Dell PowerProtect Cyber Recovery 19.19

Product Guide

Version 19.19

May 2025
Rev. 03

DELL Technologies

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

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 and Update 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 on Google Cloud Platform Deployment Guide
- Dell PowerProtect Cyber Recovery Command-Line Interface Reference Guide
- Dell PowerProtect Cyber Recovery Alerts and Events Reference Guide
- Dell PowerProtect Cyber Recovery OS Update Release Notes
- Dell PowerProtect Cyber Recovery Open Source License and Copyright Information

See the Dell Technologies Info Hub for PowerProtect Cyber Recovery to access Cyber Recovery white papers, blogs, and videos.

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, Dell PowerProtect Data Manager, and Index Engines CyberSense 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 DPADDocFeedback@dell.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

1

Introduction

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

Topics:

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), Microsoft Azure, or Google Cloud Platform.

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 is disconnected from the production network. A DD 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.

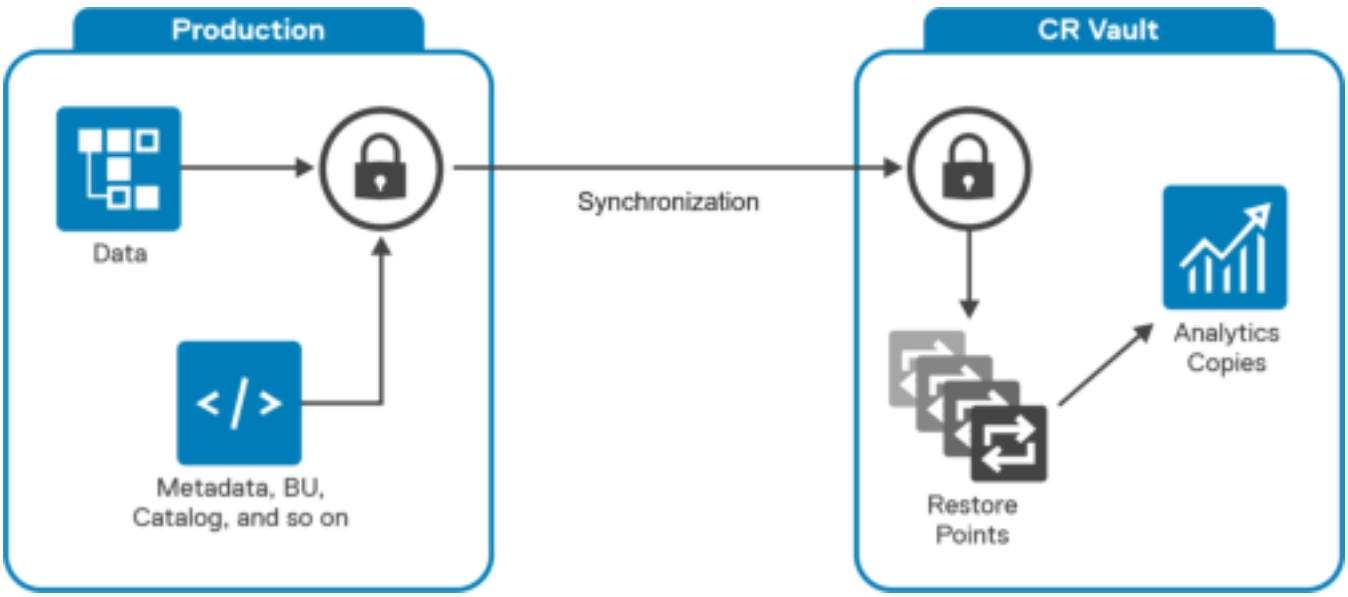


Figure 1. High-level solution architecture

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 required for a vaulted environment.

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:

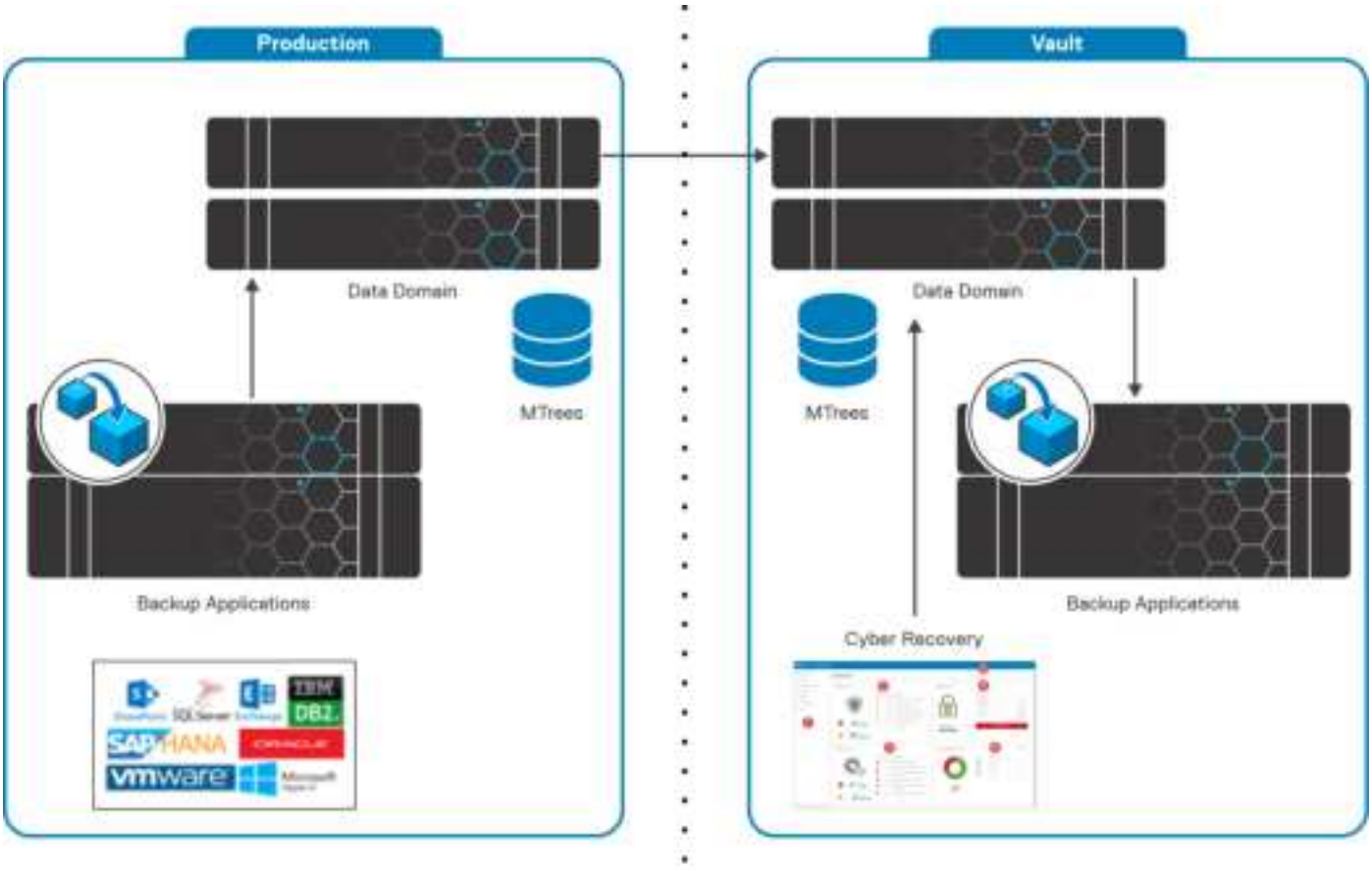


Figure 2. Cyber Recovery architecture

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, you can validate and analyze your data.

By enabling the Sheltered Harbor feature, you can protect financial data against catastrophic events in accordance with financial sector Sheltered Harbor initiative's standards.

