

Dell PowerProtect Cyber Recovery 19.11

Product Guide

Version 19.11

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Preface.....	6
Chapter 1: Introduction.....	8
What is the Dell PowerProtect Cyber Recovery solution?.....	8
Cyber Recovery architecture.....	9
Cyber Recovery operations.....	10
Configuring DD Compliance mode retention locking	11
Locking copies automatically.....	12
Management tools.....	12
Chapter 2: Getting Started.....	14
Logging in to the Cyber Recovery UI.....	14
Logging out of the Cyber Recovery UI.....	14
Activating the Cyber Recovery license.....	15
Enabling multifactor authentication.....	16
Completing initial setup with the Getting Started wizard.....	17
Cyber Recovery UI	20
Chapter 3: Storage and Applications.....	23
Assets overview.....	23
Managing storage.....	24
Managing applications.....	25
Managing vCenter servers.....	27
Resetting the host fingerprint.....	28
Chapter 4: Policies and Copies.....	29
Policies and copies overview.....	29
Policy actions.....	29
Adding and editing policies.....	30
Migrating replication contexts in policies.....	33
Running policies.....	33
Adding and editing policy schedules.....	34
Managing copies.....	36
Securing a copy.....	37
Analyzing a copy.....	37
Retrieving an analysis report.....	39
Recovering data to an alternate DD system.....	39
Cyber Recovery sandboxes.....	40
Managing sandboxes.....	40
Managing recovery sandboxes.....	41
Chapter 5: Monitoring.....	42
Monitoring the Cyber Recovery vault status.....	42
Monitoring alerts and events.....	43
Handling alerts	43


Monitoring jobs.....	43
Managing jobs.....	44
Chapter 6: Performing a NetWorker Recovery with Cyber Recovery.....	45
Recovering NetWorker data.....	45
Creating the NetWorker DD Boost user/UID for recovery.....	45
Initiating a NetWorker recovery in the Cyber Recovery UI.....	46
Chapter 7: Performing an Avamar Recovery with Cyber Recovery.....	48
Recovering Avamar data.....	48
Preparing the production-side Avamar system.....	48
Checklist for Cyber Recovery with Avamar.....	50
Creating the Avamar DD Boost account and UID for Cyber Recovery.....	51
Initiating an Avamar recovery in the Cyber Recovery UI.....	51
Performing manual steps for Avamar recovery.....	52
Cleaning up after an Avamar recovery.....	59
Chapter 8: Performing a PowerProtect Data Manager Recovery with Cyber Recovery.....	61
Recovering PowerProtect Data Manager data.....	61
Meeting prerequisites for a PowerProtect Data Manager recovery.....	61
Initiating a PowerProtect Data Manager recovery in the Cyber Recovery UI.....	62
Running a PowerProtect Data Manager recovery check.....	63
Cleaning up after a PowerProtect Data Manager recovery.....	64
Performing postrecovery steps for a PowerProtect Data Manager recovery.....	65
Chapter 9: Administration.....	66
Administration overview.....	66
Manually securing and releasing the Cyber Recovery vault.....	66
User roles.....	67
Managing users.....	67
Managing login sessions.....	68
Setting up an email server.....	69
Specifying which users receive email.....	69
Setting up a separate IP address for SMTP communication on the Cyber Recovery virtual appliance.....	69
Configuring the Postfix email service.....	70
Configuring an external email service.....	71
Managing Cyber Recovery password expiration.....	72
Resetting Cyber Recovery passwords.....	72
Resetting the IP address on the management host.....	73
Updating the SSL security certificate.....	74
Configuring a daily activity report.....	75
Configuring a telemetry report.....	76
Changing time zones.....	76
Changing the log level.....	77
Collecting logs for upload to support.....	78
Log file rotation.....	78
Protecting the Cyber Recovery configuration	78
Retrieving your preserved Cyber Recovery configuration.....	80

Deleting unneeded Cyber Recovery objects.....	80
Cyber Recovery disaster recovery.....	81
Cleaning up existing Cyber Recovery Docker containers.....	81
Restoring a Cyber Recovery software installation after a disaster.....	82
Restoring a Cyber Recovery virtual appliance deployment after a disaster	83
Chapter 10: Troubleshooting.....	85
Using the crsetup.sh script.....	85
Troubleshooting suggestions.....	86
Reviewing Cyber Recovery logs	89
Managing Cyber Recovery services.....	90
Delete devices that are recovered onto your NetWorker server.....	92
Disabling SSH access to the replication interface.....	92

Preface

As part of an effort to improve its product lines, Dell Technologies periodically releases revisions of the software and hardware. Therefore, some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features.

Contact your Dell Technologies technical support professional if a product does not function correctly or does not function as described in this document.

 **NOTE:** This document was accurate at publication time. To find the latest version of this document, go to [Dell Online Support](#).

Purpose

This guide describes how to use the Cyber Recovery solution to protect your data.


Audience

The information in this guide is primarily intended for administrators who are responsible for configuring, running, and monitoring Cyber Recovery policies.

Product Documentation

The Cyber Recovery product documentation set, available at [Dell Online Support](#), includes:

- Dell PowerProtect Cyber Recovery Release Notes
- Dell PowerProtect Cyber Recovery Installation Guide
- Dell PowerProtect Cyber Recovery Product Guide
- Dell PowerProtect Cyber Recovery Solutions Guide
- Dell PowerProtect Cyber Recovery Security Configuration Guide
- Dell PowerProtect Cyber Recovery on AWS Deployment Guide
- Dell PowerProtect Cyber Recovery on Azure Deployment Guide
- Dell PowerProtect Cyber Recovery Command-Line Interface Reference Guide
- Dell PowerProtect Cyber Recovery with Index Engines CyberSense Release Notes
- Dell PowerProtect Cyber Recovery Open Source License and Copyright Information

 **NOTE:** Also, see the documentation for the products that are integrated with Cyber Recovery, such as Dell PowerProtect DD Series Appliances, Dell Avamar, Dell NetWorker, and Dell PowerProtect Data Manager applications.

Where to get help

Go to [Dell Online Support](#) to obtain Dell Technologies support, and product and licensing information. You can also find documentation, release notes, software updates, or information about other Dell Technologies products.

You will see several options for contacting Dell Technologies Technical Support. To open a service request, you must have a valid support agreement. Contact your Dell Technologies sales representative for details about obtaining a valid support agreement or with questions about your account.

Comments and suggestions

Comments and suggestions help us to continue to improve the accuracy, organization, and overall quality of the user publications. Send comments and suggestions about this document to DPAD.Doc.Feedback@emc.com.

Please include the following information:

- Product name and version
- Document name, part number, and revision
- Page numbers
- Other details to help address documentation issues

Introduction

This section provides an overview of the Dell PowerProtect Cyber Recovery solution.

Topics:

- [What is the Dell PowerProtect Cyber Recovery solution?](#)
- [Cyber Recovery architecture](#)
- [Cyber Recovery operations](#)
- [Management tools](#)

What is the Dell PowerProtect Cyber Recovery solution?

The Cyber Recovery solution maintains mission-critical business data and technology configurations in a secure, air-gapped 'vault' environment that can be used for recovery or analysis. The Cyber Recovery vault is physically or virtually isolated from the production system or the network, depending on the type of deployment.

NOTE: You can deploy the Cyber Recovery vault on Amazon Web Services (AWS) or Microsoft Azure.

The Cyber Recovery solution enables access to the Cyber Recovery vault only long enough to replicate data from the production system. At all other times, the Cyber Recovery vault is secured and off the network. A deduplication process is performed in the production environment to expedite the replication process so that connection time to the Cyber Recovery vault is as short as possible.

Within the Cyber Recovery vault, the Cyber Recovery software creates point-in-time (PIT) retention-locked copies that can be validated and then used for recovery of the production system.

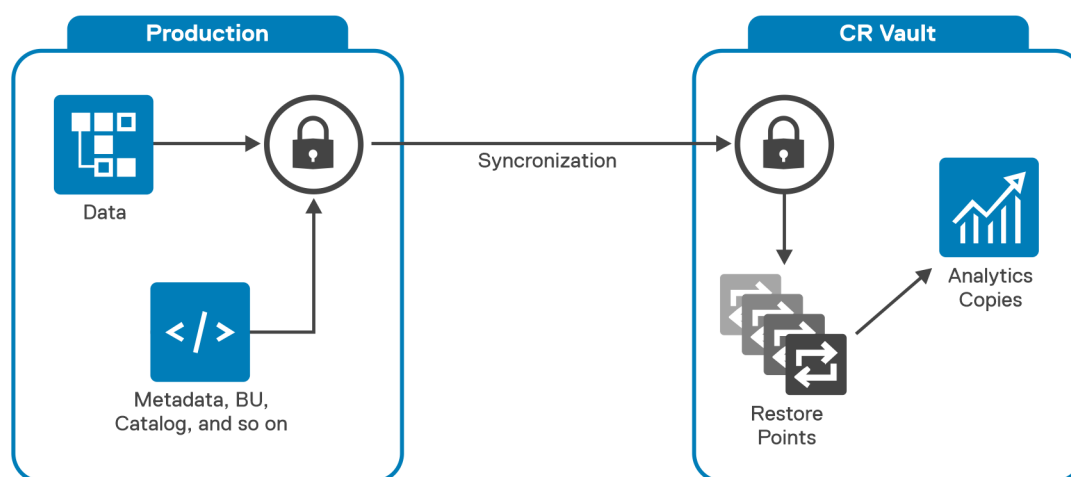


Figure 1. High-level solution architecture

NOTE: PowerProtect DD Retention Lock software provides data immutability for a specified time. Retention Lock functionality is enabled on a per-MTree basis, and the retention time is set on a per-file basis. Retention Lock is not required for Cyber Recovery but is strongly recommended as an additional cyber-resiliency measure.

A policy, which can be scheduled, orchestrates the workflow between the production environment and the Cyber Recovery vault. A policy is a combination of objects (such as PowerProtect DD storage and applications) and jobs (such as synchronization, copy, and lock).

NOTE: References to DD systems in this documentation, in the Cyber Recovery UI, and elsewhere in the product include DD systems and Data Domain systems.

Cyber Recovery architecture

The Cyber Recovery solution uses DD systems to replicate data from the production system to the Cyber Recovery vault through a dedicated replication data link.

The following diagram shows the production and Cyber Recovery vault environments:

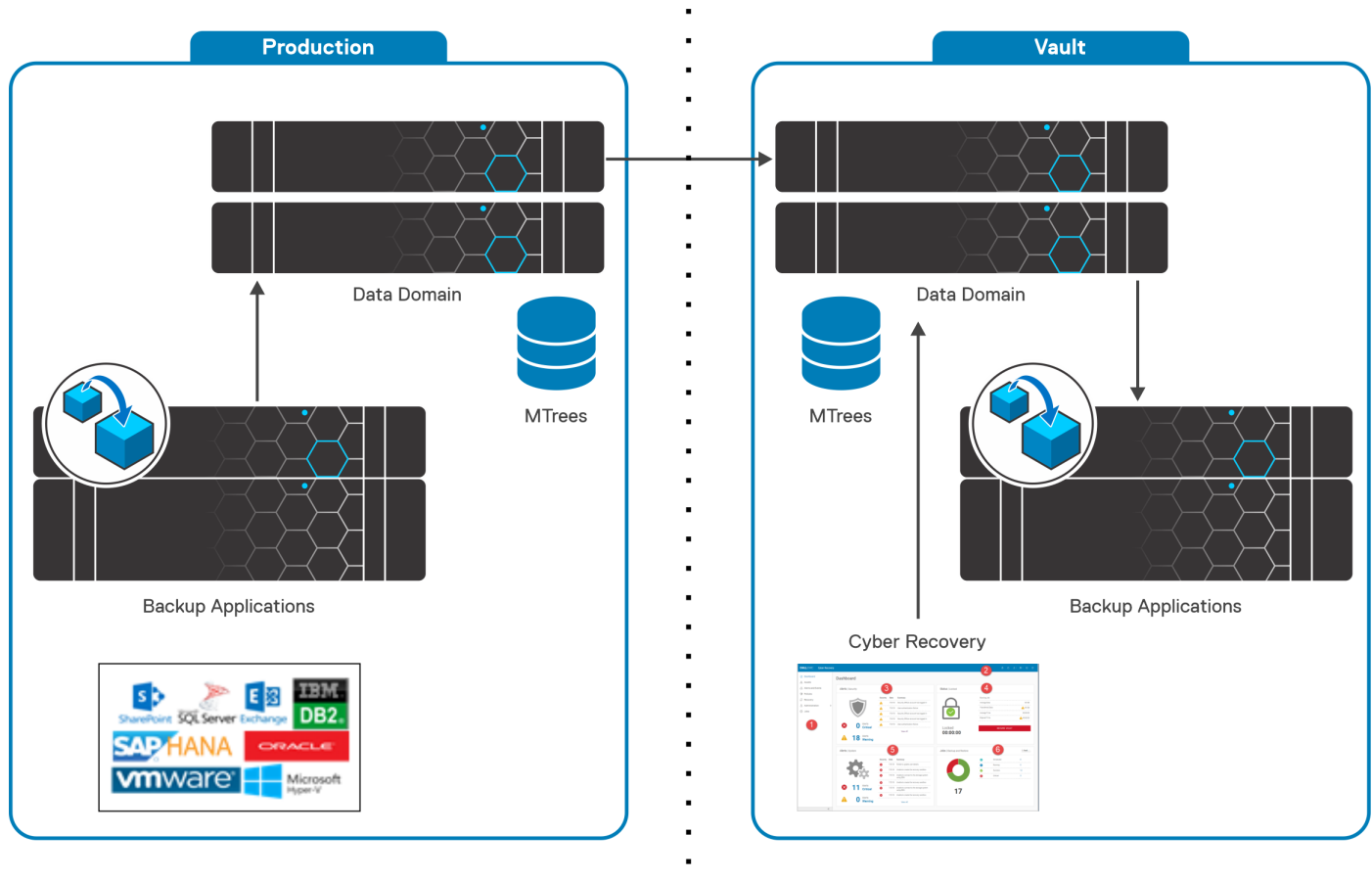


Figure 2. Cyber Recovery architecture

NOTE: Unless otherwise specified, this document uses the term Cyber Recovery vault to describe the vault environment, which includes the DD system, the management host, and backup and analytics applications.

The Cyber Recovery vault is a customer-provided secure location of the DD MTree replication destination. It requires dedicated resources including a network, and though not required but strongly recommended, a name service such as DNS and a clock source. The Cyber Recovery vault can be at another location (hosted by a service provider, for example).

Production environment

In the production environment, applications such as the Avamar, NetWorker, and PowerProtect Data Manager applications manage backup operations, which store the backup data in MTrees on DD systems. The production DD system is configured to replicate data to a corresponding DD system in the Cyber Recovery vault.

Vault environment

The Cyber Recovery vault environment includes the Cyber Recovery management host, which runs the Cyber Recovery software and a DD system. If required for application recoveries, the Cyber Recovery vault can also include NetWorker, Avamar, PowerProtect Data Manager, and other applications.

By installing and licensing the CyberSense feature, you can validate and analyze your data.

The Cyber Recovery software enables and disables the replication Ethernet interface and the replication context on the DD system in the Cyber Recovery vault to control the flow of data from the production environment to the vault environment. For short periods of time, the Cyber Recovery vault is connected to the production system over this dedicated interface to perform replications. Because the management interface is always enabled, other Cyber Recovery operations are performed while the Cyber Recovery vault is secured.

NOTE: From the DD command-line interface (CLI) and the DD user interface (UI), MTreeS are displayed using the following Cyber Recovery naming convention:

```
# /data/coll/cr-policy-<policyID>-repo
```

where *<policyID>* is the unique ID that is created when you create a Cyber Recovery policy.

Cyber Recovery operations

Recovery managers can perform continuous and iterative operations that maintain recovery data in the Cyber Recovery vault if they are needed for restoration. You can perform these operations separately or in combinations. Except for a recovery, you can also schedule operations or trigger them manually as needed.

Table 1. Cyber Recovery operations

Operation	Description
Replication	DD MTree replications are performed from the DD production system to the DD system in the Cyber Recovery vault. Each replication uses DD deduplication technology to match the data in the vault incrementally. This document refers to a replication operation as a "Sync."
Copy	A point-in-time (PIT) fast copy is made of the most recent replication. If data recovery is required, the copy serves as a PIT restore point. You can maintain multiple PIT copies to ensure an optimal number of restore points. You can mount each copy in a sandbox. The sandbox is a read/write DD fast copy inside the Cyber Recovery vault. A fast copy is a clone of files and directory trees of a PIT copy from the <code>cr-policy-<i><policy-id></i>-repo</code> MTree. Data can be scanned for malware or analyzed as needed in the sandbox.
Lock	<p>You can secure all files in a PIT copy from modification by retention locking for a specific duration. The Cyber Recovery solution supports the following DD retention locking features:</p> <ul style="list-style-type: none">• Governance archive data requirements, which are considered lenient and meant to provide relatively short durations as appropriate to achieve your recovery strategy.• Compliance archive data requirements, which are stricter than Governance archive data requirements and are recommended to secure against more threats.• The automatic retention lock functionality for Retention Lock Governance or Retention Lock Compliance Modes. <p>NOTE:</p> <ul style="list-style-type: none">• The Cyber Recovery software does not support the Indefinite Retention Hold capability of Retention Lock Governance or Retention Lock Compliance Modes.• The Cyber Recovery solution on Amazon Web Services (AWS) does not support Retention Lock Compliance mode. <p>For information about the governance, compliance, and automatic retention lock archive data requirements and how to manage them, see the DD documentation.</p>
Analyze	You can analyze locked or unlocked copies with various tools that search for indicators of compromise, suspicious files, or potential malware. These anomalies might identify a copy as an invalid source for recovery.
Recovery	You can use the data in a PIT copy to perform a recovery operation.

Table 1. Cyber Recovery operations (continued)

Operation	Description
Recovery Check	You can run a scheduled or on-demand recovery check on a PowerProtect Data Manager recovery to provide assurance that after a successful recovery a copy can be recovered.

Configuring DD Compliance mode retention locking

Configure the Cyber Recovery vault DD system for Retention Lock Compliance.

Prerequisites

The Cyber Recovery vault DD system must have a Retention Lock Compliance license.

For more comprehensive information about the procedures to configure Retention Lock Compliance on a DD system, see the *Dell EMC DD OS Administration Guide*.

About this task

DD systems support both Governance mode and Compliance mode retention locking. Compliance mode is a stricter type of retention locking, which enables you to apply retention policies at an individual file level. You cannot delete or overwrite locked files under any circumstances until the retention period expires.

NOTE:

Retention Lock Compliance mode is not supported on:

- The Cyber Recovery solution on Amazon Web Services (AWS)
- Dell EMC PowerProtect DD3300 appliance
- Dell EMC DP4400 Integrated Data Protection Appliance (IDPA)
- Dell EMC PowerProtect DD Virtual Edition (DDVE) storage appliance

Steps

1. On the Cyber Recovery vault DD system, log in as an Admin user and then add a security account with the security role:

```
# user add <account name> role security
```

The security role user can be referred to as a Security Officer.

2. Log out as the Admin user and log in again as the Security Officer user.
3. Enable security authorization:

```
# authorization policy set security-officer enabled
```

4. Log out as the Security Officer user and log in again as the Admin user.
5. Configure the Cyber Recovery vault DD system for Retention Lock Compliance:

```
# system retention-lock compliance configure
```

6. When prompted, enter the security officer credentials.
The software updates the configuration and then reboots the Cyber Recovery vault DD system, which is unavailable during the process.
7. Log in as the Admin user.
8. Enable Retention Lock Compliance:

```
# system retention-lock compliance enable
```

9. When prompted, enter the security officer credentials.

Results

You can perform Retention Lock Compliance operations on an MTree. You must be logged in to the Cyber Recovery vault DD system as an Admin user and provide the security officer credentials, when prompted.

Locking copies automatically

For deployments that are running DD OS Version 7.6 and earlier, use the automatic retention lock feature to lock copies automatically.

Prerequisites

The Cyber Recovery vault DD system must run PowerProtect DD OS Versions 6.2.1.50 through Version 7.6.

About this task

NOTE: Do not configure the automatic retention lock feature on a policy on a deployment that is running DD OS Version 7.7 and later. Later versions of DD OS and the Cyber Recovery software provide retention locking automatically when the data is copied. Using the automatic retention lock feature with this DD configuration introduces some unnecessary constraints, such as the inability to create an unlocked copy.

If the automatic retention lock feature is enabled, the Cyber Recovery software automatically locks any copies that are created on the DD system. This feature supports both Retention Lock Compliance and Retention Lock Governance.

When you enable automatic retention locking on a policy:

- The Cyber Recovery UI lists only the Secure Copy, Copy Lock, and Sync policy actions.
- You cannot disable automatic retention locking.

Steps

1. Log in to the Cyber Recovery UI.
2. Select **Policies** from the Main Menu.
3. Either add a policy or edit an existing policy.
The **Add Policy** or **Edit Policy** window is displayed.
4. Click the checkbox to enable the automatic retention lock feature.

NOTE: If you are running a version of DD OS that is earlier than Version 6.2, the checkbox is not displayed.

A Cyber Recovery copy is fully retention locked when all files are copied to the repository and a five minute delay has been applied.

Management tools

The Cyber Recovery solution provides a web-based UI, API, and CLI.

Cyber Recovery UI

The web-based Cyber Recovery UI is the primary management and monitoring tool. It enables users to define and run policies, monitor operations, troubleshoot problems, and verify outcomes.

NOTE: To access the Cyber Recovery UI, go to **https://<hostname>:14777**, where **<hostname>** is the hostname of the management host.

Cyber Recovery REST API

The Cyber Recovery REST API provides a predefined set of operations that administer and manage tasks over HTTPS. Use the REST API to create a custom client application or to integrate Cyber Recovery functionality into an existing application.

NOTE: To access the Cyber Recovery REST API documentation, go to **https://<hostname>:14780**, where **<hostname>** is the hostname of the management host.

Cyber Recovery command-line interface

The Cyber Recovery CLI (CRCLI) is a command-line alternative to the Cyber Recovery UI.

NOTE: Detailed information about the CRCLI is beyond the scope of this document. Use the `crcli help` command to view the help system or see the Dell EMC PowerProtect Cyber Recovery

Command-Line Interface Reference Guide, which provide comprehensive information about the CRCLI.

Getting Started

This section describes how to log in to the Cyber Recovery UI and activate the Cyber Recovery license. It also describes how to get started by using the Getting Started wizard.

Topics:

- [Logging in to the Cyber Recovery UI](#)
- [Logging out of the Cyber Recovery UI](#)
- [Activating the Cyber Recovery license](#)
- [Enabling multifactor authentication](#)
- [Completing initial setup with the Getting Started wizard](#)

Logging in to the Cyber Recovery UI

Cyber Recovery users can log in to the Cyber Recovery UI.

About this task


Users that are assigned the Security Officer (crso) or Admin roles can perform tasks in Cyber Recovery. A dashboard user can only view the dashboard but cannot perform any tasks.

Steps

1. Open a supported browser and go to `https://<host>:14777`, where `<host>` is the hostname of the management host where the Cyber Recovery software is installed.


The Cyber Recovery software supports the Chrome and Firefox browsers. For the most current information, see the [PowerProtect Cyber Recovery Simple Support Matrix](#).

2. Enter your username and password.
3. Click **Log In**.
4. If you enabled multifactor authentication, enter the security code in the **Security Code** field and click **Log In**.

 **NOTE:** Multifactor authentication is a time-based security mechanism. The Cyber Recovery host time cannot differ from the authenticator time by more than one minute (plus or minus). If the time differs by more than +60 seconds or -60 seconds, multifactor authentication is not enabled. For more information, see [Enabling multifactor authentication](#).

Results

The Cyber Recovery dashboard is displayed.

