Arcserve Cyber Resilient Storage Server

Installation and Setup Guide

Version 1.0

arcserve®

Legal Notices

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 may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Arcserve. This Documentation is confidential and proprietary information of Arcserve and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and Arcserve governing your use of the Arcserve software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and Arcserve.

Notwithstanding the foregoing, 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

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

Contact Arcserve

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.

Contents

Chapter 1: Introduction

Arcserve Cyber Resilient Storage complements your existing UDP 10.x installation to keep your data safe from cyberattacks and helps maintain cybersecurity compliance alignment. With Arcserve Cyber Resilient Storage, you can take immutable snapshots of an entire data store on the on-premises storage endpoint for enhanced protection against ransomware and other threats.

Arcserve Cyber Resilient Storage leverages immutable snapshots to protect your data, keeping it unchangeable and recoverable, and provides:

- A secure low footprint storage destination for UDP
- Data integrity through immutable snapshots that are protected against unauthorized modifications
- The option to create a CRS RAID volume if users want to use a software RAID

The Arcserve Cyber Resilient Storage Server is managed through a Command Line Interface (CLI) also referred to as the shell or CRS CLI. For more information, see the Command Reference Guide.

Note: This document contains the following acronyms:

- **CRS:** Arcserve Cyber Resilient Storage
- **CRS Server:** Arcserve Cyber Resilient Storage Server
- **CRS Data Store:** Arcserve Cyber Resilient Data Store
- **CRS CLI:** Arcserve Cyber Resilient Storage Server CLI

Chapter 2: Overview

This guide provides a comprehensive walkthrough for the installation and setup of the Arcserve Cyber Resilient Storage Server, also referred to as CRS Server. It covers the following:

- Hardware and network prerequisites
- Types of installation
- Initial configuration
- Network and storage setup
- Security and user management

This Installation Guide is intended to help you install, configure, and get started with the Arcserve Cyber Resilient Storage Server.

Chapter 3: Pre-Installation Checklist

This section describes the pre-requisites to install and set up the Arcserve Cyber Resilient Storage Server and contains the following topics:

Hardware Requirements

This section provides information about the recommended hardware specifications for installing and managing the Arcserve Cyber Resilient Storage Server. It includes considerations for CPU, memory, storage media, and network interfaces.

When considering a setup for the Arcserve Cyber Resilient Storage Server note the following:

- Data storage should be redundant so that a few drive failures do not cause data loss.
- To provide data storage redundancy, use a hardware RAID or CRS RAID to create a software RAID from 3 or more disks.

  Note: for a comparison between hardware RAID and software RAID, see Software RAID vs Hardware RAID.
- The current version of Arcserve Cyber Resilient Storage Server supports hardware components certified by the RedHat version 9 64-bit (x86_64) (see link).
- To provide redundancy for the OS, use a hardware RAID.

  Note: Hardware RAID can be managed at the user's end.

The current version of the Arcserve Cyber Resilient Storage supports three types of storage deployments:

- Hardware RAID for the OS and data storage
- Hardware RAID for the OS and multiple disks for data storage
- A single disk for the OS and multiple disks for data storage

Minimum Hardware Requirements

This section provides information about the minimum recommended hardware specifications for installing and managing the Arcserve Cyber Resilient Storage Server.

The minimum hardware requirements are:

- Two disks or volumes that can be detected by the Operating System
- Minimum disk space of 25 GB for the Operating System
- Separate disks for the Operating System and data stores
- The current version of Arcserve Cyber Resilient Storage Server supports hardware components certified by the RedHat version 9 64-bit (x86_64) (see link).

Requirements for Hardware RAID Configuration

The following table describes the requirements for environments using a hardware RAID configuration:

Per RAW Disk Size (in TB)	RAID5 Usable Capacity (in TB)	Physical CPUs	Suggested CPU Cores (Min)	RAM in GB (Min)
1	3.872	1	1	8
2	7.744	1	1	12
4	15.488	1	2	16
6	23.232	1	3	22
8	30.976	1	4	32
10	38.72	1	4	36
12	46.464	1	5	48
14	54.208	1	6	48
16	61.952	1	7	64
18	69.696	1	7	64
20	77.44	1	8	64
22	85.184	1	10	72
24	92.928	1	10	72
26	100.672	1	12	86
28	108.416	1	12	98
30	116.16	1	14	104
32	123.904	1	14	128
36	139.392	1	16	144

Notes:

- If your environment has hardware RAID adapters, Arcserve recommends that you use it instead of a CRS RAID.
- The current version of Arcserve Cyber Resilient Storage Server supports hardware components certified by the RedHat version 9 64-bit (x86_64) (see link).

Requirements for CRS RAID Configuration

Arcserve Cyber Resilient Storage Server uses the CRS RAID configuration over other traditional RAID arrays because CRS RAID provides better data integrity, eliminates the RAID 5 write hole and offers more flexibility in storage management.

The following table describes the requirements for environments using a CRS RAID configuration.

Important! Each RAID configuration below is created by combining the usable capacity, RAW disk capacity, and number of disks. The same configuration can be created by using different combinations.

Usable Storage Capacity in TB (without 3.2% buffer)	Total RAW Capacity	RAW disk Capacity per disk*	No. of Disks*	Suggested CPU Cores	Suggested RAM (in GB)	Minimum No. of Physical CPUs
1.936	3	1	3	1	6	1
3.872	6	2	3	1	7	1
7.744	12	4	3	1	10	1
11.616	18	6	3	2	13	1
15.488	24	8	3	2	16	1
19.36	30	10	3	2	19	1
23.232	36	12	3	3	22	1
30.976	48	16	3	4	28	1
34.848	54	18	3	4	31	1
38.72	60	20	3	4	34	1
46.464	72	24	3	5	39	1
54.208	84	28	3	6	45	1
61.952	96	32	3	7	51	1
69.696	108	36	3	7	57	1
77.44	100	20	5	8	63	1
92.928	120	24	5	10	74	1
108.416	140	28	5	11	86	1
123.904	160	32	5	13	97	1
139.392	180	36	5	14	109	1
162.624	196	28	7	17	126	1

