Arcserve Cyber Resilient Storage

Version 2.1

Installation and Setup Guide

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.

© 2026 Arcserve, including its affiliates and subsidiaries. All rights reserved. Any third-party trademarks or copyrights are the property of their respective owners.

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 1
Chapter 2: Overview 2
Chapter 3: Version Compatibility and Licensing 3
Chapter 3: Registration and Management Changes 4
Chapter 4: How to Install Arcserve Cyber Resilient Storage 5
Pre-Installation Checklist 6
Hardware Requirements 7
TCP/Network Requirements 12
Download ISO File 16
Create Bootable Media 17
Install Arcserve Cyber Resilient Storage 18
Complete Initial Configuration 20
Troubleshooting Options 23
Recovery vs Reinstall 24
Recovery 24
Reinstall 24
Differences 24
Chapter 4: Secure Boot 26
Integration with Immutability 26
Platform and Deployment Support 27
Key and Trust Management 27
Update and Upgrade Behavior 27
Benefits 27
Enable Secure Boot 28
Enable Secure Boot on VM 29
Enable Secure Boot on Arcserve Cyber Resilient Storage 31
Enroll MOK 32
Chapter 5: Deployment in Disconnected Environments 34
Chapter 6: System Health and Status Login Banner 37
Issue Resolution Guidance 39
Chapter 7: Upgrade Arcserve Cyber Resilient Storage 41
Download and Install Updates 42
Offline Update using Removable Media 44
Chapter 7: Post-Update Configuration Actions 46

Check for System Configuration and Security Policies 48
Apply Configuration Changes 49
Chapter 8: Recover Installation Environment 50
Import Pre-Existing Storage Pools 51
Chapter 9: Configure Storage 52
Naming Conventions 53
Create Storage Pool 54
Create filesystems 56
Create Data Access Token 58
Add Disk to Pool 59
Replace Disk in Pool 60
Manage Spare Disks 61
How to Use Spare Disks 62
Chapter 10: Support for Jumbo Frames 64
Chapter 11: Manage Disk Encryption 65
Disk Encryption 66
Before you begin 66
How Automatic Unlocking Works 68
Create an Encrypted Pool 70
Encrypt an Existing Pool 71
Monitor Encryption Progress 73
Verify the Result 74
Important Considerations 75
Verify an Encrypted Pool 76
Disk Encryption Status Values 77
Verify the Result 78
Important Considerations 79
Configure Security Alerts 80
Verify the Result 81
Important Considerations 82
Maintain Access Through System Updates 83
Disable Boot Measurement Checks 84
Recover and Re-enroll Pools 85
Recover a Partially Locked Pool 86
Important Considerations 87
Chapter 12: Network Management 88

Network Profile Management 89
Create Network Profile 90
List Network Profile 92
Modify Network Profile 94
Delete Network Profile 96
Switch Between Network Profiles 97
Network Bonding 98
Create Network Bond 99
Modify Network Bond 101
Delete Network Bond 102
Chapter 13: Alert Management 103
Storage Alerts 104
SMART Disk Alerts 105
Configure Email for Alerts 107
Configure Alerts 109
Chapter 14: User Management 110
Create User 111
Update User 113
Chapter 15: Time Server Management 114
NTP Falseticker Detection and Time Source Recommendations 115
Considerations for Customer-Managed NTP Servers 116
Configure Time Servers 117
Chapter 16: Work with Support 118
Generate Support Bundle 119
Upload Support Bundle 120
Enable Remote Access for Support 121
Write Support Bundle to USB Drive 123
Chapter 17: Migrate Data Stores from OneXafe 125
Chapter 18: Common Errors and Issues 126
Storage Creation Fails with "No available disks found" Error 127
Unable to Access Unconstrained Shell 128
Unable to Add Disks to Pool Created with One Disk 129
Device Name Changes on Reboot 130
Difference in Data Store Sizes 131
Different Notations in Shell and UDP Console 132
Incorrect filesystem Free Space 133

No validation message displayed even if an incorrect key is entered 134
Unable to Reset Password for Admin/Superuser Account 135
Rebuild Arcserve Cyber Resilient Storage 136
Rebuild UDP 137
As long as the logs command is running, the terminal does not time out 138
Chapter 19: Appendix 139
Command Reference 140

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 use either a hardware Raid or the CRS SW RAID for storage integrity

The Arcserve Cyber Resilient Storage Server is managed through a Command Line Interface (CLI) also referred to as the shell or CRS shell. 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 Shell:** Arcserve Cyber Resilient Storage Server shell

Chapter 2: Overview

This guide provides a comprehensive walkthrough for the installation and setup of Arcserve Cyber Resilient Storage, also referred to as CRS Server. It is intended to help you install, configure, and get started with Arcserve Cyber Resilient Storage and covers the following:

- Hardware and network prerequisites
- Types of installation
- Initial configuration
- Storage management
- Network and storage setup
- Alert management
- User management
- Time server management
- Upgrade types and procedures
- How to engage with Support
- Issues and troubleshooting

Chapter 3: Version Compatibility and Licensing

Arcserve Cyber Resilient Storage and Unified Data Protection (UDP) versions are generally interoperable. Older versions of UDP can work with newer versions of Arcserve Cyber Resilient Storage, and vice versa. However, Arcserve Cyber Resilient Storage activation is version-specific and depends on the UDP version and corresponding license.

Arcserve Cyber Resilient Storage (CRS) licensing is separate from Arcserve UDP licensing and requires customers to license both the source data protected in UDP and the CRS storage capacity. CRS is licensed as an upfront annual subscription based on the amount of data stored in its immutable storage destination (BETB), regardless of data type. Capacity is licensed in 1 TB increments, with each CRS destination requiring its own licensed capacity allocation. The licensed capacity determines the maximum amount of data (BETB) that can be stored in CRS.

Keep the following in mind:

- When buying Arcserve Cyber Resilient Storage, you must specify the UDP version in use.
- If multiple UDP versions are deployed, you must allocate Arcserve Cyber Resilient Storage licensing appropriately for each version.
- If you want to upgrade UDP, you must place a Free of Charge (FOC) order to ensure that your existing Arcserve Cyber Resilient Storage license remains valid and continues to work with the upgraded UDP Console.

Chapter 3: Registration and Management Changes

Arcserve Cyber Resilient Storage 2.1 uses the mechanism that was introduced in UDP 11 to integrate with the Arcserve Console. Arcserve Cyber Resilient Storage registers itself as a managed object in Arcserve Console (SaaS or on-premises), eliminating the need for access keys and secret keys. After registration, the Console can directly manage storage and networking through REST APIs.

This behavior differs from Arcserve Cyber Resilient Storage versions 1.0 through 1.6, which used access keys and secret keys to establish a data path to the Recovery Point Server (RPS).

Customers using UDP 10.2 or later can continue to deploy Arcserve Cyber Resilient Storage 2.1 in their environments. However, because earlier RPS and Gateway versions do not support the managed-object model, direct management through the Console is not available in those environments. To maintain compatibility with UDP 10.2 and UDP 10.3, Arcserve Cyber Resilient Storage 2.1 continues to use the access key and secret key method to establish the data path to the RPS.

Note: UDP Console supports only the access key and secret key method for establishing the data path. The managed-object model is supported only in Arcserve Console, whether deployed as SaaS or on-premises.

The following table provides a version compatibility matrix for Arcserve Cyber Resilient Storage, showing the Arcserve Console and UDP versions supported under both the managed-object and legacy registration models.

CRS Version	Release Date/Tentative Release Date	Arcserve Console version (Full Compatibility)	Arcserve Console (RPS Version - Legacy Mode)
CRS 1.0	23-Jul-25	UDP 10.2	UDP 11
CRS 1.5	6-Nov-25	UDP 10.3	UDP 11
CRS 1.6	3-Mar-26	UDP 10.3	UDP 11
CRS 2.0	3-Jul-26	UDP 11.x	UDP 10.2, UDP 10.3
CRS 2.1	10-Nov-26	UDP 11.x and above	UDP 10.2, UDP 10.3

Chapter 4: How to Install Arcserve Cyber Resilient Storage

This section explains how to install and configure Arcserve Cyber Resilient Storage.

Important! If you do not intend to configure a local NTS (Network Time Security) time server, please ensure that the system has access to the external internet. External connectivity is required for Arcserve Cyber Resilient Storage to reach public NTS time servers and maintain accurate system clock synchronization.

Specifically, this section contains the following topics:

- Pre-Installation Checklist 6
- Download ISO File 16
- Create Bootable Media 17
- Install Arcserve Cyber Resilient Storage 18
- Recovery vs Reinstall 24

Pre-Installation Checklist

This section describes the requirements to install and set up Arcserve Cyber Resilient Storage and contains the following topics:

Hardware Requirements

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

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

- Data storage should be redundant so that a drive failure does 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 supports hardware components certified by the RedHat version 9 64-bit (x86_64) (see link).
- To provide redundancy for the OS in case of drive failure, consider using a hardware RAID.

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

Arcserve Cyber Resilient Storage may be deployed on:

- A platform using an IPMI or similar system that manages how the storage drives are utilized.
- A non-managed storage platform with multiple drives available as individual storage drives.

Note: There should be a minimum of one resultant RAID for the OS and one for the data storage. The resulting RAID will be represented to the OS as a single drive that Arcserve Cyber Resilient Storage will use to store data stores on.

Minimum Hardware Requirements

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

Arcserve Cyber Resilient Storage requires two disks or volumes that can be detected by the Operating System with the following specifications:

- One drive/volume with at least 25GB storage for the installation
- One drive/volume for data stores

Hardware RAID Deployment Recommendations

This section presents the recommended hardware RAID configurations, resulting storage capacities, and suggested CPU and memory requirements for Arcserve Cyber Resilient Storage.

Note: If your environment includes hardware RAID adapters, Arcserve recommends using hardware RAID instead of CRS RAID.

RAID 5 volume (including 3.2% Buffer)	RAID5 Usable Capacity (TB) (without 3.2% buffer)	Physical CPUs (Min)	Suggested CPU Cores (Min)	RAM in GB (Min)
4	3.87	1	1	7
8	7.74	1	1	10
16	15.49	1	2	15
24	23.23	1	3	21
32	30.98	1	4	26
40	38.72	1	4	32
48	46.46	1	5	37
56	54.21	1	6	42
64	61.95	1	7	48
72	69.70	1	7	53
80	77.44	1	8	59
88	85.18	1	10	64
96	92.928	1	10	70
104	100.672	1	12	75
112	108.416	1	12	80
120	116.16	1	14	86
128	123.90	1	14	91
144	139.39	1	16	102
160	154.88	1	16	113
192	185.86	1	19	135
224	216.83	1	22	156
256	247.81	1	25	178
288	278.78	1	28	200
320	309.76	1	31	221

CRS RAID Deployment Recommendations

Arcserve Cyber Resilient Storage 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)	3.2% Buffer (in GB)	Minimum No. of Physical CPUs
1.936	3	1	3	1	6	0.064	1
3.872	6	2	3	1	8	0.128	1
7.744	12	4	3	1	12	0.256	1
11.616	18	6	3	2	13	0.384	1
15.488	24	8	3	2	16	0.512	1
19.36	30	10	3	2	19	0.64	1
23.232	36	12	3	3	22	0.768	1
30.976	48	16	3	4	32	1.024	1
34.848	54	18	3	4	32	1.152	1
38.72	60	20	3	4	36	1.28	1
46.464	72	24	3	5	48	1.536	1
54.208	84	28	3	6	48	1.792	1
61.952	96	32	3	7	64	2.048	1
69.696	108	36	3	7	64	2.304	1
77.44	100	20	5	8	64	2.56	1
92.928	120	24	5	10	74	3.072	1
108.416	140	28	5	12	98	3.584	1
123.904	160	32	5	13	98	4.096	1
139.392	180	36	5	14	109	4.608	1
162.624	196	28	7	17	126	5.376	1
185.856	224	32	7	19	144	6.144	1
209.088	252	36	7	21	161	6.912	2
216.832	252	28	9	22	167	7.168	2
247.808	288	32	9	25	190	8.192	2
278.784	324	36	9	28	214	9.216	2

309.76	352	32	11	31	237	10.24	2

Notes:

- Before adding a disk, make sure that it does not contain any filesystems from prior use. Arcserve recommends that you use new disks or disks that have been wiped clean.
- Make sure that a default usable capacity of at least ~3.2% (min 128 MB, max 128 GB) is available for the pool reserved space. This is a portion of a storage pool's capacity that the filesystem sets aside for its own critical operations.

TCP/Network Requirements

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

- At least one supported 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. See Supported Network Cards for more information.
- For a standard installation, just make sure your network cable is plugged into the network card and is active.
- If Arcserve Cyber Resilient Storage 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 table describes the firewall whitelisting requirements for Arcserve Cyber Resilient Storage access, including required ports, S3 URLs, and the URLs used for updates and support tunnel access:

Port No.	Service/Process	Inbound/Outbound	Source IP/Node	Destination IP/Node	TCP/UDP	Comments
22	SSH Admin Access	Inbound	Customer Nodes	CRS	TCP	Internal/LAN only; block at perimeter
53	DNS	Outbound	CRS	DNS Customer Server	TCP/UDP	Required for hostname resolution of Arcserve service endpoints

22-24	Support Tunnel	Outbound	CRS	supportconnect-crs.arc-serve.com	TCP	
443	Update Service	Outbound	CRS	https://-down-load-s.arc-serve.com/arcserve_family_products/crs	TCP	
443	Support Bundle Upload	Outbound	CRS	arc-serve.castle.sup-portbundles.s3-us-west-2.amazon-aws.com	TCP	
50-0-0-50-99	Data Role	Inbound	RPS - Node	CRS	TCP	Intern-al/LAN only; block at peri-meter
4460	NTS-KE key exchange	Outbound	CRS	▪ Time.cloud-flare.com ▪ Nts.netnod.se ▪ Ore-gon.-time.sys-tem76.com ▪ Brazil.-time.sys-tem76.com ▪ ntppool1.time.nl	TCP	
123	NTP Time Sync	Outbound	CRS	▪ Time.cloud-flare.com ▪ Nts.netnod.se ▪ Ore-gon.-time.sys-tem76.com ▪ Brazil.-time.sys-tem76.com ▪ ntppool1.time.nl	UDP	

Important! Some environments may have multiple network interfaces configured on the same subnet for reasons of performance, failover, or reliability. As this requires network features that are currently not supported, Arcserve strongly advises against installing Arcserve Cyber Resilient Storage in such environments.

Supported Network Cards

Arcserve Cyber Resilient Storage supports a broad range of network interface cards (NICs) to accommodate diverse performance, security, and deployment requirements. This section outlines the compatible NICs and their specifications.

Standard Ethernet Cards

- **RedHat**: Supported network card. See RedHat Catalog for more information.
- **Intel Ethernet NICs**: Most server-grade Intel NICs—including 1GbE, 10GbE, 25GbE, 40GbE, and 100GbE models (e.g., X520, X550, X710, E810)—are supported natively via kernel drivers.
- **Broadcom**: NetXtreme series NICs (e.g., BCM5720, BCM57414) are supported, offering speeds from 1GbE to 100GbE. RDMA features are included.
- **Mellanox (NVIDIA)**: ConnectX series Infiniband and Ethernet adapters are supported using MLNX_OFED drivers. The latest MLNX_OFED releases are compatible with CentOS Stream 9.

SFP and SFP+ Module Support

- **SFP Modules (1Gbps)**: CentOS Stream 9 supports standard SFP modules for up to 1Gbps, including single-mode and multi-mode optics from major vendors.
- **SFP+ Modules (10Gbps)**: Widely supported with Intel, Mellanox, and Broadcom NICs. Common modules such as 10GBASE-SR (850nm, short range) and 10GBASE-LR (1310nm, long range) are compatible, provided the NIC and its driver (e.g., ixgbe for Intel X520/X540/X550) recognize the module.
- **Third-Party SFP+ Modules**: Some NIC vendors, particularly Intel, may restrict support for third-party SFP+ modules via firmware. These restrictions can be bypassed for testing using kernel parameters (e.g., ixgbe.allow_unsupported_sfp=1). For production environments, use vendor-approved optics for full support.