 **NOTE:** For enhanced security, log out of the Cyber Recovery UI when you have completed your Cyber Recovery session.

Logging out of the Cyber Recovery UI

For enhanced security, ensure that you log out of the Cyber Recovery UI when you complete your Cyber Recovery session.


Prerequisites

You are logged in to the Cyber Recovery UI.

About this task

Cyber Recovery users are assigned a session timeout, which is the amount of idle time after which the user is logged out of the Cyber Recovery UI. To modify the session timeout, go to **Administration > Users** on the Main Menu and then select a user and edit the session timeout value.

If you close the browser window or tab while the Cyber Recovery UI is running, and then access the Cyber Recovery UI within the session timeout limit, the Cyber Recovery dashboard is displayed. You are not required to log in. However, after the session timeout expires, you must log in to the Cyber Recovery UI again.

 **NOTE:** As a best practice, we recommend that you log out of the Cyber Recovery UI when you complete your Cyber Recovery session rather than allowing the session to time out.

Steps

1. From the Cyber Recovery masthead, click the User icon.
2. Click **Logout <user role>**.

 **NOTE:** For a Dashboard user, **Logout <dashboard user>** is the only available option.


You are logged out of the Cyber Recovery session and the Cyber Recovery login page is displayed.

Activating the Cyber Recovery license

Upload the Cyber Recovery license file to activate the license.

Prerequisites

Provide a Software Instance ID, which is created at the Cyber Recovery installation, to acquire the license file from Dell Technologies. The information icon on the Masthead Navigation displays information about Cyber Recovery, including the Software Instance ID.

 **NOTE:** You can request a non-subscription or a subscription license.

When Dell Technologies provides the license file in an email message, save it to a directory of your choice. If you must bring the license file into the Cyber Recovery vault, you must enable a connection from your desktop to the Cyber Recovery vault or use a USB flash drive.

About this task

After Cyber Recovery installation, a 90-day evaluation license is activated by default. You can perform all Cyber Recovery tasks. After 90 days, you must obtain a POC (evaluation), standard (permanent), or subscription license to continue to use the Cyber Recovery software. Warning messages are displayed before the evaluation license expires.

Steps

1. From the Masthead Navigation, click the gear icon to access the **System Settings** list.
2. Click **License**.

The **License** dialog box provides the following information:

- **Expires ON**—Indicates that the date on which the license expires
- **State**—Indicates if the license is an evaluation license or is activated
- **Type**—Indicates if the type is a POC, standard, or subscription license
- **Software Instance ID**—Provides the ID that was used to acquire the license file

The **License** dialog box also provides the following information only if the applicable features are enabled:

- **Cloud Vault**—Indicates that the Cyber Recovery instance is running on Amazon Web Services (AWS) or Microsoft Azure
- **IDPA - Active**—Indicates that IDPA is enabled

3. In the **License** dialog box, click **Choose File**, select the Cyber Recovery license file, and then click **OK**.

Results

The Cyber Recovery license is activated, and you can use all the Cyber Recovery licensed features.

When the license is about to expire, an alert is displayed on the dashboard, the Alerts and Events content pane, and the toolbar.

Enabling multifactor authentication

After initial login to the Cyber Recovery UI, optionally enable multifactor authentication to provide added protection for the Cyber Recovery environment.

Prerequisites

From the Internet, download any authenticator application. Examples of authenticator applications include, but are not limited to, the following:

- Google Authenticator
- Authy
- Duo Mobile
- LastPass Authenticator

An authenticator application generates a one-time security code over an interval of time to provide two-step verification to authenticate Cyber Recovery users. The Cyber Recovery software requires a six-digit security code.

About this task

Users must enable multifactor authentication for their own accounts. Multifactor authentication is not available to Dashboard users. The Security Officer (crso) cannot enable multifactor authentication for other users, but can disable it for all users.

NOTE:

- Multifactor authentication is a time-based security mechanism. The Cyber Recovery host time cannot differ from the authenticator time by more than one minute (plus or minus). If the time differs by more than +60 seconds or -60 seconds, multifactor authentication is not enabled.
- If you enable multifactor authentication and then are unable to provide the security code, you cannot log in to your Cyber Recovery account. Contact the Security Officer (crso) to disable multifactor authentication for your account, and then enable multifactor authentication again when you can log in.
- As the Security Officer (crso), if you enable multifactor authentication and then are unable to provide the security code, use the `crsetup.sh` script to change the Security Officer (crso) password. When you change the password, multifactor authentication is disabled.
- Integrated Data Protection Appliances deployments do not support multifactor authentication.

Steps

1. Download and install the authenticator application on your mobile device or computer.
2. From the Masthead Navigation, open the drop-down list next to the person icon.
3. Click **Multi-Factor Authentication**.
The setup page is displayed.
4. Swipe right on the slider to enable the multifactor authentication.
5. Do one of the following:
 - Use the device camera to scan the QR code on the setup page to provide the security key.
 - If your use of mobile devices or cameras is restricted, click **Show Secret Key** to view the security key and then enter it into the authenticator.
6. Enter two consecutive security codes:
 - a. In the **Security Code 1** field, enter the first security code that the authenticator generates.
 - b. In the **Security Code 2** field, enter the next security code that the authenticator generates.If you enter nonconsecutive security codes, multifactor authentication is not enabled. Wait for the authenticator to generate a new security code and ensure that you enter the next consecutive security code.
7. Click **Save**.
For subsequent logins, the Cyber Recovery software prompts for a security code in addition to a username and password.
8. To disable multifactor authentication, swipe left on the slider.

The Security Officer (crso) and the Admin user, whose multifactor authentication is disabled, receive an email message that indicates that multifactor authentication is disabled. If multifactor authentication for the Security Officer (crso) is disabled, only the Security Officer (crso) receives an email message.

Completing initial setup with the Getting Started wizard

The Getting Started wizard enables you to check your Cyber Recovery deployment, create an Admin user, add storage, and deploy a protection policy quickly.

About this task

When you log in to the Cyber Recovery UI for the first time, the Getting Started wizard is displayed. The wizard guides you through the initial steps for running a policy. When you complete a step, its corresponding number changes color and the next step is highlighted. When you complete the wizard, the Cyber Recovery dashboard is displayed.

Steps

- Under **Checklist**, click **Review** to verify that you have performed the required deployment steps.
If you have not satisfied all requirements, log out and complete the deployment steps.
- Under **Users**, click **Add** and create a user with the Admin role. Complete the following fields in the **Add User** dialog box and click **Save**:

Table 2. User fields

Field	Description
Name fields	Specify the user's first name and last name.
Role	Select either: <ul style="list-style-type: none">Admin—Enables users to perform tasks in the Cyber Recovery software.Dashboard—Enables users to view the Cyber Recovery dashboard but not perform tasks. The dashboard role does not time out.
User Name (required)	Specify a username.
Phone	Specify the user's telephone number.
Email (required)	Specify an email address for alert notifications if the user is configured to receive them. NOTE: Later, if a user's email is modified, the Security Officer (crso) and the user receive an email message that indicates the change. The user's old email address, which has since been modified, receives the email message.
Password/Confirm New Password (required)	Specify and confirm the password. Password requirements include: <ul style="list-style-type: none">9–64 charactersAt least 1 numeric characterAt least 1 uppercase letterAt least 1 lowercase letterAt least 1 special character (~!@#\$%^&*()+={} :~<>?[]-_,^') When you change a password, enter and confirm both the new and existing passwords.
Session Timeout	Select the amount of idle time after which the user is logged out of the Cyber Recovery UI.

- Under **Vault Storage**, click **Add** to define the storage object. Complete the following fields in the **Add Vault Storage** dialog box and click **Save**:

Table 3. Vault storage fields

Field	Description
Nickname	Enter a name for the storage object.

Table 3. Vault storage fields (continued)

Field	Description
FQDN or IP Address	Specify the DD host by using one of the following: <ul style="list-style-type: none"> Fully qualified domain name (FQDN) IP address
Storage Username	Specify a dedicated Cyber Recovery DD administration account (for example, <code>cradmin</code>), which the Cyber Recovery software uses to perform operations with the DD system. This DD account must have the admin role.
Storage Password	Enter the password of the DD administrator.
SSH Port Number	Enter a storage SSH port number.
Reset Host Fingerprint	(Security Officer only) If you change the FQDN or IP address of the DD host, select to reset the fingerprint. The Cyber Recovery software then sends an alert message.
Tags	Optionally, add a tag that provides useful information about the storage object. The tag is displayed in the details description for the vault storage in the Assets content pane in the Cyber Recovery UI. Click Add Tag , enter the tag, and then click Add . <p>NOTE: If a tag exceeds 24 characters, the details description displays the first 21 characters followed by an ellipsis (...).</p>

- Under **Policies**, click **Add** to open the Add Policy wizard.
- On the **Policy Information** page, complete the following fields and then click **Next**:

Table 4. Policy Information page

Field	Description
Name	Specify a policy name.
Type	From the drop-down list, select either Standard or PPDM . <p>NOTE: Standard denotes NetWorker, Avamar, Filesystem, and Other policy types.</p>
Storage	Select the storage object containing the replication context that the policy will protect. <p>NOTE: You cannot edit the storage object for an existing policy.</p>
Tags	Optionally, add a tag that provides useful information about the policy. The tag is displayed in the details description for the policy in the Policies content pane in the Cyber Recovery UI. Click Add Tag , enter the tag, and then click Add . <p>NOTE: If a tag exceeds 24 characters, the details description displays the first 21 characters followed by an ellipsis (...).</p>

- On the **Replication** page, complete the following fields and then click **Next**:

Table 5. Replication page

Field	Description
Replication Contexts	<ol style="list-style-type: none"> Under Context, select the MTree replication context to protect and the interface on the storage instance that is configured for replications. Under Ethernet Port, click Select Repl Ethernet and then select the interface on the storage instance that is configured for replications. <p>NOTE:</p>

Table 5. Replication page (continued)

Field	Description
	<ul style="list-style-type: none"> There can be only one policy per replication context, except for PowerProtect Data Manager policy types, which support multiple replication contexts. Do not select the data or management Ethernet interfaces. If your DD system is running a version of DDOS that is earlier than version 7.8 and you select a Retention Lock Compliance replication context, the policy creation fails.
Replication Window	Set a timeout value in hours for how long a job for a Sync action runs before Cyber Recovery issues a warning. The default value is 0.
Enforce Replication Window	If you change the default value in the Replication Window field, the Enforce Replication Window checkbox is displayed. Enable the checkbox to stop a Sync operation that continues to run beyond the replication window limit for that policy. When the replication window limit is exceeded, the operation completes the current DD snapshot replication and does not proceed to replicate queued snapshots.

7. On the **Retention** page, complete the following fields and then click **Next**:

Table 6. Retention page

Field	Description
Retention Lock Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> (Add Policy dialog box only) None, if retention locking is not supported. The retention fields are then removed from the dialog box. Governance if it is enabled on the storage instance. (Edit Policy dialog box only) Governance-disabled. Compliance if it is enabled on the storage instance.
Enable Auto Retention Lock	<p>Optionally, if the retention lock type is Governance or Compliance, click the checkbox to enable the automatic retention lock feature. There is a five-minute delay before the lock is applied.</p> <p>NOTE: You cannot disable the automatic retention lock feature after you enable it.</p>
Retention Lock Minimum	Specify the minimum retention duration that this policy can apply to PIT copies. This value cannot be less than 12 hours.
Retention Lock Maximum	Specify the maximum retention duration that this policy can apply to PIT copies. This value cannot be greater than 1,827 days.
Retention Lock Duration	Specify the default retention duration, which is a value between the retention lock minimum and maximum values, that this policy applies to PIT copies.

If you selected a Retention Lock Compliance replication context or the Compliance Retention Lock type, the **Storage Security Credentials** page is displayed. Otherwise, the **Summary** page is displayed.

8. On the **Storage Security Credentials** page, enter the DD Security Officer (SO) username and password and then click **Next**.

NOTE: This username was created on the DD system.

9. Review the **Summary** page and either:

- Click **Finish** if you are satisfied with the summary information and want to add the policy.
- Click **Back** to return to the previous page to change the information.
- Click **Edit** to return to a specific page in the wizard to change information.

If you selected a Retention Lock Compliance replication context and your deployment is running version of DDOS that is earlier than version 7.8, the Cyber Recovery software fails to create the policy.

10. Select **Policies** in the Main Menu to run the policy.

For more information about running policies, see the *Policies and Copies* topic.

Cyber Recovery runs the policy. A message indicates that the job has started and provides a link to the appropriate Jobs page with the job details. Also, the dashboard displays the job's progress.

11. To recall the wizard at any time, select **System Settings > Getting Started** from the Masthead Navigation.

Cyber Recovery UI

The Cyber Recovery UI is the primary tool for performing and monitoring Cyber Recovery operations. It is a web application that enables you to define, run, and monitor policies and policy outcomes.

NOTE: The Cyber Recovery UI is available only in English. No other languages are supported.

The Cyber Recovery UI includes:

- Masthead Navigation icons that provide information or enable you to perform administrative tasks.
- A Main Menu that enables you to access content panes from which you perform operations such as managing assets, policies, recoveries, and users.
- The dashboard includes four tiles that provide alerts notifications that facilitate troubleshooting and error correction, the Cyber Recovery vault status, and a cumulative job type report.

NOTE: If you log in to the Cyber Recovery UI as a dashboard user, your view of the dashboard is limited and you cannot perform tasks. However, the dashboard does not time out.

The following figure shows the dashboard in the Cyber Recovery UI:

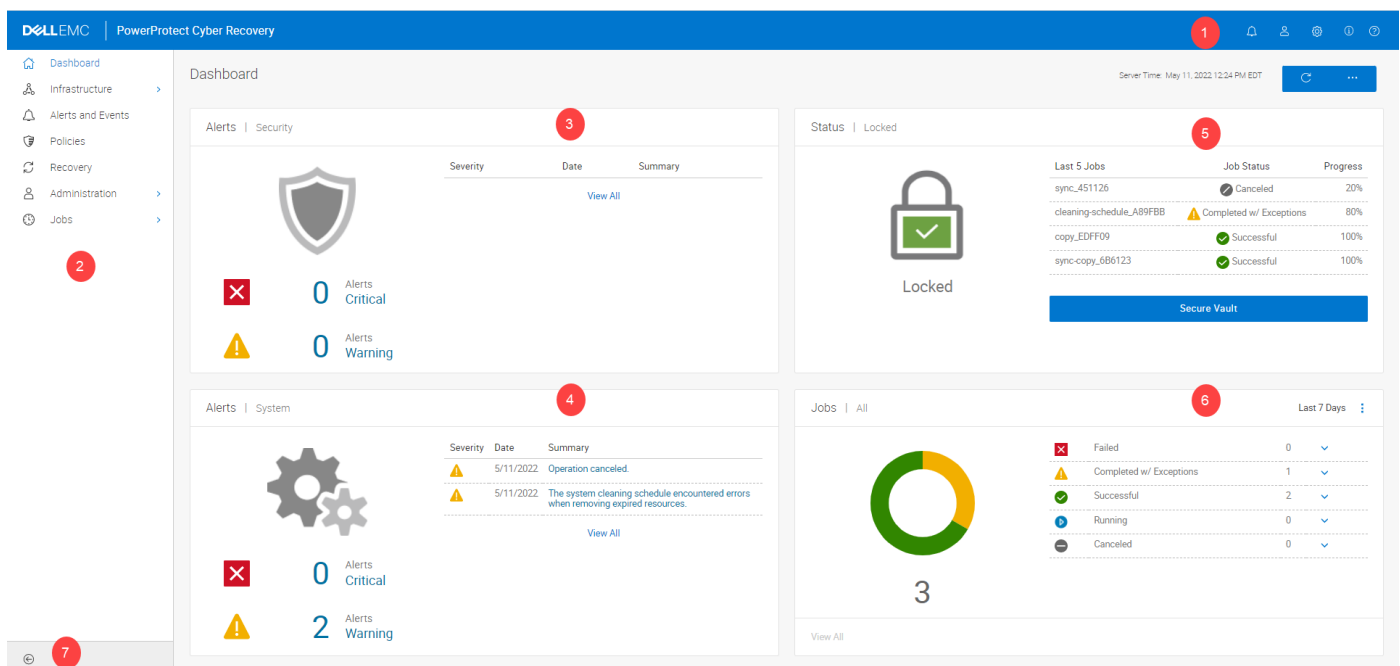


Figure 3. PowerProtect Cyber Recovery dashboard

1. The Masthead Navigation provides icons that enable you to view notifications and additional information, set system settings, and access the Getting Started wizard and online help. A dashboard user can only log out of the Cyber Recovery UI.

2. The Main Menu provides access to content panes from which you can perform operations. It is not available to a dashboard user.
3. The **Alerts|Security** tile provides details about unacknowledged alerts that identify anomalies in vault activity. For more detailed information and to see older alerts, click **View All** to be redirected to the **Alerts and Events** content pane.
4. The **Alerts|System** tile provides details about unacknowledged system events. For more detailed information and to see older alerts, click **View All** to be redirected to the **Alerts and Events** content pane.
5. The **Status** tile shows the current state of the Cyber Recovery vault. It enables you to secure the Cyber Recovery vault manually if a network event occurs when it is open and stop all replication operations. The tile also displays the five most recent jobs and their progress. For information about monitoring and manually securing the Cyber Recovery vault, see [Monitoring the Cyber Recovery Vault status](#) and [Manually securing and releasing the Cyber Recovery Vault](#).

NOTE: A dashboard user cannot secure the vault.

6. The **Jobs** tile provides the status for a cumulative list of Protection, System, and Recovery job types in the Cyber Recovery environment. Click the vertical ellipsis to change the timeframe and job type that are displayed. The heading and the pie chart change to reflect your choices. Click outside of the drop-down list to close it.

NOTE: The timeframe and job type that you select are retained while you navigate the Cyber Recovery UI content panes and when you log in again.

For more detailed information and to see older jobs:

- Click the down arrow next to a job status and then click a link, which redirects you to the Jobs content pane for that type of job.
- Click **View All**, which redirects you to the Jobs content pane for the selected job type. A single job type must be selected to enable the **View All** link.

These settings are maintained and are set when you log in again.

NOTE: The filter options and redirection are not available to dashboard users.

7. The arrow enables you to contract or expand the Main Menu.

NOTE: Your assigned role determines the functions that you can perform in the Cyber Recovery UI. For more information, see [User roles](#).

Masthead Navigation

The Cyber Recovery UI includes Masthead Navigation.

The icons in the masthead of the Cyber Recovery UI provide information or enable you to perform administrative tasks.

NOTE: A dashboard user can only log out of the Cyber Recovery UI and has no access to the other icons.

Click an icon to display information or choose a task:

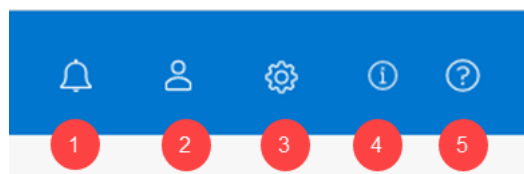


Figure 4. Masthead navigation icons

1. Provides a list of unacknowledged alerts and redirects to the **Alerts and Events** content pane when you click **View All**.
2. Indicates user settings that:
 - Identify your username
 - Enable you to set up multifactor authentication to provide added protection
 - Enable you to log out
3. Provides options to:
 - Access the Getting Started wizard
 - Configure clean-up disaster recovery backup, mail server, and log settings
 - Configure activity and telemetry reports
 - Configure and managed disaster recovery backups
 - Generate, view, download, and delete support bundles

- Enable the Security Officer (crso) to manage the number of simultaneous login sessions
 - Enable license activation
4. Displays the Cyber Recovery version and Software Instance ID
 5. Displays the Cyber Recovery online help

Storage and Applications


This section describes how to manage storage instances and applications in the Cyber Recovery UI.

Topics:

- [Assets overview](#)
- [Managing storage](#)
- [Managing applications](#)
- [Managing vCenter servers](#)
- [Resetting the host fingerprint](#)

Assets overview

Assets in the Cyber Recovery vault are represented as storage, application, and vCenter server objects.


 **NOTE:** Power on all assets before you add them to your Cyber Recovery deployment.

Storage objects

Storage objects represent storage systems, such as DD systems. Define a storage object for each DD system that is running in the Cyber Recovery vault. The Cyber Recovery software uses the DD system to perform replications, store point-in-time (PIT) copies, and apply retention locking.

Application objects

Application objects represent applications, such as Avamar, NetWorker, or PowerProtect Data Manager, or the CyberSense feature.

 **NOTE:** The CyberSense feature is only supported as a component of the Cyber Recovery solution in the Cyber Recovery vault; it is not supported on the production system.

Usually, you include Avamar, NetWorker, and PowerProtect Data Manager backup applications in the Cyber Recovery vault when the DD system is integrated with those applications in your production systems. The Cyber Recovery vault does not require these applications to protect the data because MTree replications copy all the data to the Cyber Recovery vault. However, running the applications in the Cyber Recovery vault enables you to recover and restore your data so that it can be used to rehydrate production backup applications, if necessary.

The Cyber Recovery software integrates with the CyberSense feature application, which analyzes backup data for the presence of malware or other anomalies. After you install CyberSense feature on a separate host in the Cyber Recovery vault, define an application object for it. Then, Cyber Recovery policies can call the CyberSense feature to analyze PIT copies of supported datasets.

vCenter server objects

If you plan to use PowerProtect Data Manager to perform a recovery in the Cyber Recovery vault, add a vCenter server asset. Otherwise, a PowerProtect Data Manager recovery fails.

Managing storage

Define a storage object for each DD system that is running in the Cyber Recovery vault environment. A DD system in the Cyber Recovery vault serves as the repository for the data that is replicated from the production system and protected by the Cyber Recovery solution.

About this task

If you are defining the DD system for the first time, see [Completing initial setup with the Getting Started wizard](#).

To update a DD system in the Cyber Recovery vault, ensure that there are no running Cyber Recovery jobs. There are no special considerations for updating a DD system; follow the update procedure in the relevant version of the *Dell EMC DDOS, PowerProtect DD Virtual Edition (DDVE), and PowerProtect DD Management Center (DDMC) Release Notes*.

NOTE:


If the DD system in the Cyber Recovery vault reaches its configured warning and critical space usage thresholds, the Cyber Recovery software displays the corresponding alerts on the Cyber Recovery dashboard. The default values for warning and critical thresholds are 80 percent and 90 percent respectively. If email is configured for your deployment, users receive an email notification.

If the DD system runs out of storage space, a Sync job fails. Clean up the DD system to reclaim space and then restart the Sync job.

Steps

1. From the Main Menu, select **Infrastructure > Assets**.
2. Click **Vault Storage** at the top of the **Assets** content pane.
3. Do one of the following:
 - To add a storage object, click **Add**.
 - To modify an existing object, select the object and click **Edit**.
4. Complete the following fields in the dialog box:

Table 7. Vault storage fields

Field	Description
Nickname	Enter a name for the storage object.
FQDN or IP Address	Specify the DD host by using one of the following: <ul style="list-style-type: none">• Fully qualified domain name (FQDN)• IP address
Storage Username	Specify a dedicated Cyber Recovery DD administration account (for example, <code>cradmin</code>), which the Cyber Recovery software uses to perform operations with the DD system. This DD account must have the admin role.
Storage Password	Enter the password of the DD administrator.
SSH Port Number	Enter a storage SSH port number.
Reset Host Fingerprint	(Security Officer only) If you change the FQDN or IP address of the DD host, select to reset the fingerprint. The Cyber Recovery software then sends an alert message.
Tags	Optionally, add a tag that provides useful information about the storage object. The tag is displayed in the details description for the vault storage in the Assets content pane in the Cyber Recovery UI. Click Add Tag , enter the tag, and then click Add .  NOTE: If a tag exceeds 24 characters, the details description displays the first 21 characters followed by an ellipsis (...).