Notes:

- Make sure that a default usable capacity of at least ~3.2% (min 128 MB, max 128 GB) is available for the buffer.
- The buffer is important for the following reasons:
  - Pool overfills and system instability are prevented
  - Critical operations such deletes, snapshots, metadata and so on can complete
  - Internal structures such as metadata and spacemaps are supported

Network Requirements

The following are the network requirements for the Arcserve Cyber Resilient Storage Server to communicate with UDP and RPS:

- At least one network interface card (NIC). For most installations, this is an Ethernet interface that can be configured for DHCP (automatic IP assignment) or manually with a static IP address, netmask, gateway, and DNS.
- Supported network card. See the RedHat Catalog.
- For a standard installation, just make sure your network cable is connected and the interface is enabled during setup.
- If the Arcserve Cyber Resilient Storage Server is deployed in a segmented network for security purposes, open extra ports to enable communication and data transfer. These ports allow communication between the segmented networks of both UDP and the Arcserve Cyber Resilient Storage Server.

  The following ports must be open:

  - Port Number 22 — outbound for Arcserve Support to login through the Support Tunnel
  - Port Number 443 — outbound for checking for and installing updates
  - Port Numbers 5000-5099 — for inbound data traffic

Notes:

- Network bonding is not supported in version 1.0.
- Most standard network interface cards from the Red Hat 9 Hardware Catalog work with version 1.0. Support for SFP, SFP+, QSFP, QSPF48, and Fiber Channel HBA will feature in the upcoming releases.

Chapter 4: How to Install Arcserve Cyber Resilient Storage Server

This section provides information about installing and configuring the Arcserve Cyber Resilient Storage Server, along with best practices. It also includes instructions to help you set up the server and ensure that your data remains safe, secure, and unchanged for the defined retention period.

Important! Whenever you are installing or updating the Arcserve Cyber Resilient Storage Server, or synchronizing the system time, make sure that the system is connected to the Internet.

Specifically, this section contains the following topics:

Download ISO File

You can download the Arcserve Cyber Resilient Storage Server ISO file in any one of the following ways:

- In Cloud Console, click **Try it** from the Actions menu on the Recovery Point Servers page. The Arcserve Cyber Resilient Storage Free Trials page opens. Enter your name, company details, email address, and click **Submit**. The Arcserve sales team will contact you.
- Open the Support page. From Products, click Arcserve CRS, and then click Arcserve Cyber Resilient Storage Download Link.
- In the UDP console, on the Recovery Point Servers page, right click an Arcserve Cyber Resilient Data Store and from the menu click **Try It**. The Arcserve Cyber Resilient Storage Free Trials page opens. Enter your name, company details, email address and click **Submit**. The Arcserve sales team will contact you.

Create Bootable Media

You can create a bootable media from the Arcserve Cyber Resilient Data Storage Server ISO file using any of the commonly available tools.

Note: If you are creating a bootable USB drive and the tool gives you the option to select either DD mode or ISO mode, select the DD mode.

Follow these steps:

1. Download the Arcserve Cyber Resilient Storage Server ISO file.
2. Select the desired tool to create the bootable media.
3. Insert the desired bootable media, that is, USB drive, DVD, or Blu-ray.

   Important! This action will erase all data on the removable media.
4. Follow the instructions in the tool to select the ISO file and media, then create the bootable media.

To boot from the bootable media, restart your computer and select the media from the boot menu.

Troubleshooting Options

To troubleshoot the installation during the installer run, follow these steps:

- Press Ctrl+B+1 — Go to the main installation window.
- Press Ctrl+B+2 — Go to the shell.
- Press Ctrl+B+3 — Go to the logs.
- Press Ctrl+B+4 — Go to the storage logs.
- Press Ctrl+B+5 — Go to the program logs.

Note: Use the **Alt**+**Tab** key combination to switch between the windows.

Install Arcserve Cyber Resilient Storage Server

This section explains how to install the Arcserve Cyber Resilient Storage Server and complete the initial configuration.

Follow these steps:

1. Boot the ISO file from the bootable media.
2. From the displayed options, select Arcserve Cyber Resilient Storage Server.

   The installer displays a list of disks available for installing the operating system with a disk preselected. By default, the first initialized disk is selected.
3. To choose a different disk, press any key to stop the countdown, then enter the disk number and press **Enter** to select it.

   The installer completes the OS installation and shuts down.
4. Turn on the Arcserve Cyber Resilient Storage Server and log in using the following default credentials to complete the initial configuration:
   - Username: *arcserve*
   - Password: *arcserve*

See Complete Initial Configuration for more information.

Complete Initial Configuration

This section guides you through the initial setup of the Arcserve Cyber Resilient Storage Server after the installation. The following steps are required to complete the initial configuration:

a. Create a super admin account

b. Select a time zone

c. (Optional) Modify the host name

d. (Optional) Modify the network interface

e. (Optional) Set up the storage pool

Note: If the initial configuration is interrupted at any point, you can resume from where you left off by logging in to the CLI using your default credentials.

Follow these steps:

1. Restart the Arcserve Cyber Resilient Storage Server.
2. To log in to the Arcserve Cyber Resilient Storage Server for the first time after the installation, at the login prompt, type *arcserve* as both the user name and password and then press **Enter**.

   Note: These credentials will be deleted after you complete the initial configuration. On the next log in, use the superadmin credentials you will create in the next step.
3. To create and log in as the super admin account, type a user name and password, and confirm the password when prompted, then press **Enter**.

   Notes:

   - The password must contain at least 8 characters and include an upper case letter, a lower case letter, and a number.
   - The password reset option is not available for this account. Contact Arcserve Support for assistance.
4. To set the time zone for the Arcserve Cyber Resilient Storage system, use the Arrow keys to navigate through the available time zones , then press **Enter** to select the required time zone.

   Note: If the desired time zone is not available in the list, select *UTC*.
5. To modify the hostname, type *Yes* at the prompt and type the new hostname. To continue without modifying the hostname, type in *No*.