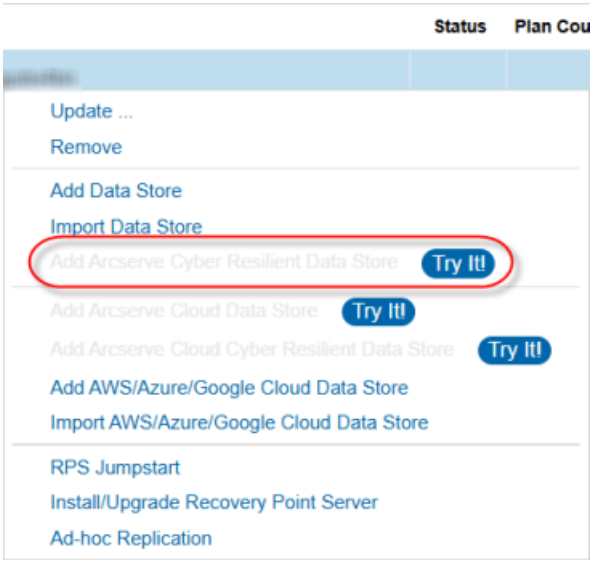
SFP28 Module Support

- **SFP28 Modules (25Gbps)**: Supported when paired with compatible NICs such as Mellanox ConnectX-4/5/6, Intel E810, or Broadcom 25Gb adapters. Native support is available in Linux kernel version 5.14 and later (included in CentOS Stream 9).

Download ISO File

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

- In Arcserve Console, click **Try it** from the Actions menu on the Recovery Point Servers page. The Arcserve Cyber Resilient Storage Trial 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 a Recovery Point Server and from the menu, click **Try It** next to **Add Arcserve Cyber Resilient Data Store**. The Arcserve Cyber Resilient Storage Trial 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 Storage 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 choose between DD mode and ISO mode, we recommend selecting DD mode. This mode creates an exact copy of the ISO file, preserving its original structure. In contrast, ISO mode may introduce a bootloader that could cause compatibility issues in certain environments.

Follow these steps:

1. Download the Arcserve Cyber Resilient Storage 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 from 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.

Install Arcserve Cyber Resilient Storage

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

Follow these steps:

1. Boot the ISO file from the bootable media.
2. Select Arcserve Cyber Resilient Storage.

   The installer displays a list of configuration options that you must complete before beginning the installation. These options are:

   1. Installation Disk
   2. Secure Boot
   3. Begin Installation

   Note: Options 1 and 2 are independent and may be completed in any sequence. Option 3, however can only be completed after both the other options are completed first.
3. When configuration option 1 (Installation Disk) is selected, the disks available for installing the operating system are listed. To select the desired disk, enter the disk number and press **Enter**.

   Note: Contents, if any, of the selected disk will be erased before the installation begins.
4. When configuration option 2 (Secure Boot) is selected, you will be prompted to enter a MOK enrollment password. If you specify a Secure Boot password, the installer creates a temporary boot entry for the Shim UEFI Key Management (MOK Manager) utility. After installation, the system boots into this utility, where you must press a key within 10 seconds and enter the same password to complete MOK enrollment, which is required for Arcserve Cyber Resilient Storage file systems to function when Secure Boot is enabled. If you miss the prompt, the password becomes invalid and you must generate a new password from the command line and repeat the enrollment process.

   Leave the password field blank if you prefer to configure secure boot later from the command line. MOK enrollment can also be initiated or repeated at any time after the installation. See Secure Boot for more information.
5. To begin the installation, enter configuration option 3 (Begin Installation) and press **Enter**.

   The installer completes the OS installation and shuts down.

6. Turn on the Arcserve Cyber Resilient Storage and log in using the following default credentials to complete the initial configuration:
   - Username: *arcserve*
   - Password: *arcserve*

After you sign in to Arcserve Cyber Resilient Storage, the Initial Configuration process starts. When the process completes, the default user account *arcserve* is removed and replaced with the new account you create during setup.

See Complete Initial Configuration for more information.

Important! For the Arcserve Cyber Resilient Storage appliance, a separate *Factory Reset* option is not needed. To perform a clean reset, boot the system from the ISO. This process automatically formats the appliance and reinstalls both the operating system and the required Arcserve components. See Recovery vs Reinstall for more information.

Complete Initial Configuration 20
Troubleshooting Options 23

Complete Initial Configuration

This section guides you through the initial setup of Arcserve Cyber Resilient Storage 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 profile
e. (Optional) Set up the storage pool
f. (Optional) Set up a time server

Note: If the initial configuration is interrupted at any point, you can resume from where you left off by logging in to the shell as user '*arcserve*'.

Follow these steps:

1. Restart Arcserve Cyber Resilient Storage.
2. To log in to Arcserve Cyber Resilient Storage 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 your next log in, use the super admin 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 may also contain special characters, but they are optional.
   - 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. At the prompt, select whether you want to create a network profile, type yes at the prompt . To continue without modifying the network profile, type *No*.
7. Enter a name for the profile, then use the arrow keys to navigate and press **Enter** to select the device.
8. Use the arrow keys to navigate and press the **Enter** key to select the network configuration method.

   Select *ipv4 Auto* or *ipv6 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 ready:

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

9. If you want the network profile to connect automatically, type Yes at the prompt, then specify an *autoconnect priority*. The autoconnect priority can be an integer between -999 and 999.

   The default autoconnect priority value set by the system is 0.

10. At the prompt, specify a value for the *MTU* (maximum transmission unit).The MTU value can be between 60 and 9000.
11. 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 or a three-disk software CRS RAID configuration.

c. To encrypt the storage pool, type *Yes*. You will be prompted to enter an encryption passphrase and confirm it. Then press **Enter**.

Important! Store your passphrase in a secure location. The passphrase is not displayed after it is set, so keep a secure backup of the passphrase in your organization's approved password management or key storage solution.

To continue without creating a storage pool, type *No*. You can create the pools later from the shell. 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.

12. To configure the time server for the system to use, do one of the following:

- Type *Yes* and press **Enter**. Then, at the prompt, type one or more NTP time server FQDNs, separated by commas.

  Notes:

  - Arcserve recommends at least three or more independent NTS servers to be configured for resilient time management. For more information, see Time Server Management.
  - Local NTP servers are used mainly in isolated or air-gapped networks (disconnected deployments) that do not have access to public internet time sources, to maintain synchronized, secure, and reliable time.

- Type *No* to let the system automatically configure the default Network Time Protocol (NTP) time server.

  The initial setup is now complete.

Troubleshooting Options

To troubleshoot the installation when the installer is running, 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.

Recovery vs Reinstall

This section explains the difference between recovery and reinstall when working with Arcserve Cyber Resilient Storage. Although both processes restore a device to a usable state, they serve different purposes and follow different approaches. Understanding this distinction helps administrators choose the appropriate method based on the issue, such as, whether the problem is a temporary failure or requires a complete system refresh.

Recovery

Recovery is a *state restoration* operation. Rather than rebuilding the appliance, recovery assumes that the underlying CRS system remains intact and focuses on returning the appliance to a previously known good state. This can include restoring configuration, services, or system functionality after a failure. Recovery does not reformat the system or reinstall the operating system; it is designed to resolve issues or roll back changes without wiping the appliance.

See Recover Installation Environment for more information.

Reinstall

The reinstall process is almost the same as the installation process, except that it is performed on a system where it has already been previously installed.

Reinstall is used when the appliance is unstable, misconfigured, or when you want to start over completely. It performs a full installation of the Arcserve Cyber Resilient Storage system. When you boot the appliance from the CRS ISO, the system disk is fully formatted and the appliance is rebuilt from scratch. This process reinstalls the CRS mini operating system and the required Arcserve components, returning the appliance to a clean, factory-like state. All existing configuration, data, and prior system state are removed.

See Install Arcserve Cyber Resilient Storage Server for more information.

Differences

The following table explains the difference between the two in detail:

Recovery	Reinstall
Restore CRS to a known, trusted operating state after a failure or corruption.	Replace the entire system with a fresh CRS image.
System instability, failed boot, cor-	Major version changes, severe cor-

rupted runtime state.	ruption, or device repurposing.
Uses the existing immutable CRS image.	Writes a new immutable CRS image.
Preserves user data and configuration stored outside the immutable layer.	User data and configuration are usually wiped unless explicitly backed up.
Minimal; only runtime state and verified components are restored.	Complete reset; everything is returned to factory or baseline state.
Faster	Slower
Low risk, as the trusted image already exists on the device.	Higher risk if backups are incomplete or image selection is incorrect.

Chapter 4: Secure Boot

Secure Boot in Arcserve Cyber Resilient Storage ensures that the system only loads with trusted and signed software components. By enforcing a cryptographically verified boot chain, Arcserve Cyber Resilient Storage protects against low-level tampering, such as bootkits or unauthorized kernel modifications.

Designed for both physical and virtual deployments, Secure Boot works seamlessly with Arcserve Cyber Resilient Storage's CentOS 9-based platform and OpenZFS storage stack, ensuring that all critical components including the bootloader, kernel, and storage modules are authenticated before initialization. This capability is enabled by default and remains enforced across system updates.

Arcserve Cyber Resilient Storage implements a full UEFI Secure Boot chain of trust, where the loader ensures that each stage is valid before proceeding to the next stage. The stages progress as follows:

```
UEFI Firmware → Signed Shim → GRUB2 → Signed Kernel → Signed OpenZFS Modules
```

- The UEFI firmware validates a signed shim loader trusted by standard platforms.
- The shim loads and verifies GRUB2.
- GRUB2 validates and loads the Linux kernel and initramfs.
- The kernel ensures that all required modules, including OpenZFS, are signed and trusted before loading.

This end-to-end validation ensures that only authorized software components are executed during startup.

Integration with Immutability

Arcserve Cyber Resilient Storage's immutable architecture strengthens Secure Boot:

- The operating system is tamper-resistant.
- Updates are delivered as signed and validated packages.

Together, these mechanisms prevent unauthorized changes from persisting and reduce the system's attack surface.

Platform and Deployment Support

Secure Boot in Arcserve Cyber Resilient Storage is designed to work across the following platforms:

- Bare metal UEFI systems
- Virtual environments, including:
  - VMware
  - Microsoft Hyper-V
  - Proxmox/KVM (OVMF/UEFI)

The Arcserve Cyber Resilient Storage ISO is preconfigured to boot successfully with Secure Boot enabled in these environments, removing the need for manual adjustments or disabling platform security features.

Key and Trust Management

Arcserve Cyber Resilient Storage supports Machine Owner Key (MOK) enrollment which allows administrators to trust Arcserve Cyber Resilient Storage-specific signing keys where required.

A guided workflow enables one-time key enrollment without disabling Secure Boot. After enrollment, all required modules, including OpenZFS, load without errors.

Update and Upgrade Behavior

All kernel and module updates are pre-signed and validated, ensuring that the system continues to boot securely after every upgrade without requiring any manual intervention or reconfiguration.

Benefits

Secure Boot strengthens Arcserve Cyber Resilient Storage's security by preventing unauthorized or tampered components from executing during startup. It simplifies deployment by working seamlessly across supported platforms without requiring configuration changes, while also supporting compliance requirements that rely on trusted boot and system integrity.

Enable Secure Boot

This section describes how to enable secure boot for your Arcserve Cyber Resilient Storage system. Enabling secure boot is a three-step process:

- Enable secure boot on your hypervisor.
- Enable secure boot on your Arcserve Cyber Resilient Storage system.
- Enroll MOK in the MOK Manager.

For more information, see the following sections.

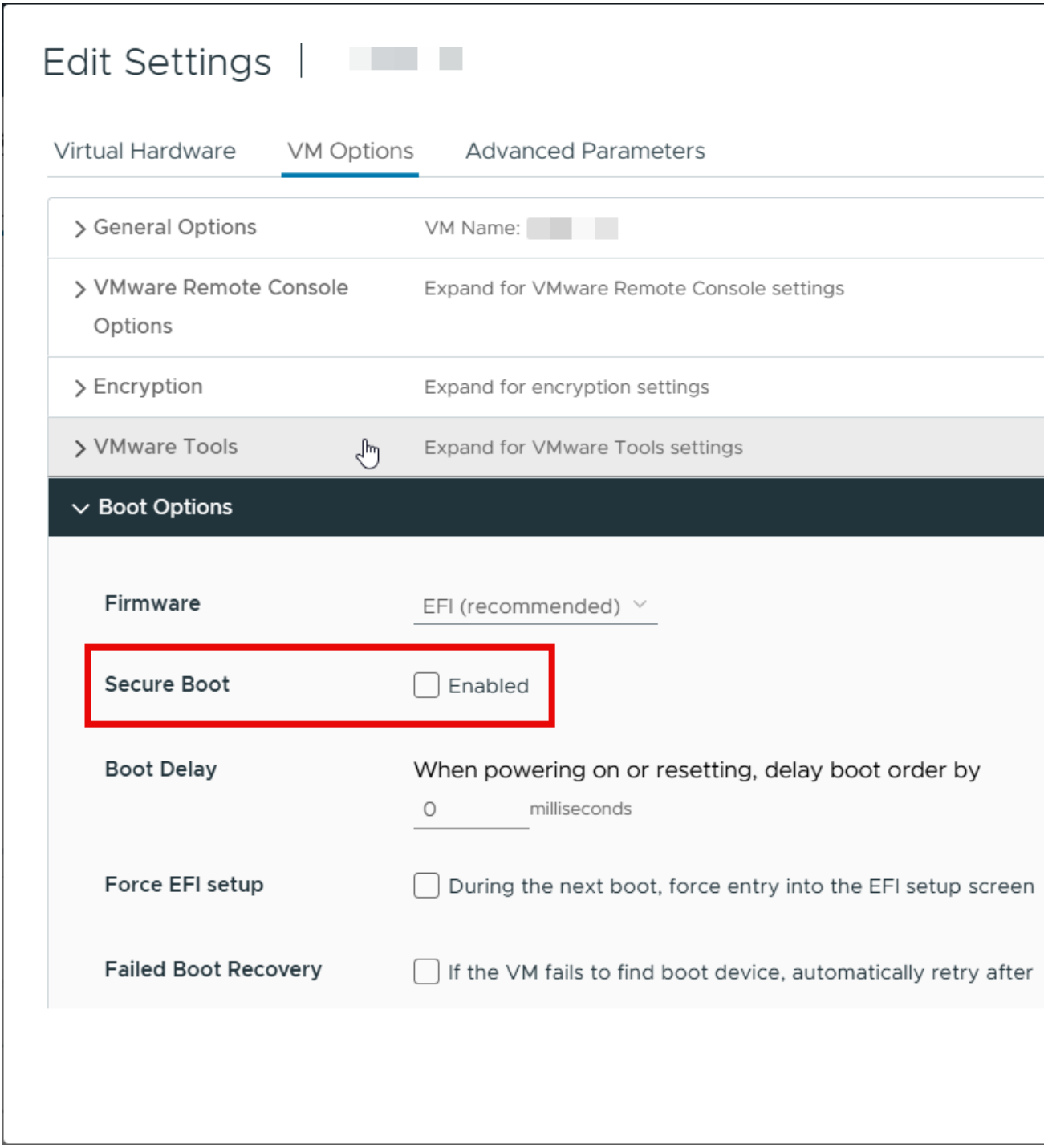
Enable Secure Boot on VM 29
Enable Secure Boot on Arcserve Cyber Resilient Storage 31
Enroll MOK 32

Enable Secure Boot on VM

This section describes how to enable Secure Boot on VMware vCenter. For other supported hypervisors, see the corresponding documentation and perform the equivalent steps in your environment.

Follow these steps:

1. Log in to vCenter.
2. In the left navigation pane, right-click your Arcserve Cyber Resilient Storage instance and select **Edit Settings**.
3. Select the VM Options tab and expand the Boot Options section.
4. Select the **Enabled** check box to enable Secure Boot.


Edit Settings
Virtual Hardware
VM Options
Advanced Parameters
General Options
VM Name:
VMware Remote Console Options
Expand for VMware Remote Console settings
Encryption
Expand for encryption settings
VMware Tools
Expand for VMware Tools settings
Boot Options
Firmware
EFI (recommended)
Secure Boot
Enabled
Boot Delay
When powering on or resetting, delay boot order by
0
milliseconds
Force EFI setup
During the next boot, force entry into the EFI setup screen
Failed Boot Recovery
If the VM fails to find boot device, automatically retry after

5. Click **OK**.

Enable Secure Boot on Arcserve Cyber Resilient Storage

This section describes how to enable Secure Boot on your Arcserve Cyber Resilient Storage system.