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/col1/cr-policy-<policyID>-repo
```

Where *<policyID>* is the unique ID that is created when you create a Cyber Recovery policy. The Cyber Recovery software adds the `cr-policy-` prefix to the name.

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 `cr-policy-<policy-id>-repo` MTree. Data can be scanned for malware or analyzed as needed in the sandbox.
Lock	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: • 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. **NOTE:** The Cyber Recovery software does not support the Indefinite Retention Hold capability of Retention Lock Governance or Retention Lock Compliance Modes. For information about the governance and compliance archive data requirements and how to manage them, see the *DDOS Administration Guide* at Dell Online Support.

Table 1. Cyber Recovery operations (continued)

Operation	Description
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.
Recovery Check	You can run a scheduled or on-demand recovery check on a PowerProtect Data Manager or a NetWorker version 19.9 and later recovery to provide assurance that after a successful recovery, a copy can be recovered.
Sheltered Harbor Copy (only if the Sheltered Harbor feature is enabled)	You can generate a copy of the most recent replication that meets Sheltered Harbor standards and requirements. A Sheltered Harbor copy operation generates archive volumes that have been validated, encrypted, and retention locked. It also generates a report with an email containing an attestation for submission to the Sheltered Harbor Monitoring Log to confirm the results for the operation.

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 DDOS Administration Guide*.

About this task

DD systems support both Governance mode and Compliance mode retention locking, which enable you to apply retention policies at an individual file level. Compliance mode is a stricter type of retention locking. 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 Dell DP4400 Integrated Data Protection Appliance (IDPA) .

Steps

1. On the Cyber Recovery vault DD system, log in as an admin user. If a security officer has not already been created, 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.

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 procedure creates the default Cyber Recovery security officer (crso) and assigns the security officer role to this user. The crso can be considered the superuser. There is only one crso per Cyber Recovery installation. The crso must perform the initial Cyber Recovery login and then create other users. Other user roles cannot modify or manage the crso. Users with the security officer role can create multiple security officers.

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

The Cyber Recovery user roles include:

- Dashboard—This role enables the user to view the Cyber Recovery dashboard but not perform tasks.
- Operator—This role enables the user to do the following:
  - Assets—View and export information
  - Policies and associated objects—Run
  - Reports—Create, schedule, and run
  - Alerts—Acknowledge and add notes
  - Cyber Recovery vault—Manually secure
  - Recovery—Run recoveries, run recovery checks, manage sandboxes, and launch applications
  - Cancel jobs
  - Password—Change for this user account
  - Multifactor authentication—Enable, disable, and configure for this user account
  - Log bundles—Generate and delete
- Admin—This role enables the user to do the following:
  - Assets—Create and manage
  - Policies and associated objects—Create, manage, and run
  - Reports—Create, schedule, and run
  - Alerts—Acknowledge and add notes
  - Cyber Recovery vault—Manually secure
  - Recovery—Run recoveries, run recovery checks, manage sandboxes, and launch applications
  - Cancel jobs
  - Password—Change for this user account
  - Multifactor authentication—Enable, disable, and configure for this user account
  - Log settings—Modify
  - Log bundles—Generate and delete
- Security officer—This role enables the user to do the following:
  - User accounts—Create, modify, enable, disable, and delete security officer, admin, and dashboard users
  - Passwords:
    - Reset dashboard, admin, and security officer user passwords
    - Change for this user account
    - Set the password policy to enhance protection and prevent unauthorized access
  - Multifactor authentication for an admin user—Disable
  - Mail server settings—Enable, configure settings, and manage allowable domains
  - Telemetry reports—Enable and configure the frequency and run date

- Cyber Recovery vault—Manually secure and release (unsecure)
- Log bundles—Generate and delete

NOTE: The security officer cannot modify, delete, enable, or disable multifactor authentication for the crso. If as the crso, you forget your password, use the `crsetup.sh` command to reset it. For instructions, see Resetting Cyber Recovery passwords.

User roles and UI operations

The following table lists which user roles can access which operations in the Cyber Recovery UI.

Table 2. User roles access

UI Component	Operation	Security officer	Admin	Operator	Dashboard
Getting started wizard and Get Started drop-down list on the masthead navigation	Review checklist	Yes	Yes	No	No
	Add user	Yes	No	No	No
	Add vault storage	No	Yes	No	No
	Add policy	No	Yes	No	No
Dashboard	View all dashboard	Yes	Yes	Yes	Yes
	Secure vault	Yes	Yes	Yes	No
	Release vault	Yes	No	No	No
	Links to alerts	Yes	Yes	Yes	No
	Filters for and links to jobs	No	Yes	Yes	No
Infrastructure > **Assets** > **Applications**	• Add • Edit • Delete • Export • View • Multilink configuration	No	Yes	View and export application assets only	No
Infrastructure > **Assets** > **VCenters**	• Add • Edit • Delete • Export • View	No	Yes	View and export application vCenter assets only	No
Infrastructure > **Storage**	• Add • Edit • Delete • Export • View	No	Yes	View and export storage assets only	No
Infrastructure > **Sheltered Harbor**	• Add • Edit • Delete • Export	No	Yes	View and export financial institution only	No
Alerts and Events > **Alerts**	• Acknowledge • Unacknowledged • Add note • Export	Yes	Yes	Yes	No

Table 2. User roles access (continued)

UI Component	Operation	Security officer	Admin	Operator	Dashboard
	• View				
Alerts and Events > **Events**	• View	Yes	Yes	Yes	No
Policies > **Policies**	• Add • Edit • Actions • Delete • Export • View • Disable	No	Yes	View and export policies, and manually run policy actions only	No
Policies > **Copies**	• Lock • Analyze • Delete • Export • Analysis report actions • View	No	Yes	Yes	No
Policies > **Schedules**	• Add • Edit • Delete • Export • View	No	Yes	View and export schedules only	No
Recovery > **Copies**	• Sandbox • Application • Alternate recovery • Recovery check • View	No	Yes	Yes	No
Recovery > **Sandboxes**	• Delete • Export • View	No	Yes	Yes	No
Recovery > **Recovery Sandboxes**	• Launch application • Cleanup • Export • View	No	Yes	Yes	No
Administration > **Users**	• View all users • Add • Edit • Disable • Delete • Set password policy • Disable other users' multifactor authentication	Yes	No	No	No
	• View (self) • Edit (self) • Disable multifactor authentication (self)	Yes	Yes	Yes	No

Table 2. User roles access (continued)

UI Component	Operation	Security officer	Admin	Operator	Dashboard
Administration > **Alert Notifications**	• Enable and disable **Receive Critical Alerts** and **Receive Warning Alerts** options	Yes	No	No	No
	• View	Yes	Yes (for self only)	Yes (for self only)	No
Reports	• Create reports • Generate reports • Scheduled reports • Export	No	Yes	Yes	No
Jobs	• View protection, system, and recovery jobs • Export protection, system, and recovery jobs • Cancel protection, system, and recovery jobs	No	Yes	View and export protection, system, and recovery jobs only	No
System Settings > **Maintenance**	• Edit • Run • View cleaning schedule	No	Yes	View cleaning schedule only	No
System Settings > **DR Backups**	• Edit • Run • View DR backup schedule	No	Yes	No	No
System Settings > **License**	• Enable • Add • View	Yes	Yes	No	No
Support > **Mail Settings**	• Enable email notifications • View server • Edit settings • Add Transport Layer Security (TLS) certificate • Change TLS certificate • Enable restricted domains	Yes	Yes (view only)	Yes (view only)	No
Support > **Log Settings**	• View • Edit	No	Yes	Yes	No
Support > **Support Bundles**	• Create • View • Delete • Download	Yes	Yes	Yes	No
Support > **Telemetry Reports**	• View • Edit	Yes	No	No	No

Table 2. User roles access (continued)

UI Component	Operation	Security officer	Admin	Operator	Dashboard
	• Disable				
System Settings > **Login Count Settings**	• Modify	Yes	No	No	No
User Settings > **Multifactor Authentication**	• Add (self) • View (self) • Disable (self)	Yes	Yes	Yes	No

Management tools

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

Cyber RecoveryUI

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 or IP address 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 available commands for your user role or see the *Dell PowerProtect Cyber Recovery Command-Line Interface Reference Guide*, which provides comprehensive information about the CRCLI.

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 or IP address of the management host.

Sheltered Harbor feature overview

Dell PowerProtect Cyber Recovery for Sheltered Harbor is a solution that meets the technical requirements of the Sheltered Harbor Turnkey Data Vaulting Solution specification.

The Cyber Recovery vault provides an isolated and encrypted environment to meet the security, confidentiality, and integrity requirements of the standard. The protected data is available for quick restoration of a known good copy to recover critical systems and resume financial services to customers. Cyber Recovery for Sheltered Harbor automatically synchronizes data between production or backup systems and the Cyber Recovery vault, and stores immutable copies.

Sheltered Harbor participants are required to send a daily attestation message that confirms successful completion of the daily archiving process. Sheltered Harbor manages the monitoring log utility, which accepts and records these daily attestation messages. Sheltered Harbor monitors these attestation messages, notes noncompliance and escalates with noncompliant participants, and provides compliance statistics to the financial industry.

Sheltered Harbor procedure

The Cyber Recovery software copies a Sheltered Harbor participant's data into the Cyber Recovery vault and ensures that it complies with the Sheltered Harbor Turnkey Data Vaulting Solution specification.

The Sheltered Harbor feature must be enabled before you can access Sheltered Harbor options and use the Sheltered Harbor feature. Each financial institution that you plan to add to the deployment requires a Sheltered Harbor license. Request a license file from Sheltered Harbor.

A Sheltered Harbor copy action performs a Cyber Recovery Secure Copy operation.

The Cyber Recovery software:

1. Performs a DD MTree replication from the DD production system to the DD system in the Cyber Recovery vault. This operation is a Sync operation.
2. Verifies that the data matches the manifest and that there are no anomalies.
3. Performs a fast copy of the replication. This operation is a Copy operation.
4. Creates an archive volume of all the data.
5. Encrypts the archive volume.
6. Retention locks the encrypted archive volume. This operation is a Lock operation.

   NOTE: The Cyber Recovery vault DD system must have a Retention Lock Governance or Compliance license. A Retention Lock Compliance license is recommended.

7. Generates a report with an email containing an attestation for submission to Sheltered Harbor to confirm that the data has been copied, verified, certified, and locked. Automated scripts that are outside of the Cyber Recovery vault can submit the attestation.

Modifying Sheltered Harbor financial institutions after updating to Cyber Recovery version 19.15.0.2 or later

If the Sheltered Harbor feature is licensed and enabled on a pre-19.15.0.2 version of Cyber Recovery, after updating to version 19.15.0.2 and later, modify any existing financial institution assets to follow the latest Sheltered Harbor license procedure.

Prerequisites

- You have requested and received a license file for each financial institution from Sheltered Harbor.
- The Cyber Recovery software is updated to version 19.15.0.2 or later.

About this task

After you have updated the software to Cyber Recovery version 19.15.0.2 or later, the Sheltered Harbor service is disabled. Any Sheltered Harbor actions and jobs do not function.

Steps

1. Run the `crsetup.sh --shenable` command to enable Sheltered Harbor.
   The Sheltered Harbor feature is now enabled.
2. From the Cyber Recovery UI, access the **Financial Institution** pane to view all existing financial institutions.
   For information about how to modify a financial institution, see Managing Sheltered Harbor financial institutions.
3. Select each financial institution and choose the license file that you received from Sheltered Harbor.
   The financial institution is updated with the license. Sheltered Harbor jobs for this financial institution will be completed successfully.

2

Getting Started

This section describes how to log in to and out of the Cyber Recovery UI, activate the Cyber Recovery license, use the Getting Started wizard, and enable multifactor authentication.

Topics:

Logging in to the Cyber Recovery UI

Log in to the Cyber Recovery UI to display the Cyber Recovery UI dashboard and perform Cyber Recovery UI operations.

Prerequisites

You have been added to the Cyber Recovery deployment as a user.

NOTE: For an initial installation, the crso user who is created during the installation procedure must first log in to the Cyber Recovery UI and add an admin user. Then, all other users that are added to the deployment can log in.

About this task

Users that are assigned the security officer, admin, or operator roles can perform tasks in the Cyber Recovery UI that are based on their roles. A dashboard user can 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 or IP address of the management host where the Cyber Recovery software is installed.

   The Cyber Recovery software supports the Google Chrome, Microsoft Edge, and Mozilla Firefox browsers. For the most current information, see E-Lab Navigator.

   The login page displays the Cyber Recovery version.
2. Enter your username and password.
3. Click **Log In**.
   a. If you enabled multifactor authentication, enter the security code in the **Security Code** field.

      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.

      The **What's New in Cyber Recovery** window, which lists new Cyber Recovery features, is displayed for all users except dashboard users.
   b. To hide the **What's New in Cyber Recovery** window for subsequent logins, swipe right on the slider at the bottom of the window.

      The **What's New in Cyber Recovery** window is displayed after a fresh installation of the Cyber Recovery software or an update to the current version.

c. To access the **What's New in Cyber Recovery** window again, click  on the masthead navigation.
d. If the security officer changed the password policy and your current password does not comply with the password policy, click **Change Password** in the error message that is displayed at the top of the pane. In the Change Password window, enter a new password that meets password policy requirements.

   As you type the characters for the password, a tooltip is displayed. The tooltip provides guidance and verification that is based on the current password policy.

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. As a security officer, 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: There is no session timeout for a dashboard user; the dashboard user is never logged out of Cyber Recovery UI automatically.

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 masthead navigation, click  .
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.

Completing initial setup with the Getting Started wizard

The Getting Started wizard guides you through the initial steps required to configure your Cyber Recovery environment.

When the Cyber Recovery installation is completed, first, the crso must log in to the Cyber Recovery UI and create at least one admin user.

When the crso logs in to the Cyber Recovery UI, the Getting Started wizard is displayed. The wizard includes two tiles that bring up the dialog boxes to add users, and to configure email server, telemetry, and log generation support settings.

The crso can select one or both wizard tiles, or bypass the wizard and display the Cyber Recovery dashboard. From the dashboard, the crso can access the configuration options from the Main Menu and the Masthead Navigation.

Then, an admin user can log in to the Cyber Recovery UI. The Getting Started wizard is displayed. The wizard includes three tiles that bring up the dialog boxes to review the deployment, define vault storage, and add a policy. The tile for adding a policy is disabled until the vault storage is defined. The admin user can select the wizard tiles, or bypass the wizard and display the Cyber Recovery dashboard. From the dashboard, the admin user can access the configuration options from the Main Menu and the Masthead Navigation.

NOTE: Because the crso and admin user can only perform specific assigned tasks, the Getting Started wizard only displays the tiles that apply to the logged-in user.

Completing the Getting Started wizard as the crso

After the Cyber Recovery software is installed, log in as the crso to add an admin user, which is required to add vault storage and create a policy.

Prerequisites

You are logged in as the crso.

About this task

When the Cyber Recovery software is installed, the crso must log in to the Cyber Recovery UI and create at least one admin user.

The Getting Started wizard guides you through the steps to add a user. It also guides you through the steps to configure email, telemetry, and support settings. The completed steps display the icon.

You can bypass the Getting Started wizard or specific steps in the wizard by clicking **Skip** on the **Getting Started** page. Later, complete the configuration from the Cyber Recovery UI or recall the Getting Started wizard steps from the System Settings option ( ) on the masthead navigation.

Steps

1. On the **Users** tile, click **Add**. Complete the fields in the **Add User** dialog box and click **Save**:

Table 3. User fields

Field	Description
Name fields (optional)	Specify the user's first name and last name.
Role	Select either: • Security officer—Enables users to create and manage user accounts, set the password policy, configure mail server settings, monitor alerts, secure and release the Cyber Recovery vault, manage support settings, and configure the number of login sessions. • Admin—Enables users to perform tasks and operations in the Cyber Recovery UI, monitor alerts, secure the Cyber Recovery vault, generate reports, and manage maintenance, disaster recovery backup, and support settings. • Operator—Enables users to view and export information, secure the Cyber Recovery vault, perform limited tasks and operation in the Cyber Recovery UI, and generate support bundles. • Dashboard—Enables users to view the Cyber Recovery dashboard but not perform tasks. The dashboard role does not time out.
User Name	Specify a username. **NOTE:** • The username is case insensitive. For example, if you add the username **admin**, you cannot add another username such as **ADMIN**, **Admin**, **ADMin**, or any other combination, The software displays an error message. Enter a unique username. • You cannot reuse the username of a deleted user.
Phone (optional)	Specify the user's telephone number.

Table 3. User fields (continued)

Field	Description
Email	Specify an email address for alert notifications. If the Cyber Recovery software is configured to send email messages, configured recipients can receive the messages. **NOTE:** Later, if a user's email is modified, the 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	Specify and confirm the password. The default password requirements include: • 9–64 characters. • At least 1 numeric character. • At least 1 uppercase letter. • At least 1 lowercase letter. • At least 1 special character (`~!@#$%^&*()+={}|:";<>?[]-_.,^'`). **NOTE:** For this release, do not use the colon (:) in the Postgres database password. The password policy that the security officer sets defines the number of characters that are required. The password policy also checks if the new password matches previous passwords or if the password includes the username. While you enter the password, a tooltip is displayed and verifies that the entries follow password rules and policy. When you change a password, enter and confirm both the new and existing passwords.
Force Password Change (optional)	When adding a user only, select the checkbox to force the user to change the password when logging in for the first time.
Session Timeout	Change the amount of idle time after which the user is logged out of the Cyber Recovery UI. The default value is 10 minutes.

2. Optionally, on the **Support** tile, click **Configure**.

   The Support pane, which includes the Mail Server, Telemetry Reports, and Support Bundles options, opens. For information about these options, see:

   - Configure mail settings
   - Configuring a telemetry report
   - Collecting logs for upload to support

3. Click **Launch** to go to the dashboard.
   The **What's New in Cyber Recovery** pane is displayed. When you click **Close**, the Cyber Recovery dashboard is displayed.

4. To recall the wizard at any time after the initial setup, click **Getting Started** under the  icon on the masthead navigation.

   The wizard steps that you completed display the  icon. The Users option includes the **Add** link. The Support option includes an **Edit** or **Configure** link. You can click the links to either complete or edit the configuration.

Results

The admin Cyber Recovery UI user can log in to the Cyber Recovery UI and use the Getting Started wizard to complete the setup of the Cyber Recovery configuration and create a policy.

Completing the Getting Started wizard as the admin user

After the Cyber Recovery software is installed, log in and review the deployment, define vault storage, and add a policy.

Prerequisites

You are logged in as the admin user.

About this task

When the Cyber Recovery software is installed and the crso has created your account as an admin user, you can check the Cyber Recovery deployment, add storage, and deploy a protection policy quickly.

The Getting Started wizard guides you through the steps to verify the deployment, add vault storage, and add a policy. The completed steps display the icon.

You can bypass the Getting Started wizard or specific steps in the wizard by clicking **Skip** on the **Getting Started** page. Later, complete the configuration from the Cyber Recovery UI or recall the Getting Started wizard steps from the System Settings option ( ) on the masthead navigation.

Steps

1. On the **Checklist** tile, click **View** to verify that you have performed the required deployment steps.

   If you have not satisfied all requirements, log out and complete the required steps.

2. On the **Vault Storage** tile, click **Add** to define the vault storage. Complete the following fields in the **Add Vault Storage** dialog box and click **Save**:

Table 4. Vault storage fields

Field	Description
Nickname	Enter a name for the vault storage.
FQDN or IP Address	Specify the DD host by using one of the following: • Fully qualified domain name (FQDN) • IP address **NOTE:** If you modify an existing FQDN or IP address, you must reenter all passwords.
Storage Username	Specify a dedicated Cyber Recovery DD administration account (for example, `cradmin`), which the Cyber Recovery software uses to perform operations with the DD system. This DD account must have the admin role. **NOTE:** If you modify the existing username, you must reenter the password.
Storage Password	Enter the password of the DD administrator.
SSH Port Number	Enter a storage SSH port number.
Reset Host Fingerprint (when editing vault storage 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 vault storage. 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 (...).

NOTE: Do not configure multiple Cyber Recovery servers to use the same DD system.

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

Table 5. Policy Information page

Field	Description
Name	Specify a policy name.
Type	From the drop-down list, select either **PPDM**, **Sheltered Harbor**, or **Standard**. **NOTE:**

Table 5. Policy Information page (continued)

Field	Description
	• Standard denotes NetWorker, Avamar, Filesystem, and Other policy types. • A PowerProtect Data Manager policy requires two MTrees for configuration. • If the Sheltered Harbor feature is not enabled, the drop-down list does not include **Sheltered Harbor**.
Storage	Select the vault storage containing the replication context that the policy will protect. **NOTE:** You cannot edit the vault storage 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 (...).

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

Table 6. Replication page

Field	Description
Replication Contexts	a. Under **Context**, select the MTree replication context to protect and the interface on the storage instance that is configured for replication. b. Under **Ethernet Port**, click **Select Repl Ethernet** and then select the interface on the storage instance that is configured for replication. **NOTE:** • There can be only one policy per replication context, except for PowerProtect Data Manager policy types, which require a minimum of two replication contexts to create a PowerProtect Data Manager policy. • Do not select the data or management Ethernet interfaces.
ServerDR Context	For a PowerProtect Data Manager deployment, select a ServerDR context from the list of replication contexts.
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. **NOTE:** If a job exceeds the time configured for the replication window, an alert is generated.
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.

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

Table 7. Retention page

Field	Description
Retention Lock Mode	Select one of the following: • (**Add Policy** dialog box only) **None**, if retention locking is not supported. The retention fields are then removed from the dialog box. **NOTE:** A Sheltered Harbor policy cannot have a retention lock type of **None**. • **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 (for existing policies only)	**NOTE:** This feature has been deprecated and will be removed in a future release. When you create a new policy or if the auto retention lock feature is disabled for an existing policy, the checkbox is not available. When editing existing policies that have the auto retention lock feature enabled, the checkbox is displayed. You cannot use the checkbox to disable the auto retention lock feature.
Min Retention Lock Period	(Only for Governance or Compliance mode) Specify the minimum retention duration that this policy can apply to PIT copies. This value cannot be less than 12 hours.
Max Retention Lock Period	(Only for Governance or Compliance mode) Specify the maximum retention duration that this policy can apply to PIT copies. This value cannot be greater than 1,827 days.
Duration	Specify the default retention duration that this policy applies to PIT copies. The value can be the retention lock minimum up to the retention lock maximum.

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.

7. 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.

8. 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 pages to change the information.

   By default, the **Policies** table lists the policies.
9. Click **Launch** to go to the dashboard.
   The **What's New in Cyber Recovery** pane is displayed. When you click **Close**, the Cyber Recovery dashboard is displayed.
10. To recall the wizard at any time after the initial setup, click **Getting Started** under the icon on the masthead navigation.

    The wizard steps that you completed display the icon. The Checklist option includes the **View** link and the Vault Storage and Policies options include the **Add** link. Uncompleted steps display a **Configure** link. You can click the links to either complete or edit the configuration.
11. 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.

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 based on your user role.

NOTE: Your assigned user role determines the displayed options and the functions that you can perform in the Cyber Recovery UI. For more information, see User roles. Because the dashboard user can only view the Cyber Recovery dashboard and not perform tasks, the options that are displayed are limited.

Depending on your user role, 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
  - Generating and scheduling reports
  - Viewing alerts, events, and jobs
- Dashboard tiles that provide alert notifications that facilitate troubleshooting and error correction, Cyber Recovery vault status, and a cumulative job type report

The following figure shows the dashboard for an admin user in the Cyber Recovery UI:

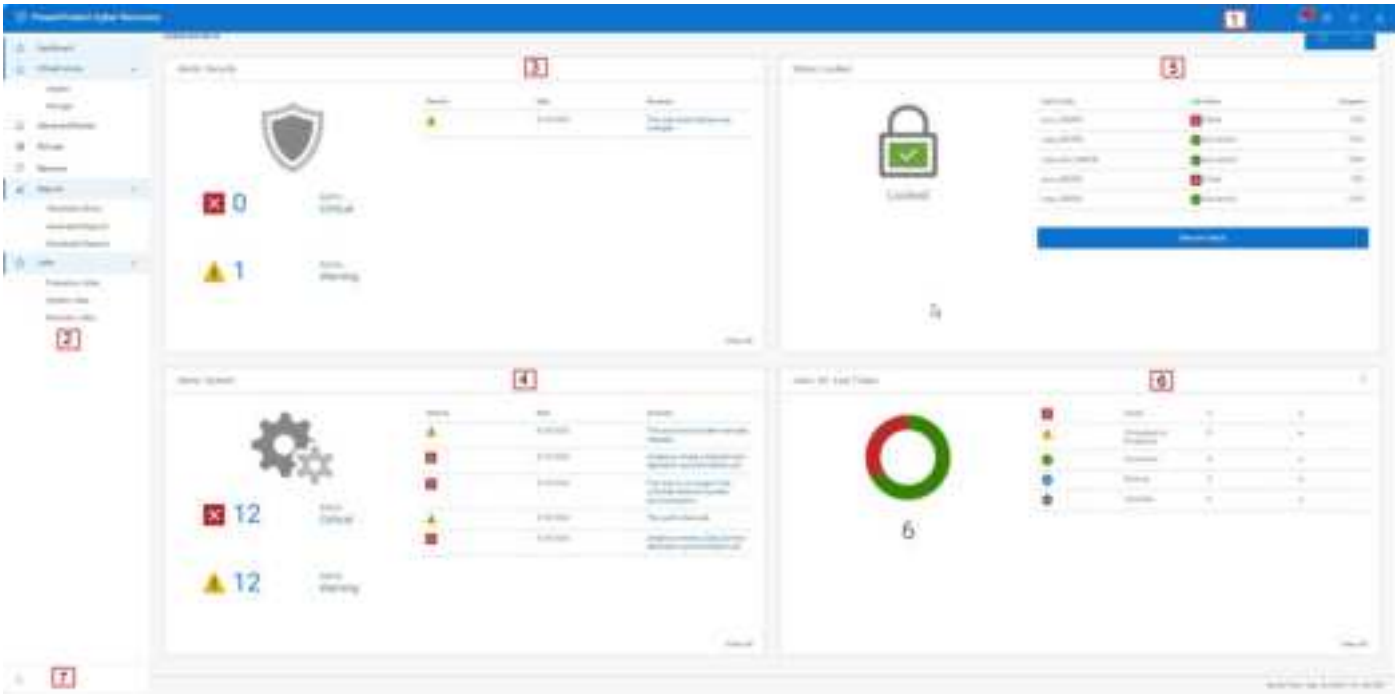


Figure 3. PowerProtect Cyber Recovery dashboard

NOTE: The dashboard for security officers and dashboard users differs.

1. The masthead navigation provides icons that enable you to view notifications and additional information, set system and user settings, and access the Getting Started wizard and online help. The only option for a dashboard user is to log out of the Cyber Recovery UI.
2. The Main Menu provides access to content panes from which you can perform tasks and operations depending on your user role. 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 about a specific alert, click its summary. To see all unacknowledged and older alerts, click **View All** to be redirected to the **Alerts and Events** content pane. The **View All** link is not displayed for dashboard users.

   NOTE: When the alert count reaches 1000 alerts, the UI displays the value as 1 K. When there are more than 1000 alerts, the UI displays the value as 1 K+ until the count reaches 2000 alerts. The UI displays the value as 2 K and then 2 K+ when there are more than 2000 alerts. For every 1000 alerts, the count increments accordingly. To see the exact number of alerts, hover over the count value so that the UI displays a tooltip with the number.

4. The **Alerts|System** tile provides details about unacknowledged system alerts. For more detailed information about a specific alert, click its summary. To see all unacknowledged and older alerts, click **View All** to be redirected to the **Alerts and Events** content pane. The **View All** link is not displayed for dashboard users.

   NOTE: When the alert count reaches 1000 alerts, the UI displays the value as 1 K. When there are more than 1000 alerts, the UI displays the value as 1 K+ until the count reaches 2000 alerts. The UI displays the value as 2 K and then 2 K+ when there are more than 2000 alerts. For every 1000 alerts, the count increments accordingly. To see the exact number of alerts, hover over the count value so that the UI displays a tooltip with the number.

5. The **Status** tile shows the current state of the Cyber Recovery vault. It enables operator, admin, and security officer users to secure the Cyber Recovery vault manually if a network event occurs when it is open and stop all replication operations. A timer indicates the length of time that the Cyber Recovery vault is secured. Only a security officer can release the vault when it is secured.

   The tile also displays the five most recent jobs and their progress. For information about monitoring and manually securing the Cyber Recovery vault, see the Monitoring the Cyber Recovery vault status and Manually securing and releasing the Cyber Recovery vault topics.

   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. If you are logged in as the admin or operator user, 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 security officers and dashboard users.

7. The  and  icons enable you to contract or expand the Main Menu.

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

Masthead navigation

The Cyber Recovery UI includes masthead navigation.

The icons on the Cyber Recovery UI masthead provide information or enable you to perform administrative tasks, depending on your user role.

Figure 4. Masthead navigation icons

NOTE: A dashboard user only has access to the  icon, which provides the option to log out of the Cyber Recovery UI.

Click a masthead navigation icon to open a pop-up window to:

1. View unacknowledged critical and warning alerts. A red numbered callout indicates the number of unacknowledged critical alerts. If there are no critical alerts, a yellow numbered callout indicates the number of unacknowledged warning alerts.

NOTE: When the alert count reaches 1000 alerts, the UI displays the value as 1 K. When there are more than 1000 alerts, the UI displays the value as 1 K+ until the count reaches 2000 alerts. The UI displays the value as 2 K and then 2 K+ when there are more than 2000 alerts. For every 1000 alerts, the count increments accordingly. To see the exact number of alerts, hover over the count value.

By default, the window displays the last 21 unacknowledged warning and critical alerts. If there are no critical alerts, the window displays the last 21 unacknowledged warning alerts.

- Use the scrollbar to view all 21 alerts.
- Click the **Critical** tab to filter by critical alerts or click the **Warning** tab to filter by warning alerts.
- Click a summary statement for an alert to open the **Alerts and Events** content pane to display the specific alert.
- Click **View All Unacknowledged Alerts** to open the **Alerts and Events** content pane to display all unacknowledged alerts.

NOTE: After you acknowledge a critical alert, the red numbered callout on the masthead navigation changes to indicate the remaining number of unacknowledged critical alerts. When you acknowledge all critical alerts, the masthead navigation shows a yellow numbered callout that indicates the number of unacknowledged warning alerts. The information in the window changes whenever you acknowledge critical and warning alerts. If there are no unacknowledged alerts, no numbered callout is displayed.

2. Access options to:
   - (Security officer and admin users only) Recall the Getting Started wizard options, based on your user access.
   - (Admin users only) Configure clean-up schedules or start an on-demand cleaning operation.
   - (Admin users only) Configure and manage disaster recovery backups.
   - (Security officer users only) Enable email server support.
   - (Security officer users only) Add and modify Transport Layer Security (TLS) certificates.
   - (Security officer users only) Enable telemetry reports.
   - Generate, view, download, and delete support bundles.
   - (Security officer users only) Manage the number of simultaneous login sessions.
   - (Security officer and admin users only) Enable license activation.
3. Access options to view:
   - The Cyber Recovery online help
   - The Cyber Recovery version, Software Instance ID, and Software Serial ID
   - The **What's New in Cyber Recovery** window, which lists new Cyber Recovery features
4. View and manage user settings that enable you to:
   - (Admin and operator users only) Display your user details such as profile, user access, and login details, and test your email.
   - Set up multifactor authentication to provide added protection.
   - Change your password.

     NOTE: An admin user cannot reset the password more than once every 24 hours.

   - Log out.

Activating the Cyber Recovery license

Upload the Cyber Recovery license file to activate the license.

Prerequisites

- You are logged in as the security officer or admin user.
- You have acquired the Cyber Recovery license file:

1. From the masthead navigation, click  and then **Software Info** to obtain the Software Instance ID, which is required to acquire the license file from Dell Technologies.

   NOTE: You can request a nonsubscription or a subscription license.

2. 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  to access the **System Settings** list.
2. Click **License**.

   The **License** dialog box provides the following information:
   - **Expires On**—Indicates 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
   - **Software Serial ID**—Provides the software serial number, which comes from the license

   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), Microsoft Azure, or Google Cloud Platform
   - **IDPA - Active**—Indicates that Integration Data Protection Appliance is enabled
   - **Sheltered Harbor**—Indicates that the Sheltered Harbor feature 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, a 30-day alert, a 14-day alert, and then a daily alert for seven days 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

- You are logged in as the security officer, operator, or admin user.
- 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. A security officer cannot enable multifactor authentication for other users, but can disable it for all users except the crso.

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 a security officer to disable multifactor authentication for your account, and then enable multifactor authentication again when you can log in.
- As the crso, if you enable multifactor authentication and then are unable to provide the security code, use the `crsetup.sh` command to change the 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, click  to open the drop-down list.
3. Click **Multifactor 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 and a user whose multifactor authentication is disabled receive an email message that indicates that multifactor authentication is disabled.

Enabling the Sheltered Harbor feature

Enable the Sheltered Harbor feature to be able to protect financial data by using the Sheltered Harbor Turnkey Data Vaulting Solution specification.

Prerequisites

- Your production environment must be configured to meet Sheltered Harbor requirements.
- Ensure that there are no jobs running.

About this task

If the Sheltered Harbor feature is not enabled, you cannot access Sheltered Harbor options.

Steps

1. Ensure that you have the lockbox passphrase, which is required for the next step.
2. From the CRCLI, run the following command and provide the lockbox passphrase at the prompt:

```
crsetup.sh --shenable
```

   The command stops the Cyber Recovery container services, enables the Sheltered Harbor services, and then starts the Cyber Recovery container services.

Results

After the Sheltered Harbor feature has been enabled, you can access Sheltered Harbor options in the Cyber Recovery UI and the CRCLI to add a Sheltered Harbor license and use the Sheltered Harbor feature.

3

Configuring and Managing Storage and Applications

This section describes how to manage vault storage and applications in the Cyber Recovery UI. Only the admin user can perform these tasks.

Topics:

Infrastructure overview

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

NOTE: Power on all vault storage, application, and vCenter assets before you add them to your Cyber Recovery deployment.

Vault storage objects

Vault storage objects represent DD systems. Define vault storage 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 the Avamar, NetWorker, PowerProtect Data Manager, or CyberSense applications.

NOTE: The CyberSense application 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 the 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 application, which analyzes backup data for the presence of malware or other anomalies. After you install the CyberSense application on a separate host in the Cyber Recovery vault, in the Cyber Recovery UI, add CyberSense as an application object. Then, Cyber Recovery policies can call the CyberSense to analyze PIT copies of supported datasets.

vCenter server objects

For an on-premises deployment, if you plan to use PowerProtect Data Manager to perform a recovery in the Cyber Recovery vault, add a vCenter server asset. Otherwise, you cannot add a PowerProtect Data Manager application to the Cyber Recovery deployment to be used to perform a recovery.

For Cyber Recovery deployments on Amazon Web Services (AWS), a vCenter server asset is not required for a PowerProtect Data Manager recovery.

Sheltered Harbor objects

If you are a Sheltered Harbor participant, secure your data and comply with the Sheltered Harbor Turnkey Data Vaulting Solution specification by adding a Sheltered Harbor license and detailed information for each financial institution.

Managing storage

In the Cyber Recovery UI, add each DD system that is running in the Cyber Recovery vault environment as vault storage. 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.

Prerequisites

- The DD system is running DDOS version 7.10, 7.13, or 8.x.
- The force-minimum-root-squash default option is set to disabled. Type the `nfs option show` command to verify the status of the option:

```
sysadmin@xxxxxxxx# nfs option show all
Option                                  Value
--------------------------------        --------------
default-export-version                  3:4
default-server-version                  3:4
nfs4-grace-period                       30
nfs4-lease-interval                     300
mountd-port                             2052
nfs4-port                               2049
nfs3-port                               2049
nfs4-domain                             xxxxx.com
nfs4-idmap-out-numeric                  always
nfs4-idmap-active-directory             disabled
nfs4-acls                               disabled
default-root-squash                     enabled
force-minimum-root-squash-default       disabled
report-mtree-quota                      disabled
--------------------------------        --------------
```

  For more information, see Knowledge Base Article 198370.

  NOTE: Access to this document depends on your login credentials. If you do not have access to the document, contact your Dell Technologies representative.

- You are logged in as the admin user.

  NOTE: An operator can only view and export information about the vault storage.

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:

- Do not configure multiple Cyber Recovery servers to use the same DD system.
- 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 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** > **Storage**.
2. Click **Systems** at the top of the **Storage** content pane.
3. Do one of the following:
   - To add vault storage, click **Add**.
   - To modify an existing object, select a DD system and click **Edit**.
4. Complete the following fields in the dialog box:

Table 8. Vault storage fields

Field	Description
Nickname	Enter a name for the vault storage.
FQDN or IP Address	Specify the DD host by using one of the following: • Fully qualified domain name (FQDN) • IP address **NOTE:** If you modify an existing FQDN or IP address, you must reenter all passwords.
Storage Username	Specify a dedicated Cyber Recovery DD administration account (for example, `cradmin`), which the Cyber Recovery software uses to perform operations with the DD system. This DD account must have the admin role. **NOTE:** If you modify the existing username, you must reenter the password.
Storage Password	Enter the password of the DD administrator.
SSH Port Number	Enter a storage SSH port number.
Reset Host Fingerprint (when editing vault storage 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 vault storage. 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**.
   By default, the **Systems** table lists the vault storage.
6. To view more detailed information that is retrieved from the DD system, such as the replication contexts and the Ethernet interface, click the vault storage row.
   The details window opens.
   a. Click the **Launch DD System Manager** to access the DD system.
   b. Click  to close the details pane.
   c. Click  to open the details pane again.
7. To customize the columns in the table that lists the DD systems, click  and select the columns to show or hide.
8. To remove vault storage, select a DD system and click **Delete**.
9. To capture information about all the vault storage in a `.csv` file, click **Export**.

   NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

   The Cyber Recovery software downloads the `systems.csv` file.

10. For information about storage capacity and MTree details for the vault storage, click **Capacity** and see Monitoring storage capacity.

Managing applications

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

Prerequisites

- You are logged in as the admin user.

  NOTE: An operator user can only view and export information about an application.

- The Avamar, NetWorker, PowerProtect Data Manager, or CyberSense applications must be installed and running at the Cyber Recovery vault location before you can define them in the Cyber Recovery UI.
- Modify and save the `/etc/ssh/sshd_config` file on the operating system of the following specified applications:
  1. For NetWorker 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 NetWorker Virtual Edition (NVE) running in the cloud, add the pound sign (#) to the beginning of the second through fourth lines, as shown in the following example:

     ```
     ## disable root login if not access from self
     # Match User root Address *,!::1,!127.0.0.1,!10.13.144.188
     # ForceCommand echo'Please login as the user admin rather than the user root.';sleep 5
     # Match all
     ## Permit local root login
     Match Address
     ::1,127.0.0.1,127.0.0.1,127.0.0.2,::1,10.13.144.188,fe80::ee:beff:fe36:cde8,<IP
     Address of workstation>
     PermitRootLogin yes
     Match all
     LogLevel INFO
     PermitRootLogin no
     ```

  3. For PowerProtect Data Manager and Avamar deployments, enable password authentication:
     - Change the `PasswordAuthentication` field value from **no** to **yes**.
  4. Run the `service sshd restart` command.
- If you plan to use CyberSense Version 8.3 or later, assign a DD Boost user to the PowerProtect DD system in the Cyber Recovery vault:
  1. Create a dedicated DD Boost user on the Cyber Recovery vault PowerProtect DD system with the same role as the backup user on the production PowerProtect DD system:

     ```
     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 Manger user, the role value is `none`. For a NetWorker or Avamar user, the role value is `admin`.

  2. Assign the DD Boost user:

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

About this task

NOTE: When adding applications:

- 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.

- The Avamar and PowerProtect Data Manager applications can be added as the admin user in the Cyber Recovery vault.
- The CyberSense application can be added as an admin user in the Cyber Recovery vault.

Steps

1. From the Main Menu, click **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**.

     The Add Vault Application wizard is displayed.
   - To modify an existing application, select the application and click **Edit**.

     The **Summary** page of the Edit Vault Application wizard is displayed. Click **Back** to go to the wizard page that you want to modify.
4. On the **Application Information** page, complete the following fields and click **Next**:

Table 9. Application Information page

Field	Description
Nickname	Enter a name for the application object.
FQDN or IP Address	Specify the application host by using one of the following: ● Fully qualified domain name (FQDN) ● IP address **NOTE:** ● If you modify an existing FQDN or IP address, you must enter the password for the updated asset. ● The hostname and IP address of the PowerProtect Data Manager server in the Cyber Recovery vault do not have to match the hostname and IP address of the production PowerProtect Data Manager server. The Cyber Recovery software validates that the IP is a PowerProtect Data Manager server and checks that the default credentials are set. Do not change the default password, or an error message is displayed.
Application Type (when adding an application only)	Select an application type: ● To represent an application in Cyber Recovery, select one of the following: ○ **CyberSense** for analysis capabilities ○ **Avamar** ○ **NetWorker** and complete the following additional fields: ■ 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: ■ In the **Application Username** field, enter the username of the application user. ■ In the **Application Password** field, enter the password of the application user. ■ (For on-premises deployments only) In the **vCenter Name** field, select a vCenter server ○ **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.

Table 9. Application Information page (continued)

Field	Description
	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 the Cyber Recovery solution deployed on Amazon Web Services (AWS) only)	Enter the AWS tag of the security group that controls access to and from the Cyber Recovery and PowerProtect Data Manager hosts. For more information, see the Dell PowerProtect Cyber Recovery AWS Deployment Guide.
Resource Group (For the Cyber Recovery solution deployed on Microsoft Azure only)	Enter the name of the resource group in which the PowerProtect Data Manager application is deployed. For more information, see the Dell PowerProtect Cyber Recovery Azure Deployment Guide.
Tags	• 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 (...).

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

Table 10. Host Authentication page

Field	Description
Host Username	Specify the operating system host administrator username, which is the username for the operating system host in the Cyber Recovery vault. **NOTE:** If you modify the host username, you must enter the password.
Host Password	Enter the password of the host administrator. **NOTE:** For a PowerProtect Data Manager deployment, the password does not have to match the production account password.
SSH Port Number	Enter an application 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.

NOTE: For more information about the PowerProtect Data Manager host username and password and their role in the PowerProtect Data Manager recovery process, see the PowerProtect Data Manager credentials topic.

6. For the NetWorker and PowerProtect Data Manager application types, on the **Application Authentication** page, complete the following fields and then click **Next**:

Table 11. Application Authentication page

Field	Description
Application Username	Enter the username of the application user. **NOTE:** • For PowerProtect Data Manager, the application username must match the application username on the production system.

Table 11. Application Authentication page (continued)

Field	Description
	• If you modify the application username, you must enter the password.
Application Password	Enter the password of the application user. **NOTE:** For PowerProtect Data Manager, the application password must match the application password on the production system.
vCenter Name (For the PowerProtect Data Manager application deployed on premises only)	Select a vCenter.

NOTE: For more information about the PowerProtect Data Manager application username and password and their role in the PowerProtect Data Manager recovery process, see PowerProtect Data Manager credentials.

7. Review the Application Summary page and either:
   - Click **Finish** if you are satisfied with the summary information and want to add the application.
   - Click **Back** to return to the previous pages to change the information.
8. If you added the CyberSense version 7.8 through 8.1 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. Otherwise, go to the next step.

   NOTE: For more information, see Configuring DD Boost user information for CyberSense.

```
# 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
```

9. Click the row of an application to open the details pane and view additional details about the application, and then:
   a. Click  to close the details pane.
   b. Click  to open the details pane again.
10. To customize the columns in the table that lists the applications, click  and select the columns to show or hide.
11. To remove an application, select the application and click **Delete**.

    You cannot delete the CyberSense application if:
    - Your deployment is running CyberSense version 8.2 or later, and multilink definitions are configured. You must delete the multilink definitions before you can delete the application.
    - It is associated with a scheduled report.
12. To capture information about all the applications in a `.csv` file, click **Export**.

    NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

    The Cyber Recovery software downloads the `apps.csv` file.

PowerProtect Data Manager credentials

A PowerProtect Data Manager recovery requires host authentication credentials and application authentication credentials.

When you add the PowerProtect Data Manager application into your Cyber Recovery deployment, the wizard in the Cyber Recovery UI prompts for two sets of users and passwords. These sets of credentials include the host username and password, and the application username and password.

NOTE: When the PowerProtect Data Manager server is deployed in the Cyber Recovery UI, it includes default credentials. The first step of the application wizard uses these default credentials to verify the FQDN or IP address as a valid PowerProtect Data Manager server and that the default credentials are set. Do not change the default credentials, otherwise, the wizard displays an error message and you cannot add the PowerProtect Data Manager application into your Cyber Recovery deployment.

Host username and host password

The host username is the operating system host administrator username for the admin account of the PowerProtect Data Manager server in the Cyber Recovery vault.

At the wizard prompt, specify the administrator username, which is typically **admin**, and a password.

NOTE: The password for the operating system host administrator username does not need to match the production account password. The password can be anything that you choose.

These credentials are used for the second phase of the recovery procedure to protect the restored data against potential attacks. After recovery, the admin and root accounts on the host server will use this password.

Application username and application password

The application username and the application password are the credentials that you use to log in to the PowerProtect Data Manager UI on the production system.

At the wizard prompt, you must specify an application username and an application password that matches the application username and the application password on the production system.

After the first phase of the recovery procedure, which performs the recovery of the PowerProtect Data Manager server, the Cyber Recovery software issues API commands. The application username and the application password are required to run the API commands.

NOTE: If the application password on the production system expires, change the application password in the Cyber Recovery vault. Otherwise, the recovery procedure fails.

Managing vCenter servers

When you install a vCenter server in an on-premises Cyber Recovery vault, you must present it to the Cyber Recovery software.

Prerequisites

You are logged in as the admin user.

NOTE: An operator user can only view export information about a vCenter server.

About this task

A vCenter server is not required for a Cyber Recovery deployment on Amazon Web Services (AWS).

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 12. 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: • Fully qualified domain name (FQDN) • IP address **NOTE:** If you modify an existing FQDN or IP address, you must reenter all passwords.
Username	Enter the username of the user logging into the vCenter server. **NOTE:** If you modify the username, you must reenter the password.
Password	Enter the password of the user logging into the vCenter server.
Tags	• 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**. **NOTE:** If a tag exceeds 24 characters, the details description displays the first 21 characters followed by an ellipsis ().

5. Click **Save**.
   The **vCenters** table lists the application.
6. Click a vCenter's row to open the details pane and view additional details about the vCenter, and then:
   a. Click  to close the details pane.
   b. Click  to open the details pane again.
7. To customize the columns in the table that lists the vCenters, click  and select the columns to show or hide.
8. To remove a vCenter, select the asset and click **Delete**.
9. To capture information about all the vCenter servers in a `.csv` file, click **Export**.

   NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

   The Cyber Recovery software downloads the `vcenter.csv` file.

Managing Sheltered Harbor financial institutions

Define a financial institution, which is required to create and run a Sheltered Harbor policy action. It is also required if you plan to change a non-Sheltered Harbor policy to a Sheltered Harbor policy. The non-Sheltered Harbor policy must not have any copies.

Prerequisites

- You are logged in as the admin user.

  NOTE: An operator user can only view and export information about a financial institution.

- The Sheltered Harbor feature must be enabled, otherwise you do not have access to the Sheltered Harbor options in the Cyber Recovery UI or CRCLI.
- A Sheltered Harbor license is required for each financial institution that you plan to add as an infrastructure object. Request a license file from Sheltered Harbor.

About this task

Financial institution information defines a depository or brokerage institution that is a Sheltered Harbor participant. The financial institution's data is protected in the Cyber Recovery vault. If the financial institution has multiple legal entities, such as deposit and brokerage accounts, create a separate institution object for each entity and a separate MTree for each MTree in the production system.

Steps

1. From the Main Menu, select **Infrastructure** > **Sheltered Harbor**.
   The **Sheltered Harbor** pane is displayed.
2. Do one of the following:
   a. To add a financial institution, click **Add Financial Institution**.
      The **Add Financial Institution** page is displayed.
   b. To modify an existing financial institution, select the financial institution and click **Edit Financial Institution**.
      The **Edit Financial Institution** page shows the current license details.
3. Under License Details, do either of the following:
   - To add a new financial institution, click **Choose File** and select the JSON license file to add the Sheltered Harbor license. Go to step 4.
   - To update the license for an existing financial institution, click **Choose File** and select the JSON license file to update the Sheltered Harbor license. Go to step 5.

   NOTE: For an existing financial institution, the existing fields typically do not need to be modified. However, if you must modify a field, click **Show Advanced Settings** to access the institution details fields and go to step 4.

   After you select a license file, the software verifies the license and displays an informational message that indicates success. If the license is not valid, the software displays an error message.
4. Complete the following fields in the dialog box:

Table 13. Financial institution fields

Field	Description
Institution ID Type	Select the identifier for the financial institution from the drop-down list: • 1-Bank • 2-Credit Union • 3-Broker
Registration ID	Enter the registration ID that the Sheltered Harbor Monitoring Log provides as a part of the registration process.
Key-encrypting Key – Public	Enter the location of the public encryption key, which is a `.pem` file, which is used to encrypt the archive encryption key.
Key-encrypting Key – Private	(Optional) Enter the location of the private encryption key, which is a `.pem` file, which is used to decrypt the archive encryption key during the data recovery test.
Envelope Signing Key – Private	Enter the location of the private signing key, which is a `.pem` file, which is used to digitally sign the secure envelope.
Envelope Signing Key – Public	(Optional) Enter the location of the public signing key, which is a `.pem` file, which is used to validate the secure envelope signature during the data recovery test.
Primary Email Address	Enter the primary email address to receive a report when a Sheltered Harbor policy is completed.
Secondary Email Address	Optionally, enter a secondary email address to receive a report when a Sheltered Harbor policy is completed.

5. Click **Save**.

The **Financial Institution** table lists the financial institution object.

6. To remove a financial institution, select the financial institution and then click **Delete**.

   NOTE: You cannot delete a financial institution if it has an associated Sheltered Harbor policy.

7. To capture information about all the financial institutions in a `.csv` file, click **Export**.

   NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

   The Cyber Recovery software downloads the `financialInstitutions.csv` file.

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

You are logged in as the admin user.

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 **Infrastructure** > **Assets** from the Main Menu and click **Applications** at the top of the **Assets** content pane.
   - Select **Infrastructure** > **Vault Storage** from the Main Menu, and click **Systems** at the top of the **Vault Storage** content pane.
2. Select an existing application or storage asset, and click **Edit**.
3. Perform the applicable step:
   - In the Host Authentication page of the Edit Vault Application wizard, change the address in the FQDN or IP address field.
   - In the Edit Vault Storage dialog box, change the address in the FQDN or IP address field.
4. Check the **Reset Host Fingerprint** checkbox.
5. Click **Save**.

4

Configuring and Managing Multiple Network Links for CyberSense

This section describes how to configure and manage multiple network links for the CyberSense version 8.2 or later application using the multilink feature. Only the admin user can perform these tasks.

Topics:

Multilink overview

The multilink feature enables you to define one or more links between a CyberSense version 8.2 or later host and one or more DD systems. A link is a network connection between a CyberSense network interface and a DD network interface.

NOTE:

- Multiple links are not supported with pre-8.2 CyberSense versions.
- Multilink configurations with CyberSense 8.2 require that CyberSense and the DD system are on the same subnet. If CyberSense and the DD system are on different subnets, multilink configurations do not work.
- Multilink configurations with CyberSense 8.3 and greater require either that:
  - CyberSense and the DD system are on the same subnet.
  - Cross-network routing is in place and that there is a workaround in place on the CyberSense server to prevent the insertion of point-to-point routing. Contact Cyber Recovery Support for the workaround.

If network bottlenecks occur, the multilink feature provides increased performance for CyberSense analyses. It enables you to take advantage of the throughput that Ethernet interfaces on the CyberSense host and the DD systems provide. CyberSense Analyze operations read data from the DD system using both the NFS and DD Boost protocols. A multilink configuration improves performance for both NFS and DD Boost read operations by load-balancing traffic across all available links.

During analysis of the data for a specific Cyber Recovery policy, one of the links in the multilink definition is chosen for the NFS mount. All NFS reads for that policy use the same link. DD Boost reads for analyzing that same policy load balance across all the links in the multilink definition. The CyberSense software assigns NFS mount links to policy analyze operations in a round-robin fashion.

You can configure multiple links between a CyberSense host and a DD system using direct connections, or through a switch. It is assumed that the physical networking and routing are in place between those interfaces.

After you create a multilink configuration, you must assign at least one DD Boost user on the CyberSense server to this multilink configuration. One user is required even if you are not using Delta Block Analysis on CyberSense to allow connectivity testing of the links. If you are using Delta Block Analysis and have different DD Boost users, you can add more users to the same multilink configuration.

After you create a multilink definition, the link and connectivity statuses are displayed as **Inactive**. Therefore, you must add a DD Boost user on the CyberSense host so that the links become **Active**. If the link status of the multilink definition is **Inactive**, you cannot run an Analyze operation.

For a CyberSense version 8.2 deployment, the link status of the multilink definition must be **Active** to run an Analyze operation. If a schedule starts an Analyze operation and the associated multilink definition is not **Active**, an alert is generated. If you attempt to analyze a copy and the associated multilink definition is not **Active**, an error message is displayed.

For a CyberSense version 8.3 or later deployment, the link status of the multilink definition can be **Active** or **Degraded** to run an Analyze operation. However, the analysis performance might not be optimal if the multilink definition is in the **Degraded** state.

If the multilink definition status changes during an Analyze job, the job might complete with a status of **Warning w/ Exception** and an analysis status of **Partial**.

The status can become **Inactive** or **Degraded** if:

- A DD or CyberSense interface is disabled.
- Cabling and switches between the interfaces are not working correctly.
- A DD Boost user is not configured on the CyberSense host.
- There is a hardware issue.

When the status becomes **Inactive** or **Degraded**, an alert is generated. The **Details** pane in the **Alerts and Events** pane provides detailed information and remedies.

Recommended workflows for the multilink feature

The workflows that are described in the following sections explain how to install or update the Index Engines CyberSense software along with the Cyber Recovery software properly.

Initial installation workflow

NOTE: You must install the software to the following required minimum versions:

- CyberSense 8.4
- Cyber Recovery 19.13

For the first installation of the Index Engines CyberSense and Cyber Recovery software, see the following workflow:

1. Install the Index Engines CyberSense software using the procedures described in the Index Engines CyberSense Initial Setup and Configuration Guide.
2. Install the Cyber Recovery software, using the procedures described in the Dell PowerProtect Cyber Recovery Installation Guide. Then, configure your Cyber Recovery deployment and create:
   - Policies
   - Copies for analysis
   - Multilink definitions
3. On the Index Engines CyberSense engine, assign DD Boost users to multilink definitions that are described in the Configuring DD Boost users section of the Index Engines CyberSense Initial Setup and Configuration Guide.

Update workflows

When you are updating the Index Engines CyberSense and Cyber Recovery software, you must update to at least the following required minimum versions:

- CyberSense 8.4
- Cyber Recovery 19.13

Two common scenarios for updating the Cyber Recovery software and CyberSense software include:

- Updating both the Cyber Recovery software and the CyberSense software
- Updating the Cyber Recovery software and installing the CyberSense software

Updating from earlier versions

If the CyberSense and Cyber Recovery software are installed in your deployment, do the following:

1. On the Index Engines engine, add DD Boost users by using the Index Engines ddboostcfg tool.
2. Update the CyberSense software to at least version 8.4. See the *Upgrading the Index Engines software section of the Index Engines CyberSense Initial Setup and Configuration Guide*.

   NOTE: If you have not added DD Boost users, the update fails.

3. Update the Cyber Recovery software to at least version 19.13. See the *Dell PowerProtect Cyber Recovery Installation Guide*.

NOTE: After the Cyber Recovery update, if Analyze schedules exist, the software automatically creates multilink definitions. It also imports the DD Boost users that were added in step 1, allowing the multilink definitions to be active.

Updating Cyber Recovery and installing CyberSense

If you are updating the Cyber Recovery software to version 19.13 or higher and installing CyberSense version 8.4 or higher, follow the procedure under the Initial Installation workflow section, updating the Cyber Recovery software in step 2 of the procedure.

About software updates and the multilink feature

If your update of the Cyber Recovery and CyberSense software results in Cyber Recovery version 19.13 or later and CyberSense version 8.2 or later, the software creates default multilink definitions.

Create DD Boost users before the update to ensure that the default links are in the **Active** state. Analyze schedules on existing Cyber Recovery deployments can then continue to run as they did before the update.

NOTE:

- Previous combinations of Cyber Recovery and CyberSense versions enabled you to create alternate storage interfaces for on-demand and scheduled Analyze operations. If the Cyber Recovery software detects alternate storage interfaces, it creates default multilink definitions that map to these alternate storage interfaces.
- Multilink configurations for Cyber Recovery version 19.13 and later with CyberSense version 8.2 and later require that CyberSense and the DD are on the same subnet. If CyberSense and the DD system are on different subnets, the multilink configurations do not work. If you cannot change the network configuration to use the same subnet, avoid updating to the combination of Cyber Recovery version 19.13 and later with CyberSense version 8.2 and later or contact Cyber Recovery Support for a workaround.
- Multilink configurations with CyberSense 8.3 and later require either that CyberSense and the DD are on the same subnet or that cross network routing is in place and there is a workaround in place on the CyberSense server to prevent the insertion of point-to-point routing. Contact Cyber Recovery Support for the workaround.
- If CyberSense is updated after the Cyber Recovery update, the multilink auto configurations occur as soon the Cyber Recovery software detects CyberSense version 8.2 or later.
- If you do not perform the preupdate steps to create at least one DD Boost user, then you must assign a DD Boost user to the default multilink configuration before the link becomes **Active**.

Configuring DD Boost user information for CyberSense

If you add the CyberSense application to your deployment, configure the user information on the CyberSense host.

About this task

You must configure the DD Boost user on the CyberSense host to ensure:

- The use of the DD Boost user with an appropriate role while reading the sandbox during the analysis process.
- The ability to perform a connectivity test on a multilink object for CyberSense version 8.2 or later running on Cyber Recovery version 19.13 or later. If this DD Boost user is not configured, the multilink object is in the **Inactive** state and Analyze operations fail.

For the multilink feature:

- On the CyberSense server, at least one DD Boost user must be configured for the DD that is associated with the multilink configuration.
- You can associate additional DD Boost users for the same multilink configuration.

Steps

1. From Cyber Recovery, identify the **storageID** for the DD system that is associated with the multilink configuration by performing one of the following steps:
   - Find the **Storage ID** field in the UI details panel by going to **Assets-** > **Vault Storage** > **DD**.
   - Find the **Data Domain ID** field in the `crcli dd list` output.
2. Use SSH to access the CyberSense host.
3. Perform the following steps:
   a. List existing storage IDs previously configured on the CyberSense host by running the `ddcfg GET` command. The following example shows the output for a deployment running CyberSense version 8.3:

```
[root@sys123 ~]# ddcfg GET

# +++ S/N AUDVEN8KK3DGBR active +++
storageid: 63d94ae3f1ce505e645d1e5e
ens161,10.1.1.1,10000=ethV0,10.1.1.11,10000
ens192,10.1.1.2,10000=ethV1,10.1.1.12,10000
ens224,10.1.1.3,10000=ehtV2,10.1.1.13,10000
ddboost-ppdm-user
ddboost-user
```

   NOTE: For a deployment running CyberSense version 8.2, the command provides output in JSON format.

   b. Add one or more DD Boost users by running either of the following commands. The second command prompts you for passwords.

   NOTE:
   - Prohibited characters in the DD Boost user password cause the multilink configuration to fail. Ensure that DD Boost user passwords do not include the following characters: `{`, `}`, `[`, `]`, `'`, `"`, or `=`.
   - When adding another user, you must specify the entire set of users including any existing users. Otherwise, the existing users are removed.

   - ```
     ddcfg PATCH <storage ID|Data Domain ID> existinguser1,pwd1 existinguser2,pwd2
     newuser,pwd3
     ```
   - ```
     ddcfg PATCH <storage ID|Data Domain ID> existinguser1 existinguser2 newuser
     password for 'existinguser1':
     password for 'existinguser2':
     password for 'newuser':
     ```

   c. Restart the dispatcher:

```
dservice dispatch restart
```

4. If your deployment is running a version of CyberSense that is earlier than version 8.2, perform the following steps:
   a. Add one or more DD Boost users:

```
ddboostcfg add
```

   b. Enter the DD host IP address, username, and password:

```
Enter hostname, username, and password for each Data Domain host you
plan to connect to using DDBoost protocol.
Reply with Enter or Ctrl-D on the Host: prompt to finish
Host: <host name>
Username: <username>
Password: <password>
```

   NOTE: For multilink configuration, enter any of the available DD interfaces that you plan to use to define an interface link.

c. Restart the dispatcher:

```
dservice dispatch restart
```

Configuring multiple links

Configure multiple links between a DD system and a CyberSense host.

Prerequisites

- You are logged in as the admin user.
- You are knowledgeable about the physical layout of your network.
- CyberSense version 8.4 or later is added to your deployment.
- If your deployment consists of Cyber Recovery version 19.13 and later with CyberSense version 8.2 and later, CyberSense and the DD system are on the same subnet. Otherwise, the multilink configurations do not work. Contact Cyber Recovery Support for a workaround.

About this task

You cannot perform an Analyze operation on a copy using the multilink feature until you configure the multilink definitions. If you choose a copy and click **Analyze**, the **Application Host** drop-down list does not include the CyberSense host.

NOTE: If a configuration is in progress and you initiate a second configuration, an error message might be displayed. Because the configuration process is quick, this scenario is unlikely.

Steps

1. In the Cyber Recovery UI, from the Main Menu, select **Infrastructure** > **Assets**.
2. Click **Applications** at the top of the **Assets** content pane.
   The table includes any CyberSense applications that are added to your deployment.
3. Under the **Interface Links** column, click **Configure**.
   The **Interface Links** pane opens. The upper left provides information about the DD systems in your deployment; the upper right lists discovered CyberSense interfaces that are available.
4. Create a DD multilink object:
   a. On the upper left, select a DD system from the **PowerProtect DD** drop-down list.
      The available interfaces that are associated with the DD system are displayed in a table below the drop-down list.
      NOTE:
      - If policies have been created, the list does not include interfaces that are being used for replications in and out of the Cyber Recovery vault and physical interfaces that are part of a bonding. For a new Cyber Recovery deployment on which no policies have been created, the list includes replication ports.
      - A DDVE system or an appliance might not display the interface speed.
   b. Select an enabled DD interface.
      You cannot select a disabled interface.
   c. On the upper right, select a CyberSense interface.
   d. Click **Add Interface Link**.
      The lower table lists the DD multilink object and the associated links between the DD system and the CyberSense host.
      The **Link Status** and **Connectivity Status** columns show as **Pending Configuration** because the configuration has not been saved and is not active yet.
   e. Optionally, add another link between the DD system and the CyberSense host.
      NOTE: You can only create one link to a specific DD interface using any of the CyberSense interfaces. For example, from the CyberSense server to the DD system, you cannot configure `CyberSense interface 1` to `DD interface 1` and `CyberSense interface 2` to `DD interface 1`.
   f. Optionally, delete the DD multilink object or the links in it:
      - Click **Remove all** to remove the DD multilink object, including the links.

- Click  to remove the associated links only. The status is **Marked for Deletion** until you save the configuration.

g. When you are satisfied with the configuration or configurations, click **Save**.

The **Assets** page is displayed and the **Interface Links** column for the CyberSense application that you configured displays the **Edit/Configure** link. Also, a system job to create the link starts and is displayed in the **System Jobs** page.

NOTE: Because a DD Boost user must be configured on the CyberSense host, the link configurations are currently in the **Inactive** state.

5. On the CyberSense host, use the `ddcfg` tool to add a DD Boost user.

When a valid DD Boost user is added, the link configurations in the Cyber Recovery UI reflect the actual connectivity status (Active or Inactive).

6. On the CyberSense host, run the `ddboost info` command to determine if there are any user access issues with the DD Boost user that was added.
7. In the Cyber Recovery UI, go to **Assets** > **Applications**.
8. To edit the multilink configuration or view the status of the links, click **Edit/Configure**.

NOTE: If an analyze operation is running, you cannot modify a configuration. Plan to modify the configuration when an analyze operation is not running.

The **Interface Links** window opens again and displays the multilink definitions.

When you open the **Interface Links** page, the link statuses are updated. While working in the **Interface Links** page, the Cyber Recovery monitor takes approximately 5 minutes to update statuses. To update the statuses immediately, click **Refresh** in the blue bar at the top of the window.

The **Link Status** column displays:

- **Pending**—The DD multilink object is waiting to be configured.
- **Configuring**—The DD multilink object configuration is in progress.
- **Configured**—The DD multilink object configuration is completed.
- **Failed**—The multilink configuration cannot be completed successfully. A check box next to the status enables you to resubmit the DD multilink object for reconfiguration.

  NOTE: If the failure is due to multilink object definitions on the Cyber Recovery system and the CyberSense system being out of sync, an alert is generated. Click **Resubmit** to resync the systems.

- **Active**—All links in the DD multilink object are in the active state and can be used for an Analyze operation.
- **Inactive**—All links in the DD multilink object are in the inactive state and cannot be used for an Analyze operation.
- **Degraded**—Only a subset of the links in the DD multilink object is active and available. You can run an Analyze operation. An alert indicates that an error has been detected. However, the Analyze operation might take longer than expected.

The **Connectivity Status** column displays:

- **Active**—The link in the DD multilink object is configured and has connectivity.
- **Inactive**—The link in the DD multilink object is configured but does not have connectivity.
- **Unknown**—Either:
  - The DD multilink object is being configured, and the connectivity test has not run yet. You might see this status if you return to the **Interface Links** window after clicking **Save**.
  - The link could not be configured, or the configuration failed.

Troubleshooting multilink issues

The following suggestions might help troubleshoot multilink issues.

Review the Cyber Recovery service logs

Review the Cyber Recovery service logs for information about multilink issues. The Cyber Recovery apps service log file might display the following errors:

- `Code:999 Message:Conflict with existing bonds`—A bond already exists on the CyberSense server for the DD system and the CyberSense IP address in the multilink definition that you are trying to create. Remove the existing bond from the CyberSense server.
- `Code:999 Message:RTNETLINK answers: File exists`—An IP route already exists on the CyberSense server for the DD system IP address used in the multilink definition that you are trying to create. Remove the existing IP route.

Removing the CyberSense software or decommissioning the CyberSense server

You cannot delete CyberSense virtual machines before removing the associated multilink definitions and the CyberSense assets from the Cyber Recovery deployment. Ensure that you follow the order of these steps:

1. Delete the multilink definitions.
2. Delete the CyberSense assets configured in the Cyber Recovery deployment.
3. Delete the CyberSense virtual machines.

NOTE: If your CyberSense application is associated with any sandbox, you cannot delete the application.

5

Configuring and Managing Policies and Copies

This section describes how to create and run policies that perform replications, create point-in-time copies, and set retention locks. The admin user can perform these tasks, and the operator user can perform a limited number of tasks.

Topics:

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 MTrees. 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.

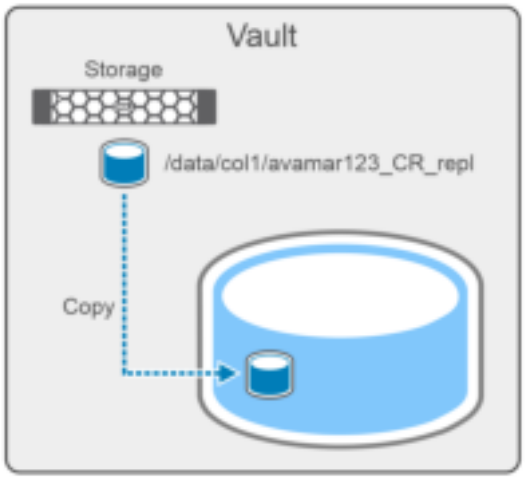
Policy actions

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

NOTE: If you have existing policies that use the deprecated 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.

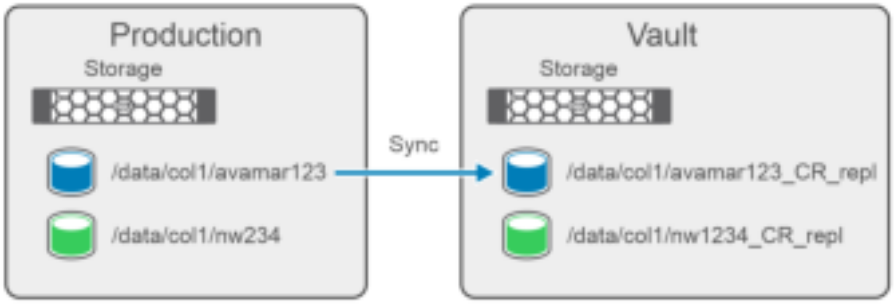


Copy Lock

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.



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.

Managing 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

- You are logged in as the admin user.

  NOTE: An operator user can only run policy actions manually, and view and export information about the policies.

- Ensure that vault storage 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.

About this task

You can create up to 50 policies for a maximum of 10 DD systems in the Cyber Recovery vault depending on the PowerProtect DD model and other factors, as well as on all supported platforms. For more information, contact your Dell representative.

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 **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 14. Policy Information page

Field	Description
Name	Specify a policy name.
Type	From the drop-down list, select either **PPDM**, **Sheltered Harbor**, or **Standard**. **NOTE:** • Standard denotes NetWorker, Avamar, Filesystem, and Other policy types. • A PowerProtect Data Manager policy requires two MTrees for configuration. • If the Sheltered Harbor feature is not enabled, the drop-down list does not include **Sheltered Harbor**.
Storage	Select the vault storage containing the replication context that the policy will protect. **NOTE:** You cannot edit the vault storage 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 15. Replication page

Field	Description
Replication Contexts	a. Under **Context**, select the MTree replication context to protect and the interface on the storage instance that is configured for replication. b. Under **Ethernet Port**, click **Select Repl Ethernet** and then select the interface on the storage instance that is configured for replication.

Table 15. Replication page (continued)

Field	Description
	NOTE: • There can be only one policy per replication context, except for PowerProtect Data Manager policy types, which require a minimum of two replication contexts to create a PowerProtect Data Manager policy. • Do not select the data or management Ethernet interfaces.
ServerDR Context	For a PowerProtect Data Manager deployment, select a ServerDR context from the list of replication contexts.
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. **NOTE:** If a job exceeds the time configured for the replication window, an alert is generated.
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 16. Retention page

Field	Description
Retention Lock Mode	Select one of the following: • (**Add Policy** dialog box only) **None**, if retention locking is not supported. The retention fields are then removed from the dialog box. **NOTE:** A Sheltered Harbor policy cannot have a retention lock type of **None**. • **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 (for existing policies only)	**NOTE:** This feature has been deprecated and will be removed in a future release. When you create a new policy or if the auto retention lock feature is disabled for an existing policy, the checkbox is not available. When editing existing policies that have the auto retention lock feature enabled, the checkbox is displayed. You cannot use the checkbox to disable the auto retention lock feature.
Min Retention Lock Period	(Only for Governance or Compliance mode) Specify the minimum retention duration that this policy can apply to PIT copies. This value cannot be less than 12 hours.
Max Retention Lock Period	(Only for Governance or Compliance mode) Specify the maximum retention duration that this policy can apply to PIT copies. This value cannot be greater than 1,827 days.

Table 16. Retention page (continued)

Field	Description
Duration	Specify the default retention duration that this policy applies to PIT copies. The value can be the retention lock minimum up to the retention lock maximum.

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 pages to change the information.

   By default, the **Policies** table lists the policies.
8. Click a policy's row to open the details pane and view additional details about a policy, and then:
   a. Click  to close the details pane.
   b. Click  to open the details pane again.
9. To customize the columns in the table that lists the policies, click  and select the columns to show or hide.
10. Disable or enable a policy:
    a. To disable a policy so that it does not run, swipe left on the slider under **Enabled**. An informational message confirms that the policy has been disabled and the **Edit** button is inactive. Also, an event is created.
    b. To sort policies by status, click **Enabled**.
    c. To filter on status, click and then click the **Enabled** or **Disabled** checkbox. Only the policies with the selected status are displayed. If you select both checkboxes, all policies are displayed.
    d. To reenable a policy, swipe right on the slider under **Enabled**. An informational message confirms that the policy has been reenabled and the **Edit** button is active. Also, an event is created.
11. To capture information about all the policy information in a `.csv` file, click **Export**.
    The Cyber Recovery software downloads the `policies.csv` file.

    NOTE: For existing policies with the automatic retention lock feature enabled, the `policies.csv` file includes the **Automatic Retention Lock** column. For newly created policies or existing policies with the auto retention lock feature disabled, the `policies.csv` file does not include the **Automatic Retention Lock** column.
12. To remove a policy, select an enabled or disabled policy and click **Delete**.

    NOTE:
    - You cannot delete a policy with associated copies or that is associated with a scheduled report.
    - If you delete a Retention Lock Compliance-enabled policy, the corresponding repository MTree is not deleted from the DD system. To delete the policy repository MTree, log in to the DD system and run the **`delete mtree <policy-repo-mtree>`** command, where **`<policy-repo-mtree>`** is **`cr-policy-<policy-id>-repo`**. For example:

      ```
      delete mtree cr-policy-665a11fa024d07d2108c48e5-repo.
      ```

      This command requires dual-authentication and prompts for DD security officer credentials to complete the command.
    - After you delete all policies with the automatic retention lock feature enabled, the exported `policies.csv` file no longer includes the **Automatic Retention Lock** column.

Managing Sheltered Harbor policies

Create a policy to copy a Sheltered Harbor participant's data into the CR Vault.

Prerequisites

The Sheltered Harbor feature must be enabled, otherwise you do not have access to the Sheltered Harbor options in the Cyber Recovery UI or CRCLI.

About this task

When you run a Sheltered Harbor policy, the Sheltered Harbor Copy action:

- Performs a replication
- Verifies the data

  NOTE: If the Business Date in the Sheltered Harbor manifest is later than the expiration date of the license for the financial institution, the Sheltered Harbor Copy action fails.

- Creates point-in-time (PIT) copy
- Archives and encrypts the data
- Generates a report with an email that contains an attestation for submission to Sheltered Harbor. The report is sent to the email address that is configured for the financial institution.

NOTE: If any step in the Sheltered Harbor Copy action fails, the email address that is configured for the financial institution receives an error report.

Managing Sheltered Harbor policies is similar to managing other policy types in the Cyber Recovery software. See Managing policies for detailed information about managing a policy.

Steps

1. Select **Policies** from the Main Menu.
2. In the **Policies** content pane, click **Add**.
3. Complete the fields in the **Add Policy** window.

   For detailed information about adding a policy, see Managing policies.

   NOTE: The **Retention Lock Type** for a Sheltered Harbor policy cannot be **None**.

4. Click **Actions** > **Sheltered Harbor Copy**.

   This action is the only one available for a Sheltered Harbor policy.

   The Cyber Recovery software creates a copy of the data that meets Sheltered Harbor standards.

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.

When you create a policy that uses a Retention Lock Compliance replication context, the Cyber Recovery UI and CRCLI prompt you for the DD 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 that is 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 Cyber Recovery vault 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 DD 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.

Prerequisites

You are logged in as the admin or operator user.

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 17. 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.
Copy Lock	Click **Copy Lock** and click **Apply** to create a point-in-time (PIT) copy and then retention lock it. 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. A timer indicates the length of time that the Cyber Recovery vault is unlocked. **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.
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**. **NOTE:** • The Secure Copy Analyze action is available only if the CyberSense application is installed in the Cyber Recovery deployment.

Table 17. Policy actions (continued)

Action	Description
	• If the deployment is using CyberSense version 8.3 or later and a multilink configuration is defined for the storage that is used by the policy to be analyzed, the drop-down list only lists the version 8.3 CyberSense host.
Sheltered Harbor Copy (only if the Sheltered Harbor feature is enabled)	Creates an encrypted retention locked copy according to the recommended Sheltered Harbor procedure. This action is the only available option for a Sheltered Harbor policy.

4. To view copies that are associated with a policy, click the number under **# Copies**.
   The number of copies that are associated with the selected policy is displayed in the **Copies** page.
   NOTE: You can view associated copies for enabled or disabled policies.

Results

The policy action 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.

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

Managing policy schedules

Schedule an action that you want the policy to perform.

Prerequisites

- You are logged in as the admin user.

  NOTE: An operator user can only view and export information about the policy schedules.

- Note that 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 Analyze or Recovery Check actions.

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 18. Schedule Information page

Field	Description
Schedule Name	Specify a schedule name.
Policy (when adding a policy only)	Select the policy that you are scheduling.

Table 18. Schedule Information page (continued)

Field	Description
Action	Select the action that the policy performs when it runs under this schedule. See Running Policies for a description of the actions. **NOTE:** If you select **Secure Copy Analyze** or **Analyze**, the wizard displays the Analyze Options step on the left menu.
Retention Lock Duration	Only if you selected **Secure Copy Analyze**, **Secure Copy**, or **Copy Lock** as the action, enter the duration of the retention lock that this policy applies to PIT copies.
Application Host	Only if you selected: • **Secure Copy Analyze** or **Analyze**, select the CyberSense host • **Recovery Check**, select the PowerProtect Data Manager or NetWorker host (which must be NetWorker version 19.9 or later) **NOTE:** If the deployment is using CyberSense version 8.3 or later, the drop-down list only lists the version 8.3 CyberSense hosts that have a multilink configuration that is defined for the storage that is used by the policy to be analyzed.

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

Table 19. Scheduling page

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

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 20. Analyze Options page

Field	Description
Content Format	The type of application or protocol that is used to perform backups. Select either: • **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. This information is included as part of the CyberSense report for informational purposes.
Files/Directories to Include	Enter the names of files and directories on the DD MTree to include in the Analyze action. Either: • Type the file and directory names, each on a separate line.

Table 20. Analyze Options page (continued)

Field	Description
	• 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	Enter the names of files and directories on the DD MTree that the Analyze action must ignore. Either: • 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. **NOTE:** • For Avamar policies, do not analyze the following directories and ensure that you exclude them: ○ GSAN/ ○ VALIDATED/ ○ DELETED/ ○ STAGING ○ VMDS ○ cur/DELETED

7. Review the **Summary** page and either:
   - 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.
   - Click **Finish** if you are satisfied with the summary information and want to add the schedule.

   The Policies page is displayed and includes the new or updated schedule. By default, the schedule is enabled.

   You cannot create or update a schedule if it will overlap an existing enabled schedule for the same policy. An error message notifies you of the failure and when the overlap will occur.

   NOTE: For a policy schedule that is disabled before you update to version 19.19, the software checks if it overlaps with an existing enabled policy schedule for the same policy. If you cannot enable the policy schedule, we recommend that you to delete and then re-create the policy schedule.
8. Disable or enable a schedule:
   a. To disable a schedule so that it does not run, swipe left on the slider under **Enabled**. An informational message confirms that the schedule has been disabled and the **Edit** button is inactive. Also, an event is created.
   b. To sort schedules by status, click **Enabled**.
   c. To filter on status, click and then click the **Enabled** or **Disabled** checkbox. Only the schedules with the selected status are displayed. If you select both checkboxes, all schedules are displayed.
   d. To reenable a schedule, swipe right on the slider under **Enabled**. An informational message confirms that the schedule has been reenabled and the **Edit** button is active. Also, an event is created.
9. To customize the columns in the table that lists the policies, click  and select the columns to show or hide.
10. Click a schedule's row to open the details pane and view additional details about the schedule, and then:
    a. Click  to close the details pane.
    b. Click  to open the details pane again.
11. Delete a schedule:

a. Select an enabled or disabled schedule.
b. Click **Delete**.

12. To capture information about all the schedules in a `.csv` file, click **Export**.

    NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

    The Cyber Recovery software downloads the `schedules.csv` file.

Managing copies

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

Prerequisites

You are logged in as the admin or operator user.

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 Recovery
- Recovering data to an alternate DD system

NOTE: You cannot analyze a Sheltered Harbor copy.

Steps

1. Select **Policies** from the Main Menu.
2. 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, the last analysis status, and the recovery status.

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

3. To customize the columns in the table that lists the copies, click  and select the columns to show or hide.
4. Click a copy's row to view additional details about the copy and then:

   a. Click  to close the details pane.

   b. Click  to open the details pane again.

   NOTE: If you run an Analyze operation using CyberSense version 8.0 or later, and the result is `Suspicious`, the **Details** pane provides a link to the analyze dashboard on the CyberSense host.

5. To retention lock a copy or extend the retention period of a locked copy, see Securing a copy.

   NOTE: By default, Sheltered Harbor copies are retention locked.

6. To analyze a copy, see Analyzing a copy.

   NOTE: You cannot analyze a Sheltered Harbor copy.

7. To retrieve a detailed report about a completed Analyze job, see Retrieving an analysis report.
8. To delete an unlocked copy or copies, select a copy or copies and then click **Delete**.

   NOTE:
   - If you click the checkbox at the head of the checkboxes column, all the copies are selected.

- The  icon next to the expiration date indicates that the copy is unlocked and that you can delete the copy. Otherwise, you cannot delete the copy.
- When you delete a PowerProtect Data Manager copy that has associated child copies, those child copies are also deleted.

9. To capture information about all the copies in a `.csv` file, click **Export**.

   NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

   The Cyber Recovery software downloads the `copies.csv` file.

Managing Sheltered Harbor copies

The **Policies** page enables you to view, secure, and delete Sheltered Harbor copies.

Prerequisites

- The Sheltered Harbor feature must be enabled, otherwise you do not have access to the Sheltered Harbor options in the Cyber Recovery UI or CRCLI.
- You must configure a financial institution object before you can create a Sheltered Harbor policy.

About this task

Managing Sheltered Harbor copies is similar to managing copies in the Cyber Recovery software. See Securing a copy for detailed information about managing policies and copies.

NOTE: If the Business Date in the Sheltered Harbor manifest is later than the expiration date of the license for the financial institution, the Sheltered Harbor Copy action fails.

Steps

1. Create a policy of type **Sheltered Harbor**.
2. Run the policy.

   The only action available for a Sheltered Harbor policy is the **Sheltered Harbor Copy** action.

   The Cyber Recovery software creates a retention-locked copy, generates a report, and sends it to the primary and secondary email addresses that are configured in the financial institution object. This attestation email is proof of successful completion of the secure copy action.
3. Select the Sheltered Harbor copy and review the details.

   The **Details** window displays information about the copy and includes an **Additional Details** section that is specific to a Sheltered Harbor copy:

   - Business date—The date of the input files that are being processed. You can create a Sheltered Harbor copy for input files with a Business Date other than the day you create the copy.

     NOTE: The Business Date cannot be later than the license expiration date, otherwise the Sheltered Harbor Copy action fails.

   - Institution ID—The same value as the Institution ID of the financial institution
   - Institution Type—The same value as the Institution Type of the financial institution
   - Filename—The name of the secure envelope that the Cyber Recovery software creates

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.

Prerequisites

- You are logged in as the admin or operator user.
- A policy has created 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  and the expiration date.

When the retention lock expires, the **Expiration Date** column displays  and the expiration date.

Analyzing a copy

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

Prerequisites

- You are logged in as the admin or operator user.
- A policy has created a PIT copy to analyze.

  NOTE: The CyberSense application 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 license is based on TiB 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 the CyberSense host has not been added to the Cyber Recovery vault, the **Analyze** button is disabled. If you do not have a valid CyberSense license, the **Analyze** button is enabled, but the job fails.

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

   NOTE: If the deployment is using CyberSense version 8.2 or later, the drop-down list only lists the version 8.2 CyberSense hosts that have multilink configurations that are defined for the storage that is used by the policy to be analyzed.

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. If you do not select a content format, the CyberSense report includes information that is based on the format that CyberSense detected.

7. Optionally, if the CyberSense host is a CyberSense version earlier than 8.2, select the network storage interface through which the CyberSense feature connects to storage.

   If the CyberSense host is running version 8.2 or later, this option is not displayed.

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, the job status is displayed as **Complete w/Exceptions**, and the last analysis status for the copy is displayed as **Suspicious**. Otherwise, the job status is displayed 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 manually or let the next job run.
    - If a multilink object that is defined for the storage in a copy's policy is not:
      - **Active** on a CyberSense 8.2 deployment
      - **Active** or **Degraded** on a CyberSense 8.3 or later deployment

      the Sync Copy Lock step of the Secure Copy Analyze action completes successfully, but the Analyze step fails.

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 **Canceling**. 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.

NOTE: The job stops after approximately 10 minutes, however, it might take longer.

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 for the copy includes an Analysis Details section. If you run an Analyze operation using CyberSense version 8.0 or later, and the result is **Suspicious**, the **Details** pane provides a link to the analyze dashboard on the CyberSense host.

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

- You are logged in as the admin user.
- 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. The email report includes obfuscated system names for security purposes. To determine the actual system IDs, create a Cyber Recovery Analyze report.

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 or a job with the **Complete w/Exceptions** status 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

- You are logged in as the admin or operator user.
- 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. Perform the following one-time steps to set up recovery to an alternate DD system.

   You need only perform these steps again if you change the name of the recovery MTree.

   a. On the Cyber Recovery vault DD system, create a recovery MTree and then enable and initialize the replication context. For example:

   ```
   mtree create /data/col1/<mtree name>