Note: Specify a hostname between 1 and 64 characters using letters, numbers and hyphens. Avoid starting or ending with a hyphen.

6. To modify the network, type in *Yes* when prompted, then select the network interface to modify and select *Auto* as the network method. To continue without modifying the network interface, type in *No*.

   Select *Auto* if DHCP is available and it is your preferred network configuration method.

   If the network segment where you want to deploy Arcserve Cyber Resilient Storage does not support DHCP, select **manual**. Make sure you have the following information:

   - IP address to be used (use only CIDR notation)
   - Default Gateway

7. Do one of the following:

   - To set up the initial storage pool, type *Yes* at the prompt and do the following:

     a. Type a name for the initial storage pool.

     b. Select the RAID/disk configuration. To select a disk for the software CRS RAID, use the arrow key to highlight and press the space bar. Repeat for each disk you want to add.

        Note: To create a new CRS RAID volume, select at least three disks or a single hardware RAID disk. Supported RAID configurations are a one-disk hardware RAID configuration and three-disk software CRS RAID configuration.

     To continue without creating a storage pool, type *No*. You can create the pools later from the CLI. For more information, see Create Storage Pool.

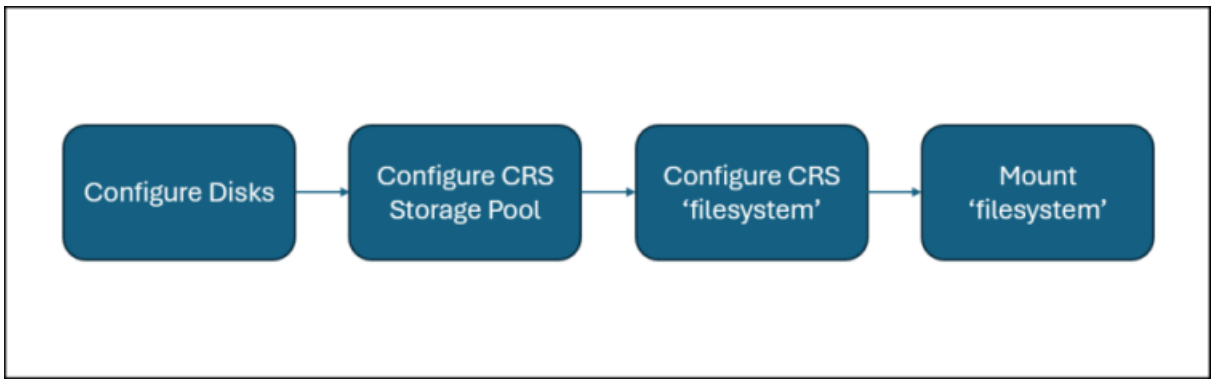
   - To import pre-existing, inactive storage pools during the recovery of an installation process, see Import Pre-Existing Storage Pools.

     The initial setup is complete.

Configure Storage

Configuring additional storage on the Arcserve Cyber Resilient Storage Server enables you to maintain immutability guarantees, avoid service disruption, and achieve seamless integration with existing data structures and access policies. This process includes critical steps and best practices to expand storage on the Arcserve Cyber Resilient Storage Server, with a focus on system compatibility, data integrity, performance impact, and regulatory compliance.

The following image shows the typical process workflow for configuring storage with UDP.



Naming Conventions

When naming an Arcserve Cyber Resilient Storage component, including datasets and pools, make sure to follow these rules:

- Component names must only contain alphanumeric characters.
- Component names can contain the following special characters:
  - Underscore (_)
  - Hyphen (-)
  - Colon (:)
  - Period (.)
- Pool names must begin with a letter and with the following restrictions:
  - Can only contain alphanumeric characters as well as underscore (_), dash (-), and period (.)
  - The beginning sequence c[0-9] is not allowed
  - The name `log` is reserved
  - Names beginning with `mirror`, `raidz`, `raidz1`, `raidz2`, `raidz3`, or `spare` are not allowed because these are reserved
  - Pool names must not contain a percent sign (%)
- Dataset names must not:
  - begin with an alphanumeric character
  - contain a percent sign (%)
- Empty components are not allowed.

Create Storage Pool

This section describes how to add a disk to a pool to create additional storage.

Note: For software RAID configurations, a minimum of three disks is required.

Follow these steps:

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command and press **Enter**:

   disk list

   A list of existing disks is displayed.
3. Next, type the following command and press **Enter**:

   pool create [-h] -n NAME -d DISKS [DISKS ...] [-f | --force | --no-force]

   where

   -n, --name

   Name of the pool.

   -d, --disks

   Name of disk(s) to add to the pool.

   Note: You can add multiple disks by separating the disk names with a space.

   -f, --force, --no-force

   Ignores warnings, and forces the pool creation, possibly overwriting existing disk data.

   Default: False

   Notes: When adding a disk, you may come across the following errors:

   - "Disk has existing data."
   - "Disk is in use and contains an unknown filesystem."
   - "Disks of different sizes are specified. Usage for all disks in the pool will be limited to the size of the smallest disk."

     To delete existing data, use the following command:

     pool create --force

     The storage pool is created on the specified disk(s).

     For more pool-related commands, see pool in the Command Reference Guide

Create filesystems

This section describes how to create a filesystem.