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
2. Enroll the DKMS key by typing the following command, then press **Enter**:

   config apply -c secure-boot

   You will be prompted to create a secure boot enrollment password.
3. At the prompt, enter a password and press **Enter**.

   You will be prompted to confirm the password.
4. Enter the password again and press **Enter**.

At this point, secure boot enforcement is initiated. Follow the sequence below to fully enable secure boot:

a. Reboot the system

b. When prompted, enter the enrollment password, then choose DKMS module signing key.

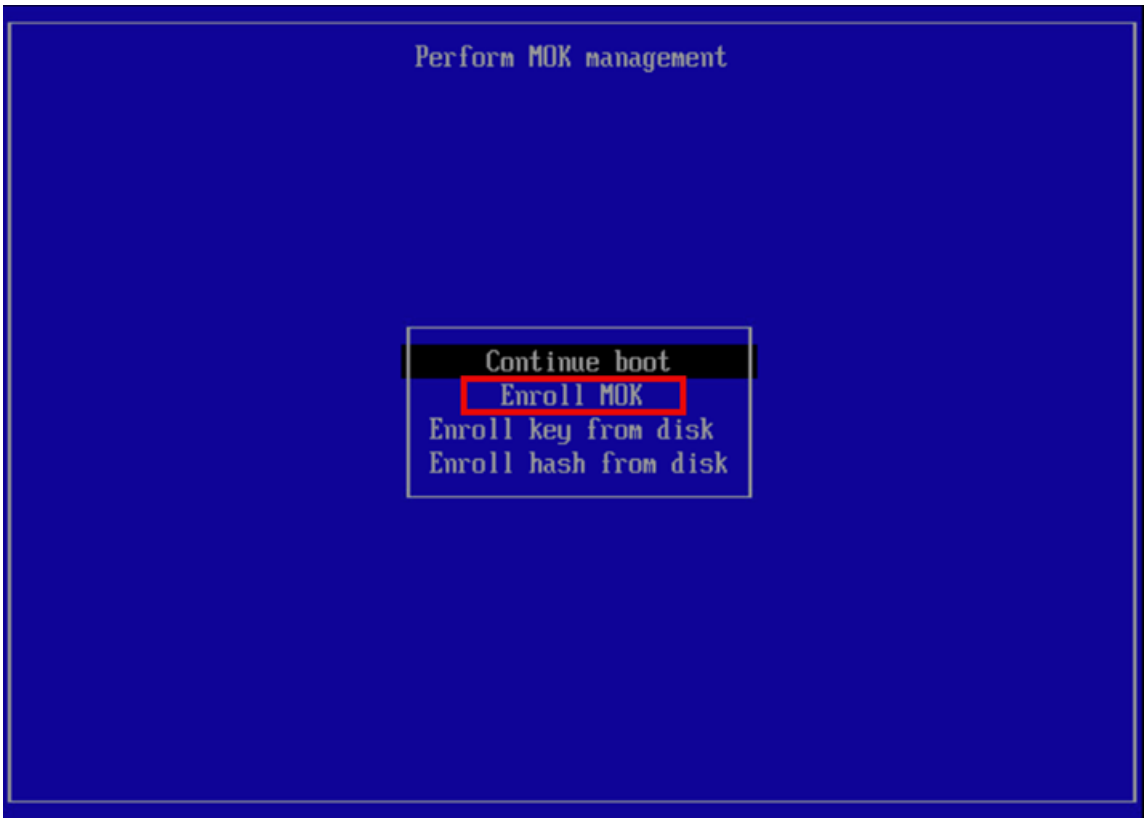
c. Enable secure boot from the MOK Manager screen, a UEFI-based interface used to manage Machine Owner Keys for Secure Boot. For more information, see Enroll MOK.

Enroll MOK

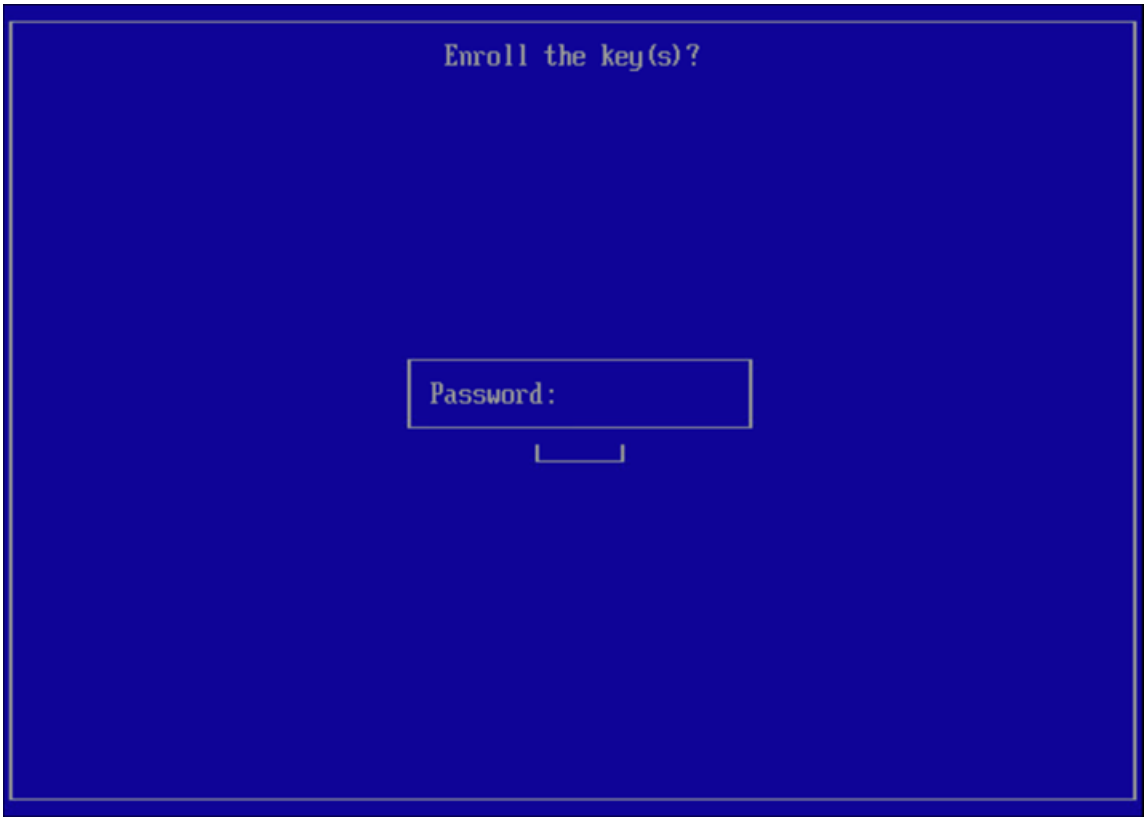
Enrolling a Machine Owner Key (MOK) is a required step in the process of enabling Secure Boot on Arcserve Cyber Resilient Storage. As part of Secure Boot configuration, MOK enrollment establishes trust between the system firmware and Arcserve Cyber Resilient Storage-specific components that are not signed by default platform keys. Completing this step allows Arcserve Cyber Resilient Storage to boot securely while maintaining compliance with Secure Boot requirements and preserving system integrity.

Follow these steps:

1. In the MOK Manager screen, click any key.
2. From the list of options displayed on the screen, select **Enroll MOK**, then select **Continue**.



   A confirmation message is displayed.
3. Select **Yes**, then in the **Password** text box, enter the Secure Boot enrollment password you created.



4. Now click **Reboot**. The system reboots and the login prompt appears.
5. Enter your login ID and password.

Secure boot is now enabled for your Arcserve Cyber Resilient Storage system.

Chapter 5: Deployment in Disconnected Environments

Arcserve Cyber Resilient Storage enables deployment in disconnected environments (dark sites) to support customers operating in security-sensitive setups. Support for disconnected deployment enables Arcserve Cyber Resilient Storage to operate in a fully air-gapped environment, with no connectivity to the internet or external networks. This capability is critical for organizations with strict data-handling policies such as government, defense, critical infrastructure, or regulated enterprises.

In a disconnected deployment, Arcserve Cyber Resilient Storage functions as a self-contained system but continues to enforce data immutability, retention policies, and auditability without reliance on external services. Therefore, support for disconnected deployment is designed to remove dependencies on online update mechanisms and network-based time synchronization while maintaining predictable and verifiable system behavior.

When deployed in a disconnected environment, the following capabilities enable secure and compliant offline operation:

- **Offline Software Updates:** Arcserve Cyber Resilient Storage supports manual software and configuration updates using removable media such as CD-ROM or USB media, eliminating the need for internet connectivity (compatible with CentOS 9 and OpenZFS).

  Compliance-relevant characteristics include:

  - Update packages are prepared, reviewed, and approved outside the disconnected environment before import.
  - Updates are validated locally to ensure integrity and authenticity.
  - Only authorized users can perform the offline update process.
  - The CLI provides a command to export full diagnostics/support bundles to USB media, including logs, configurations, and relevant system metadata.
  - No outbound or inbound network connectivity is required at any stage.

  This update model supports change control, separation of duties, and audit traceability commonly required by regulatory frameworks.

  For more information, see Offline Updates Using Removable Media.

- **Local System Time Servers (No NTS Dependency):** Administrators can configure Arcserve Cyber Resilient Storage to use a local NTS server for time synchronization during installation and ongoing operations, instead of relying on

publicly available internet-based time servers. If the local NTS server is unreachable or fails validation, the installation process provides clear error messaging and allows the administrator to reconfigure or retry.

Compliance-relevant characteristics include:

- Retention periods, immutability enforcement, and audit logs are all based on local system time.
- Time configuration is performed through controlled administrative procedures.
- Time synchronization continues to function using the local NTS server without any internet connectivity required.
- Removal of external time dependencies reduces attack surface and prevents unauthorized time manipulation via network sources.

This approach supports consistent policy enforcement in environments where external time sources are unavailable or disallowed.

Note: When deploying a private NTS time source, ensure that the certificate provided by the NTS server is signed by a certificate authority (CA) trusted by CentOS, that is, a recognized public CA. In addition, the CN (common name) in the certificate must match the server's hostname.

You can find the list of IDP sources supported by CentOS 9 here.

For more information, see step 8 in Complete Initial Configuration.

- **Write Support Bundle Offline to USB:** Arcserve Cyber Resilient Storage supports diagnostics in a way that upholds strict security and immutability requirements by allowing users to generate support bundles offline to a USB drive. This ensures that no data leaves the environment through network channels, prevents exposure of sensitive logs, and maintains the system's immutable state.

  Compliance-relevant characteristics include:

  - Ensures no outbound connections are required, maintaining the strict network isolation that defines disconnected environments.
  - Sensitive configuration or log data never leaves the secure boundary except through an approved, controlled medium (USB drive).
  - Generates diagnostics without modifying the system state or violating immutability guarantees, ensuring compliance with security and operational policies.

- Allows organizations to use established physical media procedures to safely move logs out of isolated environments.
- Ensures troubleshooting workflows do not rely on cloud connectivity, remote endpoints, or internet-based support utilities.
- Enables troubleshooting without ever connecting the environment to a network.

For more information, see Write Support Bundle to USB Drive.

Chapter 6: System Health and Status Login Banner

The System Health and Status banner displays when you log in to Arcserve Cyber Resilient Storage and provides you with immediate visibility into critical system health and status of the system. The banner aggregates and presents relevant system telemetry as soon as you sign in.



By displaying key alerts and status indicators directly upon login, the banner enables you to quickly understand the system's current health and status without running multiple additional commands for each individual issue. This helps identify issues such as hardware warnings and configuration problems at the earliest possible point.

At login, the banner presents concise, actionable information, including:

- Storage degradation, errors and threshold alerts
- Network Time Security (NTS) status
- S.M.A.R.T. disk check status
- Email alert configuration status

By surfacing this information upfront, the banner supports rapid situational awareness and helps administrators reduce the risk of missed hardware failures, or system anomalies during day-to-day operations.

Issue Resolution Guidance

This section provides guidance on how to interpret and respond to system-generated alerts and warnings displayed in the login system health banner. These alerts are designed to highlight critical or degraded system conditions that may impact functionality or user experience. The following recommendations outline the appropriate remedial steps to help you quickly identify the issue, assess its impact, and take corrective action to restore normal operation and minimize disruption.

"Disk SMART check has failed for disk '{disk_name}'."

Run the following disk list command and review the reported faults to assess the severity of the disk failure:

disk list -v -d <disk name>

Based on the findings, determine whether the disk requires replacement. If a replacement is needed, schedule it for the next maintenance window.

"A storage error has been detected on pool '{pool}'."

Run the following pool status command to review any errors reported for the pool:

pool status -v -p <pool_name>

If the issue is identified as a disk-related error, replace the affected disk during the next maintenance window.

"Storage degradation has been detected on pool '{pool}'."

Run the following pool status command to see error listed in pool:

pool status -v -p <pool name>

If this is a disk error, replace disk during the next maintenance window.

"Storage capacity threshold exceeded on pool '{pool_name}'."

Add an additional disk to the impacted pool using the following command:

pool add-disk -p <pool name> -d <disks to add to pool>

"Run [bold]time show[/bold] to diagnose"

This message appears when there is an issue with the network (for example connectivity issues) or the NTS server. Run the following command to diagnose the issue:

time show

"Run [bold]email configure[/bold] to set up the email server."

This message appears when the email server is not configured. Run the following command to set up your email server:

email config

Chapter 7: Upgrade Arcserve Cyber Resilient Storage

This section explains how to upgrade to the latest version of Arcserve Cyber Resilient Storage from an older version. Updates are performed through controlled and well-defined mechanisms that align with its security architecture and deployment model.

- In internet-connected deployments, Arcserve Cyber Resilient Storage can securely download update packages directly from approved sources, allowing timely application of software and content updates while maintaining integrity verification and auditability.
- In a disconnected deployment, where network connectivity is not available or permitted, updates are installed offline using removable media such as CD-ROMs or USB drives. This method enables updates to be introduced into an air-gapped environment in a secure, deliberate, and verifiable manner.

This section provides an overview of the Arcserve Cyber Resilient Storage update process and describes both update scenarios.

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

Download and Install Updates 42

Offline Update using Removable Media 44

Download and Install Updates

This section explains how to download and install updates to upgrade to the latest version of Arcserve Cyber Resilient Storage from an older version.

Follow these steps:

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

   update config show

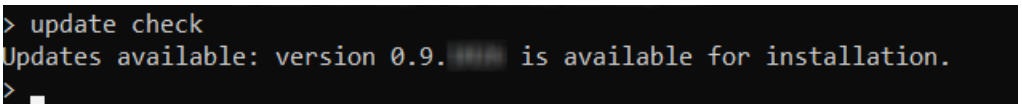
   The download channel and tag are displayed.



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

   update check

   The latest available update is listed.

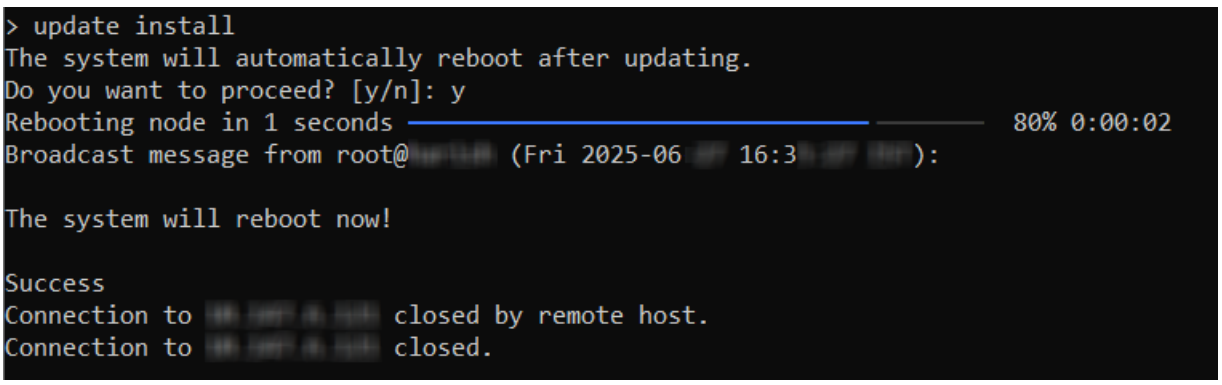


4. Next, type the following command and press **Enter**:

   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 system reboots. Arcserve recommends that you perform the system reboot during a maintenance window.