5. Click **Save**.
The **VAULT STORAGE** table lists the storage object.
6. In the storage object's row, click the icon in the **Details** column to view more detailed information that is retrieved from the DD system, such as the replication contexts and the Ethernet interface.

7. To remove a storage object, select the storage object, and then click **Delete**.

Managing applications

When you install an application in the Cyber Recovery vault, you must represent the application to the Cyber Recovery software. Applications can include the Avamar, NetWorker, and PowerProtect Data Manager applications, the CyberSense feature, or other applications.

Prerequisites

- The application must be installed and running at the Cyber Recovery vault location before you can define it in the Cyber Recovery UI.
- Modify the `/etc/ssh/sshd_config` file:
 1. For NetWorker and Avamar deployments, enable password authentication and SSH access for root on the server:
 - Change the `PasswordAuthentication` field value from **no** to **yes**.
 - Change the `PermitRootLogin` field value from **no** to **yes**.
 2. For PowerProtect Data Manager deployments, enable password authentication:
 - Change the `PasswordAuthentication` field value from **no** to **yes**.
 3. Run the `service sshd restart` command.
- If you plan to use CyberSense Version 7.8 or later, assign a DD Boost user to the PowerProtect DD system in the Cyber Recovery vault:
 1. Create a dedicated DD Boost user with the applicable role on the Cyber Recovery vault PowerProtect DD system for CyberSense to use:

```
user add <username> role <role value> uid <uid value>
```

NOTE: The role value is the user who performs the backups on the production DD system. For a PowerProtect Data Manager backup, the role value is `none`. For a NetWorker or Avamar backup, the role value is `admin`.

2. Assign the DD Boost user:

```
ddboost user assign <username>
```

Steps

1. From the Main Menu, select **Infrastructure > Assets**.
2. Click **Applications** at the top of the **Assets** content pane.
3. Do one of the following:
 - To add an application, click **Add**.
 - To modify an existing application, select the application and click **Edit**.
4. Complete the following fields in the dialog box:

Table 8. Application fields

Field	Description
Nickname	Enter a name for the application object.
FQDN or IP Address	Specify the application host by using one of the following: <ul style="list-style-type: none">• Fully qualified domain name• IP address
Host Username	Specify the host administrator username. NOTE: This username is for the operating system host.
Host Password	Enter the password of the host administrator. NOTE: For PowerProtect Data Manager, enter the password for the user admin account, which is the default account.
SSH Port Number	Enter an application SSH port number.

Table 8. Application fields (continued)

Field	Description
Application Type (when adding an application only)	<p>Select an application type:</p> <ul style="list-style-type: none"> To represent an application in Cyber Recovery, select one of the following: <ul style="list-style-type: none"> CyberSense for analysis capabilities Avamar NetWorker and complete the following additional fields: <ul style="list-style-type: none"> In the Application Username field, enter the username of the application user. The application user is usually the administrator user. In the Application Password field, enter the password of the application user, which must be the same password for the administrator user on the production DD system. PPDM and complete the following additional fields: <ul style="list-style-type: none"> In the Application Username field, enter the username of the application user. In the Application Password field, enter the password of the application user. In the vCenter Name field, select a vCenter server NOTE: If you are running a pre-19.8 version of PowerProtect Data Manager, the Cyber Recovery UI displays the Root Password and Lockbox Passphrase fields for which you must add values. FileSystem if you want to mount copies on an NFS share and examine data by using any application on the host. Selecting this option does not require you to install an application on the host. Other for other application types. NOTE: If you specify an application (in the FQDN or IP address field) and then select a different application type (in the Application Type field), the procedure fails. The application host must correspond to the application type. You cannot modify the Application Type field for an existing application.
Security Group Tag	(For Cyber Recovery deployed in Amazon Web Services (AWS) only) Enter the tag of the security group that controls access to and from the CyberSense host for Cyber Recovery deployed in Amazon Web Services (AWS).
Reset Host Fingerprint	(Security Officer only) If you change the FQDN or IP address of the DD host, select to reset the fingerprint. The Cyber Recovery software then sends an alert message.
Tags	<ul style="list-style-type: none"> Optionally, add a tag that provides useful information about the application. The tag is displayed in the Assets content pane in the Cyber Recovery UI. Click Add Tag, enter the tag, and then click Add. For Avamar, NetWorker, or PowerProtect Data Manager recoveries, add a tag that indicates the DD Boost username that is configured for the production application. NOTE: If a tag exceeds 24 characters, the details description displays the first 21 characters followed by an ellipsis (...).

- Click **Save**.
The **Applications** table lists the application.
- If you added a CyberSense Version 7.8 application, run the following commands from the CyberSense host to ensure the use of the DD Boost user while mounting the sandbox during the analysis process:

```
# iesh
# ddboostcfg add
```

```

Enter hostname, username, and password for each Data Domain host you plan to
connect to
using DDBoost protocol. Enter '*' as a hostname to enable auto probe with given
username and password. Only single probe combination is allowed. Reply with Enter
or Ctrl-D
on the Host: prompt to finish

Host: <host name>
Username: <username>
Password: <password>

# dservice restart dispatch

```

7. In the application's row, click the icon in the **Details** column to view more detailed information.
8. To remove an application, select the application and click **Delete**.

Managing vCenter servers

When you install a vCenter server in the Cyber Recovery vault, you must represent it to the Cyber Recovery software.

Steps

1. From the Main Menu, select **Infrastructure > Assets**.
2. Click **VCenters** at the top of the **Assets** content pane.
3. Do one of the following:
 - To add a vCenter, click **Add**.
 - To modify an existing vCenter, select the vCenter and click **Edit**.
4. Complete the following fields in the dialog box:

Table 9. vCenter fields

Field	Description
Nickname	Enter a name for the vCenter server.
FQDN or IP Address	Specify the vCenter server by using one of the following: <ul style="list-style-type: none"> • Fully qualified domain name • IP address
Username	Enter the username of the user logging into the vCenter server.
Password	Enter the password of the user logging into the vCenter server.
Tags	<ul style="list-style-type: none"> • Optionally, add a tag that provides useful information about the application. The tag is displayed in the Assets content pane in the Cyber Recovery UI. Click Add Tag, enter the tag, and then click Add. <p>NOTE: If a tag exceeds 24 characters, the details description displays the first 21 characters followed by an ellipsis (...).</p>

5. Click **Save**.
The **VCenters** table lists the application.
6. In the vCenter's row, click the icon in the **Details** column to view more detailed information.
7. To remove a vCenter, select the asset and click **Delete**.

Resetting the host fingerprint

If you change the hostname (that is, the FQDN or IP address) of either an application or a DD system in the Cyber Recovery vault you must reset the host fingerprint.

Prerequisites

Only the Security Officer role can carry out this task.

About this task

You must reset the host fingerprint in the following cases:

- If you change from one FQDN to a different FQDN.
- If you change from an FQDN to an IP address.
- If you change from an IP address to an FQDN.

In this case, you do not need to reset the host fingerprint:

- If you change from one IP address to a different IP address.

Steps

1. To reset the host fingerprint when changing an FQDN or IP address, do one of the following:
 - Select **Assets** from the Main Menu, and click **Applications** at the top of the **Assets** content pane.
 - Select **Assets** from the Main Menu, and click **Vault Storage** at the top of the **Assets** content pane.
2. Select an existing application or storage asset, and click **Edit**.
3. In the dialog box, change the address in the FQDN or IP address field.
4. Check the **Reset Host Fingerprint** checkbox.
5. Click **Save**.

Policies and Copies

This section describes how to create and run policies that perform replications, create point-in-time copies, and set retention locks.

Topics:

- [Policies and copies overview](#)
- [Policy actions](#)
- [Adding and editing policies](#)
- [Running policies](#)
- [Adding and editing policy schedules](#)
- [Managing copies](#)
- [Securing a copy](#)
- [Analyzing a copy](#)
- [Recovering data to an alternate DD system](#)
- [Cyber Recovery sandboxes](#)

Policies and copies overview

The Cyber Recovery solution secures data by using policies and copies.

Policies

The Cyber Recovery solution uses policies to perform replications, create point-in-time (PIT) copies, set retention locks, and create sandboxes. Note the following details about Cyber Recovery policies:


- A Cyber Recovery policy can govern one or more DD MTree. Only a PowerProtect Data Manager policy type can govern more than one MTree.
- You can create, modify, and delete policies.
- When you run a policy, you can perform a single action or carry out multiple actions in sequence. For example, you can run a policy so that it only performs a replication. Or, you can run the same policy so that it performs a replication, creates a PIT copy, and then retention locks the copy.
- You cannot run concurrent Sync or Lock actions for a policy.

Copies

Copies are the PIT MTree copies that serve as restore points that you can use to perform recovery operations. In the Cyber Recovery UI, you can retention lock a copy or analyze its data to detect the presence of malware or other anomalies. You can also delete unlocked copies.

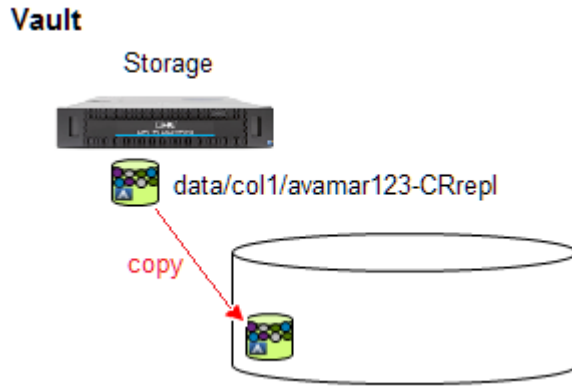
Policy actions

The Cyber Recovery UI supports the Secure Copy Analyze, Secure Copy, Sync Copy, Copy Lock, Sync, and Copy policy actions.

 **NOTE:** If you enabled the automatic retention lock feature, the Cyber Recovery UI only supports the Secure Copy Analyze, Secure Copy, Copy Lock, and Sync policy actions.

Copy

A Copy action makes a point-in-time (PIT) copy of an MTree's most recent replication in the Cyber Recovery vault and stores it in the replication archive.

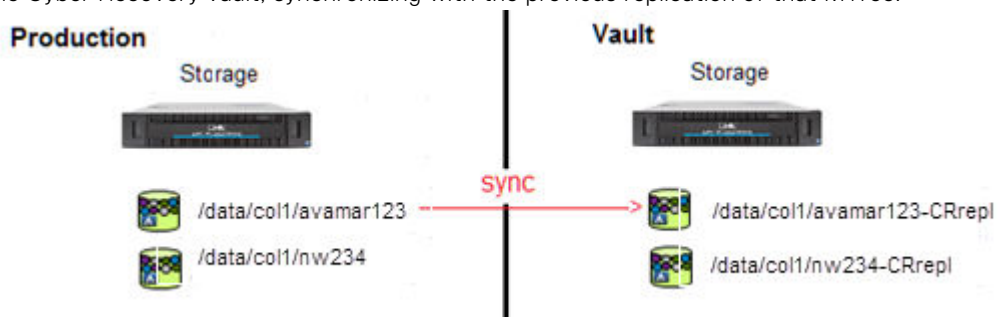


Copy Lock

A Copy Lock action retention locks all files in the PIT copy.

Sync

A Sync action (or replication) replicates an MTree from the production system to the Cyber Recovery vault, synchronizing with the previous replication of that MTree.



NOTE: From the CRCLI, you can perform a Sync action to a system other than the Cyber Recovery vault DD system. Replicate an MTree from the Cyber Recovery vault DD system to the production DD system or an alternate DD system. For more information, see [Recovering data to an alternate DD system](#).

Sync Copy

A Sync Copy action combines the Sync and Copy actions into one request. It first performs the replication and then creates a PIT copy.

Secure Copy

A Secure Copy action performs a replication, creates a PIT copy, and then retention locks all files in the PIT copy.

NOTE: You can also retention lock an existing PIT copy as described in [Securing a copy](#).

Secure Copy Analyze

A Secure Copy Analyze action performs a replication, creates a PIT copy, retention locks all files in the PIT copy, and then runs an analysis on the resulting PIT copy.

Adding and editing policies

Create policies to perform replications, make point-in-time (PIT) copies, set retention locks, and perform other Cyber Recovery operations within the Cyber Recovery vault. You can also modify existing policies.

Prerequisites

- Ensure that a storage object is available to reference in the policy and that it has an unprotected replication context.
- Policies that perform recovery or analysis operations require an application.
- To protect a Retention Lock Compliance replication context, your DD system must be running DDOS 7.8.

About this task

You can create up to 25 policies for a maximum of five DD systems in the Cyber Recovery vault. Only one policy can protect a replication context.




The Cyber Recovery software supports PowerProtect Data Manager policies that govern multiple MTrees.

You can disable a policy so that you can use the replication contexts of that disabled policy to create a new policy. If you use the contexts of a disabled policy, you cannot then enable that policy. You can use a disabled policy's copy to perform a recovery operation manually or from the **Recovery** window.

Steps

1. Select **Policies** from the Main Menu.
2. In the **Policies** content pane, do one of the following:
 - a. To create a policy, click **Add**.
The Add Policy wizard is displayed.
 - b. To modify a policy, select a policy and click **Edit**.
The **Summary** page of the Edit Policy wizard is displayed. Click **Edit** or **Back** to go to the wizard page that you want to modify.
3. On the **Policy Information** page, complete the following fields and then click **Next**:

Table 10. Policy Information page

Field	Description
Name	Specify a policy name.
Type	From the drop-down list, select either Standard or PPDM .  NOTE: Standard denotes NetWorker, Avamar, Filesystem, and Other policy types.
Storage	Select the storage object containing the replication context that the policy will protect.  NOTE: You cannot edit the storage object for an existing policy.
Tags	Optionally, add a tag that provides useful information about the policy. The tag is displayed in the details description for the policy in the Policies content pane in the Cyber Recovery UI. Click Add Tag , enter the tag, and then click Add .  NOTE: If a tag exceeds 24 characters, the details description displays the first 21 characters followed by an ellipsis (...).

4. On the **Replication** page, complete the following fields and then click **Next**:

Table 11. Replication page



Field	Description
Replication Contexts	<ol style="list-style-type: none">a. Under Context, select the MTree replication context to protect and the interface on the storage instance that is configured for replications.b. Under Ethernet Port, click Select Repl Ethernet and then select the interface on the storage instance that is configured for replications.  NOTE: <ul style="list-style-type: none">• There can be only one policy per replication context, except for PowerProtect Data Manager policy types, which support multiple replication contexts.• Do not select the data or management Ethernet interfaces.

Table 11. Replication page (continued)

Field	Description
	<ul style="list-style-type: none"> If your DD system is running a version of DDOS that is earlier than version 7.8 and you select a Retention Lock Compliance replication context, the policy creation fails.
Replication Window	Set a timeout value in hours for how long a job for a Sync action runs before Cyber Recovery issues a warning. The default value is 0.
Enforce Replication Window	If you change the default value in the Replication Window field, the Enforce Replication Window checkbox is displayed. Enable the checkbox to stop a Sync operation that continues to run beyond the replication window limit for that policy. When the replication window limit is exceeded, the operation completes the current DD snapshot replication and does not proceed to replicate queued snapshots.


5. On the **Retention** page, complete the following fields and then click **Next**:

Table 12. Retention page

Field	Description
Retention Lock Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> (Add Policy dialog box only) None, if retention locking is not supported. The retention fields are then removed from the dialog box. Governance if it is enabled on the storage instance. (Edit Policy dialog box only) Governance-disabled. Compliance if it is enabled on the storage instance.
Enable Auto Retention Lock	<p>Optionally, if the retention lock type is Governance or Compliance, click the checkbox to enable the automatic retention lock feature. There is a five-minute delay before the lock is applied.</p> <p> NOTE: You cannot disable the automatic retention lock feature after you enable it.</p>
Retention Lock Minimum	Specify the minimum retention duration that this policy can apply to PIT copies. This value cannot be less than 12 hours.
Retention Lock Maximum	Specify the maximum retention duration that this policy can apply to PIT copies. This value cannot be greater than 1,827 days.
Retention Lock Duration	Specify the default retention duration, which is a value between the retention lock minimum and maximum values, that this policy applies to PIT copies.

If you selected a Retention Lock Compliance replication context or the Compliance Retention Lock type, the **Storage Security Credentials** page is displayed. Otherwise, the **Summary** page is displayed.

6. On the **Storage Security Credentials** page, enter the DD Security Officer (SO) username and password and then click **Next**.

 **NOTE:** This username was created on the DD system.

7. Review the **Summary** page and either:
- Click **Finish** if you are satisfied with the summary information and want to add the policy.
 - Click **Back** to return to the previous page to change the information.
 - Click **Edit** to return to a specific page in the wizard to change information.

If you selected a Retention Lock Compliance replication context and your deployment is running version of DDOS that is earlier than version 7.8, the Cyber Recovery software fails to create the policy.

8. To view comprehensive policy details, do one of the following:
 - a. Click the Details icon that is next to the policy name to open the **Details** window.
 - b. Click the policy name to open the **Policy Details** pane, which provides summary information under the **Summary** tab and lists the copies that are associated with the policy under the **Copies** tab. Click **Back to Policies** to return to the policies list.

Migrating replication contexts in policies

When you create a policy with a Retention Lock Compliance replication context or modify an existing policy to add a Retention Lock Compliance replication context, the Cyber Recovery software detects the context. If your deployment is running DDOS 7.8, the Cyber Recovery software modifies a setting on the DD system in the Cyber Recovery vault. This one-time modification enables the Cyber Recovery software to support Retention Lock Compliance contexts.

When you create a policy that uses a Retention Lock Compliance replication context, the Cyber Recovery UI and CRCLI prompt you for the Security Officer (SO) credentials. By default, the security authorization for disabling replications is set to **enabled**. This setting means that the DD system continues to prompt for the SO credentials when the Cyber Recovery software attempts to disable a replication at the end of any Sync action. So that the workflow is not impeded, when you create a policy that uses a Retention Lock Compliance replication context, the Cyber Recovery software changes the setting to **disabled**. This change ensures that for subsequent workflow actions that disable replications and require SO credentials, the Cyber Recovery software is not required to provide these SO credentials.

If a replication context configured in a Cyber Recovery policy is migrated to a Retention Lock Compliance replication context using the same name, the Cyber Recovery software cannot detect this change. The replication context is migrated to a Retention Lock Compliance replication context, but the Cyber Recovery software does not modify the setting on the DD system. Unlike a policy creation, the Cyber Recovery software does not change the authorization for replication disable setting to **disabled** on the DD system if it is in the **enabled** state (the default setting). You must change the setting manually on the DD system.

Run the following command on the DD system to verify the current authorization for replication disable setting on the DD system:

```
system replication security-auth repl-disable status
```

If the status is **enabled**, run the following command on the DD system to set the authorization for replication disable setting to **disabled**:

```
system replication security-auth repl-disable disable
```

This command requires SO credentials. It provides a one-time modification on the DD and enables future Retention Lock Compliance migrations to work properly.

Running policies

Run a policy manually at any time so that it performs a specified action or actions.

Steps

1. Select **Policies** from the Main Menu.
2. Click the radio button at the beginning of the row for the policy that you want to run.
3. Click **Actions** and select one of the following:

Table 13. Policy actions


Action	Description
Copy	Click Copy and click Apply to start the Copy action. The Cyber Recovery software creates a PIT copy of the latest replication.  NOTE: If the automatic retention lock feature is enabled, the Copy action is not available from the Actions drop-down list.

Table 13. Policy actions (continued)

Action	Description
Copy Lock	Retention locks the most recent point-in-time (PIT) copy. To retention lock an earlier PIT copy, see Managing copies .
Sync	Click Sync and click Apply to start the Sync action. The Cyber Recovery software replicates the MTree from the production system to the Cyber Recovery vault. This replication synchronizes with the previous replication of the MTree. Cyber Recovery unlocks the Cyber Recovery vault to perform the replication. i NOTE: When performing a Sync action, there might be a delay of up to 15 minutes, depending on the replication cycle on the production DD system. The Cyber Recovery software itself does not initiate a replication. Instead, it waits for the production DD system to synchronize its data over the replication interface and then validates the timestamp of the replicated data on the Cyber Recovery vault DD system.
Sync Copy	Click Sync Copy and click Apply to start the Sync Copy action. The Cyber Recovery software performs a Sync and then a Copy action. i NOTE: If the automatic retention lock feature is enabled, the Sync Copy action is not available from the Actions drop-down list.
Secure Copy	Click Secure Copy , enter the retention lock duration, and then click Apply to start the Secure Copy action. The Cyber Recovery software performs a Sync, a Copy, and then a Lock action.
Secure Copy Analyze	Click Secure Copy Analyze to start a Sync, Copy, Lock, and then an Analyze action. Enter the retention lock duration and the application nickname for the CyberSense feature. Optionally, use the slider next to Advanced Options to set more options (see Analyzing a copy for information about how to set these options). Click Apply . i NOTE: The Secure Copy Analyze action is available only if the CyberSense application is installed in the Cyber Recovery deployment.

Results

The policy starts a job. A message indicates that the job has started and provides a link to the appropriate Jobs page with the job details.

You cannot choose to run concurrent Sync or Lock actions for a policy. If you run a policy, and then run the same policy with an action that performs either a sync or lock operation, Cyber Recovery displays an informational message and does not create a job. When the initial job is completed, run the policy.

i **NOTE:** You can run concurrent Copy actions on a policy.

Adding and editing policy schedules

Schedule an action that you want the policy to perform.

Prerequisites

The policy action that you want to perform might have prerequisites. For example, a point-in-time (PIT) copy must exist if you want to perform an Analyze action.

About this task

You can create multiple schedules for the same policy. However, you cannot create multiple schedules for a policy that run simultaneously. Each schedule specifies the action that the policy performs.

Steps

1. Select **Policies** from the Main Menu.
2. In the **Policies** content pane, click **Schedules**.

3. Do one of the following:
 - a. To create a schedule, click **Add** to open the Add Schedule wizard.
 - b. To modify a schedule, select a schedule and click **Edit** to open the Edit Schedule wizard.

The **Summary** page is displayed. Click **Edit** or **Back** to go to the wizard page that you want to update.
4. On the **Schedule Information** page, complete the following fields and then click **Next**:

Table 14. Schedule Information page

Field	Description
Schedule Name	Specify a schedule name.
Policy (when adding a policy only)	Select the policy that you are scheduling.
Action	<p>Select the action that the policy performs when it runs under this schedule. See Running Policies for a description of the actions.</p> <p>NOTE: If you select Secure Copy Analyze or Analyze, the wizard displays the Analyze Options step on the left menu.</p>
Retention Lock Duration	Only if you selected Secure Copy or Copy Lock as the action, enter the duration of the retention lock that this policy applies to PIT copies.
Application Host	<p>Only if you selected:</p> <ul style="list-style-type: none"> Secure Copy Analyze or Analyze, select the CyberSense host Recovery Check, select the PowerProtect Data Manager host

5. On the **Scheduling** page, complete the following fields and then click **Next**:

Table 15. Scheduling page

Field	Description
Frequency	Enter the frequency in days and hours.
Next Run Date	<p>Select the date and time to start running the policy under this schedule.</p> <p>NOTE: The Cyber Recovery UI uses the same time zone as the Cyber Recovery management host for the scheduled time.</p>

6. If you selected the **Secure Copy Analyze** or **Analyze** action, optionally complete the following fields on the **Analyze Options** page and then click **Next**:

Table 16. Analyze Options page

Field	Description
Content Format	<p>The type of application or protocol used to perform backups. Select either:</p> <ul style="list-style-type: none"> Filesystem—For backups performed without backup software and by using NFS, CIFS, BoostFS, and so on Databases—For database client-direct backups to the DD system using DD Boost for Enterprise Applications, DD Boost for Microsoft Applications, and so on Backup—For backups performed by using backup applications such as NetWorker, Avamar, PowerProtect Data Manager, and so on. <p>This information is included as part of the CyberSense report for informational purposes.</p>
Storage Data Interface	The network storage interface through which the CyberSense feature connects to storage.