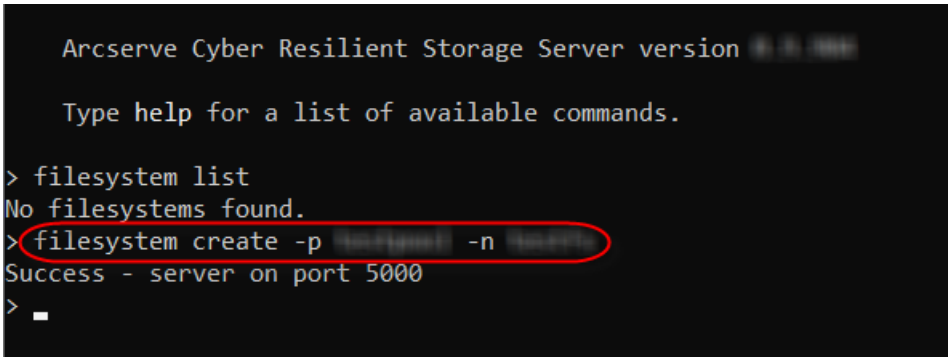
Follow these steps:

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command and press **Enter**:

   filesystem list

   A list of existing filesystems is displayed.
3. Next, type the following command and press **Enter**:

   filesystem create -p [POOL] -n [NAME]



   where

   -p, --pool

   Name of the pool.

   -n, --name

   Name of the filesystem.

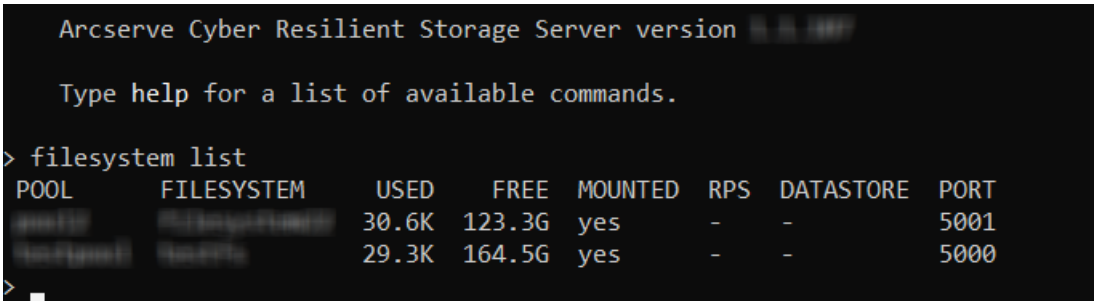
   -m, --mount, --no-mount

   Mounts the filesystem after creation.

   Default: True

   The filesystem is created.
4. To verify if the filesystem is created, type the following command and press **Enter**:

   filesystem list



Note: The port number associated with the filesystem is used when adding or importing an Arcserve Cyber Resilient Data Store in UDP and Cloud Console.

For more filesystem-related commands, see filesystem in the Command Reference Guide.

Upgrade to Newer Version of Arcserve Cyber Resilient Storage Server

This section explains how to upgrade to the latest version of the Arcserve Cyber Resilient Storage Server from an older version.

Note: Make sure that all plans and policies are paused/stopped before you go ahead with the update.

Follow these steps:

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command and press **Enter**:

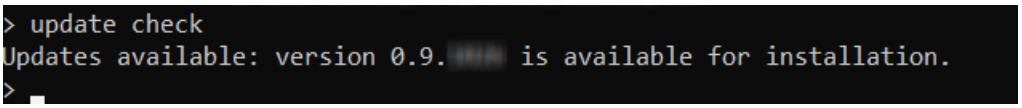
   update config show

   The channel and tag are displayed.

3. Type the following command and press **Enter**:

   update check

   The latest available update is listed.

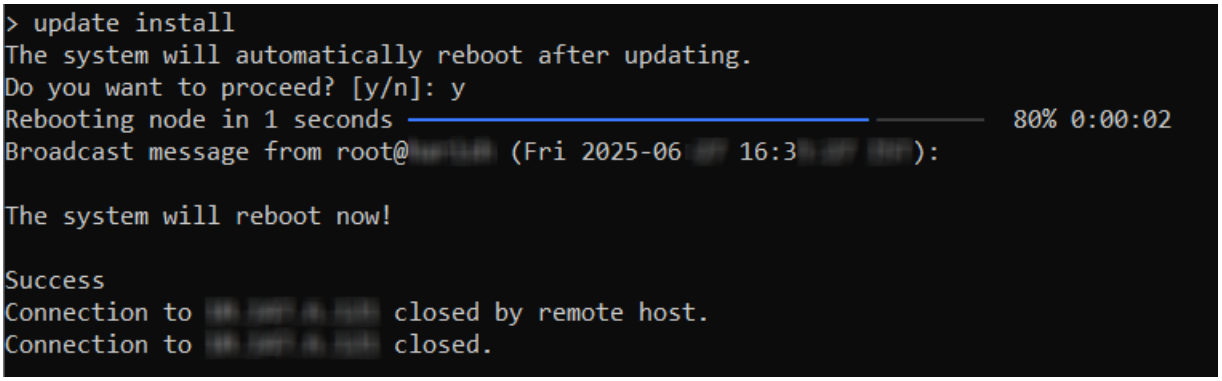


4. Next, type the following command and press **Enter**:

   update install

   A message displays that the system will reboot after the update.

5. When prompted if you want to proceed, press *y*, then press **Enter**:



The upgrade completes and the Arcserve Cyber Resilient Storage shell reboots.

Recover Installation Environment

This section provides information on how to perform a recovery of the Arcserve Cyber Resilient Storage Server installation environment. A recovery is typically performed when there is a system crash or corruption of OS environment, or failed updates or installations.

Important! Starting the recovery process without correct understanding of your environment, steps, and sequence can result in data loss. Arcserve strongly recommends that you contact Support for additional support and guidance.

The following steps are required to complete the process:

1. Reinstall the operating system. For more information, see Install Arcserve Cyber Resilient Storage.
2. Complete the initial configuration. For more information, see Complete Initial Configuration.
3. Import pre-existing storage pools. For more information, see Import Pre-Existing Storage Pools.
4. Mount filesystem
5. Restore configuration files

   Note: For assistance on steps 4 and 5, contact Arcserve Support.

Import Pre-Existing Storage Pools

This section provides information about the steps required to import pre-existing, inactive storage pools from a previous installation. Importing pre-existing pools is a critical step in the recovery process, allowing users the access to existing storage and data.

For more information about the recovery process, see Recover Installation Environment.

Follow these steps:

1. When prompted to import inactive pools, type *Yes* and press **Enter**.

   A list of inactive pools displays.