Offline Update using Removable Media

When Arcserve Cyber Resilient Storage is deployed in a disconnected environment, or when policies require updates to be delivered through non-networked methods, offline updates using removable media provides a secure and auditable way to transfer approved system or application updates into the system. This process reduces exposure to external threats and ensures updates are introduced in a controlled, verifiable manner. Even in internet-connected environments, offline update procedures may still be required for sensitive components, regulated deployments, or continuity operations. Administrators can install the offline updates using removable media, such as CD-ROMs or USB drives, to ensure that the required updates are applied as needed while maintaining immutability and security assurances.

Important!

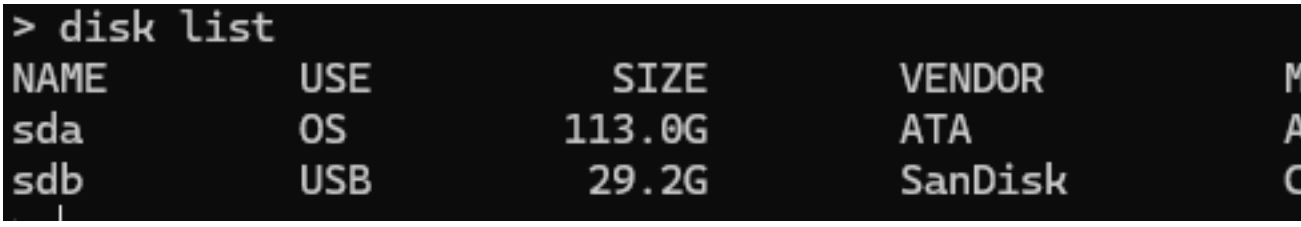
Before you begin the offline update:

- Make sure a CD-ROM or USB drive containing the updated installation media is connected to the system. Confirm that the removable media is properly seated and recognized by the system before starting the update. Use the *disk list* or *update check --offline* command to check if the correct update media is available and connected.
- Make sure that the USB drive you are using to perform the update has at least 16 GB of available storage space.
- Make sure that only one removable media device (such as a USB drive or other external media) containing the correct update media is connected to the system. Connecting multiple removable media devices may cause the update to fail or result in the wrong update media being selected.

Follow these steps:

1. After the USB drive is plugged in, to verify that it is available, enter the following command and press **Enter**:

   disk list

   This is to make sure that the USB drive is properly seated and available so the updates can be copied and installed.

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

   update check --offline

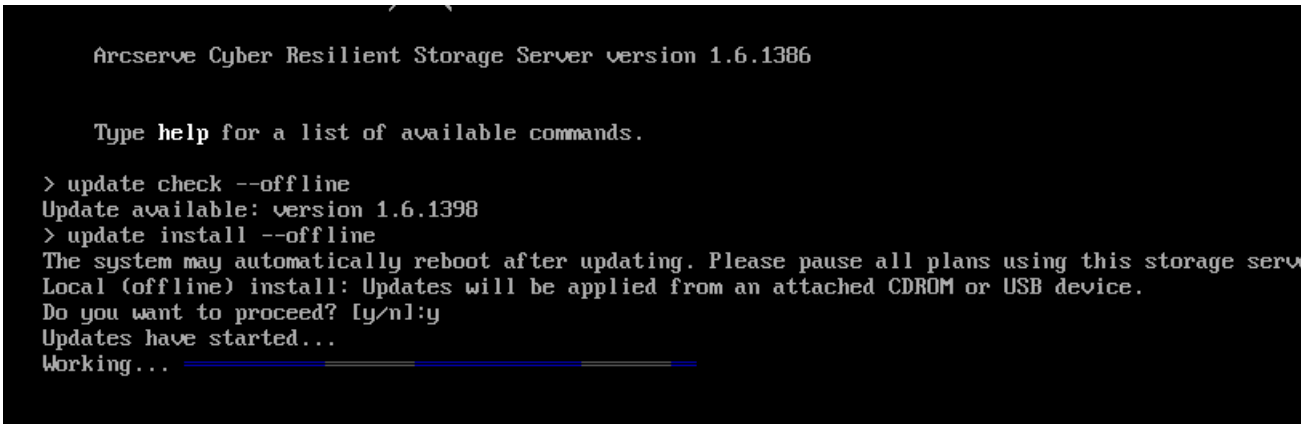


   This command checks if an update is available on the removable media and lists the available update and its version number. If no update is available, the following message is displayed:

   "*No updates found.*"

3. Now, type the following command and press **Enter**:

   update install --offline



   A confirmation message appears.

4. Type *y* to continue.

   Note: Type *n* to discontinue the update and exit the command.

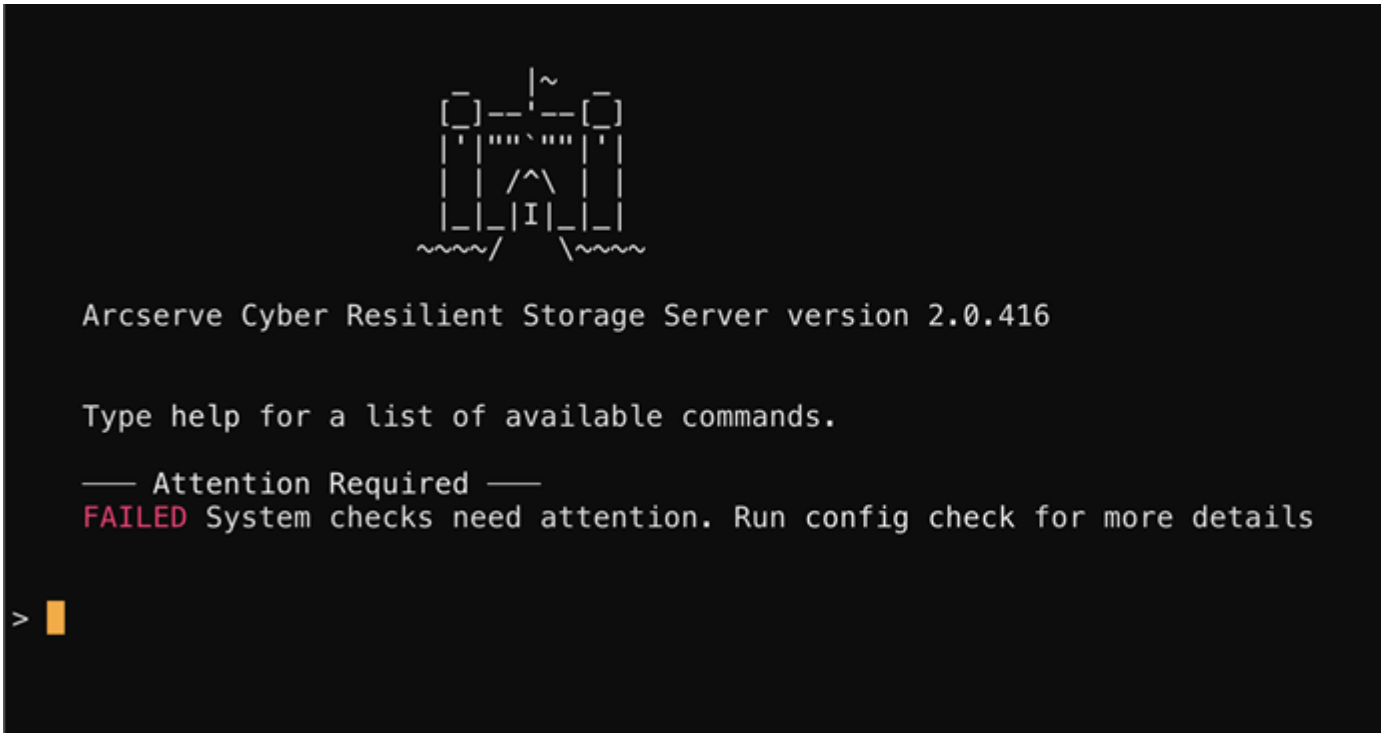
   The update process starts and a progress bar appears. After the updates are installed, the system restarts.

   Enter your credentials to sign in to the updated version of Arcserve Cyber Resilient Storage. You can use the username and password created during or after the initial configuration.

Chapter 7: Post-Update Configuration Actions

After an upgrade, there are some configuration changes that cannot be finalized during the installation and must be applied once the system is running the updated software. The Post-Update Configuration Actions feature helps you complete the configuration changes in a consistent, predictable, and verifiable state.

To manage this, Arcserve Cyber Resilient Storage evaluates the current system and application configuration against the expected state for the new software version. If there are differences, the system notifies you of pending configuration actions when you log in.



You can review and apply these changes at an operationally suitable time using a dedicated finalization command. The process is designed to be transparent and controlled:

- Users can see whether configuration updates are pending
- A clear list of required updates is provided before execution
- Each action is applied in a repeatable (idempotent) way
- Detailed results are reported, including guidance if any step fails

By applying the configuration updates after the system is fully upgraded and running, Arcserve Cyber Resilient Storage avoids partial or inconsistent configurations and applies all changes in the correct runtime context. This approach supports reli-

able system operation while giving administrators clear visibility and control over post-upgrade actions.

Important! Once applied, these configuration changes are permanent and cannot be reversed.

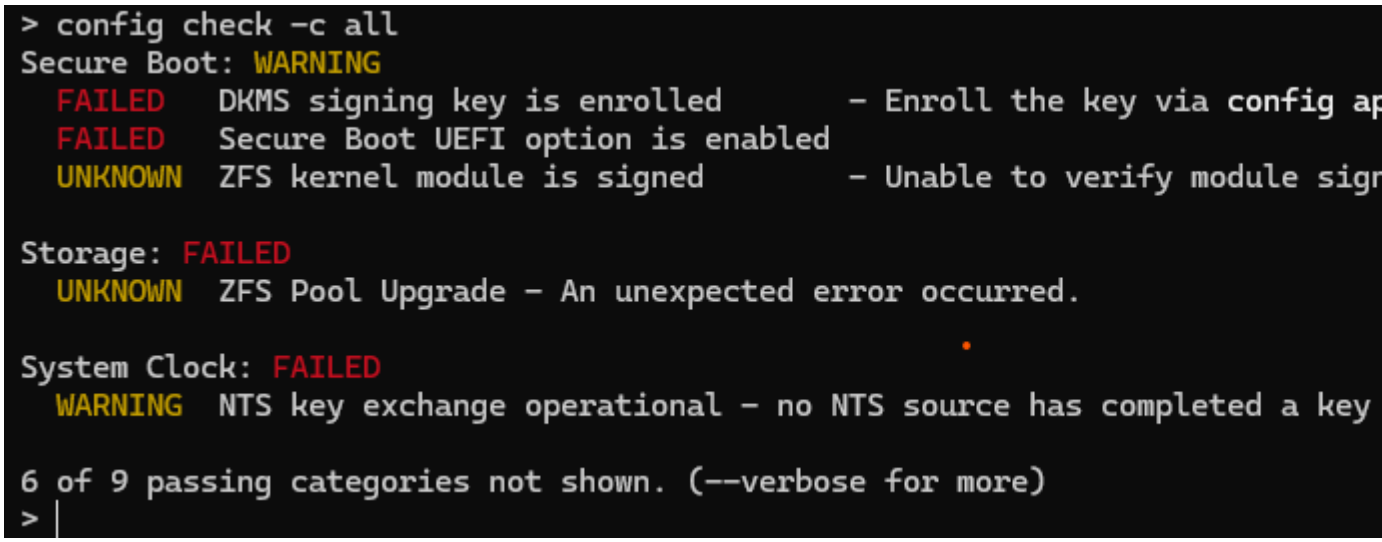
When these commands are run, the system:

- Compares the current system and application configuration with the desired target state defined by the product version.
- Applies all required configuration changes necessary for correctness without requiring further manual steps from the user.
- Produces a clear, human-readable report that shows what changed, what was already compliant, and what failed.

Check for System Configuration and Security Policies 48
Apply Configuration Changes 49

Check for System Configuration and Security Policies

Some settings and policies can only be applied after the upgrade. The configuration check command checks and lists the pending post-update configuration changes.



Use the command in the following syntax.

```
config check [-h] [-v] -c CATEGORY
```

where

-v, --verbose

Shows all information, including from healthy categories.

-c, --category

Possible choices: arcserve-support-access, root-access, secure-boot, system-clock, time, security, system, all

For more information on categories, see check in the Command Reference Guide.

Apply Configuration Changes

This section explains how to run the command that applies configuration changes to the system after an upgrade.

Use the following command to apply to bring the system configuration and security policies into the desired state.

```
config apply [-h] [-v] -c CATEGORY
```

where

-v, --verbose

Shows the per-rule results after applying.

Default: False

-c, --category

Possible choices: arcserve-support-access, root-access, secure-boot, system-clock, time, security, system, all

For more information on categories, see apply in the Command Reference Guide.

Chapter 8: Recover Installation Environment

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

Important! Please be advised that attempting to recover the installation environment entirely on your own without guidance from our support team may result in system instability, data loss, or further complications. To ensure the integrity and proper functioning of your Arcserve Cyber Resilient Storage system, **do not proceed with steps 4 and 5 on your own**.

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

   Important! For assistance on steps 4 and 5, contact Arcserve Support.

Import Pre-Existing Storage Pools 51

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 9: Configure Storage

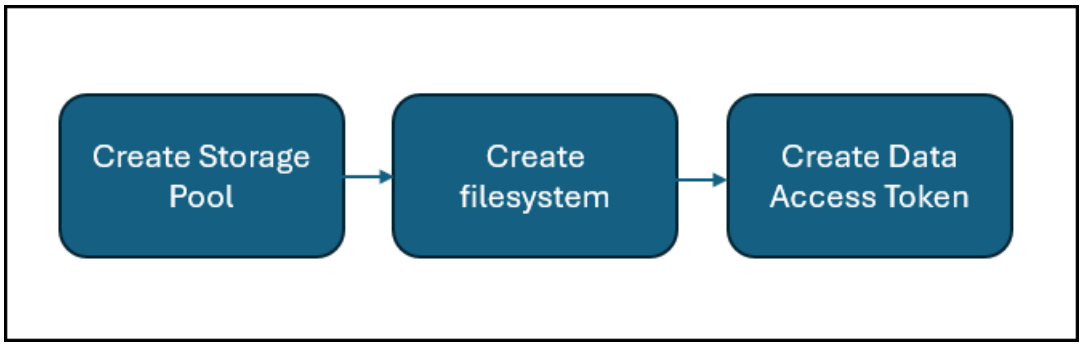
Configuring additional storage on the Arcserve Cyber Resilient Storage enables you to maintain immutability guarantees, avoid service disruption, and achieve seamless integration with existing data structures and access policies.

This process includes critical steps and best practices designed to:

- Maintain system compatibility
- Preserve data integrity
- Minimize performance impact

By following these guidelines, you can effectively scale your storage infrastructure while maintaining operational reliability and security.

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



Naming Conventions 53
Create Storage Pool 54
Create filesystems 56
Create Data Access Token 58
Add Disk to Pool 59
Replace Disk in Pool 60
Manage Spare Disks 61
How to Use Spare Disks 62

Naming Conventions

Follow these rules when naming an Arcserve Cyber Resilient Storage component, including datasets and pools:

- 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 contain alphanumeric characters, 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
  - Must not contain a percent sign (%)
- Dataset names must:
  - begin with an alphanumeric character
  - not contain a percent sign (%)
  - not use reserved names
- 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 a software RAID configuration, a minimum of three disks is required.

Follow these steps:

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

   disk list

   A list of existing disks is displayed. This will show you which disks are available to add to the pool.
3. Type the following command and press **Enter**:

   pool create [-h] -p POOL -d DISKS [DISKS ...] [-P {single,double,triple}] [-e] [-F] [-l {none,signed-boot}]

   where

   -p, --pool

   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.

   -P, --parity

   Parity for the pool.

   Possible choices: single, double, triple.

   -e, --encrypt

   Enables encryption for the pool. If enabled, a passphrase will be prompted for during pool creation. This passphrase will be required to import the pool in the future.