Table 16. Analyze Options page (continued)

Field	Description
Files/Directories to Include	<p>Enter text files and directories on which you want the Analyze action to run. Either:</p> <ul style="list-style-type: none"> Type the file and directory names, each on a separate line. Click Choose File to select a file that contains a list of the files and directories (one per line) to include. This file is on the host on which the Cyber Recovery UI is running. Files must be text (.txt) files. This option overwrites the content in the text box with the content in the file.
Files/Directories to Exclude	<p>Enter text files and directories that you want the Analyze action to ignore. Either:</p> <ul style="list-style-type: none"> Type the file and directory names, each on a separate line. Click Choose File to select a file that contains a list of the files and directories (one per line) to exclude. This file is on the host on which the Cyber Recovery UI is running. Files must be text (.txt) files. This option overwrites the content in the text box with the content in the file.

- Review the **Summary** page and either:
 - Click **Finish** if you are satisfied with the summary information and want to add the schedule.
 - Click **Back** to return to the previous page to change the information.
 - Click **Edit** to return to a specific page in the wizard to change information.

Managing copies

The **Policies** page enables you to view, secure, analyze, and delete point-in-time (PIT) copies.


About this task

To use the data in a PIT copy to perform a recovery operation, see the following sections:

- [Performing an Avamar recovery with Cyber Recovery](#)
- [Performing a NetWorker recovery with Cyber Recovery](#)
- [Performing a PowerProtect Data Manager recovery with Cyber Recover](#)
- [Recovering data to an alternate DD system](#)

Steps

- Select **Policies** from the Main Menu.
- Click **Copies** at the top of the **Policies** content pane to display a list of existing copies. Each row shows the copy and its associated policy, the copy creation date, the retention lock expiration date, an analysis assessment, and the recovery status.

 **NOTE:** The row does not show child copies that are associated with a PowerProtect Data Manager copy. The **Details** window provides information about child copies, as described in the following step.
- To view additional details about a copy, click the Details icon that is next to the copy name.

The **Details** window displays additional information.
- To retention lock a copy or extend the retention period of a locked copy, see [Securing a copy](#).
- To analyze a copy, see [Analyzing a copy](#).
- To retrieve a detailed report about a completed Analyze job, see [Retrieving an analysis report](#).
- To delete an unlocked copy, select the copy and then click **Delete**.

 **NOTE:**

- If the **Expiration Date** column for a copy displays a date, the copy is retention locked and cannot be deleted.
- When you delete a PowerProtect Data Manager copy that has associated child copies, those child copies are also deleted.

You can also view, lock, analyze, and delete copies by policy. From the **Policies** content pane, click the policy name to display the **Policy Details** page. Then click **Copies**.

Securing a copy

Secure a point-in-time (PIT) copy for a specific retention period during which the data in the PIT copy can be viewed, but not modified. If a copy is already retention locked, you can extend (but not decrease) the current retention period.

Prerequisites


A policy must create the PIT copy.

About this task

When a copy's retention period expires, the data is no longer protected from deletion.

Steps

1. Select **Policies** from the Main Menu.
2. On the **Policies** content pane, click **Copies** to display the list of existing copies.
3. Select the copy that you want to secure and click **Lock**.
4. In the **Lock** dialog box, specify the retention period and click **Save**.

 **NOTE:** The **Policy Retention Lock Range** field displays the minimum and maximum retention value of the policy. Specify a duration within this range.

Results


The retention lock is set. The **Expiration Date** column changes from **No lock set** and displays the expiration date and a locked icon. When the retention lock expires, the **Expiration Date** column displays the expiration date and an unlocked icon.

Analyzing a copy

Analyze a point-in-time (PIT) copy by using the CyberSense feature in the Cyber Recovery vault.

Prerequisites

A policy must create the PIT copy to analyze.

 **NOTE:** The CyberSense feature is only supported as a component of the Cyber Recovery solution in the Cyber Recovery vault; it is not supported on the production system.

About this task

A CyberSense feature license is based on TB capacity. If you:

- Exceed the licensed capacity, the analysis is completed and the Cyber Recovery software provides an alert. Until you update the licensed capacity, you receive the alert every time you run an Analyze operation. There is a 90-day grace period for you to increase the licensed capacity.
- Do not increase the licensed capacity after 90 days, the Analyze operation status is **Partial Success** and the Cyber Recovery software indicates that security analytics were not generated because the license is invalid.
- Let the license expire, the Analyze operation fails. The Cyber Recovery software indicates that there is a missing or invalid license.

Steps

1. Select **Policies** from the Main Menu.

2. On the **Policies** content pane, click **Copies** to display the list of existing copies.

You cannot run an analysis concurrently on a copy of the same policy. Otherwise, the Cyber Recovery software displays an informational message and does not create a job. When the initial job is completed, run the analysis on the copy. You can run concurrent analyses on copies of different policies.

3. Select the copy to analyze, and click **Analyze**.

If you do not have a valid license for the CyberSense feature, the **Analyze** button is disabled.

4. From the **Application Host** list box, select the application nickname for the CyberSense feature.

5. Use the slider next to **Advanced Options** to set more options.

6. Optionally, select a content format from the drop-down menu.

Choose from:

- **Filesystem**—For backups performed without backup software and by using NFS, CIFS, BoostFS, and so on
- **Databases**—For database client-direct backups to the DD system using DD Boost for Enterprise Applications, DD Boost for Microsoft Applications, and so on
- **Backup**—For database client-direct backups to the DD system using DD Boost for Enterprise Applications, DD Boost for Microsoft Applications, and so on.

This information is included as part of the CyberSense report for informational purposes.

7. Optionally, select the network storage interface through which the CyberSense feature connects to storage.

8. Optionally, enter text files and directories on which you want the Analyze action to run.

Either:

- Type the file and directory names, each on a separate line.
- Click **Choose File** to select the files and directories that are on the host on which the Cyber Recovery UI is running. Files must be text (.txt) files. This option overwrites the content in the text box with the content in the file.

9. Optionally, enter text files and directories that you want the Analyze action to ignore.

Either:

- Type the file and directory names, each on a separate line.
- Click **Choose File** to select the files and directories that are on the host on which the Cyber Recovery UI is running. Files must be text (.txt) files. This option overwrites the content in the text box with the content in the file.

10. Click **Apply**.

An informational message indicates that an analyze job is started and the **Last Analysis** column shows *Analysis in Progress*. To view the job's progress, click the link in the informational message or click **Jobs > Protection Jobs > Running** from the Main Menu.

If the analysis indicates possible malware or other anomalies, the Cyber Recovery software generates an alert and the job status is listed as **Failed**. Otherwise, the job status is listed as **Successful**.

NOTE: If you started an Analyze action on a copy, and then start a Secure Copy Analyze action on the copy, the Sync, Copy, and Lock actions complete successfully. However, if the original Analyze action has not completed, the Analyze step of the Secure Copy Analyze action fails. Wait until the original Analyze action has completed and then run the Analyze action on the new copy.

11. Optionally, cancel a running analysis, otherwise go to the next step:

- a. Click **Jobs > Protection Jobs** from the Main Menu.
- b. Click the **Running** tab.
- c. Click the radio button for the running Analyze job, click **Cancel**, and confirm the request.

An informational message indicates that the job will be canceled and the job status shows as *Canceled*. The **Status** pane on the dashboard status also shows the job status and progress percentage. The Cyber Recovery software generates an event for the cancel request.

When the job is canceled, you can immediately start another Analyze job.

The Cyber Recovery software generates an event for the cancel request. When the job is canceled, you can immediately start another Analyze job.

12. When the analysis is complete, return to the list of copies under **Policies > Copies** to view the copy details.

The **Last Analysis** column shows the results as **Suspicious**, **Good**, or **Partial**. The details pane associated with the copy includes an Analysis Details section.

If you canceled an analysis job that is in progress or the analysis skips any files, the **Last Analysis** column shows the result as **Partial** and the job status is **Canceled**. An email message and the logs indicate that the analysis job was partially successful.


If the analysis detects an anomaly, the **Last Analysis** column shows the result as **Suspicious** and the job status is **Failed**. An alert notifies you about the anomalies. Acknowledge the alert, otherwise the report for the next analysis includes the anomaly along with any new anomalies.

If an Analyze job fails, the Cyber Recovery software generates an alert.

Retrieving an analysis report

Retrieve a detailed analysis report about a completed Analyze job.

Prerequisites

- Configure an email service on the CyberSense server when you deploy the CyberSense application. You do not need to configure any additional email settings on your Cyber Recovery deployment.
 **NOTE:** CyberSense sends the analysis report. If the email service is not configured on the CyberSense server, the analysis report is not sent.
- Ensure that you have a Mail Transfer Agent (MTA) running to enable email notifications. Set up the MTA to accept the email that the Index Engines software generates. For more information, see the CyberSense documentation.

About this task

The analysis report is in the `copy-name.csv` format.

Steps

1. Select **Policies** from the Main Menu.
2. Click **Copies** at the top of the **Policies** content pane.
3. Select an analyzed copy.
4. Click **Analysis Report Actions**, and select either from the list menu:
 - **Download Analysis Report** to download an analysis report for a specified copy to the location configured for download in the browser.
 - **Email Analysis Report** to send an analysis report for a specified copy in an email message. In the list menu, enter at least one valid email address. You can then specify multiple email addresses. Click **Apply**.

An analysis report is only available for a successfully completed Analyze job for a single copy. If an Analyze job fails, the Cyber Recovery software generates an error.

The **Analysis Report Actions** button is disabled if you request a report for:

- Partially completed, failed, or canceled analysis jobs
- Multiple copies; you can request a report for only one analyzed copy at a time

Recovering data to an alternate DD system

Perform a replication action and recover data to a DD system other than the Cyber Recovery vault DD system.

Prerequisites

The production and Cyber Recovery vault DD systems must include an additional replication context. From the Cyber Recovery vault, enable the replication context and initialize it.

About this task

An alternate recovery recovers a point in time (PIT) copy quickly from the Cyber Recovery vault to the DD production system or an alternate DD system. The alternate DD system can be at any location.

Steps

1. Create a recovery MTree on the Cyber Recovery vault DD system, and then enable and initialize the replication context.

The replication source must be on the Cyber Recovery vault DD system and replication destination must be on the production DD system or an alternate DD system.

2. Run the `CRCLI recovery` command.

The following is an example of the command to recover data to an alternate DD system:

```
crcli recovery run -action recover-to-alternate --copypname cr-copy-  
policy1-20180202000102 --recoveryMtree /data/coll/cr-recover-to-alternate --  
ethernetPort ethV1 --watch 15
```

Cyber Recovery sandboxes

A sandbox is a unique location in the Cyber Recovery vault in which you can perform read/write operations on a point in time (PIT) copy. This copy is a read/write copy of the locked data in the Cyber Recovery vault.

The Cyber Recovery software supports two types of sandboxes:

- System sandboxes—The Cyber Recovery software enables you to create custom sandboxes manually to perform operations by using applications that are not in the Cyber Recovery default list. A sandbox can contain only one PIT copy, however, you can create multiple sandboxes for one PIT copy. You create sandboxes as needed for data analysis or validation operations. The CyberSense feature software automatically creates a system sandbox when you initiate an analyze operations on a PIT copy.
- Recovery sandboxes—The Cyber Recovery software automatically creates recovery sandboxes when you initiate a Networker, Avamar, or PowerProtect Data Manager recovery.

Managing sandboxes


Create a system sandbox to perform data analysis or validation operations.


About this task

You can create sandboxes as needed for data analysis or validation operations. The CyberSense feature, which analyzes backup data for the presence of malware or other anomalies, requires a sandbox.

Steps

1. From the Main Menu, click **Recovery**.
2. On the **Recovery** content pane, click **COPIES** and select a PIT copy from the list.
3. Click **Sandbox**.
4. In the Sandbox dialog box:
 - a. Select an application host that is configured in the Cyber Recovery vault.
 - b. Enter a unique sandbox name.

 **NOTE:** The **cr** prefix is appended to the custom sandbox name. For example, if you enter **MySandbox**, the sandbox name displays as **cr-MySandbox**.
 - c. Indicate if you want to mount the file system. Enter where you want to mount the data if you do not want to use the default.

 **NOTE:** Cyber Recovery supports mount operations for UNIX operating systems only. The host is available by using SSH.
 - d. Click **Apply**.

This step starts a job. A message indicates that the job has started and provides a link to the appropriate Jobs page with the job details.
5. From the **Recovery** content pane, click **SANDBOXES**:
 - a. View the list of sandboxes.

The row does not show child sandboxes that are associated with a PowerProtect Data Manager sandbox. The **Details** window provides information about child copies, as described in the following step.

- b. To view details about a sandbox, click the sandbox's row.

The **Details** window displays the information.

- c. To remove a sandbox, select a sandbox and then click **Delete**.

When you delete a PowerProtect Data Manager sandbox that has associated child sandboxes, those child sandboxes are also deleted.

Managing recovery sandboxes

The Cyber Recovery software creates a recovery sandbox during a recovery operation and populates it with the selected copy. The sandbox is available to the application host.

Prerequisites

Run a recovery operation.

About this task

The **Recovery Sandboxes** pane is empty until you run a recovery operation.

Steps

1. From the Main Menu, click **Recovery**
2. On the **Recovery** content pane, click **Recovery Sandboxes**.
3. Do one of the following:
 - a. To view the recovery details, select the `recoverapp_<ID>` name.
 - b. To validate success, click **Launch App** to access the NetWorker or PowerProtect Data Manager UI in the Cyber Recovery vault.

The **Launch App** button is not available unless a recovery has completed successfully.
 - c. To clean up for an existing recovery, click **Cleanup**.

Monitoring

This section describes how to use the dashboard in the Cyber Recovery UI to monitor Cyber Recovery operations and take corrective steps when necessary.

NOTE: For information about Cyber Recovery auditing and logging capabilities, see the *Dell EMC PowerProtect Cyber Recovery Security Configuration Guide*.

Topics:

- [Monitoring the Cyber Recovery vault status](#)
- [Monitoring alerts and events](#)
- [Monitoring jobs](#)

Monitoring the Cyber Recovery vault status

The Cyber Recovery vault status indicates if the vault connection to the production system is open (Unlocked) or closed (Locked). The Cyber Recovery vault is in the Locked state unless the Cyber Recovery software is performing a replication.

After Cyber Recovery software installation and initial configuration, the Cyber Recovery vault might be unlocked. This behavior is as designed. An initialization might be in progress while you are configuring the Cyber Recovery environment, therefore, the port must be open. The Cyber Recovery software creates a job for the initial Sync operation, which you can use to monitor the operation. When the initialization is complete, the port closes automatically.






NOTE: You cannot create another Sync job while the initial Sync job is running.

If necessary, the Security Officer or an Admin user can manually lock the vault and close the connection. For more information, see [Manually securing and releasing the Cyber Recovery vault](#).

To view the Cyber Recovery vault connection status, click **Dashboard** in the Main Menu. The state is displayed under **Status**.

The following table describes the connection states:

Table 17. Cyber Recovery connection states

Status	Icon	Description
Locked		All configured replication connections are closed because no replication is being performed. If a replication policy is run, the Cyber Recovery software opens the connection and changes the vault state to Unlocked.
Unlocked		One or more replication network connections are open because a replication is being performed. The state returns to Locked when the replication completes.
Secured		All replication network connections are secured because the Security Officer or an Admin user manually locked the connection due to a security breach. You cannot initiate any replication policy actions. When the Cyber Recovery vault is released and returns to the Locked state, you can then run replication policies.
Degraded		If there are multiple DD systems in the Cyber Recovery vault and one DD system is unable to communicate with the Cyber Recovery software, the vault status is Degraded. This scenario can occur if you change either the FQDN or the IP address of the DD system. An alert notifies you about the Cyber Recovery vault status.
Unknown		If there are multiple DD systems in the Cyber Recovery vault and all the DD systems are unable to communicate with the Cyber Recovery software, the vault status is Unknown. This scenario can occur if you do not create policies when you first install the Cyber Recovery software or if you change either the FQDNs or IP addresses of the DD systems. An alert notifies you about the Cyber Recovery vault status.

Monitoring alerts and events

The Cyber Recovery software generates notifications about alerts and events.

You can view alerts and events from:

- The dashboard
- The Alerts and Events content pane
- The icon in the Masthead Navigation (alerts only)

An alert indicates that an event occurred and might require you to take action.

Alert categories include:

- **System**—Indicates a system issue that might compromise the Cyber Recovery system such as a failed component
- **Storage**—Indicates storage issues such as insufficient disk space
- **Security**—Indicates that a user cannot log in or malware might have been detected

The Alerts content pane enables you to view additional details, acknowledge, and add notes for an alert.

Events indicate system events, such as the start of a job, completion of a retention lock, Security Officer login, and updated user information. The Events content pane enables you to view additional details for an event by clicking the details icon.

Handling alerts


An alert indicates that you might have to take action.

Steps


1. Select **Alerts and Events** from the Main Menu.
The content pane lists the alerts.
2. To view details about an alert, click the Details icon at the beginning of the row.
The **Details** pane displays additional details about the alert.
3. Take any necessary actions to resolve the problem.
4. Select an alert or multiple alerts and click **Acknowledge**.

The **Acknowledge** column now displays a flag icon for each selected alert.

If you click the select all checkbox at the head of the checkboxes column, all the alerts on the current page are selected.

 **NOTE:** The dashboard and the Navigation Masthead no longer show these alerts. Only the five most recent unacknowledged alerts are displayed on the dashboard and from the drop-down list on the Navigation Masthead.

5. Optionally, click **Unacknowledge** to remove the acknowledgment from the alert.
The unacknowledged alerts are displayed on the dashboard and from the drop-down list on the Navigation Masthead again.
6. To add a note about an alert, select the alert and click **Add Note**. Enter a note into the **Add Note** window.

 **NOTE:** You can add only one note to an alert at a time. You cannot add a note to multiple alerts at a time.


The note is displayed in the alert's **Details** pane.

Monitoring jobs

When you run a policy, a recovery operation, a system backup, or a cleaning operation, the Cyber Recovery software creates a job.

The **Jobs** option on the Main Menu enables you to select these types of jobs:

- **Protection Jobs**—Includes jobs for Copy, Sync, Sync Copy, Secure Copy, Analyze, and Secure Copy Analyze actions and when you delete a copy
- **System Jobs**—Includes jobs for a cleaning operation and disaster recovery backup
- **Recovery Jobs**—Includes jobs for sandbox creation and deletion, recovery check, and application recovery and cleanup

 **NOTE:** When a cleaning operation deletes copies, the deletion step is shown as a Protection job type.

The **Jobs** content panes show the job status, which indicates the job's progress. It lists jobs that are running, successfully completed, canceling, or canceled. When a job is completed, its status is either **Successful**, **Completed w/Exceptions**, or **Failed**. If a job's status is **Failed**, a critical alert is also associated with the job.

The **Running** tab also includes the option to cancel a running job.

The Security Officer (crso) can set up a daily Cyber Recovery job activity report. User-defined values determine when the report is generated. For more information, see [Configuring a daily activity report](#).


Managing jobs

Manage jobs and view job details from the Jobs content pane.

Prerequisites

A policy, a recovery operation, a system backup, or a cleaning operation has been run, which creates a job.

Steps

1. From the Main Menu, select a job type from the Jobs list menu.
The content pane for completed jobs of the specified type opens. It displays categorized job status links at the top of the content pane and a list of the jobs.
 2. To access a list of running jobs, click the **Running** tab.
The content pane for running jobs of the specified type opens. It displays categorized job status links at the top of the content pane and a list of the jobs.
 3. To refresh the content pane, click the refresh icon.
To select how often the content pane refreshes, click the ellipsis next to the refresh icon and select a time from the list. There is also an option to show a timer.
 4. To view details about a job, do the following from either the **Completed** or **Running** tab:
 - a. To see jobs with a specific status, click a job status link at the top of the content pane. To list all jobs again, click the **Total** link.
 - b. For additional information about a job, click the row for the job.
In the Details window, the **Details** tab provides job information and the **Step Log** tab shows the progress of each task in the job. In the Running tab, the step log shows the steps that are completed, in process, and not yet started. In the Completed tab, the step log shows the steps that were completed successfully, the step on which an action was canceled or failed, and any actions that were not started due to a cancellation or failure. Click the arrow on the right to close the window.
 - c. To customize the columns in the table that lists the jobs, click the gear icon and select the columns to show or hide.
 - d. To manage which jobs are displayed, click the funnel icon in each column to set a filter.
The filtered content is displayed and a lozenge with the filter value is shown above the table. If the status filter includes multiple values, hover over the lozenge to see all values. You can also use the search field above the column titles.
 - e. To clear a specific filter, click the **X** in the lozenge. To click all the filters, click **Clear Filters**.
 - f. To sort the jobs, click the column title.
 5. To download an Excel spreadsheet that contains job details for currently filter content, click **Export** on either tab.
 6. To cancel a running job:
 - a. Click the **Running** tab.
 - b. Click the radio button next to the name of the job that you want to cancel.
 - c. Click **Cancel** and confirm that you want to cancel the job.
An informational message indicates that the job is being canceled and the Cyber Recovery software generates an alert for the cancel request.
The progress and the step of the cancellation process is displayed. Go to the **Step Log** tab in the **Details** window to see on which step the process was canceled.
When the cancellation is completed, the job is no longer displayed in the Running pane.
-  **NOTE:** You can cancel only one job at a time.
- d. Click the **Completed** tab to verify that the job shows the Canceled status.

Performing a NetWorker Recovery with Cyber Recovery

This section describes how to use the Cyber Recovery UI to recover data from NetWorker point in time copies.

NOTE: Cyber Recovery Version 19.9 and later support the addition of the NetWorker application running on Windows to the Cyber Recovery environment. For NetWorker on Windows, Cygwin is required and a mount operation is not supported for a NetWorker sandbox. Versions earlier than Cyber Recovery Version 19.11 do not support backup applications running on Windows or the addition of Windows applications to the Cyber Recovery environment.

Topics:

- [Recovering NetWorker data](#)
- [Creating the NetWorker DD Boost user/UID for recovery](#)
- [Initiating a NetWorker recovery in the Cyber Recovery UI](#)

Recovering NetWorker data

Use a point-in-time (PIT) copy to rehydrate NetWorker data in the Cyber Recovery vault.

The NetWorker application must be added as the root user in the Cyber Recovery vault. The Cyber Recovery software uses NetWorker commands such as `nsrdr`, which require root permissions.

Before a recovery operation, run application and server backups in the production environment. Then, perform a Secure Copy policy operation to copy data to the Cyber Recovery vault environment.

From the Cyber Recovery UI, initiate a recovery.

NOTE: You can only run one recovery job per application at a time.

Creating the NetWorker DD Boost user/UID for recovery

Before performing a NetWorker recovery, create the DD Boost account that is associated with the copy in the Cyber Recovery vault.

Steps

1. To determine the UID required for recovery, log in to the CRCLI and run the following command on the management host:

```
# crcli login -u <Cyber Recovery user>
# crcli policy list-copy --policyname <policy name> -c <copy name>
```

Note the output from this command, as shown in the following example:

```
# Source Storage UID: 503
```

2. To determine if the account exists for this UID, log in to the DD system in the Cyber Recovery vault and run the following command:

```
# user show list
```

- If the output lists the UID, you can proceed with the recovery procedure.

- If the output does not show that the UID exists, go to the next step.

3. Create the UID:

- When adding the application asset, if you defined a tag, reference the tag to determine the production system DD Boost username.
- Create the username and account by running the following command:

```
# user add <NetWorker_ddboostname> uid <UID from user show list output>
```

- For earlier versions, run the `user add` command until you get the UID required for recovery. For example, if you have a UID 510, you might have to create up to nine temp accounts. Note that user add on the DD system starts at UID 500.