2. Use the arrow keys to navigate and press the spacebar to select the required pools.

   The selected pools are imported.

3. To verify that the pools have been imported, type the following command and press **Enter**:

   pool list

Chapter 5: Configure Additional Storage

After installation and initial configuration, your Arcserve Cyber Resilient Storage Server is fully operational with default settings. However, many deployments may require further customization to support complex environments, improve performance, or meet specific organizational requirements.

This chapter provides instructions on how to configure additional storage options. These configrations are recommended for users who want to fine-tune their setup, enhance scalability, or align the system with existing infrastructure standards.

This section contains the following topics:

Configure Disks

This section contains the following topics:

Add Disk to Pool

This section provides the steps required to add a disk to a pool to create additional storage.

Follow these steps:

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command and press **Enter**:

   disk list

   A list of existing disks is displayed.
3. To add a disk, type the following command and press **Enter**:

   pool add-disk [-h] [-n POOL_NAME] -d DISK_NAME [DISK_NAME ...]

   where

   -n, --pool-name

   Name of the pool.

   -d, --disk-name

   Name of the disk(s) to add to the pool.

   The disk is added to the pool. Wait for some time for the resilvering process to complete and check if the pool is ready for use by using the following command:

   disk status

   To check if the new disk is added to the pool, use the following command:

   disk list

   Note: When a new disk is added to a storage pool, it is not immediately ready for use. The system must perform a process called "resilvering", which involves copying and verifying the data across the new or replaced disk to ensure redundancy and consistency within the pool. This process can take some time depending on the size of the data and the speed of the hardware. The storage pool will only be fully operational and considered safe to use when the resilvering process has completed successfully.

   For more pool-related commands, see pool in the Command Reference Guide.

Replace Disk in Pool

This section provides the steps to replace a disk in a storage pool. A storage disk in a RAID array is typically replaced when it fails or is predicted to fail soon.

Important! When replacing a disk in a pool, it is important to note that the RAID array contains disks of the same size. So even if you replace a smaller disk with one that has greater storage capacity, the new disk's capacity will be limited to the size of the smallest disk in the array.

Follow these steps:

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command and press **Enter**:

   disk list

   A list of existing disks is displayed.
3. To replace a disk, type the following command and press **Enter**:

   pool replace-disk [-h] -n POOL -o OLD_DISK -d NEW_DISK

   where

   -n, --pool

   Name of the pool containing the disk to replace.

   -o, --old-disk

   Name of the old disk to replace.

   -d, --new-disk

   Name of the new disk that will replace the old disk.

   To check if the new disk is added to the pool, use the following command:

   pool list

   Note: When an existing disk is replaced in a storage pool, it is not immediately ready for use. The system must perform a process called "resilvering", which involves copying and verifying the data across the new or replaced disk to establish redundancy and consistency within the pool. This process can take some time depending on the size of the data and the speed of the hardware. The storage pool will only be fully operational and considered safe to use when the resilvering process has completed successfully.

   For more pool-related commands, see pool in the Command Reference Guide.

Chapter 6: Storage Alerts

This section provides an overview of storage alerts.

Configuring storage alerts is essential for maintaining the optimal performance of your Arcserve Cyber Resilient Storage Server. It allows you to proactively monitor capacity usage and avoid unexpected storage exhaustion, which can lead to service disruptions. Alerts help identify abnormal patterns in data growth, access rates, or error logs that may indicate potential threats, such as ransomware attempts or system faults. Since Arcserve Cyber Resilient Storage is designed to prevent data alteration or deletion, alerts ensure that write-once-read-many (WORM) policies are being correctly enforced without affecting accessibility. Alerts also facilitate better capacity planning by providing real-time insights into usage trends, allowing for timely scaling or archiving actions. Alerts act as an early warning system that safeguards data integrity while ensuring consistent performance and regulatory compliance.

Alerts can be triggered for the following issues:

- **storage-degraded:** This indicates that Arcserve Cyber Resilient Storage is no longer functioning in its optimal state but is still operational. It usually means one or more components (e.g. disks) have failed or are not functioning properly, causing redundancy to be compromised or performance to be reduced.
- **storage-error:** This indicates that a critical failure or unrecoverable error has taken in the Arcserve Cyber Resilient Storage system that has likely affected data availability or integrity.
- **storage-state-changed:** This indicates a change in the status or configuration of the storage system, which may or may not be problematic on its own.
- **system-clock:** This indicates an issue or discrepancy with the system clock or time synchronization, which can affect storage systems and distributed environments.

Configure Email for Alerts

This section provides information on how to configure email addresses to receive alerts.

Follow these steps::

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command and press **Enter**.

   email configure [-h] -H HOST [-P PORT] [-u USERNAME] [-n SENDER_ADDRESS] [-s] [-t] [-x SUBJECT_PREFIX]

   where

   -H, --host

   SMTP server hostname

   -P, --port

   SMTP server port (default: 25, 465, or 587 based on –ssl or –starttls)

   -u, --username

   SMTP server username

   -n, --sender-address

   Sender email address (default: username)

   -s, --ssl

   Encrypt the initial connection

   Default: False

   -t, --starttls

   Upgrade the connection with STARTTLS (ignored if –ssl is set)

   Default: False

   -x, --subject-prefix

   Prefix to add to the subject line of emails

   When prompted, type the SMTP server password, then press **Enter**.

The specified email address is configured to receive email alerts.

To test if the your email configuration works, use the following command to send a test email to the recipient:

email test [-h] -r RECIPIENT_ADDRESS

where

-r, --recipient_address

Recipient's email address

For more email-related commands, see Email in the Command Reference Guide.

Configure Alerts

This section provides information on how to configure email addresses to receive alerts.

Follow these steps::

1. At the command prompt, type the following command and press **Enter**.

   alert create [-h] -t TYPE -r RECIPIENTS [RECIPIENTS ...]