   -F, --force, --no-force

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

   Default: False

   -l, --system-integrity-level

System integrity level for the pool (encrypted pools only).

Possible values: *none*, *signed-boot*

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."

  This happens when you are using a disk that was previously used and the data stored in the disk was not erased. Make sure that the disks listed are the ones you want to use for this pool before proceeding.

  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.

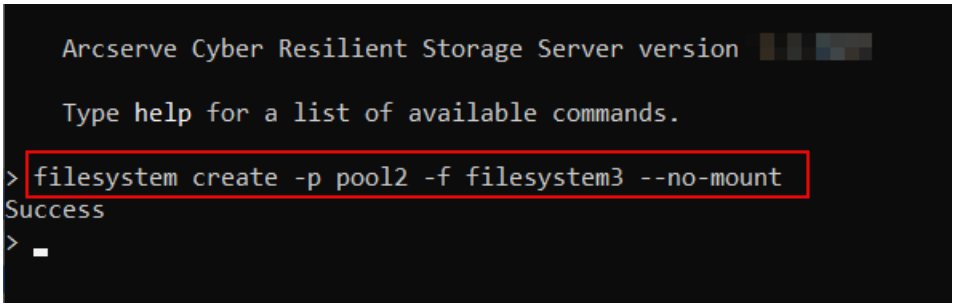
Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
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 [-h] -p POOL -f FILESYSTEM [-m | --mount | --no-mount]



   where

   -p, --pool

   Name of the pool.

   -f, --filesystem

   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 Arcserve Console.

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

Create Data Access Token

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

For more information, see:

- Add a Cyber Resilient Storage Account in the UDP Solutions Guide
- Add an Arcserve Cyber Resilient Storage Account in the Arcserve Console User Guide

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
2. 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.

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 Arcserve Cyber Resilient Storage.
2. To add a disk, type the following command and press **Enter**:

   pool add-disk [-h] [-p POOL] [-t [DISK_TYPE]] -d DISK

   where

   -p, --pool

   Name of the pool.

   -t, --disk-type

   The type of disk to add to the pool. Available types are *data* and *spare*.

   If no type is specified, the disk will be added as a *data* type disk.

   -d, --disk

   Name of the disk(s) to add to the pool.
3. If the pool is encrypted, enter the pool encryption passphrase and press **Enter**. See Disk Encryption for more information.

   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 Arcserve Cyber Resilient Storage.
2. To replace a disk, type the following command and press **Enter**:

   pool replace-disk [-h] -p POOL -d DISK -n NEW_DISK

   where

   -p, --pool

   Name of the pool containing the disk to replace.

   -d, --disk

   Name of the old disk to replace.

   -n, --new-disk

   Name of the new disk that will replace the old disk.
3. If the pool is encrypted, enter the pool encryption passphrase and press **Enter**. See Disk Encryption for more information.

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

   pool list

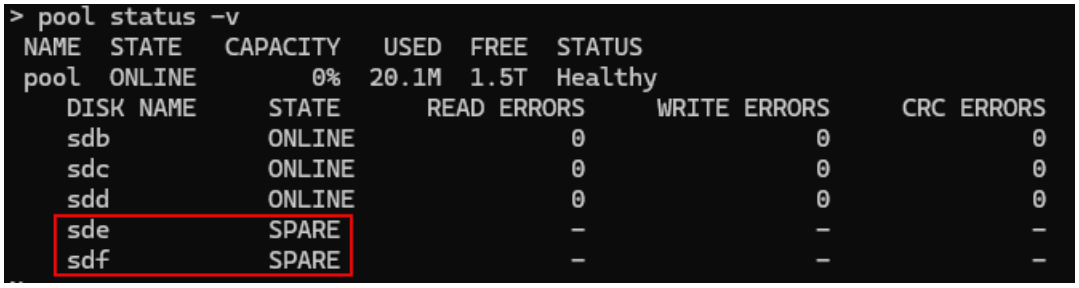
   Note: When an existing disk is replaced in a storage pool, it is not immediately ready for use. The system must perform a process called "resilvering", which involves copying and verifying the data across the new or replaced disk to establish redundancy and consistency within the pool. This process can 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.

Manage Spare Disks

In modern data storage systems, reliability and availability are essential for maintaining data integrity and minimizing downtime. One effective way to improve fault tolerance is by using spare disks in storage pools.

The Arcserve CRS RAID supports the use of spare disks, also known as hot spares. Spare disks are standby drives that automatically activate when an active disk fails. This setup is especially important in environments where continuous data access and uptime are critical.



Adding spare disks to a storage pool is a proactive way to improve reliability, fault tolerance, and recovery speed. Benefits include:

- **Automatic Failure Recovery:** When a disk fails, a spare disk automatically replaces it. The system rebuilds data onto the spare disk, reducing downtime and the risk of data loss.
- **Improved Redundancy:** Spare disks serve as backups for hardware failures. This is especially important in RAID or CRS configurations, where redundancy is vital.
- **Minimized Risk During Rebuilds:** Rebuilding data onto a spare disk is faster and safer than waiting for manual replacement. It shortens the time the pool remains in a degraded state.

How to Use Spare Disks

You can add a spare disk to a storage pool the same way you add a regular disk. However, unlike active disks, a spare disk remains idle until a disk failure occurs. Two types of disks can be added to a pool:

- **Data:** This disk is added as part of the RAID configuration and actively stores user data and parity (if applicable). It participates in day-to-day read/write operations.
- **Spare:** This is an unused disk added to the RAID array that does not store data during normal operation and acts as a standby. It is always online but not used, and remains idle until an active disk fails. In the event of a disk failure, it is automatically brought online to replace the failed disk. The system rebuilds the lost data onto the spare disk using redundancy methods such as parity or mirroring.



For example, in a RAID 5 configuration with four data disks and one spare disk, the data disks store user data. If one disk fails, the spare disk automatically turns online and rebuilds the lost data.

Notes:

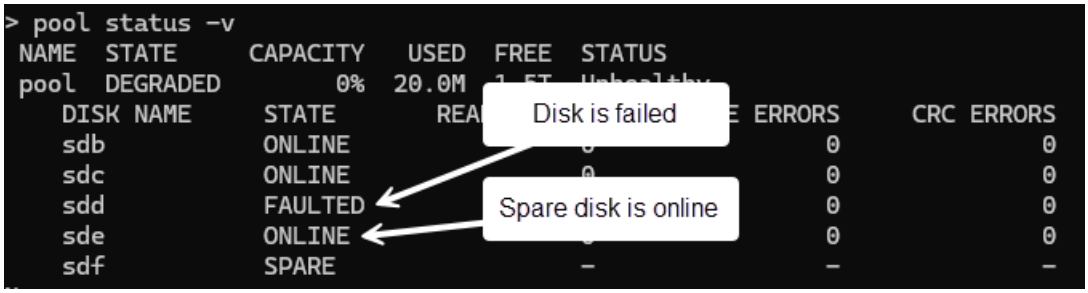
- The size of the spare disk must be equal to or larger than the size of the largest disk in the pool.
- Up to 15 spare disks can be added to a pool.
- If the pool is encrypted, you will be prompted to provide the pool encryption passphrase. See Disk Encryption for more information.

To add a spare disk, type *spare* for the disk type parameter *[-t [DISK_TYPE]]* in the following command:

```
pool add-disk [-h] [-p POOL] [-t [DISK_TYPE]] -d DISK
```

For more information on the parameters, see add-disk in the Command Reference Guide.

After a spare disk has taken over a failed disk, use the *pool status* command to see the status of the disks in the pool. The pool status should show that the spare disk is online and the status of the failed disk is 'FAULTED'.



Once a spare disk becomes active, you can manage the pool in one of the following two ways:

- Replace the failed disk: Add a new disk to the pool. This option requires resilvering, which may take time and resources. Once resilvering is complete, the spare disk is released back to the pool.
- Continue with the spare disk: The spare is already online and resilvered, so no additional effort is needed. Remove the failed disk from the pool using the following command:

  pool remove-disk

  This will return the pool to an online state. Then consider adding a new disk to the pool as a spare to support future failures.

Chapter 10: Support for Jumbo Frames

Arcserve Cyber Resilient Storage supports jumbo frames to boost data transfer efficiency and performance across high-speed networks. By enabling Ethernet frames larger than the standard 1,500 bytes (typically up to 9,000 bytes), the system reduces protocol overhead and minimizes the number of packets sent during large data transfers. This helps lower CPU usage, ease network congestion, and increase throughput for key operations like replication, backup, and recovery.

Jumbo frame support also enhances cyber resilience by enabling faster synchronization and reducing latency during data validation and integrity checks. The Arcserve Cyber Resilient Storage infrastructure works seamlessly with network devices configured for jumbo frames, helping prevent fragmentation and packet loss. These optimizations improve overall performance and reinforce the system's ability to maintain data availability, integrity, and rapid recovery in the face of cyber threats or disruptions.

To enable jumbo frames, specify the maximum transmission unit value for the *[--mtu MTU]* parameter in the following command:

```
network profile modify [-h] -p PROFILE [-d DEVICE] [-b BIND_TO] [--ipv4 IPV4] [--
ipv6 IPV6] [-a ADDRESS] [-g GATEWAY] [--dns [DNS ...]] [--mtu MTU] [--autoconnect
| --no-autoconnect]
            [-r AUTOCONNECT_PRIORITY]
```

For jumbo frames to work seamlessly, note the following:

- All devices in the data path (NICs, switches, routers) must support jumbo frames.
- Mixed environments where some devices support jumbo frames and others do not require careful MTU configuration.
- The minimum and maximum supported values for IPv4 and IPv6 are dependent on what the network interface can support.
- Jumbo frames benefit large data transfers but do not improve performance for small transactions or latency-sensitive applications.

For detailed information on the command syntax and parameters, see modify in the Command Reference Guide.

Chapter 11: Manage Disk Encryption

This section describes how to manage disk encryption and contains the following topics:

Disk Encryption

Disk encryption helps protect data stored on Arcserve Cyber Resilient Storage from unauthorized access. When data at rest is encrypted, information remains unreadable without the appropriate encryption credentials, even if physical storage media is removed, stolen, or accessed outside the intended environment.

When you create an encrypted storage pool, you must specify a passphrase. This passphrase protects the data stored on all disks in the pool.

The passphrase is required not only to import an encrypted pool, but also when performing certain pool management operations, such as adding disks to an existing encrypted pool. If you lose the passphrase, you may be unable to perform administrative tasks on the pool or access the encrypted data.

Once a passphrase is set, it cannot be changed because the passphrase cannot be recovered or modified later. Arcserve strongly recommends backing it up and storing it securely before completing the pool configuration.

Tip: Keep a secure backup of the passphrase in your organization's approved password management or key storage solution.

Important!

- Store your passphrase in a secure location. The passphrase is not displayed after it is set, whether it was configured during the Initial Configuration or later.
- These instructions apply only to Arcserve Cyber Resilient Storage releases that support disk encryption. Installing or updating to a supported release does not automatically encrypt existing pools.

Before you begin

Before enabling disk encryption, make sure that:

- The system is running a release that supports disk encryption.
- A Trusted Platform Module (TPM) is available and functioning correctly. TPM is the security component used for automatic unlocking.
- The pool encryption passphrase is stored securely outside Arcserve Cyber Resilient Storage. You will need it if automatic unlocking fails.
- A current backup of the pool that you want to encrypt exists.
- Adequate maintenance time is available because conversion can take several hours.

Perform all procedures in the management shell. Replace the example pool name (backup) and disk names with values from your environment.

How Automatic Unlocking Works

When you enable encryption in Arcserve Cyber Resilient Storage, the behavior depends on the System Integrity Level configured during encryption.

Arcserve Cyber Resilient Storage encrypts each disk in a pool and stores an unlocking credential in the TPM. This credential allows the pool to unlock automatically during startup. The System Integrity Level determines whether automatic unlocking also validates the platform boot measurements stored in the Platform Configuration Registers (PCRs).

If these measurements change, including after a legitimate software update, the pool might remain locked until it is imported manually with its passphrase. Examples include:

- Adding or removing disks
- Adding or removing memory
- Changing CPU resources
- Modifying boot-related settings
- Other hardware or configuration changes, including software updates

When Arcserve Cyber Resilient Storage detects that the current system state no longer matches the recorded signature, it assumes that the system configuration has changed and does not automatically unlock the encrypted storage pool. In this situation, you must manually unlock and import the pool by using the *pool import* command.

By tying the encryption keys to the validated system state, Arcserve Cyber Resilient Storage helps protect encrypted data from unauthorized access if the underlying system configuration is modified.

The following table describes how automatic unlock works based on the System Integrity Level:

System Integrity Level	Automatic Unlock Behavior
none	Arcserve Cyber Resilient Storage encrypts only the data at rest. In this mode, the encrypted storage can be accessed normally after a reboot because no hardware or system-state validation is performed.
signed-boot	Arcserve Cyber Resilient Storage records its own configuration settings, and the system's hardware and boot con-

	figuration at the time encryption is configured. This recorded state acts as a trusted system signature that is used to automatically unlock the encryption passphrase.

Create an Encrypted Pool

Before creating an encrypted storage pool, identify the disks that are available on the system. Use the *disk list* command to display the available disks and verify the disks you want to use. Creating an encrypted pool permanently erases all data on the selected disks, so carefully confirm the disk names before you proceed.

Note: Replace the example pool name (backup) and disk names with values from your environment.

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
2. Type the following command and press **Enter**:

   pool create -p backup -d sdb sdc sdd sde sdf sdg -P double -e -l signed-boot

   where

   -p, --pool

   Name of the pool containing the disk.

   -d, --disk

   Name(s) of the disk(s).

   -P, --parity

   Parity for the pool.

   Possible choices are: single, double, or triple.

   -e, --encrypt

   Enables encryption

   -l, --system-integrity-level

   Select *signed-boot* to create the encrypted pool with signed-boot protection. Select *none* to create the encrypted pool without signed-boot protection.
3. When prompted, confirm the operation and enter the passphrase twice.

   The pool is encrypted.

   Note: Omitting the *-l* parameter causes automatic unlocking to be enabled without boot-measurement validation.

Encrypt an Existing Pool

This section describes how to encrypt an existing pool.

Before you begin:

- Verify that the pool is in the *online* state.
- Ensure that the pool uses parity-based redundancy.
- Create a current backup of the pool data.
- Make sure that you have enough time for the conversion to complete without interruption.

Notes:

- Replace the example pool name (backup) and disk names with values from your environment.
- Idle spare disks are encrypted and re-added without resilvering.

Important! The pool remains accessible during conversion, but performance might be reduced. Redundancy is temporarily reduced while individual disks are being converted.

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
2. Enter the following command to verify the pool status:

   pool status -p backup

   Confirm that the pool is online before continuing.
3. Enter the following command to start the encryption process:

   pool modify -p backup -e -l signed-boot
4. When prompted, confirm the operation.
5. Enter the new encryption passphrase.
6. Re-enter the passphrase to confirm it.

Arcserve Cyber Resilient Storage begins to convert the pool to an encrypted pool. During conversion, one active disk at a time is processed and the following sequence of activities happens:

a. The disk goes offline.

b. The contents of the disk are erased and the disk is encrypted.

c. The disk contents are rebuilt from the remaining disks.

d. The disk turns online before processing of the next disk begins.

e. Idle spare disks are re-added without resilvering.

Monitor Encryption Progress

This section describes how to monitor the status of an encryption conversion and verify that the process is progressing normally.

Before you begin:

- Keep the shell session that started the encryption process open.
- Open a second shell session to monitor the progress of the encryption process.

Note: Replace the example pool name (backup) and disk names with values from your environment.

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
2. Enter the following command to list the active jobs:

   job list

   Note the job ID associated with the encryption operation.
3. Enter the following command to view detailed information for the encryption job:

   job list -j <job-id>

   Replace <job-id> with the job ID returned by the previous command.
4. Enter the following command to check for the pool status:

   pool status -p backup

   Review the output for:

   - Current pool health
   - Resilvering activity
   - Disk rebuild progress
   - Any warnings or errors
5. Repeat steps 2-4 as needed until the encryption job is complete.

Verify the Result

This section describes how to verify the results of an encryption job.

