDP management service on the local appliance machine.
4. From the UDP Console of local machine, follow these steps:
    a. Select *All nodes* in Nodes view.
    b. Right click and select *Update*.
    c. Click **OK** to update all the nodes.
5. Select all RPS nodes in Recovery Point Servers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

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

# Best Practices to perform Virtual Standby (VSB) task for which the monitor is another Appliance

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

*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 select *Deploy Now*.
   c. Click **OK** to deploy all plans.

The VSB task is supported successfully.

# Chapter 14: Acknowledgements

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

This section contains the following topics:

# 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/ |
| Localization Required | |
| Platform(s) Required | Windows 2012 R2 |
| Component URL | http://the.earth.li/~sgtatham/putty/0.64/x86/ |
| Component Version URL | http://the.earth.li/~sgtatham/putty/0.64/x86/ |
| Description | On the appliance machine, we use putty.exe to communicate with the Linux Backup Server to change the system locale and UDP Linux locale. |
| Features | Appliance |
| License Text | http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html<br>*PuTTY is copyright 1997-2015 Simon Tatham.*<br>*Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, and CORE SDI S.A.*<br>*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:*<br>*The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.* |

| | |
|---|---|
| | *THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.* |
| Copyright Text | http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html<br>*PuTTY is copyright 1997-2015 Simon Tatham.*<br>*Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, Christopher Staite, and CORE SDI S.A.*<br>*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:*<br>*The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.*<br>*THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.* |
| License URL | |
| Intended Usage | On the appliance machine, we use putty.exe to communicate with the Linux Backup Server to change the system locale and UDP Linux locale. |
| Modifications Required | No |
| Type of Distribution to Customer Binary | |