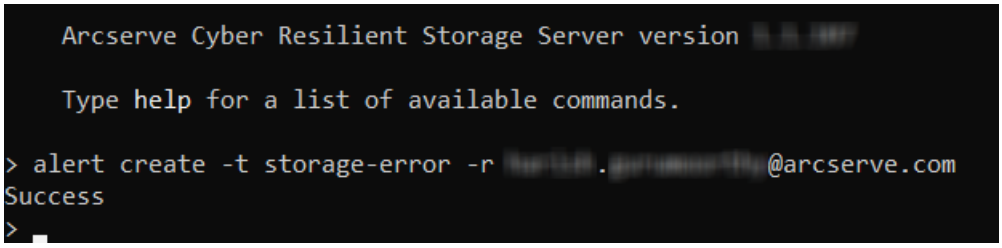
   where

   -t, --type

   The type for which to create the alert. For more information, see Storage Alerts.

   -r, --recipients

   List of recipients for the alert.



   The specified alert type is created and the recipient is notified by email every time it is triggered.

   For more alert commands, see Alert in the Command Reference Guide.

Chapter 7: Security and User Management

Arcserve Cyber Resilient Storage has two sets of credentials for managing your installation.

The following table describes the types of users and the functions they are allowed to perform:

Management Users		Data Plane Credential
Use CLI for managing	**Use CLI for managing**	**Use AccessKeyID for Data Store Communication**
User	Key management	Create data store
Role change for users	Network	Import data store
Keys	Storage	Mount snapshot for creating read-only data store
Network	Endpoint management	-
Storage	-	-
User management	-	-

This section contains the following topics:

Setup Management Users

This section provides information on how to create, modify and assign permissions to a user, and contains the following topics:

Create User

This section provides information on how to create and assign permissions to a new user.

Follow these steps:

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command:

   user list

   A list of existing users is displayed.
3. Next, type the following command press **Enter**:

   user create [-h] -u USERNAME [-r {admin,super_admin}]

   where

   -u, --username

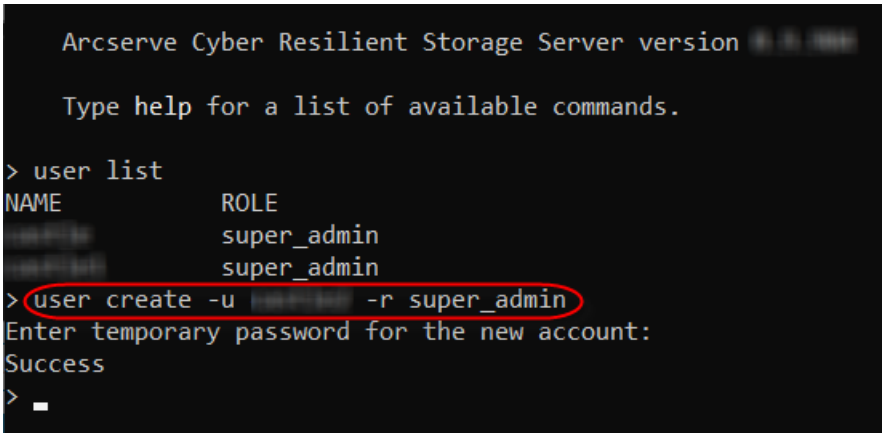
   Username for the new account.

   -r, --role

   Role for the new account. Possible choices: admin, super_admin.

   Default: 'admin'

   For more information on user roles and their functions, see Security and User Management.
4. When prompted, type a password for the new user and press **Enter**.



   The new user is created.

   Note: Use the following command to delete a user:

   user delete [-h] -u USERNAME

For more user-related commands, see user in the Command Reference Guide.

Update User

This section provides information on how to update a user.

Follow these steps:

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command:

   user list

   A list of existing users is displayed.
3. Type the following command press **Enter**:

   user update [-h] -u USERNAME [-r {admin,super_admin}]

   where

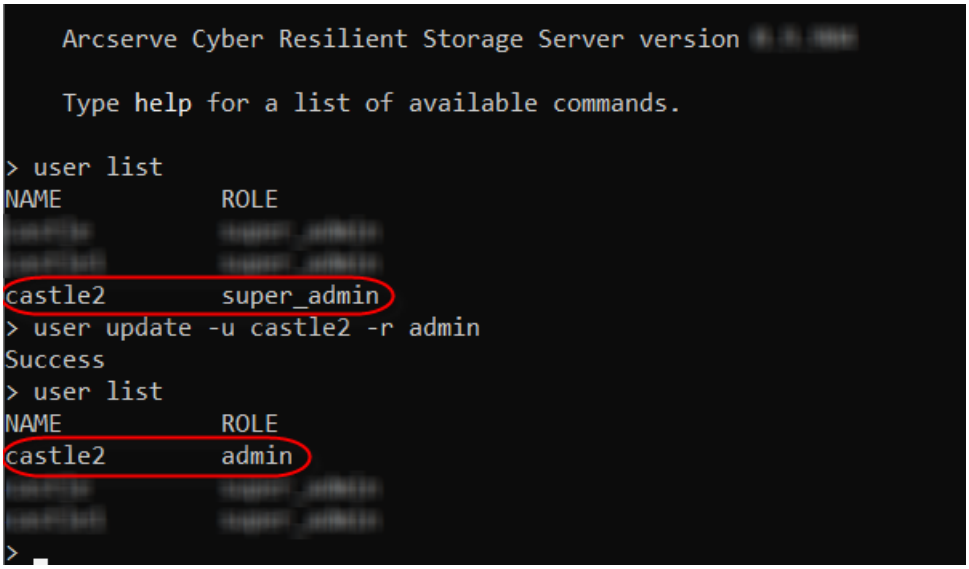
   -u, --username

   Username of the account to modify.

   -r, --role

   New role for the new account. Possible choices: admin, super_admin

   The user is updated.



For more user-related commands, see user in the Command Reference Guide.

Create Access Keys

This section provides information on how to create an access key. This access key is used when setting up an Arcserve Cyber Resilient Storage account in UDP and Cloud Console.

For more information, see Add a Cyber Resilient Storage Account in the UDP Solutions Guide.