Initiating a NetWorker recovery in the Cyber Recovery UI

Initiate a recovery in the Cyber Recovery UI. After you initiate a recovery, the Cyber Recovery software uses the latest system device to complete the recovery operation automatically.

Prerequisites

Ensure that the following prerequisites are met before you initiate a NetWorker recovery:

- You have obtained the credentials for the Cyber Recovery vault host on which the NetWorker application is installed and for the NetWorker application.
- The NetWorker server host in the Cyber Recovery vault has the same IP address and hostname as the NetWorker production host.
 - NOTE:** It is not mandatory that the IP address of the server host in the Cyber Recovery vault be the same as the NetWorker production host. However, if you use a different IP address, you might encounter issues with components and agents referring to the NetWorker server by IP address, which require manual intervention. You can avoid these issues if the IP addresses are the same.
- The NetWorker application is installed in the Cyber Recovery vault and defined as an application asset in Cyber Recovery.
- The DD Boost user within the vault has the same UID as the production DD Boost user.
- A policy has created a point-in-time (PIT) copy to use for the recovery.
- The UID associated with this copy has been created in the Cyber Recovery vault DD system.
- If your deployment includes NetWorker on Windows, ensure that a Windows host and Cygwin are installed in the Cyber Recovery vault, and Cygwin OpenSSH is enabled. For more information, see the Dell PowerProtect Cyber Recovery Installation Guide.

Steps

1. Select **Recovery** from the Main Menu.
2. On the **Recovery** content pane, select the copy, and then click **Application**.

NOTE: If you select a Windows copy, ensure that you select the NetWorker on Windows application. If you select a copy that does not match the operating system, the recovery operation fails.

3. In the **Application** dialog box, do the following:

- Select a NetWorker application host.
- Enter the DD Boost username and password.
- Optionally, enter the name of the folder that includes the last bootstrap backups.


NOTE: If you do not complete this field, the software scans all volumes in the MTree. By completing this field, the automated NetWorker recovery is faster.

- Click **Apply**.

The Cyber Recovery software runs a job to create a recovery sandbox, populates it with the selected copy, and then makes the sandbox available to the application host.

4. Wait for the recovery application job to complete creating the sandbox.

The recovery sandbox is created for the NetWorker application. The latest NetWorker configuration is recovered.

5. Click the job `recoverapp_<ID>` name and view the status detail.
The Status Detail provides the name of the newly created sandbox.
 6. Click **Recovery Sandboxes** from the top of the **Recovery** pane and do the following:
 - a. To view the recovery details, select the `recoverapp_<ID>` name.
 - b. To validate success, click **Launch App** to access the NetWorker UI in the Cyber Recovery vault.
The **Launch App** button is active only when the recovery is completed successfully.
 - c. To delete the sandbox, click **Cleanup**.
 7. (Optional) Run the following commands, which are not part of the automated recovery procedure:
 - To populate the recovered media database with the latest save sets, run the `scanner -i <device name>` command on each device that was created during the recovery.
 - To rebuild the client file indexes, run the `nsrck -L7` command. This step is required for browsing files and database recovery.
-  **NOTE:** The `scanner -i` and `nsrck -L7` commands are optional, however, they might be required for certain scenarios. For more information, see the *NetWorker Server Disaster Recovery Best Practices Guide*.

Performing an Avamar Recovery with Cyber Recovery

This section describes how to use the Cyber Recovery UI and CRCLI to recover data from Avamar point-in-time copies.

Topics:

- [Recovering Avamar data](#)
- [Preparing the production-side Avamar system](#)
- [Checklist for Cyber Recovery with Avamar](#)
- [Creating the Avamar DD Boost account and UID for Cyber Recovery](#)
- [Initiating an Avamar recovery in the Cyber Recovery UI](#)
- [Performing manual steps for Avamar recovery](#)
- [Cleaning up after an Avamar recovery](#)

Recovering Avamar data


Use a point-in-time (PIT) copy to rehydrate Avamar data in the Cyber Recovery vault.

The Avamar application must be added as the root user in the Cyber Recovery vault. The Cyber Recovery software uses Avamar commands that require root permissions.

Before a recovery operation, run application and server backups in the production environment. Then, perform a Secure Copy policy operation to copy data to the Cyber Recovery vault environment.

A recovery operation is a two-step process:

1. From the Cyber Recovery UI, copy the PIT copy into a read-writable sandbox.
2. Perform manual recovery steps on the application host.

 **NOTE:** You can only run one recovery job per application at a time.

Preparing the production-side Avamar system

Optionally, perform the following procedure if you want to create a checkpoint before performing a Secure Copy policy operation:

Steps

1. Log in to the production Avamar server as root user and run a checkpoint operation. This step might take some time.
 - a. Type **su admin -c "mcserver.sh --flush"**:

```
root@ave-03:~/#: su admin -c "mcserver.sh --flush"
=== BEGIN === check.mcs (preflush)
check.mcs                                     passed
=== PASS === check.mcs PASSED OVERALL (preflush)
Flushing Administrator Server...
Administrator Server flushed.
```

- b. Type **mccli checkpoint create**:

```
root@ave-03:~/#: mccli checkpoint create
0,22624,Starting to create a server checkpoint.

root@ave-03:~/#: mccli checkpoint show
```



```
0,23000,CLI command completed successfully.
Tag                Time                Validated Deletable
-----
cp.20180316130025  2018-03-16 09:00:25 EDT Validated No
cp.20180316130301  2018-03-16 09:03:01 EDT          No
cp.20180316151143  2018-03-16 11:11:43 EDT          No
```

- c. Type **mccli checkpoint validate --cptag=<cp tag name>**:

```
root@ave-03:~/#: mccli checkpoint validate --cptag=cp.20180316151143
0,22612,Starting to validate a server checkpoint.
Attribute Value
-----
tag          cp.20180316151143
type         Full
```

```
root@ave-03:~/#: mccli checkpoint show
0,23000,CLI command completed successfully.
Tag                Time                Validated Deletable
-----
cp.20180316130301  2018-03-16 09:03:01 EDT          No
cp.20180316151143  2018-03-16 11:11:43 EDT Validated No
```

2. On the Cyber Recovery host, run a Secure Copy policy action for the DD MTree.
3. Validate the size of the production DD system MTree that was replicated is the same as the replicated MTree on the destination DD system and the Cyber Recovery MTree.
 - a. Type **mtree list**, as shown in the following code example:

```
sysadmin@crmgmthost# mtree list
Name                Pre-Comp (GiB)  Status
-----
/data/coll/avamar-1560177494-repl  4.2            RO/RD
/data/coll/backup              0.0            RW
/data/coll/cr-policy-5d5ad66394422f0001ced229-repo  0.0            RW/RLGE
/data/coll/cr-policy-5d5ad69994422f0001ced22a-repo  4.2            RW/RLGE
/data/coll/nw02-repl           0.0            RO/RD
-----
D      : Deleted
Q      : Quota Defined
RO     : Read Only
RW     : Read Write
RD     : Replication Destination
RLGE   : Retention-Lock Governance Enabled
RLGD   : Retention-Lock Governance Disabled
RLCE   : Retention-Lock Compliance Enabled
```

- b. Verify that the production-, target-, and policy-replicated MTrees are the same.

Checklist for Cyber Recovery with Avamar

Perform the following tasks for the Avamar system in the Cyber Recovery vault:

Table 18. Avamar prerequisites

Done	Task	Notes
	Review the latest KB articles. NOTE: Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.	In particular, ensure that you review the following KB articles: <ul style="list-style-type: none"> Knowledge Base Article Number 188334 at https://www.dell.com/support/kbdoc/en-us/000188334/avamar-install-upgrades-in-a-cyber-recovery-vault—The Avamar server in the Cyber Recovery vault can be used for rollbacks to a point in time of the production Avamar server. This step can leave Avamar in a state that can cause issues during future updates to the Avamar server. Knowledge Base Article Number 181972 at https://www.dell.com/support/kbdoc/en-in/000181972—If you encounter any issues restoring the MCS; applies to Avamar 19.3 and later. Knowledge Base Article Number 119875 at https://www.dell.com/support/kbdoc/en-in/000017578—For information about run levels.
	Ensure that your Avamar deployment is up to date.	See the latest KB articles.
	Add the Avamar application as the root user.	n/a
	Obtain the credentials for the host on which the Avamar application is installed.	n/a
	Ensure that the Avamar version and build are identical to the production system.	n/a
	Ensure that the Avamar fully qualified domain (FQDN) name is identical to the production system.	You can use a different IP address in the Cyber Recovery vault. The FQDN must be identical.
	Ensure that all Avamar credentials such as MCUser/GSAN accounts have the same passwords.	For Avamar services to start properly, the Avamar credentials must be the same.
	Ensure that the DD Boost username and UID in the Cyber Recovery vault match the credentials of the production system.	Ensure that DD Boost username and UID are configured in the Cyber Recovery vault before performing the Cyber Recovery steps.
	Obtain Avamar licenses, if necessary.	n/a
	Establish Avamar applications in the Cyber Recovery vault.	This task enables rehydrating applications in the Cyber Recovery vault
	Ensure that DD OS version in the Cyber Recovery vault is compatible with the Avamar application.	Ensure that the DD OS version works with the Avamar application.
	Configure the DD hostname in the Avamar application.	Set this hostname in the Cyber Recovery vault for the Avamar application to perform its recovery.

Creating the Avamar DD Boost account and UID for Cyber Recovery

Before performing an Avamar recovery, create the DD Boost account that is associated with the copy in the Cyber Recovery vault.

Steps

1. To determine the UID required for recovery, log in to the CRCLI and run the following command on the management host:

```
# crcli login -u <Cyber Recovery user>
# crcli policy list-copy --policyname <policy name> -c <copy name>
```

For example:

```
# crcli login -u User1
crso password:

User login successful
# crcli policy list-copy -n policy1 -c cr-copy-policy1-2020120914175
```

Note the output from this command, as shown in the following code example:

```
Source Storage UID      : 502
```

Where 65534 is the UID that you associated with this policy.

2. To determine if the account exists for this UID, log in to the DD system in the Cyber Recovery vault and run the following command:

```
# user show list
```

- If the output lists the UID, you can proceed with the recovery procedure.
- If the output does not show that the UID exists, go to the next step.

3. Create the UID:

- a. When adding the application asset, if you defined a tag, reference the tag to determine the production system DD Boost username.
- b. If you are running DDOS 6.2.1.50 or later, create the username and account by running the following command:

```
# user add <username> uid <UID> role admin
```

Where the UID value is the UID that you identified in step 1.

For example:

```
# user add avdd uid 500 role admin
```

Initiating an Avamar recovery in the Cyber Recovery UI

Initiate a recovery in the Cyber Recovery UI and then complete the recovery by performing manual steps on the application server in the Cyber Recovery vault.

Prerequisites

This procedure assumes:

- The Avamar application is installed in the Cyber Recovery vault and defined as an application asset in Cyber Recovery.
- A policy has created a point-in-time (PIT) copy to use for the recovery.

- The UID associated with this copy has been created in the Cyber Recovery vault DD system.

Steps

1. Log in to the Cyber Recovery UI.
2. Select **Recovery** from the Main Menu.
3. On the **Recovery** content pane, select the copy and click **Application**.
4. In the **Recovery** dialog box, select the Avamar application host and click **Apply**.
The Cyber Recovery software runs a job to create a recovery sandbox, populates it with the selected copy, and then makes the sandbox available to the application host.
5. Wait for the recovery application job to complete creating the sandbox.
The recovery sandbox is created for the Avamar application.
6. Click **Recovery Sandboxes**.
7. Click the `avamar-<SYSTEMID>` name, as shown in the following example, and view the status detail:

```
avamar-1560177494
```

NOTE:

- Record the `avamar-<SYSTEMID>` name, which the following steps require. The SYSTEMID is also known as the `hfsctime`
- The Status Detail provides the name of the newly created sandbox. Use this name for the following recovery steps.

Performing manual steps for Avamar recovery

After initiating an Avamar recovery in the Cyber Recovery UI, perform the following steps on the Avamar server host in the Cyber Recovery vault.

Prerequisites

- You have performed the UI steps initiating the recovery as described in *Initiating an Avamar recovery in the Cyber Recovery UI*.
- Prepare a table or document to record Cyber Recovery, Avamar, and other usernames and passwords.


About this task

Use a PuTTY or SSH session that is connected to the Avamar server in the Cyber Recovery vault to perform the following commands.

Steps

1. Stop the Avamar services on the Avamar server:
 - a. Log in as `admin` to the Avamar system.
 - b. Check if Avamar services are running:

```
dpnctl status
```


 **NOTE:** If GSAN is not running, go to step 2. Otherwise, got to the next step.

- c. Create an `ssh-agent` session:

```
ssh-agent bash
ssh-add ~admin/.ssh/admin_key
```

- d. Stop the Avamar processes:

```
dpnctl stop all
```

 **NOTE:** This step might take some time to stop all Avamar processes.

- e. Type **y** to confirm that you want to shut down the instance:


```
Do you wish to shut down the local instance of EM Tomcat?

Answering y(es) will shut down the local instance of EM Tomcat
n(o) will leave up the local instance of EM Tomcat
q(uit) exits without shutting down

y(es), n(o), q(uit/exit): y
```

- f. When the process is completed, run the `dpnctl status` command to verify the results, as shown in the following example:

```
dpnctl status
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/admin_key)
dpnctl: INFO: gsan status: not running
dpnctl: INFO: MCS status: down.
dpnctl: INFO: emt status: down.
dpnctl: INFO: Backup scheduler status: down.
dpnctl: INFO: Maintenance windows scheduler status: unknown.
dpnctl: INFO: Unattended startup status: disabled.
dpnctl: INFO: avinstaller status: up.
dpnctl: INFO: ConnectEMC status: up.
dpnctl: INFO: ddrmaint-service status: down.
dpnctl: INFO: [see log file "/usr/local/avamar/var/log/dpnctl.log"]
```

 **NOTE:** The preceding output might differ depending on the Avamar version.


2. Switch to `root` by typing the following command :

```
su -
```

Type the root password.

3. Ensure that all references to the DD system point to the Cyber Recovery vault IP address.

Edit the `/etc/hosts` file to alias the production DD FQDN as the Cyber Recovery vault DD system IP address.

 **NOTE:** In the following example, `ddve-prod-05` is the name of the production DD system and `192.168.2.106` is the IP address of the Cyber Recovery vault DD system (also known as `ddve-cr-06`). The FQDNs and short names for both DD systems are assigned to the `192.168.2.106` IP address.

```
cat /etc/hosts
127.0.0.1 localhost.localdomain localhost
::1 localhost.localdomain localhost
#(ave-03 is the production hostname
# but the IP specified must point to the vault IP.)
192.168.2.83 ave-03.vcorp.local ave-03
192.168.2.106 ddve-prod-05.vcorp.local ddve-prod-05 ddve-cr-06.vcorp.local ddve-cr-06
```

4. Verify that the production DD hostname resolves to the Cyber Recovery vault IP address:

```
ping ddve-05.vcorp.local
```

The IP address of the Cyber Recovery vault DD is displayed. Press `Ctrl-c` to exit the ping utility.

5. Optionally, run the following command on the Cyber Recovery vault DD system to verify that the MTree on the Cyber Recovery vault DD system matches the production MTree name:

```
mtree list
```

The Cyber Recovery software creates a recovery sandbox with the same name that Avamar uses in production system. The HFS creation time (`hfsctime`) value follows the `avamar_` prefix. For example, the recovery sandbox is created as `avamar_1491947551` and the `hfsctime` value is `1491947551`. Use this value in the following steps.

NOTE: The `hfsctime` was previously referred to as `SYSTEMID`.

6. On the Cyber Recovery vault DD system, ensure that the `ddboost` user name matches the name on the production system, including the UID. Ensure that you use the `ddboost` user that you set on the Cyber Recovery vault DD system.

user show detailed ddboostuser

```
sysadmin@ddve72# user show detailed ddboostuser
User:                                ddboostuser
Uid:                                518
Role:                                admin
Last Login From:                     <unknown>
Last Login Time:                     never
Status:                              enabled
Password Last Changed:               Mar 29, 2022
Disable Date:                        never
Minimum Days Between Password Change: 0
Maximum Days Between Password Change: 90
Warning Days Between Password Change: 7
Disable Days After Expire:           never
Force Password Change at Next Login:  no
sysadmin@ddve72#
```

7. As `root`, run a checkpoint restore operation from the Avamar recovery vault by using the `HFS` Time of the Avamar DD Boost storage-unit:
 - a. Run the following command:

```
cprestore --hfsctime=1491947551 --ddr-server=ddve-05.vcorp.local --ddr-user=ddboost
```

NOTE: The `hfsctime` value comes from the `avamar-<SYSTEMID>`, which you recorded from the preceding steps. Only the number is needed.

- b. When prompted, enter the `ddboost` user password.
The script displays a list of restorable checkpoints and asks which one you want to restore (similar to the following example):

```
Mount NFS path 'ddve-05.vcorp.local:/data/col1/avamar-1491935387/GSAN' to
'ddnfs_gsan'
Mount path 'ddnfs_gsan' already is mounted... skipping.

There are 4 available checkpoints.
  cp.20180315171722
  cp.20180316130025
  cp.20180316151143

Checkpoint to restore or 'quit' to stop?
```

NOTE: The preceding values differ on all systems. Use the production-side checkpoint that was replicated to the Cyber Recovery vault.

- c. Enter the checkpoint that you want to restore, for example `cp.20180316151143`. When prompted, type `yes` to confirm your entry.
The restore procedure is performed from the recovery sandbox, and the script terminates with messages that confirm the operation. This step might take several minutes.
 - d. When prompted, type the `ddboost` user password.
 8. On the Cyber Recovery vault DD system, perform the following steps:
 - a. Log in to the Cyber Recovery vault DD CLI as an admin user.
 - b. Create the checkpoint snapshot by using the same checkpoint name that you selected in step 7a:

```
snapshot create <checkpoint name> mtree <name of avamar mtree/sandbox>
```

For example:

```
snapshot create cp.20190826122838 mtree /data/col1/avamar-1560177494
```

- c. On the Avamar server in the Cyber Recovery vault, run the following command:

```
cplist
```

This command confirms that the Avamar server detects the checkpoint that is restored.

9. Roll back the GSAN on the vault Avamar server:

- a. Using a checkpoint from step 7a, start a rollback recovery of the checkpoint:

```
rollback.dpn --cptag=cp.<checkpoint name> --noddrollback --nogetserverlogs 2>&1 | tee -a rollback.out
```

- b. Wait for the GSAN to complete the startup, running, and full access run levels.

NOTE: For more information about run levels, see Knowledge Base Article Number 119875 at <https://www.dell.com/support/kbdoc/en-in/000017578>. Access to this document depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

The rollback is complete when the prompt and a `status.dpn` output is displayed, as shown in the following example:

```
wait.dpn --runlevel=fullaccess --hfsaddr=avamard --verbose
Checking for server ready. Please wait.
0.0 state=ONLINE runlevel=startup
sleep 10
Checking for server ready. Please wait.
0.0 state=ONLINE runlevel=running
sleep 10
Checking for server ready. Please wait.
0.0 state=ONLINE runlevel=fullaccess
```

NOTE: If the GSAN startup exceeds 300 seconds, allow it to continue. The run will either finish or end with an error. If it ends with an error, see the `/data01/cur/gsan.log` file and Knowledge Base Article Number 119875 at <https://www.dell.com/support/kbdoc/en-in/000017578>. Access to this document depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

10. Rollback MCS and start remaining services:

- a. As admin, type the following:

```
hostname -f  
mcserver.sh --restore --norestart --v
```

- b. When prompted, type the FQDN of the Avamar server from step b.
c. Press Enter to keep port 27000.
d. Wait for the MCS database to restore.

11. Restore the lockbox credentials:

- a. Type `su -` to switch to root.
b. Got to the `cd /home/admin` directory.
c. Ensure that you have the most recent `lockbox_restore.pl` script by viewing Knowledge Base Article Number 181972 at <https://www.dell.com/support/kbdoc/en-in/000181972>. If you do not have the latest version, download the script from the link in the Knowledge Base Article.
Access to the Knowledge Base Article depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.
d. Run the `lockbox_restore.pl` script:

```
./lockbox_restore.pl
```

12. Start the MCS:

- a. Type `su - admin` to switch to admin:

- b. Run the following command:

```
mcserver.sh --start --v
```

13. To validate that all required services are up and running, do the following:

- a. Run the `dpnctl status` command, as shown in the example:

dpnctl status

```
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/admin_key)
dpnctl: INFO: gsan status: up
dpnctl: INFO: MCS status: up.
dpnctl: INFO: emt status: up.
dpnctl: INFO: Backup scheduler status: down.
dpnctl: INFO: Maintenance windows scheduler status: suspended.
dpnctl: INFO: Unattended startup status: disabled.
dpnctl: INFO: avinstaller status: up.
dpnctl: INFO: ConnectEMC status: up.
dpnctl: INFO: ddrmaint-service status: up.
dpnctl: INFO: [see log file "/usr/local/avamar/var/log/dpnctl.log"]
```

NOTE: The preceding output might differ depending on the Avamar version. Note that the scheduler is down and the Maintenance window scheduler is suspended.

- b. Start any subsystems that are stopped:

```
dpnctl start <subsystem>
```

NOTE: Leave the scheduler and maintenance processes as down.