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
2. Type the following command and press **Enter**:

   pool status -p backup
3. Confirm that:
   - The pool status is online
   - No resilver operations are active
   - All disks have completed encryption processing

Important Considerations

- Do not close the shell session that started the encryption process until the operation completes.
- Do not interrupt the conversion process by rebooting or shutting down the system while encryption jobs are running.
- Running the encryption command in the background by appending the ampersand symbol *&* is not supported.
- If the encryption process is interrupted, contact Arcserve Support before attempting recovery actions.

Verify an Encrypted Pool

This section describes how to verify the state of an encrypted pool after it is created, converted, imported or recovered.

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
2. Type the following command and press **Enter** to display the pool configuration:

   pool list -p backup
3. Type the following command and press **Enter** to display the pool status:

   pool status -p backup
4. Type the following command and press **Enter** to display the disk information:

   disk list
5. Review the output and verify that:
   - Encryption is enabled for the pool.
   - The correct system integrity level is configured.
   - The pool status is online.
   - No resilver operations are active.
   - All encrypted disks are unlocked.
6. Verify that applications and services can access data in the pool.

Disk Encryption Status Values

The following table describes the disk encryption status values reported by Arcserve Cyber Resilient Storage. These values help you determine whether a disk is encrypted and whether it is currently unlocked.

Status	Description
OK	The disk is encrypted and unlocked.
Needs Unlock	The disk is encrypted but remains locked.
-	The disk is not encrypted.

Verify the Result

The verification is successful when all of the following conditions are true:

- The pool status is online
- Encryption is enabled
- The configured system integrity level matches the intended setting
- All encrypted disks report a status of OK
- No resilvering or recovery operations are in progress
- Applications can access pool data successfully

Important Considerations

- Investigate any disk with a status of *Needs Unlock* before returning the pool to production use.
- A system integrity level of *Unknown* does not indicate that integrity validation is disabled. Verify the configuration and resolve the condition before proceeding..
- If the pool is not online or encrypted disks remain locked, review the pool recovery procedures or contact Arcserve Support before attempting recovery actions.

Configure Security Alerts

This section describes how to configure security alerts.

Security alerts help you identify conditions that could prevent encrypted pools from unlocking automatically or indicate potential platform integrity issues. Configure alerts to receive notifications when Arcserve Cyber Resilient Storage detects TPM-related problems, boot integrity changes, or other disk encryption events that might require administrative action.

The following alerts identify conditions that may affect automatic unlocking:

Alert	Severity	Recommended action
TPM missing or inaccessible	Warning	Verify TPM availability and confirm access to the recovery passphrase.
TPM self-test failed	Critical	Contact Arcserve Support.
Boot measurements changed	Critical	Verify whether a planned software update or maintenance activity caused the change. Investigate unexpected changes before accepting a new boot state.

Note: Configure email delivery before creating security alerts. You can use the email test command to verify that notifications are delivered successfully. See Configure Email for Alerts for more information.

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
2. Type the following command and press **Enter**:

   alert create -t system-boot-integrity -r storage-admin@example.com

   Replace storage-admin@example.com with the email address that should receive alert notifications.
3. Type the following command and press **Enter** to verify that the alert was created successfully:

   alert list
4. Type the following command and press **Enter** to test the email delivery:

   email test -r storage-admin@example.com
5. Confirm that the test email is received by the specified recipient.

Verify the Result

The configuration is successful when:

- The alert appears in the alert list.
- The test email is delivered successfully.
- Administrators can receive notifications from the Castle system.

Important Considerations

- Configure at least one alert recipient before enabling disk encryption in a production environment.
- Software updates and firmware changes can modify boot measurements and trigger integrity-related alerts. Review these alerts and verify that the changes were expected before taking action.
- Periodically test alert delivery to ensure that administrators continue to receive notifications after email or infrastructure changes.

Maintain Access Through System Updates

This section describes how to keep pools accessible through a system update.

An update can change the boot measurements used by *signed-boot*. Before updating, note that some pools might not unlock automatically afterward. Make sure you have their passphrases available and pause any backup plans that use the device. Then choose one of the following options..

Disable Boot Measurement Checks

Use this option to prevent a pool from remaining locked after the update because of changed boot measurements. This option temporarily disables boot measurement checks before the update.

Follow these steps:

1. Before installing the update, change the integrity level of each affected pool to *none*.

   ```
   pool modify -p backup -l none
   ```

2. When prompted, enter the pool's current passphrase.
3. Verify that the integrity level is set to *none*.

   ```
   pool list
   ```

   Encryption remains enabled, but boot measurement checks are temporarily disabled.
4. Install the update and restart Arcserve Cyber Resilient Storage when prompted.
5. After the update is complete, restore the pool's protection by setting the integrity level back to *signed-boot*.

   ```
   pool modify -p backup -l signed-boot
   ```

6. Verify that the integrity level is now *signed-boot*.

   ```
   pool list
   ```

Important! Have the pool passphrase available before updating, and pause any backup jobs that use the device. Changing only the -l option updates the integrity level and does not repeat disk conversion.

Recover and Re-enroll Pools

Use this option if you want to keep the current integrity level during the update and recover any pools that do not unlock automatically afterward.

Follow these steps:

1. Install the update and restart Arcserve Cyber Resilient Storage.
2. Check for pools that did not import automatically.

   ```
   pool list-inactive
   ```

3. Import each inactive pool individually.

   ```
   pool import -p backup
   ```

4. When prompted, enter the pool's current passphrase.
5. If Arcserve Cyber Resilient Storage asks whether to enable automatic unlocking in the future, select one of the following:
   - *Yes* to enroll the pool using the current boot measurements and restore automatic unlocking.
   - *No* to import the pool without updating its automatic-unlock enrollment.
6. After the pool is imported, verify that:
   - The pool is available.
   - Any eligible file systems are mounted.
   - Required data services have started successfully.

Important! If a pool that requires recovery does not appear in the inactive pool list, or if the import operation fails, contact support. Do not initialize the disks or recreate the pool.

The same recovery procedure can be used during deployment if the setup wizard detects an existing encrypted pool that it cannot import automatically.

Recover a Partially Locked Pool

This section describes how to recover a partially locked pool. A partially locked pool occurs when some encrypted disks in a pool are unlocked while one or more encrypted disks remain locked. This condition can prevent the pool from being imported completely and typically requires intervention from an administrator to unlock the remaining disks.

A partially locked pool is indicated by an asterisk (*) next to the pool or disk name in command output:

```
NAME    | DISKS     | ENCRYPTED | SYSTEM INTEGRITY
backup* | sde*      | Yes       | Signed Boot
```

In this example:

- backup* indicates a partially imported pool.
- sde* indicates a disk that remains locked.

The disk column can also include spare disks and *missing_...* placeholders for unavailable members.

Important! Unlocking a pool cannot restore a disk that is physically missing or has failed.

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
2. Type the following command and press **Enter** to import the partially locked pool, using its name without the asterisk:

   pool import -p backup
3. If prompted, enter the pool passphrase.
4. Wait for Arcserve Cyber Resilient Storage to unlock the remaining encrypted disks and complete the pool import process.
5. Verify that the import operation completes successfully.

Important Considerations

- Do not initialize disks or attempt to recreate the pool while it is in a partially locked state.
- A partially locked pool can occur if the unlock process is interrupted or if one or more disks fail to unlock during startup.
- If the pool cannot be imported successfully, contact Arcserve Support for assistance before attempting any recovery actions.

Chapter 12: Network Management

The Network Management section provides guidance on configuring, maintaining, and optimizing the network settings required for Arcserve Cyber Resilient Storage to operate reliably and securely within your infrastructure.

This section contains the following topics:

Network Profile Management

Network profiles in Arcserve Cyber Resilient Storage are predefined sets of network and security settings that control how it connects to and behaves on a network. They are used to simplify deployment, enforce consistency, and strengthen security across the environment. Administrators define and assign these profiles to Arcserve Cyber Resilient Storage during deployment and ongoing operations, ensuring that connectivity, access control, and integration with backup or management systems are all handled in a standardized, auditable way.

Arcserve Cyber Resilient Storage provides several network profile management commands that let you define, select, and enforce predefined network configurations without changing the underlying system state. Because the storage is immutable, these commands typically load, activate, or switch between read-only network profiles at runtime instead of modifying files on disk. This approach ensures consistent, tamper-resistant network behavior across reboots while still allowing controlled connectivity changes.

These commands are valuable because they operate outside the data immutability boundary; they manage access and communication, not the stored data itself. This design allows administrators to maintain, monitor, and secure the system without compromising the integrity of immutable storage.

To manage network profiles, use the following command:

```
network profile [-h] {create,list,delete} ...
```

Arcserve Cyber Resilient Storage provides the following network profile management commands:

Create Network Profile

The *network profile create* command creates a new network configuration profile without immediately affecting active networking.

Use the following command to create a network profile:

```
network profile create [-h] -p PROFILE -d DEVICE [-b BIND_TO] [--ipv4 IPV4] [--
ipv6 IPV6] [-a ADDRESS]
            [-g GATEWAY] [--dns [DNS ...]] [--mtu MTU] [--autoconnect] [-r
AUTOCONNECT_PRIORITY]]
```

This command:

- Does not modify live network settings.
- Writes profile metadata to a protected config store.
- May require elevated privileges or an admin role.

Scenario

Create an IPv4 Profile called *foo* on the device *bar*, set to automatically get its IPv4 configuration from the network and to become active immediately.

```
::> network profile create -p foo -d bar --ipv4 auto --autoconnect true
```

Result

A new profile called ‘foo’ created against the device ‘bar’ and activated immediately after creation. This configures a connection on the device ‘bar’, getting its IPv4 configuration details from DHCP in the network.

Scenario

Create an IPv4 Profile called *foo_2* on the device *bar* specifying its address information manually and to become active immediately.

```
::>network profile create -p foo_2 -d bar --ipv4 manual -a 192.168.0.100/24 -g
192.168.0.1 --dns 1.1.1.1 --autoconnect true
```

Result

A new profile called *foo_2* created against the device *bar*. This configures a connection on the device *bar* to use 192.168.0.100 as the address with a netmask of

255.255.255.0 and route through the gateway 192.168.0.1. It will use DNS 1.1.1.1 for all FQDN queries and become active immediately. Since ‘autoconnect’ is set to ‘true’ and the priority has not been specified, it will replace the profile ‘foo’ on device ‘bar’, and become the active profile.

For detailed information on the command syntax and parameters, see create in the Command Reference Guide.

List Network Profile

The *network profile list* command displays existing network profiles.

Use the following command to list network profiles:

```
network profile list [-h] [-d DEVICE] [-v | --verbose | --no-verbose]
```

Scenario

Display all profiles configured in the Arcserve Cyber Resilient Storage device.

```
network profile list
```

Result

```
> network profile list
PROFILE NAME        DEVICE        ACTIVE        ADDRESSES              GATEWAY              DNS
ens192              ens192        True          [redacted]/22          10[redacted]/32      10.[redacted]
lo                  lo            True          [redacted]/8           -                    -
ens224              -             False         -                      -                    -
```

Scenario

Display only profiles set against a specific device.

```
network profile list -d ens192
```

Result

```
> network profile list -d ens192
PROFILE NAME        DEVICE        ACTIVE        ADDRESSES              GATEWAY              DNS
ens192              ens192        True          [redacted]/22          [redacted]/32        [redacted]
```

Scenario

Display all details of profiles set against a specific device.

```
network profile list -d ens192 -v
```

Result

```
> network profile list -d ens192 -v
------------------------------------------------------------
PROFILE NAME          ens192
DEVICE                ens192
ACTIVE                True
TYPE                  802-3-ethernet
MAC ADDRESS           00:50:56:A8:61:A4
AUTOCONNECT           True
AUTOCONNECT PRIORITY  -
METHOD                auto
IPV4 ADDRESSES        [redacted]/22
IPV4 DNS              [redacted]/32
IPV4 GATEWAY          [redacted]/32
IPV6 ADDRESSES        fe[redacted]4/64
IPV6 DNS              -
IPV6 GATEWAY          -
```

For detailed information on the command syntax and parameters, see list in the Command Reference Guide .

Modify Network Profile

The *network profile modify* command modifies a network connection.

Use the following command to modify a network profile:

```
network profile modify [-h] -p PROFILE [-d DEVICE] [-b BIND_TO] [--ipv4 IPV4] [--
ipv6 IPV6] [-a ADDRESS] [-g GATEWAY] [--dns [DNS ...]] [--mtu MTU] [--autoconnect
| --no-autoconnect]
            [-r AUTOCONNECT_PRIORITY]
```

Scenario

Modify an IPv4 Profile called *foo_2* on the device *bar*, set to automatically get its IPv4 configuration from the network.

```
::> network profile modify -p foo_2 --ipv4 auto
```

Result

The result will change the profile called *foo_2* created against the device *bar* to switch from the manual configuration and retrieve the IPv4 network configuration from the network via DHCP.

Scenario

Modify an IPv4 Profile called *foo_2* on the device *bar* to become the active profile.

```
::> network profile modify -p -p foo_2
```

Result

The result will change the profile called *foo_2* created against the device *bar* to become active.

Scenario

Modify the profile called *foo* on the device bar to now specify its IPv6 configuration.

```
::>network profile modify -p foo --ipv6 manual -a 2001:db8::2/64 -g
"2001:db8::1" --dns "2001:4860:4860::8888"
```

Result

Updates the profile *foo* created against the device *bar* to have configuration for the IPv6 network family manually applied. For IPv6, it will use 2001:db8::2 for the address with an address range from 2001:0db8:0000:0000:0000:0000:0000:0000 to 2001:0db8:0000:0000:ffff:ffff:ffff:ffff and route through the gateway at 2001:db8::1. It will use DNS 2001:4860:4860::8888 for all FQDN queries. As the *--set-active* parameter is not specified, it will not become active on device *bar*, leaving configuration *foo_2* as the active configuration there.

For detailed information on the command syntax and parameters, see modify in the Command Reference Guide.

Delete Network Profile

The *network profile delete* command deletes an existing network connection profile.

Use the following command to delete a network profile:

```
network profile delete [-h] profile_name
```

For detailed information on the command syntax and parameters, see delete in the Command Reference Guide .

Switch Between Network Profiles

Arcserve Cyber Resilient Storage lets users operate seamlessly across different environments without changing approved configurations. Administrators can define and lock down preset network profiles—such as a corporate LAN profile, a remote-work profile, or a VPN-enforced public network profile. Users can switch between these profiles as needed, but they cannot modify the underlying settings. This approach ensures consistent security policies, prevents configuration drift, and maintains compliance while still offering controlled flexibility.

You can activate or deactivate configured network profiles as needed using the commands below.

When a network profile is activated, the previously active network profile, if any, is deactivated. To activate an inactive network profile, use the following command:

```
network profile up [-h] -p PROFILE
```

To deactivate an active network profile, use the following command:

```
network profile down [-h] -p PROFILE
```

Important! When multiple network profiles are configured to autoconnect (that is, their autoconnect setting is set to *True*), the device selects the profile based on the following rules:

- Profiles with a lower autoconnect priority value are chosen first because a lower value indicates a higher priority.
- If multiple profiles share the same priority, the device connects to the profile that was most recently activated.

For detailed information on the command syntax and parameters, see up and down in the Command Reference Guide.

Network Bonding

Network bonding is a networking capability that combines two or more physical network interfaces into a single logical interface. Network bonding enables administrators to combine multiple physical network interfaces (NICs) into a single logical interface, improving network reliability and availability. Network bonding is fully integrated into the web-based management interface, allowing you to create, configure, monitor, and manage bonded interfaces without relying on command-line tools.

Arcserve Cyber Resilient Storage uses the *active-backup* (Active/Passive) mode, in which one NIC actively handles all traffic, while the standby NIC automatically takes over in the event of a failure, ensuring uninterrupted connectivity without requiring complex switch-side configurations.

Administrators can easily assign member NICs, view real-time status, and manage both runtime and persistent configurations. Built-in role-based access control (RBAC) ensures that only authorized users can make network changes, while comprehensive audit logging provides full visibility into all configuration activities.

By simplifying setup and management, network bonding enhances operational efficiency, reduces configuration errors, and strengthens system resilience, delivering a consistent and modern management experience across the Arcserve Cyber Resilient Storage system.