Follow these steps:

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command and press **Enter**:

   key list

   A list of existing keys is displayed.
3. Next, type the following command press **Enter**:

   key create [-h] -i ID [-c [COMMENT]]

   where

   -i, --id

   Identifier for the access key

   -c, --comment

   Optional comment

   The new key is created and the ID and Secret Access Key are displayed. Copy the key and keep it safe.

   For more key-related commands, see key in the Command Reference Guide.

Chapter 8: Working with Support

This section provides information on how to work with Arcserve Support to troubleshoot your system. Collaborating with our support team to quickly identify and resolve problems will help you get your system back up and running and minimize downtime.

Specifically, this section contains the following topics:

Upload Support Bundle

This section provides information on how to create and upload a support bundle.

By generating a support bundle, you can securely share logs, configuration details, and other diagnostic information that helps the Arcserve Support team pinpoint issues and provide a quick resolution.

Follow these steps:

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command and press **Enter**:

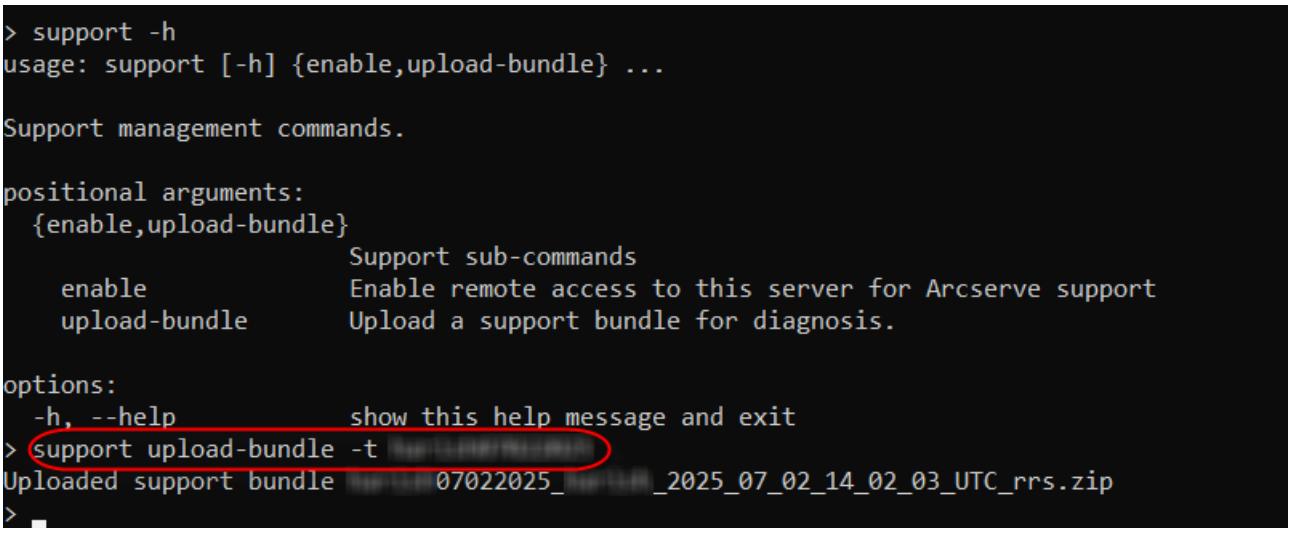
   support upload-bundle [-h] [-t TAG]

   where

   -t, --tag

   An optional tag to easily identify the support bundle. This tag must be a single string.

   Note: By default, the bundle name is prefixed by the tag, followed by the machine name and the time at which the support bundle was generated. Use the tag to make the bundle easily identifiable.



The support bundle is created and uploaded to a relay server from where Arcserve Support can access and read through the bunde to diagnose the issue (s) and provide a solution.

Enable Remote Access for Support

This section provides information on how to enable remote access for Arcserve Support.

Follow these steps:

1. Log in to the Arcserve Cyber Resilient Storage Server.
2. At the command prompt, type the following command and press **Enter**:

   support enable [-h] [-r RELAY] [-p PORT]

   where

   -r, --relay

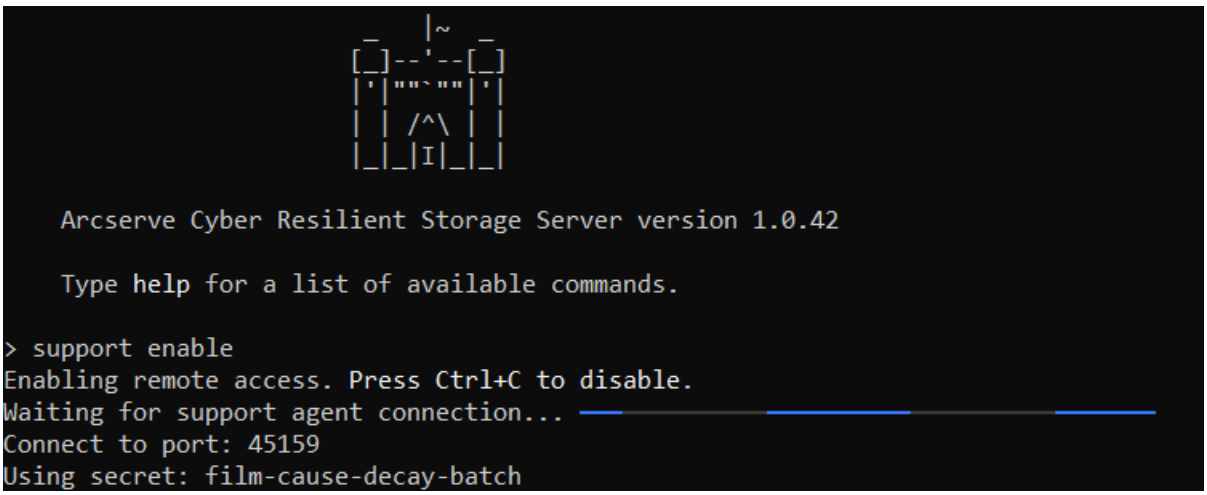
   Overrides the relay server address (optional).