14. Type **exit** and switch back to root.

15. As root, add the SSH key for the Cyber Recovery production DD FQDN to the newly restored Avamar server in the Cyber Recovery vault, as shown in the following example:

```
cat ~admin/.ssh/ddr_key.pub | ssh ddboost@ddve-05.vcorp.local adminaccess add ssh-key
```

16. Update the security configuration on the newly restored Avamar server by entering the following commands:

- a. Regenerate the security certificates:

enable_secure_config.sh --certs

```
Exporting MC Root CA certificate
Certificate stored in file <chain.pem>
Creating GSAN server certificates
Generating key/cert pair for ave-03.vcorp.local / 0.0

Reloading GSAN certificates for new changes to take effect

Done
```

- b. Verify the session security settings:

enable_secure_config.sh --showconfig

Current Session Security Settings

```
-----
"encrypt_server_authenticate"           ="true"
"secure_agent_feature_on"               ="true"
"session_ticket_feature_on"             ="true"
"secure_agents_mode"                   ="secure_only"
"secure_st_mode"                       ="secure_only"
"secure_dd_feature_on"                  ="true"
"verifypeer"                           ="yes"
```

Client and Server Communication set to Authenticated mode with Two-Way/Dual Authentication.


```
Client Agent and Management Server Communication set to secure_only mode.
Secure Data Domain Feature is Enabled.
```

- c. If your results do not match the output in the preceding step, that is, if the output shows false and unsecure_only settings, go to the next step. Otherwise, go to substep f.
- d. Run the following command to enable security:

```
enable_secure_config.sh --enable-secure-all
```

- e. Run the following command to verify that false and unsecure_only settings are changed to true and secure_only:


```
enable_secure_config.sh --showconfig
```

```
Current Session Security Settings
-----
"encrypt_server_authenticate" = "true"
"secure_agent_feature_on" = "true"
"session_ticket_feature_on" = "true"
"secure_agents_mode" = "secure_only"
"secure_st_mode" = "secure_only"
"secure_dd_feature_on" = "true"
"verifypeer" = "yes"
```

- f. Restart the Avamar MCS services:

```
su admin -c 'mcserver.sh --restart --v'
=== BEGIN === check.mcs (poststart)
check.mcs                                     passed
=== PASS === check.mcs PASSED OVERALL (poststart)

Administrator Server shutdown initiated.
Stopping Administrator Server...
Administrator Server stopped.
Database server is running...
INFO: Starting messaging service.
INFO: Started messaging service.
=== BEGIN === check.mcs (prestart)
check.mcs                                     passed
=== PASS === check.mcs PASSED OVERALL (prestart)
Starting Administrator Server at: Fri Mar 16 14:15:37 EDT 2018
Starting Administrator Server...
Administrator Server started.
INFO: Starting Data Domain SNMP Manager....
INFO: Connecting to MCS Server: ave-03.vcorp.local at port: 7778...
INFO: Successfully connected to MCS Server: ave-03.vcorp.local at port: 7778.
INFO: Trap listeners status:
INFO: Listening to port 163 for traps from [ddve-05.vcorp.local]
INFO: Data Domain SNMP Manager started.
```

 **NOTE:** The preceding output might differ depending on the Avamar version.

- g. Edit the DD system configuration (similar to the following example):

```
mccli dd edit --name=ddve-05.vcorp.local
0,31005,Data Domain system updated but the hostname may not be valid.
Attribute      Value
-----
dd             ddve-05.vcorp.local
hostname       ddve-05.vcorp.local
ipv6Hostname   ddve-05.vcorp.local
ipv4Hostname   ddve-05.vcorp.local
```

- h. Confirm the DD system properties (similar to the following example):

```
mccli dd show-prop --name=ddve-05.vcorp.local
0,23000,CLI command completed successfully.
Attribute                                     Value
```


```

-----
IPv4 Hostname                ddve-05.vcorp.local
IPv6 Hostname                N/A
Total Capacity (post-comp size) 821.9 GiB
Server Utilization (post-comp use%) 1%
Bytes Protected              9.6 GB
File System Available (post-comp avail) 812.9 GiB
File System Used (post-comp used) 9.1 GiB
User Name                    ddbboost
Default Replication Storage System Yes
Target For Avamar Checkpoint Backups Yes
Maximum Streams For Avamar Checkpoint Backups 1
Maximum Streams              16
Maximum Streams Limit        16
Instant Access Limit          32
DDOS Version                  6.0.1.0-556307
Serial Number                  AUDVEWUJ7TS3V1
Model Number                   DD VE Version 3
Encryption Strength            none
Authentication Mode             none
Monitoring Status              OK
-----

```

- i. From the DD system, revoke token access for DD Boost (similar to the following example):

```
ssh <Data Domain CR username>@<vault Data Domain> "ddbboost user revoke token-access <ddbboost user for this Avamar system>"
```

 **NOTE:** The <ddbboost user> is the user that you are using on the Cyber Recovery vault.

For example

```
ssh cradmin@ddve-05.vcorp.local "ddbboost user revoke token-access ddbboostuser"
EMC Data Domain Virtual Edition
Password:
**** User "ddbboostuser" does not have a token key.
```

When prompted, use the cradmin password from the Cyber Recovery vault.

- j. Switch to root and stop the Avamar Agent service:

```
su -
/etc/init.d/avagent stop
```

- k. Clear the Avamar client ID (CID):

```
cd /usr/local/avamar/var/client
rm -f cid.bin
```

- l. Edit the client properties so that the value for --name= is the FQDN of the Avamar server in the Cyber Recovery vault, as shown in the following example:

```
mccli client edit --domain=/MC_SYSTEM --name=ave-03.vcorp.local --activated=false
0,22211,Client was updated.
```

- m. Start the Avamar Agent service:

```
/etc/init.d/avagent start
avagent Info <5008>: Logging to /usr/local/avamar/var/client/avagent.log
avagent Info <5417>: daemonized as process id 4134
avagent Info: Client Agent started.
```

17. Log in to the Avamar UI using the MCUser on the Avamar host server:

- Verify that the DD system is displayed in the main window.
- Verify that the data that is represented on the DD system matches that of the Avamar DD system.
- Verify that all the policies, clients, and other configuration items match those items of the production system.

- d. If you cannot perform a recovery in the Cyber Recovery vault because the DD system in the recovery sandbox is red, type the following command:

```
enable_secure_config.sh --undo --enable-secure-all
```

Then, type the `su - admin` command to switch to admin and, restart the MCS by typing the `mcserver.sh --restart --v` command.

18. If you cannot perform a recovery in the Cyber Recovery vault because the DD system in the recovery sandbox is red:

- a. Type the following command:

```
enable_secure_config.sh --undo --enable-secure-all
```

- b. Type the `su - admin` command to switch to admin
- c. Restart the MCS by typing the `mcserver.sh --restart --v` command.

19. See Avamar standard operating procedures to reactivate clients in the Cyber Recovery vault and perform the required application recoveries.

i **NOTE:** For information about enabling instant access for VMware image restores for the Recovery Sandbox, see Knowledge Base Article Number 000197934 at <https://www.dell.com/support/kbdoc/en-us/000197934/powerprotect-cyber-recovery-to-enable-avamar-instant-access-in-the-vault>. Access to this document depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

Cleaning up after an Avamar recovery

After the Avamar recovery is completed, delete the sandbox .

Steps

1. To delete the recovery sandbox, do the following:
 - a. From the Cyber Recovery Main Menu, click **Recovery** and then click **recovery sandboxes**.
 - b. Select the recovery sandbox.
 - c. Click **Cleanup**.
2. After the sandbox is cleaned up, bring down the Avamar processes by stopping the Avamar services on the Avamar server:

- a. Log in to the Avamar system as admin.

```
su admin
```

- b. Check if the processes are running.

```
dpnctl status
```

If the Avamar processes are still running, go to the next step. Otherwise, the procedure is complete.

- c. Create an ssh-agent session:

```
ssh-agent bash
ssh-add ~admin/.ssh/admin_key
```

- d. . Run the following command to stop the processes on Avamar.

```
dpnctl stop
```

This step might take some time.

- e. Type **y** to confirm that you want to shut down the instance:

```
Do you wish to shut down the local instance of EM Tomcat?

Answering y(es) will shut down the local instance of EM Tomcat
n(o) will leave up the local instance of EM Tomcat
q(uit) exits without shutting down
```

```
y(es), n(o), q(uit/exit): y
```

- f. When the process is completed, run the `dpnctl status` command to verify the results, as shown in the following example:

dpnctl status

```
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/admin_key)
dpnctl: INFO: gsan status: not running
dpnctl: INFO: MCS status: down.
dpnctl: INFO: emt status: down.
dpnctl: INFO: Backup scheduler status: down.
dpnctl: INFO: Maintenance windows scheduler status: unknown.
dpnctl: INFO: Unattended startup status: disabled.
dpnctl: INFO: avinstaller status: up.
dpnctl: INFO: ConnectEMC status: up.
dpnctl: INFO: ddrmaint-service status: down.
dpnctl: INFO: [see log file "/usr/local/avamar/var/log/dpnctl.log"]
```

 **NOTE:** The preceding output might differ depending on the Avamar version.

Results

The system is ready for another recovery operation.

Performing a PowerProtect Data Manager Recovery with Cyber Recovery

This section describes how to use the Cyber Recovery UI to recover data from PowerProtect Data Manager point-in-time copies.

Topics:

- [Recovering PowerProtect Data Manager data](#)
- [Meeting prerequisites for a PowerProtect Data Manager recovery](#)
- [Initiating a PowerProtect Data Manager recovery in the Cyber Recovery UI](#)
- [Running a PowerProtect Data Manager recovery check](#)
- [Cleaning up after a PowerProtect Data Manager recovery](#)
- [Performing postrecovery steps for a PowerProtect Data Manager recovery](#)

Recovering PowerProtect Data Manager data

Use a point-in-time (PIT) copy to rehydrate PowerProtect Data Manager data in the Cyber Recovery vault.

You can initiate a PowerProtect Data Manager recovery by using the Cyber Recovery UI or the CRCLI. You then complete the recovery from the PowerProtect Data Manager application in the Cyber Recovery vault.

 **NOTE:** You can only run one recovery job per application at a time.

When you initiate a recovery, the Cyber Recovery software prepares your environment so that you can run a PowerProtect Data Manager recovery from the application console. As part of this process, the software creates a production DD Boost username and password on the DD system, and reboots the PowerProtect Data Manager appliance. It also takes a VM snapshot of the PowerProtect Data Manager appliance that you use to revert the PowerProtect Data Manager software after you complete the recovery.

After a successful recovery, you can run a recovery check to ensure that a copy can be recovered.

During the check, the state of the backup copy shows as **In-progress**. When the recovery check is completed successfully, the data backup copy shows as **Recoverable**.

If the recovery check fails, the state of the backup copy shows as **Failed**. Alerts in the dashboard and an email message notify you of the state. The alerts are either:

- **Warning**—The backup copy is partially recoverable.
- **Critical**—The backup copy is unrecoverable.

Meeting prerequisites for a PowerProtect Data Manager recovery

Ensure that the following prerequisites are met before you initiate a PowerProtect Data Manager recovery:

- See the following documentation, which is available on the Customer Support website at <https://www.dell.com/support>:
 - The *Preparing for and Recovering From a Disaster* chapter in the *PowerProtect Data Manager Administration and User Guide*
 - *PowerProtect Data Manager for Oracle RMAN Agent User Guide*
 - *PowerProtect Data Manager for Microsoft Application Agent SQL Server User Guide*
- Ensure that the Cyber Recovery vault DD system is running DD OS Version 6.2.1.50 or later.
- Deploy the PowerProtect Data Manager appliance in the Cyber Recovery vault:
 - Ensure that the version is the same as the version of the production system.

- Leave PowerProtect Data Manager in the default state. When you log in to PowerProtect Data Manager, the default state is either **New Install** or **Restore Backup**.
- Do not modify the default passwords.
- Modify the `/etc/ssh/sshd_config` file to enable password authentication:
 - Change the `PasswordAuthentication` field value from **no** to **yes**.
 - Run the `service sshd restart` command.
- Do not use the following special characters in the VM name in vCenter, otherwise the Cyber Recovery software cannot detect the PowerProtect Data Manager VM:
`%, &, *, $, #, @, !, \, /, :, *, ?, ", <, >, [,], |, ;, '`
- Ensure that the UIDs that are associated with the production PowerProtect Data Manager DD Boost users are available on the DD system in the Cyber Recovery vault.
- Use either the Cyber Recovery UI or the CRCLI to define the PowerProtect Data Manager application as a Cyber Recovery application asset. When defining the PowerProtect Data Manager application:
 - Configure the application using the credentials of the PowerProtect Data Manager application on the production system.
- **NOTE:** After 90 days, the root and admin accounts expire on the PowerProtect Data Manager appliance. Change the root and admin account passwords back to the default values used when the PowerProtect Data Manager virtual appliance was deployed. Otherwise, a recovery action fails because the former passwords are not valid.
- To be able to create a snapshot as part of the recovery procedure, use the same value for the FQDN or hostname that is shown in the vCenter user interface under the DNS name.
- Ensure that there are no snapshots of the PowerProtect Data Manager virtual machine that is deployed in the vCenter server.
- Create a Cyber Recovery policy for the VM data and DR backup.
- Run application and DR backups in the PowerProtect Data Manager production environment. Then, perform a Secure Copy policy operation to copy data to the Cyber Recovery vault environment.

Initiating a PowerProtect Data Manager recovery in the Cyber Recovery UI

Initiate a recovery in the Cyber Recovery UI. The Cyber Recovery software completes the recovery operation automatically.

Prerequisites

Ensure that you meet all the prerequisites that are listed in [Meeting prerequisites for a PowerProtect Data Manager recovery](#).

About this task

The Cyber Recovery software prepares your environment so that you can run a VM recovery from the PowerProtect Data Manager application console. It creates a DD Boost username and password, which matches the production DD Boost username and password, on the DD system in the Cyber Recovery vault. This username and password are required to perform the DR backup. The Cyber Recovery software then reboots the PowerProtect Data Manager appliance.

NOTE:

- The recovery procedure sets the operating system root and admin passwords for all PowerProtect Data Manager versions to the values that you specified in the admin password field when you added the PowerProtect Data Manager application object to the Cyber Recovery deployment.

NOTE:

If the PowerProtect Data Manager recovery procedure fails to restore either the admin or root password, the Cyber Recovery software shows the job status as `Warning`. Optionally, reset either the admin or root password for additional security.

- **NOTE:** If the passwords are not reset, the data backup copy is marked as recoverable and you can use it to recover the PowerProtect Data Manager backup data.

- When using the DD Boost storage unit to perform the PowerProtect Data Manager DR backup, the Cyber Recovery software creates the DD Boost user using UID 800. If UID 800 is unavailable, the next sequential available UID is assigned.

Steps

1. Select **Recovery** from the Main Menu.
2. On the **Recovery** content pane, select the copy, and then click **Application**.
3. In the **Application** dialog box, select a PowerProtect Data Manager application host, and then click **Apply**.
The Cyber Recovery UI software runs a job to create a recovery sandbox, populates it with the selected copy, and then makes the sandbox available to the application host.
4. Optionally, cancel the recovery, otherwise go to the next step:
 - a. Select **Jobs** from the Main Menu.
 - b. Select the running recovery job.
 - c. Click **Cancel Job**.
The recovery job is canceled and the Cyber Recovery software automatically deletes the sandbox, reverts the VM back to the virtual snapshot, and the DD system shows the status of the MTree that was associated with the sandbox is deleted.
5. Wait for the recovery job to complete.
A recovery sandbox is created for the PowerProtect Data Manager application.
6. Click **Recovery Sandboxes** from the top of the **Recovery** pane and do the following:
 - a. To view the recovery details, select the `recoverapp_<ID>` name.
 - b. To validate success, click **Launch App** to access the PowerProtect Data Manager UI in the Cyber Recovery vault.
The **Launch App** button is active only when the recovery is completed successfully.
 - c. To delete the sandbox, click **Cleanup**.

Results

The latest PowerProtect Data Manager configuration is recovered.

Next steps

After the recovery is completed, do the following:

- [Run a recovery check](#)
- [Perform postrecovery steps](#)

Running a PowerProtect Data Manager recovery check

Run a scheduled or on-demand PowerProtect Data Manager recovery check to ensure that after a successful recovery a copy can be recovered.

About this task

When the Cyber Recovery software completes a recovery check action, the copy's status is marked as recoverable or nonrecoverable. The Cyber Recovery software reverts PowerProtect Data Manager back to its initial state from which you can run a recovery. However, you can run a recovery manually to determine if the copy is recoverable and manually perform the cleanup.

Steps

1. Schedule a recovery check.
 - a. Select **Policies** from the Main Menu.
 - b. Click **Schedules** at the top of the **Policies** content pane.
 - c. Click **Add** and complete the following fields in the dialog box:

Table 19. Add schedule fields

Field	Description
Schedule Name	Specify a schedule name.
Policy	Select the policy that you are scheduling.

Table 19. Add schedule fields (continued)

Field	Description
Action	Select Recover Check from the drop-down list.
Frequency	Enter the frequency in days and hours.
Next Run Date	Select the date to start running the policy under this schedule.
Next Run Time	Select the time to start running the policy under this schedule.

d. Click **Save**.

The recovery check runs, using the values that you defined in the recovery check schedule.

2. Run an on-demand recovery check.

a. Select **Recovery** from the Main Menu.

b. Under **Copies**, select a copy.

c. Click **Recovery Check**.

The recovery check runs immediately.

Results

The recovery check procedure does not provide the option to access the PowerProtect Data Manager UI. The procedure recovers the PowerProtect Data Manager server and then automatically cleans up the recovery, regardless of whether the recovery is successful or fails. You cannot recover a VM, but the copy can be recovered when necessary.

Cleaning up after a PowerProtect Data Manager recovery

After the PowerProtect Data Manager recovery is completed, delete the sandbox and DD boost storage unit.

About this task

You can perform this task by using the Cyber Recovery UI or the CRCLI.

Steps

1. Delete the sandbox that was created when you initiated the PowerProtect Data Manager recovery.

a. From the Main Menu, click **Recovery** and then click **Recovery Sandboxes** from the top of the **Recovery** pane.

b. Select the recovery sandbox.

c. Click **Cleanup**.

The sandbox is deleted, and the Cyber Recovery software reverts the PowerProtect Data Manager software to the snapshot that was created when you initiated the recovery.

2. Optionally, on the DD system, run the `filesys clean start` command.

This step deletes the DD Boost storage unit. If you choose not to perform this step, the DD Boost storage unit is deleted during the next scheduled cleaning operation.

Results

The system is ready for another recovery operation.

Performing postrecovery steps for a PowerProtect Data Manager recovery

After the PowerProtect Data Manager recovery is completed, perform postrecovery steps.

About this task

You can perform this task by using the Cyber Recovery UI or the CRCLI.

Steps

1. To validate success, click **Launch App** to access the PowerProtect Data Manager UI in the Cyber Recovery vault.

The **Welcome to PowerProtect Data Manager** window opens.

NOTE: For Version 19.5 and later deployments, a PowerProtect Data Manager recovery disables all services. When you access the PowerProtect Data Manager UI after the recovery, it displays an alert that indicates that the services are not running. Click the alert to restart the services.

2. To verify the recovery for SQL, Oracle, and file system workloads, do the following:
 - For Windows deployments:
 - a. Go to `C:\Program Files\DPSAPPS\AgentService`.
 - b. Run the `unregister.bat` command to unregister the agent.
 - c. If necessary, delete the `ssl` folder from the Agent Service folder.
 - d. Run the `register.bat` command to register the host with PowerProtect Data Manager again.
 - e. From the PowerProtect Data Manager Main Menu, go to **Protection > Protection Policies**. Select the policy and click **Set Lockbox** to run the configuration job again.
 - For Linux deployments:
 - a. Go to `/opt/dpsapps/agentservice`.
 - b. Run the `unregister.bat` command to unregister the agent.
 - c. If necessary, delete the `ssl` folder from the Agent Service folder.
 - d. Run the `register.bat` command to register the host with PowerProtect Data Manager again.
 - e. From the PowerProtect Data Manager Main Menu, go to **Protection > Protection Policies**. Select the policy and click **Set Lockbox** to run the configuration job again.

Administration

This section describes Cyber Recovery administrative tasks.

Topics:

- [Administration overview](#)
- [Manually securing and releasing the Cyber Recovery vault](#)
- [User roles](#)
- [Managing users](#)
- [Managing login sessions](#)
- [Setting up an email server](#)
- [Managing Cyber Recovery password expiration](#)
- [Resetting Cyber Recovery passwords](#)
- [Resetting the IP address on the management host](#)
- [Updating the SSL security certificate](#)
- [Configuring a daily activity report](#)
- [Configuring a telemetry report](#)
- [Changing time zones](#)
- [Changing the log level](#)
- [Collecting logs for upload to support](#)
- [Log file rotation](#)
- [Protecting the Cyber Recovery configuration](#)
- [Retrieving your preserved Cyber Recovery configuration](#)
- [Deleting unneeded Cyber Recovery objects](#)
- [Cyber Recovery disaster recovery](#)

Administration overview


You can perform administrative tasks from either the Cyber Recovery UI or on the management host by using the Cyber Recovery command-line interface (CRCLI).

Manually securing and releasing the Cyber Recovery vault

If a security breach occurs, the Security Officer or an Admin user can manually secure the Cyber Recovery vault. During this time, the Cyber Recovery software performs no replication operations.

To secure or release (unsecure) the Cyber Recovery vault, log in to Cyber Recovery and access the dashboard. Under **Status**, do one of the following:

- To secure the Cyber Recovery vault if you suspect a security breach, click **Secure Vault** so that the Cyber Recovery vault status changes from **Locked** to **Secured**. All Sync policy operations stop immediately and no new Sync policy operations can be initiated. The Cyber Recovery software also issues an alert that the Cyber Recovery vault is secured.

 **NOTE:** All non-Sync policies can be run in the Cyber Recovery vault while it is secured.

- To unsecure the vault when you are confident that there is no longer a security threat, click **Release Vault**. The Cyber Recovery vault status returns to **Locked**. Sync policy operations can now be initiated.

For more information about the Cyber Recovery vault status, see [Monitoring the CR Vault status](#).

User roles

Cyber Recovery users are assigned roles that determine the tasks that they can perform in the Cyber Recovery vault environment.

The Cyber Recovery installation creates the default crso user and assigns the Security Officer (crso) role to this user. The Security Officer user must perform the initial Cyber Recovery login and then create users. There is only one Security Officer per Cyber Recovery installation; you cannot create another Security Officer.

NOTE: Do not confuse the Cyber Recovery Security Officer with the DD Security Officer for DD Compliance retention locking.

There are three Cyber Recovery user roles:

- **Dashboard**—This role enables the user to view the Cyber Recovery dashboard but not perform tasks.
- **Admin**—This role has the following permissions:
 - Create, modify, and disable dashboard users
 - Create, manage, and run policies and associated objects
 - Acknowledge and add notes to alerts
 - Change administrative settings
 - Modify own user account
 - Change own password
 - Manually secure and release (unsecure) the Cyber Recovery vault
- **Security Officer**—This role has the following permissions:
 - All Admin permissions
 - Create, modify, and disable users
 - Change and reset user passwords
 - Change the Security Officer password
 - Set the duration after which passwords expire for all users
 - Disable multifactor authentication for an Admin user
 - Configure the daily activity report
 - Configure the number of login sessions

NOTE: If as the Security Officer, you forget your password, use the `crsetup.sh` script to reset it. For instructions, see [Resetting Cyber Recovery passwords](#).

Managing users

The Security Officer (crso) creates, modifies, and disables users, and disables Admin user multifactor authentication.

About this task

The Security Officer (crso) can:

- Enable and disable users, but not delete them
- Disable multifactor authentication for Admin users, but not enable it
- Enable Security Officer (crso) multifactor authentication

Steps

1. Select **Administration > Users** from the Main Menu.
2. Do one of the following:
 - To create a user, click **Add**.
 - To modify a user, click the radio button at the beginning of the row for a user and click **Edit**.
3. Complete the following fields in the dialog box.

Table 20. User fields

Field	Description
Name fields	Specify the user's first name and last name.

Table 20. User fields (continued)

Field	Description
Role	Select either: <ul style="list-style-type: none"> Admin—Enables users to perform tasks in the Cyber Recovery software. Dashboard—Enables users to view the Cyber Recovery dashboard but not perform tasks. The dashboard role does not time out.
User Name (required)	Specify a username.
Phone	Specify the user's telephone number.
Email (required)	Specify an email address for alert notifications if the user is configured to receive them. <p>NOTE: Later, if a user's email is modified, the Security Officer (crso) and the user receive an email message that indicates the change. The user's old email address, which has since been modified, receives the email message.</p>
Password/Confirm New Password (required)	Specify and confirm the password. Password requirements include: <ul style="list-style-type: none"> 9–64 characters At least 1 numeric character At least 1 uppercase letter At least 1 lowercase letter At least 1 special character (~!@#\$%^&*()+={} :~<>?[]-_,^') When you change a password, enter and confirm both the new and existing passwords.
Session Timeout	Select the amount of idle time after which the user is logged out of the Cyber Recovery UI.

4. Click **Save**.
5. Enable and disable users:
 - a. Select the user and click **Disable**.
 - b. Click **Disabled Users** at the top of the content pane and note that the table lists the newly disabled user.
 - c. Select the user and click **Enable**. The table no longer lists the user.
 - d. Click **Enabled Users** at the top of the content pane and note that the table lists the newly enabled user.
6. Disable multifactor authentication for an Admin user:
 - a. Select the user.
 - b. Click **Disable MFA**.
The Security Officer (crso) and the Admin user, whose multifactor authentication is disabled, receive an email message that indicates that multifactor authentication is disabled. When the Admin user logs in, the slider in the **Setup Multifactor Authentication** window is set to the disabled position.

NOTE: The Security Officer (crso) and Admin users, if they can log in, can disable multifactor authentication for their own accounts by using the slider in the **Multi-Factor Authentication** window. See [Enabling multifactor authentication](#).

Managing login sessions

The Security Officer (crso) can set the number of maximum simultaneous login sessions.

Prerequisites

You must be logged in as the Security Officer to change login session settings.