Create Network Bond

This section describes the prerequisites for creating a network bond and the steps required to create a bond. Before creating a Bond device, it is important to understand how profiles are managed and what conditions must be met for successful creation.

Prerequisites

- Although a Bond device requires a profile to operate, the individual member devices must not have an active profile assigned at the time of Bond creation. If a device already has an active profile, the system prevents the Bond device from being created and displays an error. To avoid this, make sure that any existing profile on the device is removed or brought down before you begin. Once the device no longer has an active profile, it becomes eligible to be added as a bond member.
- A bond device must include at least two member devices. These devices work together as part of the bond configuration and are required for the bond to function correctly.

Follow these steps:

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

   ```
   network bond create [-h] -b BOND -m MEMBERS [MEMBERS ...]
   ```

   where

   -b, --bond

   The name for the bond.

   -m, --members

   The member devices in the bond. Enter the member names separated by a space. There must be at least two members in a network bond.

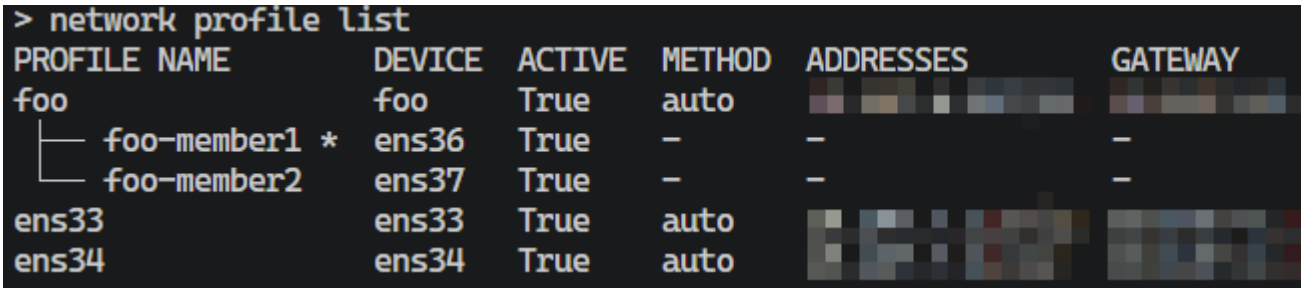
   ```
   > network bond create -b foo -m ens36 ens37
   Success
   ```

   The system automatically creates a connection profile for the bond device and the members that are a part of the bond.

2. Verify that the bond is created. To do this, at the command prompt, enter the following command and press **Enter**:

```
network profile list
```

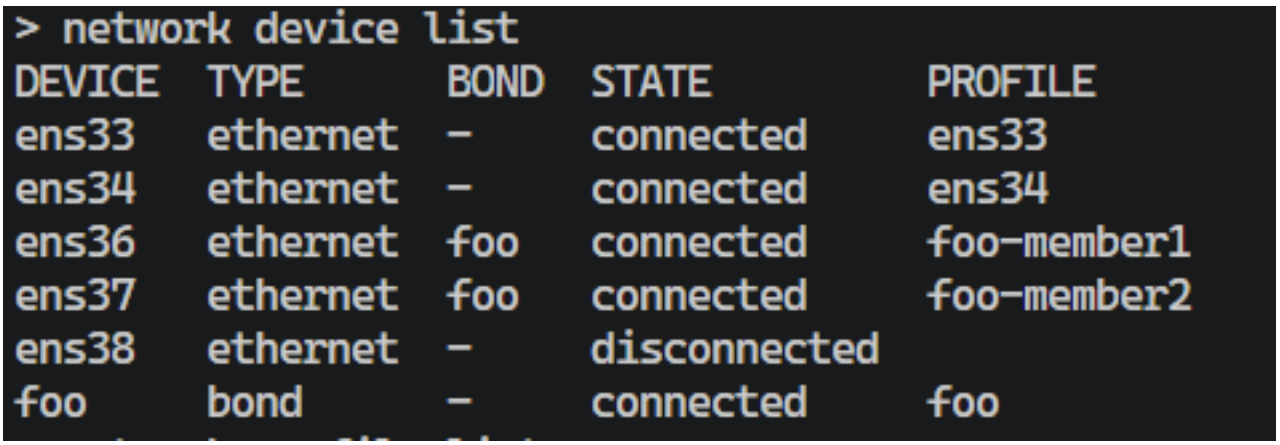
The command lists all the profiles. If a network bond has member devices, they are listed under the network bond. The asterisk next to a member indicates that it is the active device handling all traffic. If the active device fails, the standby device automatically takes over.



3. After a network bond is created, to verify the status of the devices in your network, at the command prompt enter the following command and press **Enter**:

```
network device list
```

The list of devices is displayed:



You can see that the two devices used in creating the network bond are listed against under the bond we just created and their membership of the bond is listed under the *PROFILE* column.

Modify Network Bond

You can add or remove members from an existing network bond.

Use the following command to modify a network bond:

```
network bond modify [-h] -b BOND_DEVICE [-a ADD_MEMBERS [ADD_MEMBERS ...]] ...]]
[-r REMOVE_MEMBERS [REMOVE_MEMBERS ...]]
```

where

-b, --bond

Name of the bond device to modify.

-a, --add_members

Add devices as bond members.

-r, --remove_members

Member devices to remove from the network bond.

Delete Network Bond

To delete a network bond, use the following command:

```
network bond delete [-h] -b BOND
```

where

-b, --bond

The name of the bond to delete.

Chapter 13: Alert Management

The Alert Management section describes how Arcserve Cyber Resilient Storage monitors system events and notifies administrators of important conditions that may require attention. Timely and accurate alerts are essential for maintaining the health, security, and performance of the device, especially in environments where data integrity and compliance are critical. This section covers the types of alerts the system generates and provides guidance on interpreting and responding to them appropriately.

Specifically, this section covers the following topics:

Storage Alerts

This section provides an overview of storage alerts.

Setting up storage alerts is critical to maintaining optimal performance on Arcserve Cyber Resilient Storage. Alerts enable proactive monitoring of capacity usage, helping you prevent unexpected storage exhaustion that could disrupt services.

By tracking data growth, access rates, and error logs, alerts can detect abnormal patterns that may signal potential threats such as ransomware activity or system faults. Because Arcserve Cyber Resilient Storage enforces write-once-read-many (WORM) policies to prevent data alteration or deletion, alerts also help apply these policies correctly without compromising accessibility.

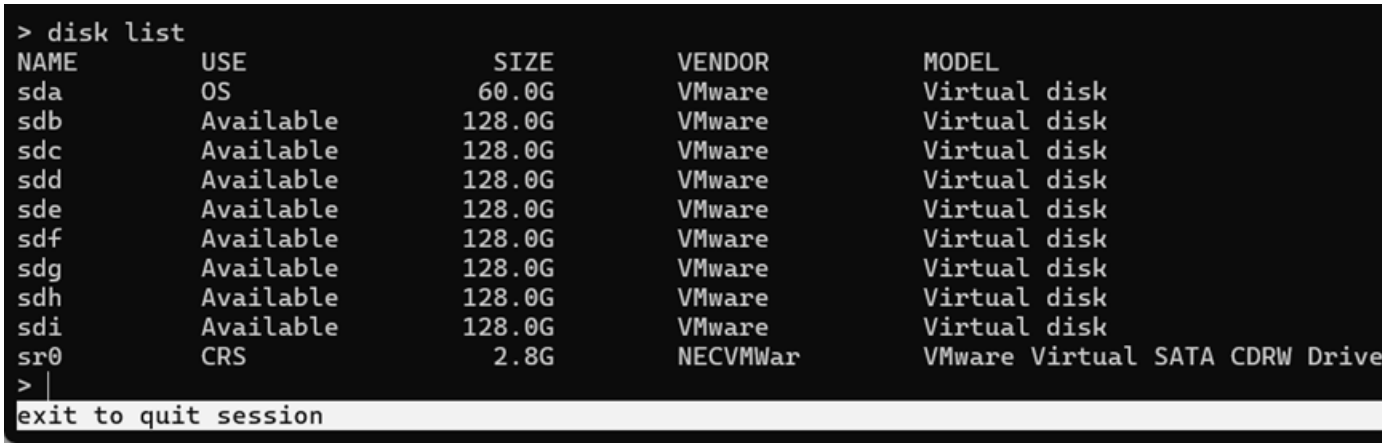
In addition, alerts support effective capacity planning by providing real-time insights into usage trends. This allows for timely decisions around scaling or archiving. Ultimately, alerts serve as an early warning system that protects data integrity, ensures consistent performance, and supports regulatory compliance.

Alerts can be triggered for the following issues:

- **disks-smart-status:** This indicates that one or more disks in the Arcserve Cyber Resilient Storage system have reported issues through their onboard S.M.A.R.T. monitoring. These warnings indicate potential disk failures. To avoid any risk to your data, investigate and address these issues as soon as possible.
- **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.
- **storage-threshold:** This indicates that the used storage capacity has reached or exceeded a predefined threshold, which can reduce the pool's capacity to store new data. The alert triggers when storage exceeds 80% of the pool capacity and clears when it drops below 75%.
- **system-clock:** This indicates an issue or discrepancy with the system clock or time synchronization, which can affect storage systems and distributed environments.

SMART Disk Alerts

Arcserve Cyber Resilient Storage uses SMART (Self-Monitoring, Analysis, and Reporting Technology) disk telemetry to give administrators continuous insight into the health and reliability of the system's physical storage media. Because Arcserve Cyber Resilient Storage is an immutable storage platform, it relies on long-term disk stability to ensure that data remains durable, verifiable, and unchanged.



Depending on the disk type and storage technology, SMART monitors a range of critical attributes, including:

- Read/write error rates
- Reallocated or unstable sectors
- I/O reliability indicators
- Mechanical wear (for HDDs)
- Flash endurance (for SSDs)
- Temperature or power irregularities

The following table provides a comparison of the commonly monitored SMART attributes across different disk types:

SMART Attribute	S(ATA)	NVME	SCSI
READ_ERROR_RATE	Yes	--	--
REALLOC_SECTOR_COUNT	Yes	--	--
TEMPERATURE	Yes	Yes	Yes
POWER_ON_HOURS	Yes	Yes	Yes
POWER_CYCLES	Yes	Yes	--
UNSAFE_SHUTDOWNS	Yes	--	--
SEEK_ERROR_RATE	--	--	--
COMMAND_TIMEOUT_COUNT	--	--	--

CRC_ERROR_COUNT	--	--	--
MEDIA_ERRORS	--	Yes	Yes
AVAILABLE_SPARE	--	Yes	--

When these attributes exceed defined thresholds or exhibit unusual trends, Arcserve Cyber Resilient Storage generates alerts. These alerts help administrators identify early signs of hardware degradation, detect disks at risk of failure, and schedule proactive maintenance before availability or durability are impacted.

Configure Email for Alerts

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

Follow these steps::

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

   email config [-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 ...]

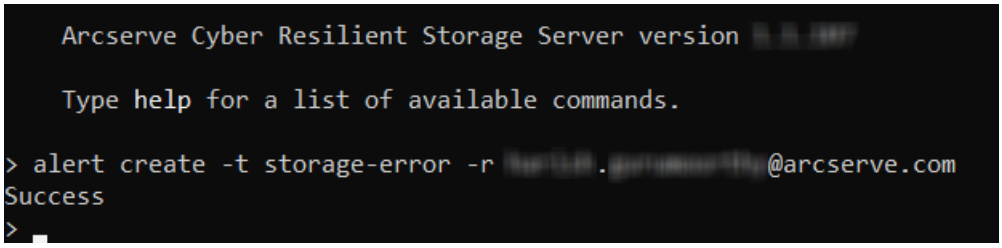
   where

   -t, --type

   The type for which to create the alert. For more information, see Storage Alerts and SMART Disk 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 14: User Management

Arcserve Cyber Resilient Storage has two user roles for managing your server environment. These roles are:

- **admin:** Has full access to operational and management tasks, such as configuring settings and managing data protection features. However, admin users cannot create or manage user accounts.
- **super admin:** Has full system privileges, including all admin capabilities. In addition, super admins can create, modify, and delete user accounts.

This section contains the following topics:

Create User 111

Update User 113

Create User

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

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
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.

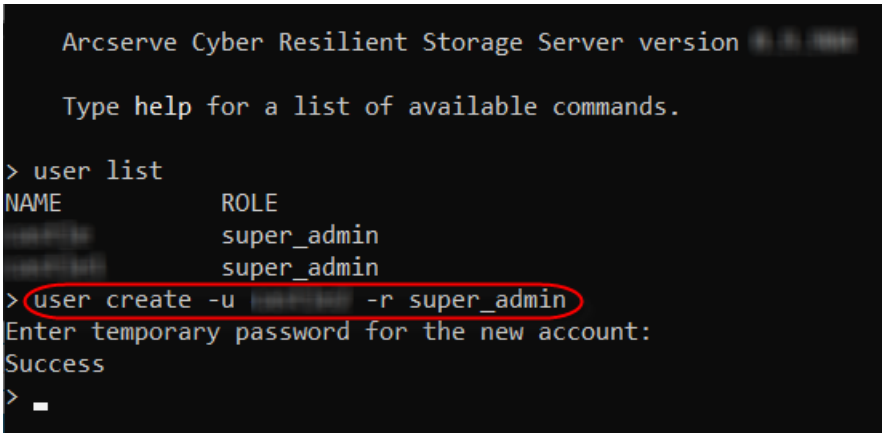
   Default: 'admin'

   The password must contain:

   At least 8 characters

   Caand include an upper case letter, a lower case letter, and a number. Passwords can also include symbols.

   For more information on user roles and their functions, see 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 Arcserve Cyber Resilient Storage.
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

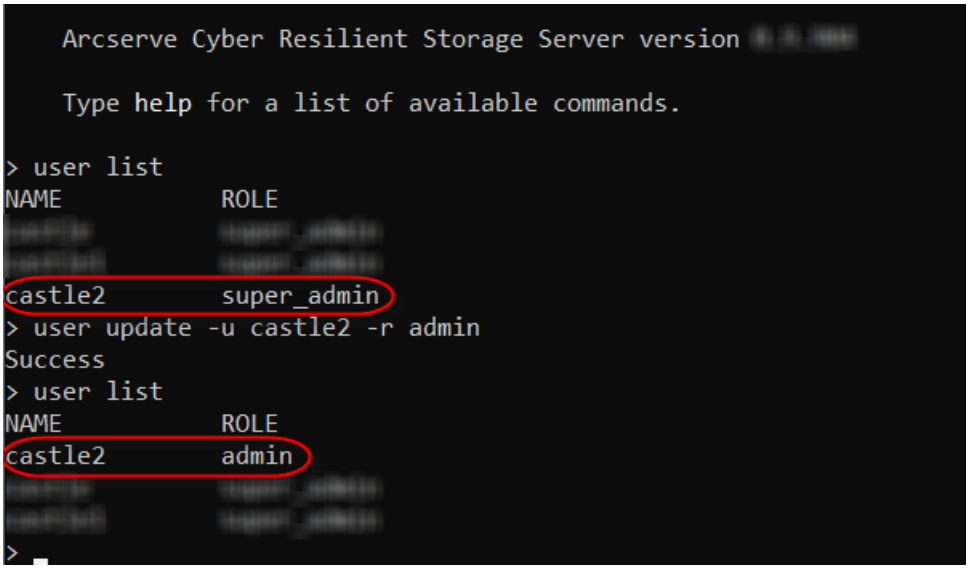
   -u, --username

   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.

Chapter 15: Time Server Management

This section contains the following topics:

NTP Falseticker Detection and Time Source Recommendations

Arcserve Cyber Resilient Storage uses chrony for time synchronization. When more than one time source is configured, chrony automatically performs falseticker detection, which compares all configured time sources and excludes any source whose reported time does not agree with the majority. This behavior is always enabled and cannot be disabled. It applies equally to the default NTS servers provided with Arcserve Cyber Resilient Storage and to any customer-configured local NTP servers.

The effectiveness of falseticker detection depends on the number of configured time sources:

Number of servers	Behavior
1 server	A faulty clock cannot be detected.
2 servers	Chrony can detect that the servers disagree but cannot determine which one is correct, so neither source is selected.
3 servers	One faulty server can be identified and outvoted by the other two servers.
4 servers	A faulty server can be outvoted even if another server becomes unavailable. This configuration aligns with NTP best practices. *RFC 8633* recommends using at least four time sources.