   Default: ''

   -p, --port

   Overrides the relay server port (optional).

   Default: 0



A random port number and a password are generated. The support user must enter the port number and secret key at their end to connect to your Arcserve Cyber Resilient Storage Server via the support tunnel. The port number-password combination can be used only once.

In this example, the port number is *45159* and the password is *film-cause-decay-batch*.

When a support user is connected, the following message is displayed on your CLI:

"*Remote support access has started. Use Ctrl+C at any time to stop it.*"

Note: After support access is disabled, use the following command to make sure that the appliance is locked and access to external users is restricted:

support enable [-h] [-r RELAY] [-p PORT]

Chapter 9: Common Errors and Issues

This chapter provides information about the most common errors and issues encountered when deploying or managing the Arcserve Cyber Resilient Storage Server. Specifically, it covers the following topics:

Unable to Access Root Shell

Symptom

Unable to access the root shell from the admin or superuser account. Both these accounts have limited commands with which users can manage and troubleshoot the system.

Solution

You can only use commands available in the Arcserve Cyber Resilient Storage Server CLI. Contact Arcserve Support for assistance with commands outside the scope of the CLI.

Unable to Add Disks to Pool Created with One Disk

Symptom

After deleting the default pool, created a new pool and added one disk. While trying to add another disk, I get the following error:

"*Adding disk failed. Error: Unable to add disks to pools created with one disk.*"

Solution

Arcserve Cyber Resilient Storage Server does not support adding disks to single disk (initial) pools.

Device Name Changes on Reboot

Symptom

Device name, especially the OS drive partition name changes every time on reboot.

Solution

Device numbers are dynamically assigned during the boot process and the order in which devices are discovered can vary. Arcserve Cyber Resilient Storage Server relies on Device GUID.

Difference in Data Store Sizes

Symptom

The same data store shows different sizes in UDP Console and Arcserve Cyber Resilient Storage Server.

Solution

For Arcserve Cyber Resilient Storage Server v1.0, all storage reporting is only from the CLI.

Different Notations in CLI and UDP Console

Symptom

Why does the Access Key use different notations in the UDP console and CLI?

Solution

The Access Key is referred to as ID in the Arcserve Cyber Resilient Storage Server CLI while in the UDP console, it is referred to as Access Key.

Incorrect filesystem Free Space

Symptom

When a disk of higher capacity is added to a RAID array, the free space command does not take the higher disk space into account and shows incorrect information.

Solution

If the new disk is of lower capacity than the already existing disks, the system will throw an error. If the disk capacity is higher than that of the other disks in the pool, it will only use the size of the already existing disks. This is the expected behavior of a RAID array.

IP Address Format Expectation Unclear

Symptom

Users are unable to continue because IP address format expectation is not clear; they would not know that masking is required.

Solution

The IP address must be entered in CIDR format so that it is masked.

No validation message displayed even if an incorrect key is entered

Symptom

When adding an Arcserve Cyber Resilient Storage account to UDP, there is no validation message displayed even if an incorrect key is entered. The system accepts and saves the configuration regardless of the key's validity.

Solution

This is a known limitation with Arcserve Cyber Resilient Storage v1.0.

Unable to Reset Password for Admin/Superuser Account

Symptom

When a user forgets their login password, they are unable to reset the password for their admin/superuser account.

Solution

Users cannot reset the password on their own. Contact Arcserve Support to do a repair install.

Pool Creation Fails in 2-Disk Setup

Symptom

Pool creation fails in a 2-disk setup with '*Mirror Redundancy Not Supported*' error.

Solution

This is expected behavior for Arcserve Cyber Resilient Storage Server v1.0.

Can a user customize the RAID level?

Symptom

Does Arcserve Cyber Resilient Storage Server allow users to decide which RAID to use (RAIDZ1/2/3) when creating a pool?

Solution

Only RAIDZ1 is available for Arcserve Cyber Resilient Storage Server v1.0 if you are configuring a pool with more than three disks.

Rebuild Arcserve Cyber Resilient Storage

In case the installation becomes non-operative or you are unable to boot because of a hardware failure of the OS disk or any other Operating System issue, if the data store disk is separate, you can always do a repair installation to rebuild the Arcserve Cyber Resilient Storage box.

See Recovering Installation Environment for more information.

Rebuild UDP

If your UDP RPS server crashes but the Arcserve Cyber Resilient Storage Server is intact, you can recreate the data store with the import data store option. Follow the steps below to rebuild UDP:

- Reinstall UDP
- Create a new access key ID/secret key combination
- On the UDP server, create a new authentication profile
- Use the new authentication profile to import the data store by pointing to the existing pool, filesystem, and port

See the *UDP Solutions Guide* for more information.

Unable to Boot ISO with Secure Boot Enabled

Symptom

If Secure boot is enabled, the ISO does not boot. It goes into PXE boot mode.

Solution

Secure boot is not supported for Arcserve Cyber Resilient Storage v1.0.

Why am I unable to import ad hoc snapshots?

Symptom

Why am I unable to import the ad hoc snapshot that I created and why do I see no record of it in the logs?

Solution

You can only import a snapshot as a read-only data store in Arcserve Cyber Resilient Storage Server v1.0. Regular snapshot (read-write) import only works from the Show Snapshots list window in UDP and Cloud Console.

Can the user check the storage allocation (used space and free space) report on UDP?

Symptom

As a user, can I check the storage allocation report on UDP?

Solution

All storage reporting is only from the Arcserve Cyber Resilient Storage Server CLI.

As long as the logs command is running, the terminal does not time out

Symptom

As long as the logs command is running, the terminal does not time out.

Solution

This is expected behavior for Arcserve Cyber Resilient Storage Server v1.0.

Chapter 10: Appendix

This section contains the following topics:

Command Reference

The Arcserve Cyber Resilient Storage documentation also includes a Command Reference Guide that contains the list of the available shell commands, along with the syntax and description. For more information, see the Command Reference Guide.