About this task

The login session count uses a first in, first out priority. If a specific user and role exceeds the number of simultaneous logins, that user's earliest session is no longer a valid Cyber Recovery session and the session is logged out. The user must log in to the Cyber Recovery software again.

Steps

1. From the Masthead Navigation, select the gear icon to access the **System Settings** menu.

2. Click **Login Count Settings**.

The **Login Count Settings** dialog box opens and shows the default session login values, which are:

- Security Officer—One login session
- Admin—Three login sessions
- Dashboard user—Three login sessions

3. Set the maximum number of login sessions for the Security Officer, Admin, and Dashboard user.

The maximum number of login sessions for:

- The Security Officer is three sessions
- Admin and Dashboard users is five sessions

Setting up an email server

If your configuration allows email to leave the Cyber Recovery vault, specify which users receive email notifications about alerts and connect to an SMTP email server.

Optionally, enable and configure the option to use an external email service. For more information, see [Configuring the Postfix email service](#) and [Configuring an external email service](#).

i **NOTE:** If you use Postfix to route and deliver Cyber Recovery email notifications, you can use a second Ethernet adapter to configure a separate IP address for SMTP communication. For information about how to add a virtual Ethernet adapter, see [Setting up a separate IP address for SMTP communication](#).

If you are using the Cyber Recovery vault on Amazon Web Services (AWS), you must set up Amazon Simple Email Service (SES). For more information about setting up Amazon SES, see [Amazon Simple Email Service Documentation](#).

Specifying which users receive email

Specify which users receive email notifications about alerts.

About this task

Later, if a user's email is modified, the Security Officer (crso) and the user receive an email message that indicates the change. The user's old email address, which has since been modified, receives the email message.

Steps

1. Select **Administration > Alert Notifications** from the Main Menu.
The table lists Cyber Recovery users, their email addresses, and roles.
2. For each user that you want to receive email messages, select either or both the **Receive Critical Alerts** and **Receive Warning Alerts** checkboxes.
If you select **Receive Warning Alerts**, by default, the user also receives critical alerts.
3. To send a test email to the user, click **SEND TEST EMAIL**. Contact the intended user to verify that the email was received.

Setting up a separate IP address for SMTP communication on the Cyber Recovery virtual appliance

Optionally, if you want to separate mail traffic from management traffic, add a virtual Ethernet adapter to configure a separate IP address for SMTP communication.

Prerequisites

The Cyber Recovery virtual appliance is installed to a VMware ESXi host in the Cyber Recovery vault.

About this task

When you add a virtual Ethernet adapter, your configuration includes two IP addresses for:

- DD communication

- SMTP communication

Steps

1. Access the VMware vSphere Web Client.
2. Power off the Cyber Recovery virtual appliance virtual machine (VM).
3. Right-click the VM and select **Edit Settings**.
4. Expand the **New device** drop-down list.
5. Select **Network** and click **Add**.
6. Select the network type from the list and click **Finish**.
7. Power on the VM.
8. Log in as **admin** and run the `su` command to switch to root.
9. Use the YaST tool to configure the second virtual Ethernet adapter.
10. Restart the VM so that the changes take effect.

Next steps

When this procedure is completed, you can configure Postfix to route and deliver Cyber Recovery email notifications. See [Configuring the Postfix email service](#).

Configuring the Postfix email service

Postfix is an open-source mail transfer agent that is included with most non-Windows systems.

Prerequisites

If you plan to add an extra virtual Ethernet adapter on the Cyber Recovery virtual appliance, see [Setting up a separate IP address for SMTP communication](#).

About this task

After you have configured an SMTP email server in the Cyber Recovery UI, use Postfix to route and deliver Cyber Recovery email notifications to Cyber Recovery users.

 **NOTE:** If your system has an active firewall, ensure that port 25 is open on the firewall.

Steps

1. If necessary, open port 25 on the firewall:

```
# iptables -I INPUT -p tcp --dport 25 -j ACCEPT
```

2. Open `/etc/postfix/main.cf` in an editor, and modify it as shown in the following examples:

- a. Add the inet address of the virtual Ethernet adapter or network interface card (NIC) that is used for SMTP communication:

```
# RECEIVING MAIL
#
# Note: you need to stop/start Postfix when this parameter changes.
#
inet_interfaces = all
#inet_interfaces = $myhostname
#inet_interfaces = $myhostname, localhost
#inet_interfaces = localhost
```

 **NOTE:** Ensure that you do not uncomment more than one `inet_interface`.

- b. Add the fully qualified domain name (FDQN) of the management host:

```
# INTERNET HOST AND DOMAIN NAMES
#
```

```
# The myhostname parameter specifies the internet hostname of this
# mail system. The default is to use the fully-qualified domain name
# from gethostname(). $myhostname is used as a default value for many
# other configuration parameters.
#
myhostname = <FDQN of the Cyber Recovery host>
```

- c. Add the mail server name:

```
# INTERNET OR INTRANET
#
# The relayhost parameter specifies the default host to send mail to
# when no entry is matched in the optional transport (5) table. When
# no relayhost is given, mail is routed directly to the destination.
#
# On an intranet, specify the organizational domain name. If your
# internal DNS uses no MX records, specify the name of the intranet
# gateway host instead.
#
# In the case of SMTP, specify a domain, host, host:port, [host]:port,
# [address] or [address]:port; the form [host] turns off MX lookups.
# If you're connected via UUCP, see also the default_transport parameter.
#
relayhost = <mail server name>
#
```

3. Reload the Postfix configuration file.

```
# postfix reload
```

4. Stop and start Postfix:

```
# postfix stop
# postfix start
```

5. Optionally, check the Postfix status:

```
# postfix status
```

Configuring an external email service

After you have configured an SMTP email server in the Cyber Recovery UI, enable the option to use an external email service to route and deliver Cyber Recovery email notifications to Cyber Recovery users.

About this task

NOTE: If you are using the Cyber Recovery solution on Amazon Web Services (AWS), Amazon Simple Email Service (SES) is the only option to manage email operations. For more information about setting up Amazon SES, see the *Dell PowerProtect Cyber Recovery AWS Deployment Guide* and the [Amazon Simple Email Service Documentation](#).

If you do not enable this option, by default, the Cyber Recovery software uses Postfix as the default email service.

Steps

1. From the Masthead Navigation, click the gear icon to access the **System Settings** list.
2. Click **Support > Mail Server Settings**.
3. In the **Mail Server Settings** dialog box, enable this option.
The dialog box displays configuration fields.
4. Enter or modify the values in the following fields:

Table 21. Mail server settings fields

Field	Description
Mail Server	Specify the Cyber Recovery email server.
Port	Specify a port number. The default port number is 25.
Sender's Email Address	Specify the email address that delivers Cyber Recovery alert messages. The default value is <code>noreply@cyberrecovery</code> .
Username	Optionally, specify the username for the email server that is configured to work with the Cyber Recovery software.
Password	Optionally, specify the password for the email server that is configured to work with the Cyber Recovery software.


5. Click **Save**.

Managing Cyber Recovery password expiration

The Security Officer (crso) can set a duration after which passwords expire for all users. Users must then change their passwords.

About this task

Only the crso can set the password expiration duration and view the expiration policy.

 **NOTE:** You cannot set a password expiration duration for an individual user; the duration applies to all users.

Steps

1. Select **Administration > Users** from the Main Menu.

2. Click **Settings**.

The **Settings** button is not displayed for Admin and dashboard users.

3. In the **User Password Settings** window, enter the number of days after which the passwords expire and click **Save**.

When the passwords are about to expire within four to 15 days, a yellow warning message is displayed. This alert indicates the number of days before password expiration. Users can dismiss the message.

When the passwords are about to expire within one to three days, a red warning message is displayed. This alert indicates the number of days before password expiration. Users cannot dismiss this message.

Users also receive alerts and email messages about the number of days before password expiration.

If users do not change their passwords before they expire, the Cyber Recovery software forces them to change their passwords at the next login. If multifactor authentication is enabled, the software prompts users for a security code.

Resetting Cyber Recovery passwords

For security purposes, use the `crsetup.sh` script to change the Cyber Recovery lockbox passphrase and the Cyber Recovery database and Security Officer (crso) passwords.

Prerequisites

- You must provide the lockbox passphrase, which is created during the Cyber Recovery installation.
- Ensure that there are no jobs running before you change the passwords. Otherwise, the Cyber Recovery vault might go to an unsecured state.
- This procedure is disruptive; it shuts down the Docker container services.

About this task

- The Cyber Recovery software uses a lockbox resource to securely store sensitive information, such as credentials for application resources and databases. The lockbox securely manages sensitive information by storing the information in an encrypted format.
- Cyber Recovery microservices communicate with the MongoDB database to access policies and other persisted data. The database is password-protected and only accessible by the microservices that run in the Cyber Recovery environment.
- As the Security Officer, use the Cyber Recovery UI or Cyber Recovery CRCLI to change the crso password. However, if you forget the crso password or if there is a change in Security Officer, use the `crsetup.sh` script.

Steps

1. Log in to the management host and go to the Cyber Recovery installation directory.
2. Enter the following command:

```
# ./crsetup.sh --changepassword
```

3. Note the cautionary message.
It is highly recommended that you create a Cyber Recovery DR backup before changing the password.
4. When prompted, indicate if you want to create a Cyber Recovery DR backup:
 - If you type **y**, got to the next step.
 - If you type **n**, got step 6.
5. When prompted, enter the MongoDB password.
The Cyber Recovery software creates a DR backup.
6. When prompted, enter **y** to continue the procedure.
The script stops the Docker container services.
7. When prompted, enter the current lockbox passphrase.
If you enter an incorrect passphrase, the procedure exits and restarts the Docker container services.
8. Optionally, enter and confirm the new lockbox passphrase when prompted.
If you choose not to change the lockbox passphrase, the script then displays the prompt to change the MongoDB password.
9. Optionally, enter and confirm the new database password when prompted.
If you choose not to change the MongoDB password, the script then displays the prompt to change the crso password.
10. Optionally, enter and confirm the new crso password when prompted.

Results

The passwords are changed, and the script restarts the Docker container services.

NOTE:

- If you enter an incorrect password twice at the confirmation prompts, the script makes no changes and restarts the services
- If you (as the Security Officer (crso) user) had multifactor authentication enabled, it is disabled when the services start again. Re-enable multifactor authentication.

Resetting the IP address on the management host

When you reset the IP address on the management host in the Cyber Recovery vault, run the `crsetup.sh` script to ensure that the Cyber Recovery software runs properly.

Prerequisites

You must have the lockbox password to enter at the `crsetup.sh` script prompt.

Steps

1. Modify the IP address of the Cyber Recovery management host.

2. Restart the network service:

```
# service network restart
```

3. Restart Docker:

```
# service docker restart
```

4. Run the `crsetup.sh --address` script:

```
# ./crsetup.sh --address
Do you want to continue[y/n]: y
.
.
.
Enter lockbox password:
```

5. Verify that all Cyber Recovery containers are up and running:

```
# docker ps -a
```

6. Log in to the Cyber Recovery UI and confirm that you can access the Cyber Recovery software.

Updating the SSL security certificate

Update an SSL security certificate in the Cyber Recovery deployment with a custom security certificate.

Prerequisites

- The Cyber Recovery software is installed, and the deployment is up and running.
- You have knowledge about managing security certificates.
- Your browser is set up to accept security certificates.

About this task

You can replace an SSL security certificate with your own security certificate. For example, replace the SSL security certificate with a CA-signed certificate to avoid a warning message when you access the Cyber Recovery UI. The operating system and web browser for the Cyber Recovery deployment automatically trust and authenticate this certificate.

Steps

1. Log in to the Cyber Recovery management host.
2. Generate a certificate signing request (CSR), which is required to apply for a CA-signed certificate:
 - a. Run the `crsetup.sh --gencertrequest` script.
 - b. At each prompt, either enter the information for your deployment or press Enter to omit the information and go to the next prompt.
 - c. When prompted, confirm the information that you provided.
 - d. Enter the lockbox passphrase.


The script lists the following information, which is essential for the certificate:

- DNS name of the Cyber Recovery management host
- IP address of the Cyber Recovery management host
- URIs for HTTPS access and connections

 **NOTE:** You must use these exact values when you submit the CSR to the CA.

The `crsetup.sh` script generates a certificate signing request file: `CRSERVICE.csr`.

3. Submit the `CRSERVICE.csr` file to the CA to apply for a CA-signed certificate.

 **NOTE:**

- Ensure that you submit the exact information from the previous step to the CA.

- The Cyber Recovery software uses the name `CRSERVICE` by default to generate the certificate. However, you can use any meaningful file name for your deployment.

The CA returns a `<certificatename>.crt` file.

4. Add the CA-signed certificate to the Cyber Recovery deployment:

- Copy the `<certificatename>.crt` file (returned by the CA) into the same directory on the Cyber Recovery management host.
- Run the `crsetup.sh --addcustcert` script.
The script stops the Docker container services.
- At the prompt, enter the full path where the `<certificatename>.crt` file is located.

For example:

```
/opt/dellemc/cr/bin/<certificatename>.crt
```

- Enter the lockbox passphrase.

The script displays an informational message that indicates that the signed certificate has been added successfully, and then restarts the Docker container services.

NOTE: The Cyber Recovery software validates the certificate and key files and verifies the information from the CSR (as described in step 2). It also validates the certificate start date, which must be current, and the certificate duration, which must exceed one year.

The script starts the Docker container services whether the addition of the certificate succeeds or fails.

Configuring a daily activity report

As the Security Officer (crso), set up a daily Cyber Recovery activity report.

Prerequisites

- You have a valid email address.
- The mail server is enabled. For more information, see [Setting up an email server](#).

NOTE: The Cyber Recovery software can generate and send an activity report without user authentication settings for an external mail server. However, we recommend that you include authentication settings for an external mail server.

About this task

The activity report provides information for all Cyber Recovery jobs for the duration of the configured frequency. Only the Security Officer (crso) receives the report.

Steps

1. From the Masthead Navigation in the Cyber Recovery UI, click the gear icon to access the **System Settings** list.
2. Click **System Reports**.
3. In the **System Reports** dialog box, click the **Activity Report** tab and swipe right on the slider to enable the option.
4. Complete the **Frequency** and **Next Run** fields, and then click **Save**.

NOTE: The Cyber Recovery UI uses the same time zone as the Cyber Recovery management host for the scheduled time.


The maximum number of days is 31 and the minimum number of hours is 1.

Configuring a telemetry report

Set up a Cyber Recovery telemetry report that is sent to Dell Technologies for troubleshooting purposes.

Prerequisites

- You have a valid email address.
- The mail server is enabled. For more information, see [Setting up an email server](#).

 **NOTE:** The Cyber Recovery software can generate and send a telemetry report without user authentication settings for an external mail server. However, we recommend that you include authentication settings for an external mail server.

About this task


The telemetry report provides information about Cyber Recovery components, such as:

- Policies
- Applications
- Cyber Recovery versions for installations and updates
- Cyber Recovery services
- Vault DD storage
- Mail server

To run a telemetry report on demand, use the CRCLI. For information about the CRCLI, see the *Dell PowerProtect Cyber Recovery Command-Line Interface Reference Guide*.

Steps

1. From the Masthead Navigation in the Cyber Recovery UI, click the gear icon to access the **System Settings** list.
2. Click **System Reports**.
3. In the **System Reports** dialog box, click the **Telemetry Report** tab.
4. Swipe right on the slider to enable the option.
5. Complete the **Frequency** and **Next Run** fields, and then click **Save**.

 **NOTE:** The Cyber Recovery UI uses the same time zone as the Cyber Recovery management host for the scheduled time.

The maximum number of days is 30, and the minimum is 1 day.

Changing time zones

Change the current time zone of the Cyber Recovery deployment.

About this task

To change the current time zone of the Cyber Recovery deployment, set the new time zone on the Cyber Recovery management host, and then restart the Docker containers. The containers synchronize with the time zone of the Cyber Recovery management host.

Steps

1. Do either of the following:
 - Log in to the Cyber Recovery management host as root.
 - Log in to the Cyber Recovery virtual appliance as admin and then change to root.
2. View the current time settings. For example:

```
timedatectl
    Local time: Thu 2021-07-01 14:02:39 EDT
    Universal time: Thu 2021-07-01 18:02:39 UTC
        RTC time: Thu 2021-07-01 18:02:39
        Time zone: America/New_York (EDT, -0400)
    NTP enabled: yes
```

```
NTP synchronized: yes
RTC in local TZ: no
    DST active: yes
Last DST change: DST began at
    Sun 2021-03-14 01:59:59 EST
    Sun 2021-03-14 03:00:00 EDT
Next DST change: DST ends (the clock jumps one hour backwards) at
    Sun 2021-11-07 01:59:59 EDT
    Sun 2021-11-07 01:00:00 EST
```

3. View the current time settings in one of the containers. For example:

```
docker exec -it cr_edge_1 date
Thu Jul 1 14:03:02 EDT 2021
```

4. Change the time zone on the Cyber Recovery management host. For example:

```
timedatectl set-timezone America/Chicago
```

5. Verify the new time zone setting on the Cyber Recovery management host:

```
date
Thu Jul 1 13:08:26 CDT 2021
```

6. Restart the Cyber Recovery services to propagate the new time zone into the Cyber Recovery Docker containers:

```
/opt/dellemc/cr/bin/crsetup.sh --restart
```

7. Verify that the new time zone is in effect in one of the CR containers. For example:

```
docker exec -it cr_edge_1 date
Thu Jul 1 13:09:00 CDT 2021
```

Changing the log level

Change the logging level that is used to add information to the Cyber Recovery log files.

About this task

Cyber Recovery supports two log levels:

- Info—Provides contextual details relevant to software state and configuration.
- Debug—Provides granular details to aide analysis and diagnostics.

The default log level is Info.

Steps

1. From the Masthead Navigation, click the gear icon to access the **System Settings** list.
2. Click **Support > Log Settings**.
3. In the **Service Log Level** dialog box, do one of the following:
 - Click the **Set All** radio button to change the level for all logs.
 - Click a radio button to set the level for each specific log.
4. Click **Save**.

Collecting logs for upload to support

Collect all logfiles in an archive file so that they can be uploaded to Dell Technologies support to facilitate troubleshooting.


Steps


1. From the Masthead Navigation, click the gear icon to access the **System Settings** list.
2. Click **Support > Support Bundles**.
3. Click **Generate Log Bundle**.

The operation status is displayed as Running. When the operation is complete, the operation status is displayed as Success.

The logfiles are collected and added to a `.tar` file in the `opt/dellemc/cr/var/log` directory. Also, Cyber Recovery triggers a log collection on all associated DD systems in the vault environment.

4. To view these collections, click **Settings** (gear icon) in the PowerProtect DD Management Center and select **System > Support > Support Bundles**.
5. Download a support bundle:
 - a. Click the link for the support bundle name, which is displayed for a successfully or partially successfully generated support bundle.

 **NOTE:** If the support bundle status is Running or Failed, you cannot download it.

- b. At the browser prompt, indicate that you want to download multiple files.
The support bundle is downloaded. It consists of the:
 - Log files in the support bundle.
 - A checksum file, which contains the checksum value for the downloaded bundle. The checksum value is calculated using SHA-256.
6. Delete a support bundle:
 - a. Select the radio button next to a support bundle.
 **NOTE:** You can delete only one support bundle at a time.
 - b. Click **Delete** and click **Delete** again to confirm the request.
 7. Click **OK** to dismiss the **Success** window.

Log file rotation

The Cyber Recovery software creates a log file for each Cyber Recovery service.

When the log file reaches the maximum size of 50 MB, the software saves it as an archive file and creates a new log file. When that new log file reaches 50 MB, it is also saved as an archive file and another new log file is created. The logfile archive count uses a first in, first out priority. When there are 10 archive files, the Cyber Recovery software deletes the oldest archive file and replaces it with the newest archive file. The maximum number of archive files available is 10.

Protecting the Cyber Recovery configuration

Configure a disaster recovery (DR) backup to preserve Cyber Recovery configuration data and policies in case the management server fails. We strongly recommend that you configure a DR backup to protect your Cyber Recovery configuration.

Prerequisites


Create an MTree on the Cyber Recovery vault DD system for the Cyber Recovery software to use for a DR backup.

About this task

The backup data is stored on a separate MTree on the DD system in the Cyber Recovery vault for a set period.

After you configure a DR backup, it runs at the frequency that you scheduled. You can also run an on-demand DR backup.

Other than an Analyze job, if another job is running at the time that you schedule a DR backup or initiate a manual backup, the DR backup does not run. Ensure that you do not schedule other jobs (other than an Analyze job) for the same time as the DR backup.


 **NOTE:** After you perform a DR backup while an Analyze job is running, delete the resulting stale sandboxes. Otherwise, you cannot run another Analyze job.

Steps

1. From the Masthead Navigation, click the gear icon to access the **System Settings** list.


2. Select **DR Backups**.

The **Disaster Recovery Backups** dialog box is displayed.

 **NOTE:** By default, DR backups are disabled.

3. Click **Configuration** and do the following:

- a. Swipe right on the slider to enable a DR backup.
- b. Select the DD system on which to store the backup data.
- c. Specify an MTree on which to store the backup data.
- d. Set the frequency of the DR backups and the time for the next run.

 **NOTE:** The Cyber Recovery UI uses the same time zone as the Cyber Recovery management host for the scheduled time.

e. Click **Save**.

An informational message indicates that the configuration has been created successfully.

f. If necessary, edit the fields in the Configuration window and click **Save**.

An informational message indicates that the configuration has been updated successfully.

4. Click **Manage Backups**.

A list of all previously created DR backups is displayed in order of the newest to the oldest, depending on the cleaning schedule.

5. To run a DR backup, click **Backup Now**.

You must create an enabled configuration before you can run an on-demand DR backup.

The new DR backup is displayed at the top of the list.

6. To set retention limits for DR backups, click **Maintenance** from the **System Settings** list.

The retention time settings include a minimum of one day and a maximum of 90 days.

 **NOTE:**

- The DR backup must be enabled otherwise it is not included in the cleaning schedule and the retention limit is not enforced.
- If the only remaining DR backup is expired, the Cyber Recovery software does not delete it, ensuring that there is always at least one DR backup available.

Results

Backup data is now available if you must recover your Cyber Recovery configuration.

Next steps

If you change the MTree used for a DR backup, new NFS exports are created. The previous NFS exports remain. Optionally, delete the previous NFS exports on the DD system.

Retrieving your preserved Cyber Recovery configuration

Use a disaster recovery (DR) backup to return your Cyber Recovery configuration to the state before a management server failure. Retrieve the backup data and then perform a recovery.

Prerequisites

Ensure that you have a DR backup of your Cyber Recovery configuration.

About this task

DR backups are stored on a separate MTree on the DD system in the Cyber Recovery vault.

Steps

1. On the DD system, create an NFS export to map to the Cyber Recovery management host on which you want to perform the recovery. Ensure that you use the `no_root_squash` option for the NFS export:

```
nfs add /data/coll/drbackups <hostname>(no_root_squash)
```

2. On the Cyber Recovery management host, mount the NFS export to a specific directory:

```
mount <DD hostname>:/data/coll/drbackups /mnt/drbackups
```

The DR backup files are accessible for the recovery procedure.

3. Access the backup data and perform the recovery.
4. After you recover the Cyber Recovery configuration, perform the following cleanup steps:
 - a. On the Cyber Recovery management host, run the following command:

```
umount /mnt/drbackups
```

- b. On the DD system, remove the NFS export that you created in step 1:

```
nfs del /data/coll/drbackups <hostname>
```

The DR backup files are no longer accessible to the Cyber Recovery management host.

Deleting unneeded Cyber Recovery objects


Delete alerts, events, expired and unlocked copies, DR backups, and jobs when they are no longer needed.