For reliable operation, configure at least three NTP servers, and four servers whenever possible. Arcserve Cyber Resilient Storage already validates this recommendation for redundancy through the System Clock configuration check, which generates a warning when fewer than three servers are configured.

Considerations for Customer-Managed NTP Servers

When using local NTP servers, make sure that the following requirements are met:

1. **Use independent time sources**

   Multiple NTP servers should not rely on the same upstream reference. For example, if three local NTP servers all synchronize to a single GPS receiver or a single domain controller, an upstream fault can cause all three servers to report the same incorrect time. Because the servers remain in agreement, chrony cannot detect the error. Each NTP server should synchronize to an independent upstream reference source.

2. **Prefer authenticated time synchronization**

   Standard NTP does not provide authentication. While falseticker detection can identify faulty or misconfigured servers, it cannot protect against an attacker who can spoof or modify NTP traffic across multiple servers. Network Time Security (NTS) mitigates this risk by authenticating time synchronization traffic, and Arcserve Cyber Resilient Storage prioritizes NTS-enabled servers whenever possible. When both NTS and unauthenticated NTP servers are configured, Arcserve Cyber Resilient Storage allows an unauthenticated NTP server to influence the system clock only when its reported time agrees with the NTS servers.

Configure Time Servers

To configure one (not recommended) or more time servers, use the following command:

```
time config [-h] -s SERVERS [SERVERS ...] [-F]
```

where

-s, --servers

Fully-qualified domain name or IP address of one or more time server(s) to use. Three or more servers are recommended. Before configuration, each server is checked for NTS support. Servers that do not support NTS are flagged for confirmation because they cannot authenticate time updates. An unauthenticated or spoofed time source could alter the system clock and cause retention-based snapshots to be deleted prematurely.

-F, --force

Accept server(s) that do not support NTS without confirming. Not recommended.

Time servers can also be configured as part of the initial configuration at the time of installation. See step 12 of Complete Initial Configuration for more information.

Chapter 16: Work 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:

Generate Support Bundle 119

Generate Support Bundle

When troubleshooting issues, support personnel may request a support bundle. A support bundle contains diagnostic data that helps identify and resolve problems efficiently. Arcserve Cyber Resilient Storage provides two methods for generating this bundle, depending on the deployment environment and connectivity options.

- **Create and upload the bundle directly:** In environments where Arcserve Cyber Resilient Storage is connected to external networks through an internet connection, you can run a command that generates the support bundle and automatically uploads it to a secure location that is accessible to support personnel.
- **Write the bundle to a USB drive:** For disconnected deployments where external connectivity is not permitted, Arcserve Cyber Resilient Storage allows you to generate the support bundle locally and save it to a USB drive. You can then transfer the bundle securely to support personnel for offline analysis.

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 Arcserve Cyber Resilient Storage.
2. At the command prompt, type the following command and press **Enter**:

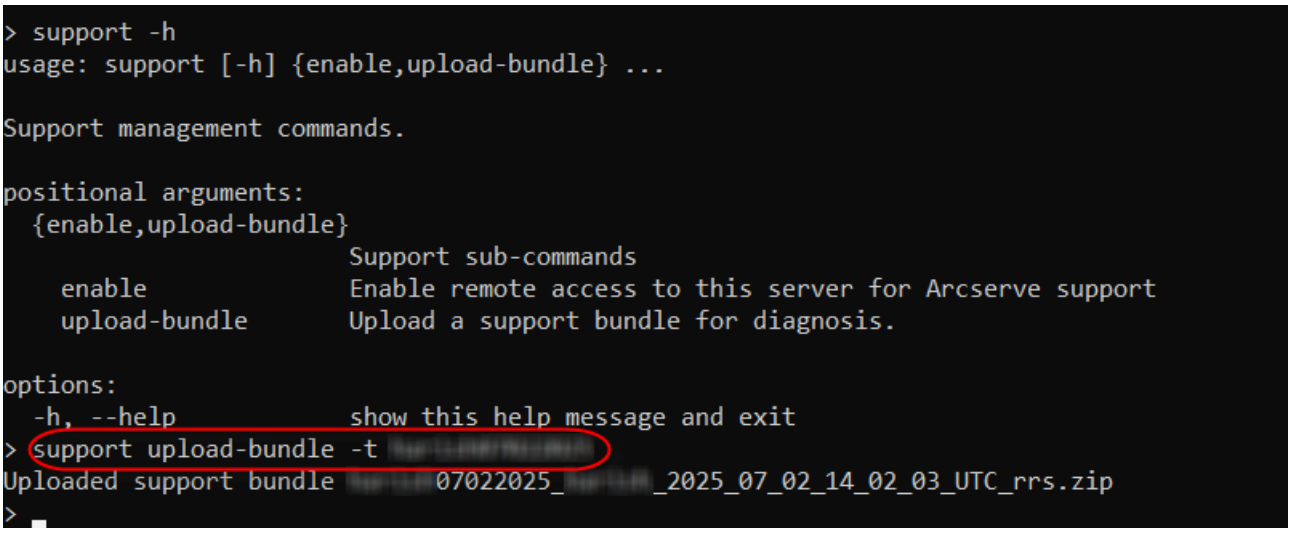
   support upload-bundle [-h] [-t TAG]

   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

When Arcserve Cyber Resilient Storage is connected to external networks through an internet connection, support personnel can remotely access the support bundle that is uploaded to a secure location.

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

Follow these steps:

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

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

   where

   -r, --relay

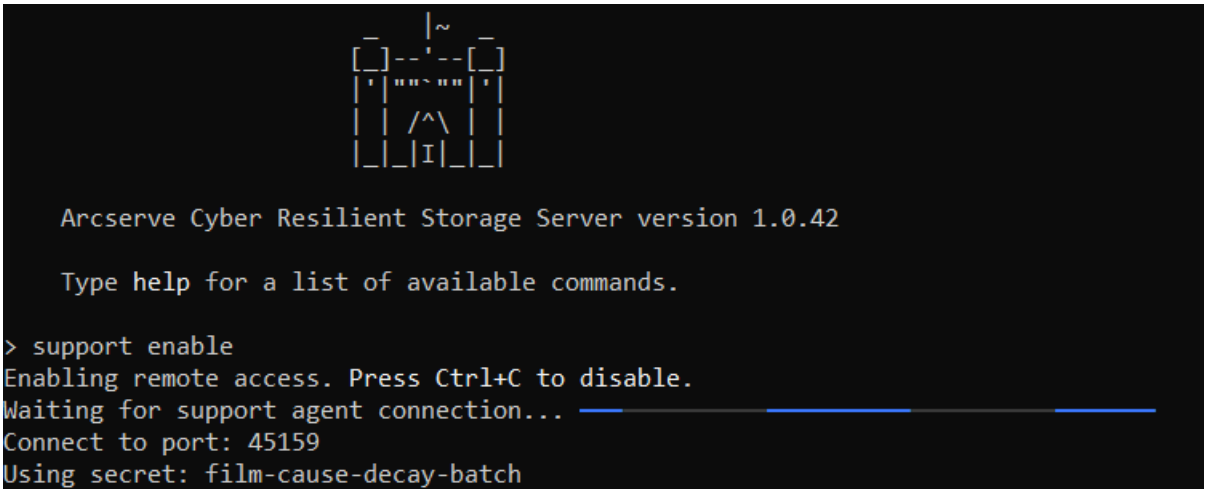
   Overrides the relay server address (optional).

   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 Arcserve Cyber Resilient Storage 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 shell:

"*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]
```

Write Support Bundle to USB Drive

When deployed in a disconnected environment, Arcserve Cyber Resilient Storage operates without any external network connectivity to meet security and compliance requirements. Because outbound communication is completely restricted, users cannot send diagnostic data or system logs to support teams using the standard methods.

To address this limitation, Arcserve Cyber Resilient Storage provides the ability to write support bundles directly to a USB drive. This allows users to extract the required system logs and diagnostic information from the disconnected environment. Support personnel can then access the data offline to troubleshoot issues, perform analysis, and help restore system functionality without compromising the integrity of the disconnected deployment.

This section describes how to write the support bundles to a USB drive.

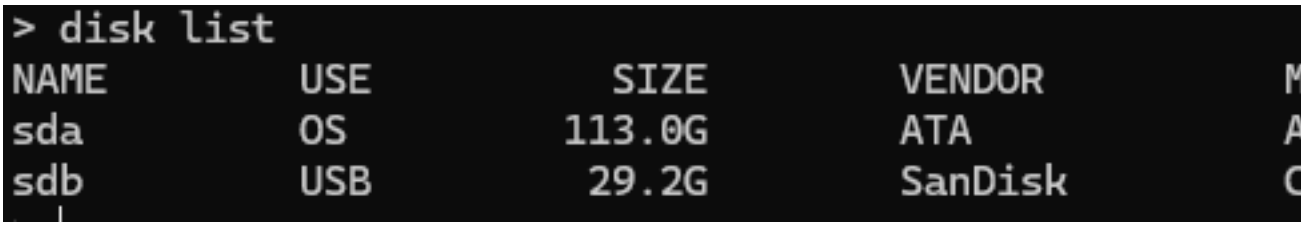
Important!

- Before you begin, make sure the USB drive is connected and available to the Arcserve Cyber Resilient Storage system.
- Make sure that the USB drive you are using has a minimum of 16 GB of available storage space.

Follow these steps:

1. Log in to Arcserve Cyber Resilient Storage.
2. After the USB drive is plugged in, to verify that it is available, enter the following command and press **Enter**:

   disk list

   This is to make sure that the USB drive is properly seated and available so the support bundle can be copied to it.
3. At the command prompt, type the following command and press **Enter**:

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

   where

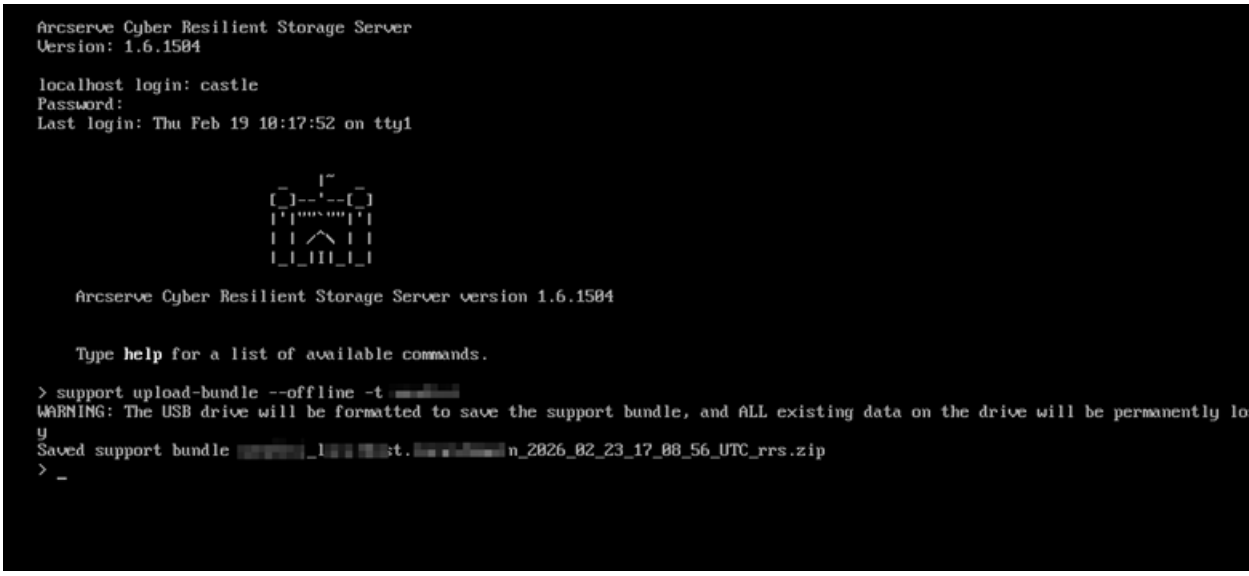
-o, --offline

Saves the support bundle to a USB drive.

-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 with the tag when provided, followed by the machine name and domain names, and the date and time at which the support bundle was generated.



The following warning message is displayed:

The USB drive will be formatted to save the support bundle, and ALL existing data on the drive will be permanently lost. Do you want to proceed?

4. Type *y* to continue. A progress bar is displayed.

   Note: Typing *n* will exit the command.

   After the support bundle is successfully copied, the CLI displays a message that the file is saved.

Chapter 17: Migrate Data Stores from OneXafe

This section describes the essential steps and considerations for migrating data from OneXafe to Arcserve Cyber Resilient Storage. The migration process involves replicating data stores from OneXafe storage to Arcserve Cyber Resilient Storage.

Data migration from OneXafe is initiated through the UDP Console. If the OneXafe system (source) and Arcserve Cyber Resilient Storage (destination) are located in different networks, make sure that both the systems are connected to the internet and accessible from the UDP Console. Internet connectivity is not required if both the systems are within the same network, but they must be accessible from the UDP Console.

To preserve data integrity, security, accuracy, and system continuity, it is essential to perform the migration with careful planning and verification. A well-executed migration helps prevent data loss, corruption, and downtime.

Some of the things to keep in mind before and after the migration are:

- Understand the size, structure, and performance of your current data. Identify dependencies and any constraints that could affect the migration.
- Perform verification checks after the migration to confirm that all files are present, accessible, and functioning as expected. Typically, these checks could be record count/file count check, checksum/hash verification, data sampling/spot checks or any of the commonly used verification checks.
- Schedule migrations to avoid disrupting business operations.
- For large transfers, consider migrating during off-peak hours to reduce network impact.

For detailed information on the migration process, see How to Replicate Data Between Data Stores Managed from a UDP Console.

Chapter 18: Common Errors and Issues

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

Storage Creation Fails with "No available disks found" Error 127
Unable to Access Unconstrained Shell 128
Unable to Add Disks to Pool Created with One Disk 129
Device Name Changes on Reboot 130
Difference in Data Store Sizes 131
Different Notations in Shell and UDP Console 132
Incorrect filesystem Free Space 133
No validation message displayed even if an incorrect key is entered 134
Unable to Reset Password for Admin/Superuser Account 135
Rebuild Arcserve Cyber Resilient Storage 136
Rebuild UDP 137
As long as the logs command is running, the terminal does not time out 138

Storage Creation Fails with "No available disks found" Error

Symptom

In a fresh Arcserve Cyber Resilient Storage deployment, during the initial configuration, the storage pool creation fails with the message "*No available disks found*", and the *disk list* command reports "*Failed to initialize libzfs library.*". The "*Failed to start Load Kernel Modules.*" error is also seen.

Solution

This issue occurs when secure boot is enabled on the system but has not been completed in the setup, that is, Machine Owner Key (MOK) enrollment is not completed. When Secure Boot is enabled, the ZFS kernel modules used by Arcserve Cyber Resilient Storage must be trusted and properly signed. If the MOK enrollment step is skipped, the required kernel modules cannot be loaded, which leads to a *libzfs* initialization failure. As a result, Arcserve Cyber Resilient Storage cannot detect available disks or create the storage pool. In this scenario, the system may also display the error message: "*Failed to start Load Kernel Modules.*".

To fix this issue, enroll the MOK key.

For more information, see Enable Secure Boot.

Unable to Access Unconstrained Shell

Symptom

Unable to access an unconstrained shell such as bash, even as an admin or super admin user. 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 shell. These limitations are applied to maintain the integrity and security of the system. Contact Arcserve Support for assistance with commands outside the scope of the shell.

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, users get the following error:

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

Solution

Arcserve Cyber Resilient Storage 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 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.

Solution

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

Different Notations in Shell and UDP Console

Symptom

The Access Key uses different notations in the UDP console and shell.

Solution

The UDP console and the Arcserve Cyber Resilient Storage shell use different terminology for access keys.

Incorrect filesystem Free Space

Symptom

When a disk of higher capacity is added to a pool, 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.

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, and currently there is no workaround to this.

Unable to Reset Password for Admin/Superuser Account

Symptom

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

Solution

If a super admin user has forgotten their password, a reinstall is required.

If an admin user has forgotten their password, the super user can reset their password.

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 Arcserve Cyber Resilient Storage 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.

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 v1.0.

Chapter 19: Appendix

This section contains the following topics:

Command Reference 140

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.