Prerequisites

To ensure that the DR backup is included in the cleaning schedule, enable and configure a DR backup from the **DR Backup** option under **System Settings**. The Cyber Recovery software deletes a DR backup using the same process as an unlocked copy.

About this task

By setting a Cyber Recovery cleaning schedule, you can avoid system slowdown. The Cyber Recovery software provides a default cleaning schedule, which you can modify.

 **NOTE:** If the only remaining backup is expired, the Cyber Recovery software does not delete it, ensuring that there is always at least one DR backup available.

Steps


1. From the Masthead Navigation, click the gear icon to access the **System Settings** list.

2. Select **Maintenance**.

The **Cleaning Schedule** window in the **Maintenance** dialog box is displayed.

3. To modify the default cleaning schedule:

- a. Specify the frequency for when the schedule runs, the time that the schedule runs next, and the age of the objects to delete.

 **NOTE:** The Cyber Recovery UI uses the same time zone as the Cyber Recovery management host for the scheduled time.

The **Delete unlocked copies older than** field affects locked and unlocked copies differently. An unlocked copy is deleted after the set numbers of days. A locked copy is deleted after the set number of days after the retention lock expires. For example, a copy is retention locked for 14 days and the **Delete unlocked copies older than** field is set to 7 days. After 14 days, the file is unlocked and then after 7 days it is deleted. That is, after 21 days, the copy is deleted.

b. Click **Save**.

The cleaning operation runs, using the values that you defined in the cleaning schedule.

4. To run the cleaning schedule on demand, click **Clean Now**.

The cleaning operation runs immediately, using the values that you defined in the cleaning schedule. An informational message indicates that the job has started and provides a **View Jobs** link that redirects you to the **System Jobs** content pane.

Cyber Recovery disaster recovery

The Cyber Recovery `crsetup.sh` setup script with the `recover` option enables you to perform a recovery after a disaster.

In some cases, it might be necessary to clean up existing Cyber Recovery Docker containers before you restore the Cyber Recovery software. These cases can include, but are not limited to:

- An update failed.
- You deleted the Cyber Recovery directory by mistake.
- The uninstallation section of the setup script does not allow removal of the Cyber Recovery software.

See [Cleaning up existing Cyber Recovery Docker containers](#).

After you clean up the existing Docker containers, follow the procedures to restore the Cyber Recovery software for either a Cyber Recovery software installation or a Cyber Recovery virtual appliance deployment. See:

- [Restoring a Cyber Recovery software installation after a disaster](#)
- [Restoring a Cyber Recovery a virtual appliance deployment after a disaster](#)

Cleaning up existing Cyber Recovery Docker containers

If necessary, clean up existing Cyber Recovery containers before you run the restore procedure after a disaster.

Steps

1. Identify the Cyber Recovery containers that are running:

```
docker container ls --filter name=cr_
```

The output shows the running Cyber Recovery containers. The following list is an example of what you might see:

- `cr_swagger`
- `cr_ui`
- `cr_edge`
- `cr_clouds`
- `cr_shelteredharbor`
- `cr_system`
- `cr_schedules`
- `cr_policies`
- `cr_vcenter`
- `cr_mgmtdds`

- cr_apps
- cr_notifications
- cr_vault
- cr_users
- cr_mongo
- cr_registry

NOTE:

- Each container name includes a suffix, which differs depending on your version of Docker Compose.
- If the Cyber Recovery instance is not running on or Amazon Web Services (AWS), the cr_clouds container is not displayed.
- If the Cyber Recovery instance is not running in a Sheltered Harbor deployment, the cr_shelteredharbor container is not displayed.

2. Stop all the running Cyber Recovery containers:

```
docker container stop `docker container ls -q --filter name=cr_`
```

3. Remove all the stopped Cyber Recovery containers:

```
docker container rm `docker container ls -a -q --filter name=cr_`
```

4. Verify that all Cyber Recovery containers are removed:

```
docker container ls -a --filter name=cr_
```

No containers are listed.

5. List the Cyber Recovery images that are associated with the containers that you removed:

```
docker images | grep localhost:14779/cr_
```

6. Remove all the Cyber Recovery container images:

```
docker image remove `docker images | grep localhost:14779/cr_ | awk '{ print $3 }'`
```

7. Verify that all the Cyber Recovery container images have been removed:

```
docker images | grep localhost:14779/cr_
```

The images that were listed in step 5 are no longer listed and the cleanup is complete.

8. Perform to the Cyber Recovery software restore procedure (see [Restoring a Cyber Recovery software installation after a disaster](#)).

Restoring a Cyber Recovery software installation after a disaster

Use the `crsetup.sh` setup script with the `recover` option to perform a disaster recovery.

Prerequisites

Before you perform this procedure:

- Have a Cyber Recovery backup tar package that was created before the disaster. Otherwise, you cannot complete this procedure.
- Delete the Cyber Recovery installation directory.
- If necessary, clean up existing Docker containers before you begin this procedure. See [Cleaning up existing Cyber Recovery Docker containers](#).

About this task

For information about how to install the Cyber Recovery software, see the Dell PowerProtect Cyber Recovery Installation Guide.

Steps

1. Install the same version of the Cyber Recovery software that was running before the disaster occurred.

If you were running an installation that included patch updates, install the patch updates also.

NOTE: We recommend that when you reinstall the Cyber Recovery software for this procedure that you use the same password that was used in the previous installation for the crso account, the MongoDB database, and the lockbox. This same password makes it easier to complete the recovery procedure. We also recommend that you use the same installation locations.

2. When the installation is complete, start the UI and validate that the configuration is empty.
3. Close the UI.
4. Start the Cyber Recovery software restore procedure:
 - a. Run the `crsetup.sh` setup script:

```
crsetup.sh --recover
```

- b. Type **y** to continue:

```
Do you want to continue [y/n]:
```

- c. Type **y** to confirm and continue:

```
Are you REALLY sure you want to continue [y/n]:
```

- d. Type the full path to the Cyber Recovery backup tar package location, for example:
`/tmp/cr_backups/cr.19.2.1.0-3.2019-09-19.08_02_09.tar.gz`
- e. Type the newly installed MongoDB password.

```
Please enter the newly installed MongoDB password:
```

NOTE: This password is the password that you created when you reinstalled the Cyber Recovery software in step 1.

- f. Type the lockbox passphrase for the original installation, that is, the installation before the disaster:

```
Enter the previously saved lockbox passphrase:
```

The Cyber Recovery restore operation proceeds and then returns a success message when it completes:

```
19.02.19 08_45_20 :  
19.02.19 08_45_20 : Cyber Recovery has been successfully recovered onto this system  
19.02.19 08_45_20 :
```

5. Log in to the Cyber Recovery UI or the CRCLI and validate that the previous installation has been restored.

Restoring a Cyber Recovery virtual appliance deployment after a disaster

Return your system to the state that it was in after the Cyber Recovery virtual appliance deployment. Then, use the `crsetup.sh` setup script with the `recover` option to perform a disaster recovery.

Prerequisites

Before you perform this procedure:

- Have a Cyber Recovery backup tar package that was created before the disaster. Otherwise, you cannot complete this procedure.
- Delete the Cyber Recovery installation directory.
- If necessary, clean up existing Docker containers before you begin this procedure. See [Cleaning up existing Cyber Recovery Docker containers](#).

About this task

For information about how to install the Cyber Recovery software, see the Dell PowerProtect Cyber Recovery Installation Guide.

Steps

1. Redeploy the Cyber Recovery virtual appliance.

You can either:

- Download and deploy the version of the Cyber Recovery virtual appliance that you want to run.
- Deploy the version of the Cyber Recovery virtual appliance that is currently in the Cyber Recovery vault. If necessary, update to a later version.

2. Start the Cyber Recovery software restore procedure:

- a. Run the `crsetup.sh setup` script:

```
crsetup.sh --recover
```

- b. Type **y** to continue:

```
Do you want to continue [y/n]:
```

- c. Type **y** to confirm and continue:

```
Are you REALLY sure you want to continue [y/n]:
```

- d. Type the full path to the Cyber Recovery backup tar package location, for example:

```
/tmp/cr_backups/cr.19.2.1.0-3.2019-09-19.08_02_09.tar.gz
```

The Cyber Recovery restore operation proceeds and then returns a success message when it completes:

```
19.02.19 08_45_20 :  
19.02.19 08_45_20 : Cyber Recovery has been successfully recovered onto this system  
19.02.19 08_45_20 :
```

3. Log in to the Cyber Recovery UI or the CRCLI and validate that the previous installation has been restored.

Troubleshooting

This section describes tasks that you can perform to troubleshoot Cyber Recovery issues.

Topics:

- [Using the crsetup.sh script](#)
- [Troubleshooting suggestions](#)
- [Reviewing Cyber Recovery logs](#)
- [Managing Cyber Recovery services](#)
- [Delete devices that are recovered onto your NetWorker server](#)
- [Disabling SSH access to the replication interface](#)

Using the crsetup.sh script

Run the `crsetup.sh` script to install, manage, verify, and remove the Cyber Recovery software. Other options enable functions for management and troubleshooting. This topic provides a reference for the options used in the procedures in this guide.

Syntax

```
crsetup.sh <option>
```

Options

The following options, including the corresponding flags, determine the result of the `crsetup.sh` script.

--addcustcert, -y

Add the custom CA-signed certificates to the Cyber Recovery system.

--address, -a

Update the IP address of the Cyber Recovery management host.

--changepassword, -w

Change the passphrase or password for the Cyber Recovery lockbox, MongoDB, and the Security Officer (crso), and create a Cyber Recovery backup, which enables you to restore your data if you forget your lockbox passphrase. If multifactor authentication is enabled, it is disabled when you change the Security Officer (crso) password.

--check, -c

Run the configuration check to validate proper installation requirements.

--deploy, -d

Configure the Cyber Recovery software (OVA only).

--forcecreate, -f

Force recreation of the Cyber Recovery containers.

--gencertrequest, -j

Generate a certificate-signed request (CRSERVICE.csr) file.

--help, -h

Display the help content.

--install, -i

Install the Cyber Recovery software.

--irprop, -t
Display the IR script information for Cyber Recovery configuration.

--recover, -r
Recover the Cyber Recovery software.

--restart, -e
Stop and then start all services.

--save, -b
Save the Cyber Recovery software configurations.

--securereset, -l
Reset the Cyber Recovery root certificates and encryption keys. This option stops the Cyber Recovery services, regenerates the certificates and stores them in the lockbox, and then starts the Cyber Recovery services.

--start, -s
Start the Cyber Recovery software.

--stop, -p
Stop the Cyber Recovery software.

--uninstall, -x
Uninstall the Cyber Recovery software.

--upgcheck, -k
Run a pre-update readiness check.

--upgrade, -u
Update the Cyber Recovery software.

--verifypassword, -v
Verify the lockbox passphrase and the MongoDB and crso passwords.

Troubleshooting suggestions

The following table lists possible Cyber Recovery problems and suggested remedies.

Table 22. Troubleshooting suggestions

If you cannot	Do the following
Install the Cyber Recovery software	<ul style="list-style-type: none"> • Ensure that the <code>crsetup.sh --check</code> script verifies all prerequisites before continuing. • Ensure that you are using a stable version of Docker. • Set Docker to start on reboot with the <code>systemctl enable docker</code> command. • Find the <code>crsetup.sh</code> logs in the directory from which you run <code>crsetup.sh</code>. • If your system has an active firewall, ensure that the following ports are open on the firewall: <ul style="list-style-type: none"> ◦ 14777 (for Cyber Recovery UI) ◦ 14778 (for the Cyber Recovery REST API) ◦ 14779 (for the Cyber Recovery Registry - local management host access) ◦ 14780 (for the Cyber Recovery API Documentation)
Log in to the Cyber Recovery UI	<ul style="list-style-type: none"> • Check the edge and users service logs. • Ensure that your DNS settings are resolvable. • If your system has an active firewall, ensure that the following ports are open on the firewall: <ul style="list-style-type: none"> ◦ 14777 (for Cyber Recovery UI) ◦ 14778 (for the Cyber Recovery REST API)

Table 22. Troubleshooting suggestions (continued)



If you cannot	Do the following
	<ul style="list-style-type: none"> 14779 (for the Cyber Recovery Registry - local management host access) 14780 (for the Cyber Recovery API Documentation)
Start the Cyber Recovery software after a reboot due to an unlabeled context type and custom policies.	<p>In an SELinux environment, if the Cyber Recovery software does not start after a reboot due to unlabeled context type and custom policies, do the following:</p> <ol style="list-style-type: none"> Assuming that the Cyber Recovery software is installed in <code>/opt/dellemc/cr</code>, change the SELinux context, as shown in the following example: <pre>chcon -u system_u -t bin_t /opt/dellemc/cr/bin/cradmin chcon -u system_u -t bin_t /opt/dellemc/cr/bin/crcli chcon -u system_u -t bin_t /opt/dellemc/cr/bin/crsetup.sh chcon -u system_u -t bin_t /opt/dellemc/cr/bin/crshutil chcon -u system_u -t bin_t /opt/dellemc/cr/bin/crssshutil</pre> Reboot the system. <p>The following is an example of the SELinux context:</p> <pre>root@hostname \$ ls -Z /opt/dellemc/cr/bin/ -rwxr----- . root root system_u:object_r:bin_t:s0 cradmin -rwxr----- . root root system_u:object_r:bin_t:s0 crcli -rwxr----- . root root system_u:object_r:bin_t:s0 crsetup.sh -rwxr----- . root root system_u:object_r:bin_t:s0 crshutil -rwxr----- . root root system_u:object_r:bin_t:s0 crsshutil</pre>
Enable multifactor authentication	<p>Because multifactor authentication is a time-based security mechanism, the Cyber Recovery host time cannot differ from the authenticator time by more (plus or minus) than one minute. If the time differs by more than +60 seconds or -60 seconds, multifactor authentication is not enabled. Set the Cyber Recovery host time so that it differs no more than a minute (plus or minus) from the authenticator time.</p> <p> NOTE: If you modify the Cyber Recovery host time, stop and then restart the Cyber Recovery services.</p> <p>To avoid this scenario, internal NTP configuration is recommended.</p>
(For crso only) Log in because multifactor authentication is enabled and you are unable to provide the security code	<p>As the crso, type <code>crsetup.sh --changepassword</code> or <code>crsetup.sh -w</code> to change the crso password and disable multifactor authentication. Enable multifactor authentication again after you log in.</p>
Change the application type	<p>Delete the application and then add a new application and choose the appropriate application type.</p>
Run a job	<p>Check the schedules, policies, or mgmtdds service logs.</p>
Complete a successful Sync job	<p>If the DD system on the Cyber Recovery vault exceeds the space usage threshold, clean up the DD system to reclaim space. Then, restart the Sync job.</p>
Receive alert email messages	<ul style="list-style-type: none"> If your system has an active firewall, ensure that port 25 is open on the firewall. Verify your Postfix or email configuration and check that you added the email for alert notifications.
Secure the Cyber Recovery vault	<p>Check the vault service logs.</p>
Recover or analyze	<p>Check the apps, mgmtdds, and policies service logs.</p>
Run a subsequent Analyze job after performing a DR backup while running an Analyze job	<p>Wait for the currently running Analyze job to finish, delete the stale sandboxes, and then run the Analyze job again.</p>

Table 22. Troubleshooting suggestions (continued)


If you cannot	Do the following
	<p> NOTE: When you perform a DR backup while an Analyze job is running, the Cyber Recovery software marks the Analyze job as critical even though it is still running.</p>
Run a policy, sandbox, or recovery due to mount errors from the DD system	<p>Ensure that the NFSv4 and NFSv3 settings on the DD system are configured to run NFS operations:</p> <ol style="list-style-type: none"> 1. From the DD UI, got to Protocols > NFS and then click Options. 2. To run an NFSv3 server only, ensure that the values for the Default Export Version and Default Servers Version fields are set to NFSv3. 3. To run an NFSv4 server only, ensure that the values for the Default Export Version and Default Servers Version fields are set to NFSv4 and the NFSv4 ID Map Out Numeric field is set to always. 4. To run both an NFSv3 and NFSv4 server, ensure that the values for the Default Export Version and Default Servers Version fields are set to NFSv3 and NFSv4 and the NFSv4 ID Map Out Numeric field is set to always.
Complete a NetWorker recovery operation cleanly. For example, if you encounter a problem during the automated recovery process.	<p>Perform a manual cleanup:</p> <ol style="list-style-type: none"> 1. Shut down NetWorker. For example: /etc/init.d/networker stop 2. For the resource database, complete the following steps: <ol style="list-style-type: none"> a. Find the latest <code>resdb (/nsr/res.cr.<timestamp>)</code> directory. b. Remove the current <code>/nsr/res</code> directory. c. Restore the previous resource database by renaming the <code>res.cr.<timestamp></code> directory to the following: <code>/nsr/res</code> For example: mv /nsr/res.cr.1554828308 /nsr/res 3. For the media database, complete the following steps: <ol style="list-style-type: none"> a. Find the latest <code>mm (/nsr/mm.cr.<timestamp>)</code>. b. Remove the current <code>/nsr/mm</code> directory. c. Restore the previous media database by renaming the <code>/nsr/mm.cr.<timestamp></code> directory to the following: <code>/nsr/mm</code> For example: mv /nsr/mm.cr.155512814 /nsr/mm 4. For the index database, complete the following steps: <ol style="list-style-type: none"> a. Find the latest <code>index (/nsr/index.cr.<timestamp>)</code>. b. Remove the current <code>/nsr/index</code> directory. c. Restore the previous index directory by renaming the <code>/nsr/index.cr.<timestamp></code> directory to the following: <code>/nsr/index</code> For example: mv /index/mm.cr.151231326 /nsr/index 5. Restart NetWorker. For example: /etc/init.d/networker start

Reviewing Cyber Recovery logs

The Cyber Recovery software generates both a JSON and a text logfile for each service.

The log files are stored in the `<installation directory>/var/log/<component>` directory, where *component* is one of the following Cyber Recovery components:

Table 23. Cyber Recovery component log directories

Cyber Recovery component	Log directories
cradmin	Anything that is related to lockbox activity.
crcli	Anything that is related to the CRCLI.
crsetup	Anything that is related to the <code>crsetup.sh</code> script.
edge service	The routing for all calls from REST clients, the Cyber Recovery CLI, and the Cyber Recovery UI, as well as the logic for setting system log levels, licensing, and dashboard.  NOTE: This service is the entry point for all REST API calls.
apps service	Anything that is related to applications that are associated with Cyber Recovery, including CyberSense feature used for copy analysis, NetWorker, Avamar, and PowerProtect Data Manager instances, and file system hosts.
mgmtdds service	All communication with the Cyber Recovery vault DD.
notifications service	All the system notifications (alerts and events) and SMTP email messages.
policies service	Anything that is related to policies, jobs, copies, and sandboxes.
schedules service	All the system schedules, cleaning schedules, and action endpoints.
users service	Anything that is associated with users, including addition, modification, and authentication operations.
vault service	Anything that is related to the status of the vault, and opening and closing managed interfaces.
nginx service	Anything that is related to the web server that runs the Cyber Recovery UI.
swagger service	Anything that is related to the Cyber Recovery REST API container.
system service	Anything that is related to DR backups and log bundle creation.
vcenter service	Anything that is associated with vCenter objects.
clouds service	Anything that is related to the Cyber Recovery vault on Amazon Web Services (AWS).

All Cyber Recovery logfiles use the following log message format:

```
[<date/time>] [<error type>] <microservice name> [<source file name>: <line number>] :  
message
```

For example:

```
[2018-08-23 06:31:31] [INFO] [users] [restauth.go:63 func1()] : GET /irapi/users Start  
GetUsers
```

Log Levels

The following table describes the log levels by order from low to high. Each log level automatically includes all lower levels. For example, when you set the log level to INFO, the log captures all INFO, WARNING, and ERROR events.

The default log level is INFO.

Table 24. Log levels

Log Level	Purpose	Example
ERROR	Reports failures in the execution of some operation or task that usually requires manual intervention.	<ul style="list-style-type: none"> Replication failure due to an incorrect password Sandbox creation failure due to the mount point already in use
WARNING	Reports unexpected technical or business events that might indicate a potentially harmful situation, but do not require immediate attention.	<ul style="list-style-type: none"> Corrupted or truncated file Policy 1 hour over the sync timeout period of 6 hours
INFO	Reports information about the progress of an operation or task.	<ul style="list-style-type: none"> Synchronization started Creating a point-in-time copy Scanning for malware
DEBUG	Captures highly granular information for debugging or diagnosis.	This level is typically useful to administrators, developers, and other users.

Managing Cyber Recovery services

Start and stop Cyber Recovery Docker container services manually if there is an unexpected event on the management host.

Use the `crsetup.sh` script that is in the Cyber Recovery installation directory. To stop or start the Docker container services, use the `--stop` and `--start` options. To stop and then immediately restart the services, use the `--restart` option.

Enter the following command to stop the Docker container services:

```
# ./crsetup.sh --stop
```

The following Cyber Recovery Docker container services stop in this order:


Table 25. Cyber Recovery Docker container services

Service	Function
swagger	Provides access to the Cyber Recovery REST API documentation
ui	Manages Cyber Recovery UI actions
edge	Acts as the gateway to the Cyber Recovery services
clouds	Provides access to supported cloud vendors; the current cloud vendor is Amazon Web Services (AWS)
system	Manages internal Cyber Recovery system-level activities such as cleaning, DR backups, creating log bundles, and so on
schedules	Manages Cyber Recovery schedule actions
policies	Manages Cyber Recovery policy actions
vcenter	Manages the vCenter server objects that are required for PowerProtect Data Manager deployments
mgmtdds	Manages the DD actions in the Cyber Recovery vault
apps	Manages storage system and applications in the Cyber Recovery vault actions
notifications	Manages alert, event, email, and log actions
vault	Manages CR Vault actions
users	Manages the Cyber Recovery Admin users and the Security Officer user actions
mongo-auth	Manages the database

Enter the following command to start the Docker container services:

```
# ./crsetup.sh --start
```

The Docker container services start again.


 **NOTE:** At this time, you cannot stop and start an individual Docker container service.

Delete devices that are recovered onto your NetWorker server

After an automated NetWorker recovery using the Cyber Recovery software completes, manually delete devices that the procedure recovered onto your NetWorker server.

About this task

Your NetWorker server might include other devices that were there before the Cyber Recovery backup recovery job.

 **NOTE:** Only delete devices that the Cyber Recovery software recovered onto your NetWorker server. Ensure that you do not delete devices that you must keep.

Steps

1. Unmount the NetWorker sandbox from the Cyber Recovery management host:

```
umount /opt/dellemc/cr/mnt/cr-rec-ldpda240_1604
```

2. Go to the NetWorker UI.
3. From the **Protection** tab, perform the following tasks:
 - a. Delete newly added clients.
 - b. Delete newly added policies.
 - c. Delete newly added groups.
 - d. Delete any other newly added protection types.
4. From the **Devices** tab, perform the following tasks:
 - a. Delete newly added devices.
 - b. Delete newly added DD system.
 - c. Delete newly added storage nodes (if necessary).
5. From the **Media** tab, perform the following tasks:
 - a. Delete newly added disk volumes.
 - b. Delete newly added media pools.
 - c. Delete any other newly added media types.

Disabling SSH access to the replication interface

Disable SSH access to the replication interface on the Cyber Recovery vault DD system.

About this task

The Cyber Recovery software works with a replication data link between the vault-environment and production-environment DD systems. The Cyber Recovery software communicates with all DD systems by using SSH.

Optionally, use the following procedure on the DD host to restrict SSH inbound access for the Cyber Recovery management host:

Steps

1. On the management host, obtain the hostname.
2. Log in to the DD host and enter the following command:

```
adminaccess ssh add <hostname>
```

where <hostname> is the hostname from step 1.

3. Use the DD net filter functionality.
For information about how to use the net filter functionality, see the DD documentation.

Results

SSH is blocked on all interfaces except the management interface.