   replication add source mtree://<Vault DD Name>/data/col1/<MTREE Name> destination
   mtree://<Production alternate DD>/data/col1/<MTREE Name>-repl

   replication modify mtree://<Production alternate DD>/data/col1/<MTREE Name>-repl
   connection-host <Production DD Replication IP Address>
   ```

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

   b. On the production or alternate DD system, run the following command, using the same syntax as in the previous step:

   ```
   replication add source mtree://<Vault DD Name>/data/col1/<MTREE Name> destination
   mtree://<Prod DD>/data/col1/<MTREE Name>-repl
   ```

   c. On the production or alternate DD system, run the following command, ensuring that you use the Cyber Recovery vault replication IP address in place of *<Production DD Replication IP Address>*:

   ```
    replication modify mtree://<Production alternate DD>/data/col1/<MTREE Name>-repl
   connection-host <Vault Replication IP Address>
   ```

   d. On the Cyber Recovery vault DD system, run the following command:

   ```
   replication initialize mtree://<Production alternate DD>/data/col1/<MTREE Name>-repl
   ```

2. Log in to the Cyber Recovery UI as the admin user.
3. From the Main Menu, click **Recovery**.
4. Select the copy that you want to recover and click **Alternate Recovery**.
5. In the **Alternate Recovery** dialog box, do the following:
   - For the **Repl Context** field, select the replication context from the drop-down list.

     NOTE: The context is displayed as *source MTree>>destination MTree*.

   - For the **Ethernet** field, select an Ethernet interface from the drop-down list.
6. Click **Apply**.

The recovery job is started.

7. When the job is completed, on the production or alternate DD system, fast copy the data to the appropriate MTree or storage unit as required by the backup application that you are using. Run the following command:

```
filesys fastcopy source <folder of source MTree> destination <folder of destination MTree>
```

Where:

- *<folder of source MTree>* is the folder of the MTree that was replicated.
- *<folder of destination MTree>* is the folder of the MTree that the backup application recommends or where you want the data.

8. Depending on which backup application you use, see the application's documentation for information about how to perform a DR recovery.

For more detailed information, contact Dell Support.

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.

Admin and operator users can perform these tasks.

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. Create sandboxes as needed for data analytics, validation operations, or recovery for other backup applications or data. The CyberSense software automatically creates a system sandbox when you initiate an analyze operation 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.

NOTE: A Sheltered Harbor deployment does not support recovery sandboxes. A Sheltered Harbor recovery creates a system sandbox that contains the encrypted Sheltered Harbor archive volume. For more information, see Performing a Sheltered Harbor recovery.

Managing sandboxes

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

Prerequisites

You are logged in as the admin or operator user.

About this task

You can create sandboxes as needed for data analysis or validation operations. The CyberSense, 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. You can access the host 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** pane 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** pane displays the information.

      NOTE: If you ran an Analyze operation, there is a link for the CyberSense host.
   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.
   d. To capture information about all the sandboxes in a `.csv` file, click **Export**.

      NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

      The Cyber Recovery software downloads the `sandboxes.csv` file.

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

- You are logged in as the admin or operator user.
- A recovery operation has been run.

About this task

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

NOTE:

- If an application is associated with a recovery sandbox, you cannot delete the application. If you try to delete such an application, the software displays an error message.
- A Sheltered Harbor deployment does not support recovery sandboxes. A Sheltered Harbor recovery creates a system sandbox that contains the encrypted Sheltered Harbor archive volume. For more information, see Performing a Sheltered Harbor recovery.

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 been completed successfully.
   c. To clean up for an existing recovery, click **Cleanup**.

d. To capture information about all recovery sandboxes in a `.csv` file, click **Export**.

NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

The Cyber Recovery software downloads the `recoverysandboxes.csv` file.

Performing a Sheltered Harbor recovery

Use a Sheltered Harbor copy, which is protected using Sheltered Harbor standards, to rehydrate data in the Cyber Recovery vault.

Prerequisites

The Sheltered Harbor feature must be enabled, otherwise you do not have access to the Sheltered Harbor options in the Cyber Recovery UI or CRCLI.

About this task

The Cyber Recovery software does not provide an automatic procedure to recover a Sheltered Harbor copy. You must perform a manual recovery.

Managing Sheltered Harbor sandboxes is similar to managing other sandbox types in the Cyber Recovery software. See Managing sandboxes for detailed information about adding a managing a sandbox.

Steps

1. From the Main Menu, click **Recovery**.
2. Select a Sheltered Harbor copy from the list of copies.
3. Click **Sandbox**.
4. Complete the fields in the **Sandbox** window.

   See Managing sandboxes for detailed information about managing sandboxes.

   The Cyber Recovery software creates a sandbox that contains the encrypted Sheltered Harbor archive volume.
5. Perform a recovery using your institution's recovery procedure.

6

Managing Reports

This section describes how to create and manage reports that provide detailed information about Cyber Recovery components and operations. Only the admin and operator users can perform these tasks.

Topics:

About reports

Admin and operator users can create report schedules or on-demand reports that provide information about Cyber Recovery activities.

A wizard provides access to a template library that contains predefined standard templates for various reporting categories. The wizard guides you through the template to create a report. You cannot delete these standard templates.

The wizard provides templates for capacity and utilization reports and jobs reports:

- The CyberSense License Utilization template generates or schedules a report that summarizes license details and capacity status for CyberSense assets in the deployment.
- The Job Summary template generates or schedules a report that summarizes job activities for a specific duration.
- The Sync Report template generates a detailed Sync replication report.
- The Analyze Report template generates a detailed CyberSense Analyze report.

The wizard enables you to:

- Apply multiple filters that are relevant for a report
- Preview a report after you select filters
- Schedule a report
- Specify how to deliver the report, either as a download or in an email message

When you complete the wizard, depending on the occurrence or recurrence of the scheduling that you choose:

- A schedule for a report is listed on the **Scheduled Reports** page. From this page, you can edit, delete, run, duplicate, and disable report schedules.
- An on-demand report is run and listed on the **Generated Reports** page. From this page, you can download and delete reports. You can also run a report again.

The Cyber Recovery UI provides details about reports and report schedules. The details include which user created them and when, the size and the checksum value for generated reports, details about report schedules, and so on. The status indicates if the report creation is successful; if the report creation fails, an alert is generated, and the status indicates failure.

The Export option enables you to capture information about all the scheduled and generated reports in a `.csv` file. The software generates a `scheduledReports.csv` file and a `generatedReports.csv` file.

Creating a CyberSense License Utilization report

Use the Reports wizard to create CyberSense license utilization reports and report schedules.

Prerequisites

- You are logged in as the admin or operator user.

- CyberSense version 8.3 and later is added to the deployment.

About this task

The wizard enables you to configure the assets, filters, schedule, and delivery method of the report.

The assets include:

- Servers, which are the CyberSense servers that are added as an application from the **Assets** pane and are used to analyze the point-in-time copies.
- Hosts, which are the VMs in the backup.

NOTE: The Cyber Recovery software does not support CyberSense license inheritance or the license rotation feature for CyberSense server instances. If you have configured license inheritance for CyberSense instances, the Cyber Recovery software ignores the license capacity of the inherited license server.

Steps

1. From the Main Menu, click **Reports** > **Template Library**.
2. On the **CyberSense License Utilization** tile, click **Generate** to open the wizard for a CyberSense license report.
   The Generate Report wizard opens. The report family, which is the category of report, is listed on the top right-side of the pane.
3. On the **Details** pane, complete the following fields and click **Next**:

Table 21. Details fields

Field	Description
Report Name	Enter a unique name for the report. The report name must start with an alphanumeric character and can include hyphens (-) and underscores (_). It cannot include spaces or special characters.
Description	Optionally, enter details that describe the report. The maximum number of characters is 400 characters. The description must use alphanumeric characters and can include hyphens (-), underscores (_), periods (.) and spaces. It cannot include special characters. The description must start with an alphanumeric character.
Type	Select whether you want to schedule a report or if you want to generate an on-demand report immediately.

   The subsequent wizard pages list whether the report is scheduled or on demand on the top right-side of the pane.
4. On the **Assets** pane, do the following to indicate which assets you want to include in the report and click **Next**:
   a. Click **All Assets** > **Servers** to view a list of all CyberSense servers in the Cyber Recovery deployment. The report includes all the servers.
   b. Click **Select Assets** > **Servers** to select a specific CyberSense server or servers. The report includes only the specified servers.
   c. Click **All Assets** > **Hosts** to view a list of all the hosts for which an Analyze action was run using the CyberSense server. The report includes all the hosts.
   d. Click **Select Assets** > **Hosts** to select a specific host or hosts for which an Analyze action was run using the CyberSense server. The report includes only the specified hosts.

   NOTE:
   - The table does not list CyberSense servers running versions earlier than version 8.3.
   - Select either **Server** or **Hosts**; you cannot select both options.

5. Optionally, on the **Filters** pane, select filter options:
   a. Click **Available** and display the filter options by either expanding the drop-down list next to the **Report Range** and **Capacity Status** labels or clicking **Expand All** at the bottom of the pane.
   b. Do the following:
      - Optionally, modify the report range, which is set to the default of data for one day. For an on-demand report, you can also enable either the **Specific date** or **Custom range** options to set a specified report range. The maximum value is 365 days.
      - Optionally, choose to report the capacity status. You can select **Exceeded** or **OK**, or both options.

NOTE: A numbered callout next to the Capacity Status label indicates how many filter options that you have chosen.

Click  next to each option or click **Collapse All** to close the drop-down lists.

c. Click **Selected** to list the filter options that you have chosen.
   - Click **Edit** to modify the report range values.
   - If you do not want a selected Capacity Status filter option, click **X** to remove it from the list.
   - If you do not want any of the selected Capacity Status filter options, click **Clear All** to void the entire list.

d. Click **Generate Preview** to preview the report that is based on the filter settings that you have chosen.

   NOTE:
   - The preview report shows only limited information. Run the report for complete information.
   - If no jobs were performed, the software does not create a report preview and generates an alert.

e. Optionally, click **Preview in popup mode** above the displayed preview to view the preview report in a separate window.

f. Optionally, click **Available**, modify the filter options, and then click **Refresh Preview** at the bottom of the **Report Preview** pane.

g. Click **Next**.

6. On the **Scheduling** pane, specify the range of a report, the start time and date, and its recurrence. Then click **Next.**
7. On the **Delivery** pane, if you selected **On Demand** in the Details step of the wizard (see step 3), do the following. Otherwise, got to step 8.
   - Click **Download Now (csv)** so that the report is downloaded when you complete the wizard, click **Next**, and go to step 10.
   - Click **Send as an Email** to deliver an email message with the report. Go to step 9.
   - Click both **Download Now (csv)** and **Send as an Email**. Go to step 9.
8. On the **Delivery** pane, do one of the following:
   - Disable the **Send as an email** option to generate a report that you can view and then download manually, and click **Next**. You can edit the schedule to add the email delivery option at any time.
   - Enable the **Send as an email** option to send a report in an email message. Go to the next step.
9. On the **Delivery** pane, complete the following fields, and click **Next**:

Table 22. Email fields

Field	Description
Email Subject (required)	Enter a meaningful subject line.
Recipients (required)	Click **Add recipients**, enter an email address, and press Enter. To add another email address, click **Add additional recipients** and enter another email address. **NOTE:** If domain restrictions are enabled, only email addresses in the allowed domains receive the report. When the report is generated, a critical alert lists the users and report schedules that are associated with email addresses that are not allowed.
Cc	Optionally, click **Add recipients** and enter an email address to send a copy of the mail.
Bcc	Optionally, click **Add recipients** and enter an email address to send a blind copy of the mail.
Message	Optionally, enter a message. The maximum number of characters is 400 characters.
Send Report Output As	Select if you want the report to be: • A .csv file attachment • Embedded in the body of the email

Table 22. Email fields

Field	Description
	• Both a .csv file attachment and embedded in the body of the email

An email message provides information about the selected report filters, job summary, and the report. If you run a report that is configured such that no license data is available for the specified time range and filter settings, the report status is displayed as `Failed w/ Exceptions`. The email messages contain only the report filters information.

10. Review the **Summary** pane and:
    - Click **Edit** on the right or the step on the left to return to a specific pane to modify information such as the filter and asset selection.
    - Click the **Preview Report** icon in the Filters row to preview the report.
    - Click **Back** to return to the previous panes to modify the information.
    - For an on-demand report, click **Generate** if you are satisfied with the summary information and want to create the report.

      The following occurs:

      - An informational message indicates that the report was generated and provides a link to view the report.
      - Depending on the settings that you selected on the **Delivery** pane, the report is downloaded or sent as an email message.
      - The **Generated Reports** page lists the report and its status.
      - There is no entry on the **Scheduled Reports** page.
    - For a Scheduled report, click **Schedule** if you are satisfied with the summary information and want to create the report.

      The following results occur:

      - A message indicates that the report has been scheduled.
      - A message indicates that an email message is sent when the report runs.
      - A link to the **Scheduled Reports** pane, which lists the report schedule, is displayed.

    NOTE: If you run a report that is configured such that no license data is available for the specified time range and filter settings, the report status is displayed as **Failed w/ Exceptions**. For a **Successful** status, modify the configuration and specify a time range and filter settings that include license data.

Creating a Job Summary report

Use the Reports wizard to create Cyber Recovery daily job reports and report schedules.

Prerequisites

You are logged in as the admin or operator user.

Steps

1. From the Main Menu, click **Reports** > **Template Library**.
2. On the **Job Summary** tile, click **Generate** to open the wizard for a daily job report.
   The Generate Report wizard opens. The report family, which is the category of report, is listed on the top right-side of the pane.
3. On the **Details** pane, complete the following fields and click **Next**:

Table 23. Details fields

Field	Description
Report Name	Enter a unique name for the report. The report name must start with an alphanumeric character and can include hyphens (-) and underscores (_). It cannot include spaces or special characters.
Description	Optionally, enter details that describe the report. The maximum number of characters is 400 characters. The description must use alphanumeric

Table 23. Details fields (continued)

Field	Description
	characters and can include hyphens (-), underscores (_), periods (.) and spaces, It cannot include special characters. The description must start with an alphanumeric character.
Type	Select whether you want to schedule a report or if you want to generate an on-demand report immediately.

The subsequent wizard pages list whether the report is scheduled or on demand on the top right-side of the pane.

4. Optionally, on the **Filters** pane, select filter options:
   a. Click **Available** and display the filter options by either expanding the drop-down list next to each item or clicking **Expand All** at the bottom of the pane.
   b. Optionally, modify the report range, which is set to the default of data for one day. The maximum value is 365 days.
      For an on-demand report, you can also enable the **Specific date** or **Custom range** options to set a specified report range.
   c. Select one or more filter options.
      - If you do not choose any options, the report includes all job types, policies, and statuses.
      - If you choose a job type, such as **Protection**, but no options, the report includes all jobs that are of the selected job type. For example, all protection jobs are displayed
      - If you choose a job type, such as **Protection**, and a policy name, only jobs that are of the selected job type for the policy are displayed. For example, only protection jobs for the specified policy are displayed.

      A numbered callout next to each item indicates how many filter options that you have chosen.

      Click  next to a specific open list or click **Collapse All** to close all the drop-down lists.
   d. Click **Selected** at the top to list the filter options that you have chosen.
      - Click **Edit** to modify the report range values.
      - If you do not want a selected filter option, click **X** to remove it from the list.
      - If you do not want any of the selected filter options, click **Clear All** to void the entire list.
   e. Click **Generate Preview** to preview the report based on the filter settings that you have chosen.
      NOTE: If no jobs were performed, the software does not create a report preview and generates an alert.
   f. Optionally, click **Preview in popout mode** above the displayed preview to view the preview report in a separate window.
   g. Optionally, click **Available** or **Selected**, add or delete filter options, and then click **Refresh Preview** at the bottom of the **Report Preview** pane.
   h. Click **Next**.
5. On the **Scheduling** pane, specify the range of a report, the start time and date, and its recurrence. Then click **Next**.
6. On the **Delivery** pane, if you selected **On Demand** in the Details step of the wizard (see step 3 of this procedure), do the following. Otherwise, got to step 7.
   - Click **Download Now (csv)** so that the report is downloaded when you complete the wizard, click **Next**, and go to step 9.
   - Click **Send as an Email** to deliver an email message with the report. Go to step 8.
   - Click both **Download Now (csv)** and **Send as an Email**. Go to step 8.

   When you select **Send as an Email**, the email settings fields are displayed.
7. On the **Delivery** pane, do one of the following:
   - Disable the **Send as an email** option to generate a report that you can view and download manually, and click **Next**. You can edit the schedule to add the email delivery option at any time.
   - Enable the **Send as an email** option to send a report in an email message. Complete the following fields and click **Next**.
8. On the **Delivery** pane, complete the following fields, and click **Next**:

Table 24. Email fields

Field	Description
Email Subject (required)	Enter a meaningful subject line.

Table 24. Email fields (continued)

Field	Description
Recipients (required)	Click **Add recipients**, enter an email address, and press Enter. To add another email address, click **Add additional recipients** and enter another email address. **NOTE:** If domain restrictions are enabled, only email addresses in the allowed domains receive the report. When the report is generated, a critical alert lists the users and report schedules associated with email addresses that are not allowed.
Cc	Optionally, click **Add recipients** and enter an email address to send a copy of the mail.
Bcc	Optionally, click **Add recipients** and enter an email address to send a blind copy of the mail.
Message	Optionally, enter a message. The maximum number of characters is 400 characters.
Send Report Output As	Select if you want the report to be: ● A .csv file attachment ● Embedded in the body of the email ● Both a .csv file attachment and embedded in the body of the email

An email message provides information about the selected report filters, a job summary, and the job report. If you run a report that is configured such that no jobs were performed for the specified time range and filter settings, the report status is displayed as `Failed w/ Exceptions`. The email messages contain only the report filters information.

9. Review the **Summary** pane and:
   - Click **Edit** on the right or the step on the left to return to a specific pane to modify information.
   - Click the **Preview Report** icon in the Filters row to preview the report.
   - Click **Back** to return to the previous panes to modify the information.
   - For an on-demand report, click **Generate** if you are satisfied with the summary information and want to create the report.

     The following occurs:

     - An informational message indicates that the report was generated and provides a link to view the report.
     - Depending on the settings that you selected on the **Delivery** pane, the report is downloaded or sent as an email message.
     - The **Generated Reports** page lists the report and its status.
     - There is no entry on the **Scheduled Reports** page.
   - For a Scheduled report, click **Schedule** if you are satisfied with the summary information and want to create the report.

     The following results occur:

     - A message indicates that the report has been scheduled.
     - A message indicates that an email message is sent when the report runs.
     - A link to the **Scheduled Reports** pane, which lists the report schedule, is displayed.

NOTE: If you run a report that is configured such that no jobs were performed for the specified time range and filter settings, the report status is displayed as **Completed w/ Exceptions**. For a **Successful** status, modify the configuration and specify a time range and filter settings that include jobs that were performed.

Creating a Sync or Analyze report

Use the Sync Report or Analyze Report wizards to create detailed Sync replication or CyberSense Analyze reports and report schedules.

Prerequisites

- You are logged in as the admin or operator user.
- Sync or Analyze jobs have been run.

About this task

The wizards enable you to choose the assets and configure filters, the schedule, and the delivery methods of the report.

NOTE: The reports do not include information about Sync or Analyze jobs generated on Cyber Recovery versions earlier than version 19.16.

Steps

1. From the Main Menu, click **Reports** > **Template Library**.
2. On either the **Sync Report** or **Analyze Report** tile, click **Generate** to open the applicable wizard.
   The Generate Report wizard opens. The top right-side of the pane displays the template name.
3. On the **Details** pane, complete the following fields and click **Next**:

Table 25. Details fields

Field	Description
Report Name	Enter a unique name for the report. The report name must start with an alphanumeric character and can include hyphens (-) and underscores (_). It cannot include spaces or special characters.
Description	Optionally, enter details that describe the report. The maximum number of characters is 400 characters. The description must use alphanumeric characters and can include hyphens (-), underscores (_), periods (.) and spaces, It cannot include special characters. The description must start with an alphanumeric character.
Type	Select whether you want to schedule a report or if you want to generate an on-demand report immediately after you complete the wizard.

   Subsequent wizard pages list whether the report is scheduled or on demand on the top right-side of the pane.

4. On the **Assets** pane, click  next to the DD system to expand the list and view the associated policies. Then, click **Next**.
5. Optionally, on the **Filters** pane, select filter options:
   a. Click **Available** and display the filter options by either expanding the drop-down list next to the **Report Range** label or clicking **Expand All** at the bottom of the pane.
   b. Optionally, modify the report range, which is set to the default of one day. The maximum value is 365 days.
      For an on-demand report, you can also enable the **Specific date** or **Custom range** options to set a specified report range. You cannot select future dates.
   c. Click  next to the **Report Range** label or click **Collapse All** to close the drop-down lists.
   d. Click **Selected** to list the filter options that you have chosen.
   e. Click **Edit** to modify the report range values.
   f. Click **Generate Preview** to preview the report that is based on the filter settings that you have chosen.
      NOTE: If no jobs were performed, the software does not create a report preview and generates an alert.
   g. Optionally, click **Preview in popout mode** above the displayed preview to view the preview report in a separate window.
   h. Optionally, click **Available**, modify the filter options, and then click **Refresh Preview** at the bottom of the **Report Preview** pane.

i. Click **Next**.

6. If you selected a Scheduled report, on the **Scheduling** pane, specify the range of a report, the start time and date, and its recurrence. Then click **Next**.

   If you chose an on-demand report, the wizard does not display the **Scheduling** pane.

7. On the **Delivery** pane, if you selected **On Demand** in the Details step of the wizard (see step 3 of this procedure), do the following. Otherwise, got to step 8.
   - Click **Download Now (csv)** so that the report is downloaded when you complete the wizard, click **Next**, and go to step 10.
   - Click **Send as an Email** to deliver an email message with the report. Go to step 9.
   - Click both **Download Now (csv)** and **Send as an Email**. Go to step 9.
8. On the **Delivery** pane, do one of the following:
   - Disable the **Send as an email** option to generate a report that you can view and then download manually, and click **Next**. You can edit the schedule to add the email delivery option at any time.
   - Enable the **Send as an email** option to send a report in an email message. Go to the next step.
9. On the **Delivery** pane, complete the following fields, and click **Next**:

Table 26. Email fields

Field	Description
Email Subject (required)	Enter a meaningful subject line.
Recipients (required)	Click **Add recipients**, enter an email address, and press Enter. To add another email address, click **Add additional recipients** and enter another email address. **NOTE:** If domain restrictions are enabled, only email addresses in the allowed domains receive the report. When the report is generated, a critical alert lists the users and report schedules that are associated with email addresses that are not allowed.
Cc	Optionally, click **Add recipients** and enter an email address to send a copy of the mail.
Bcc	Optionally, click **Add recipients** and enter an email address to send a blind copy of the mail.
Message	Optionally, enter a message. The maximum number of characters is 400 characters.
Send Report Output As	Select if you want the report to be: • A .csv file attachment • Embedded in the body of the email • Both a .csv file attachment and embedded in the body of the email

10. Review the **Summary** pane and:
    - Click **Edit** on the right or the step on the left to return to a specific pane to modify information such as the filter and asset selection.
    - Click the **Preview Report** icon in the Filters row to preview the report.
    - Click **Back** to return to the previous panes to modify the information.
    - For an on-demand report, click **Generate** if you are satisfied with the summary information and want to create the report.

      The following occurs:

      - An informational message indicates that the report was generated and provides a link to view the report.
      - Depending on the settings that you selected on the **Delivery** pane, the report is downloaded or sent as an email message.
      - The **Generated Reports** page lists the report and its status.
      - There is no entry on the **Scheduled Reports** page.
    - For a Scheduled report, click **Schedule** if you are satisfied with the summary information and want to create the report.

The following results occur:

- A message indicates that the report has been scheduled.
- A message indicates that an email message is sent when the report runs.
- A link to the **Scheduled Reports** pane, which lists the report schedule, is displayed.

NOTE: If you run a report that is configured such that no Sync or Analyze jobs were performed for the specified time range and filter settings, the report status is displayed as **Failed w/ Exceptions**. For a **Successful** status, modify the configuration and specify a time range and filter settings that include license data.

Managing generated reports

The **Generated Reports** page lists the reports that have run either as scheduled reports or on-demand reports.

Prerequisites

- You are logged in as the admin or operator user.
- A report has been run.

About this task

The Generated Reports page lists the report name, creation date, the report type (Jobs or Capacity & Utilization), whether the report is scheduled or on demand, and the completion status.

NOTE: If a report is not complete, the software generates partial Cybersense reports that you can download or receive in an email message.

Steps

1. From the Main Menu, click **Reports** > **Generated Reports**.

   The page lists scheduled and on-demand reports that have been run. It includes the name of the report and when it was created, identifies the report family (**Jobs** or **Capacity & Utilization**), indicates if the report was scheduled or run on demand, and indicates if the report was run successfully or if there were exceptions.
2. To download a report:
   a. Select a report.

      You cannot download a report with the **Failed** status. For a **Capacity & Utilization** report, you can download a report with the **Completed w/Exceptions** status.

      NOTE: If a partial report is generated after the report schedule runs, you can download the partial report. If you selected the option to send the report output as an email attachment in the report wizard, the partial report is attached to the report email message.

   b. Click **Download**.
3. To run a report again:
   a. Select a report.

      You can select only one report at a time. The status of the report can be either Successful or Failed.
   b. Click **Run Now**.
   c. For reports that were created as on-demand reports, the **Run Report Now** pane is displayed. If necessary, modify the report configuration and click **Generate**.

      For scheduled reports, go to the next substep.
   d. Click **View Report** in the informational message to see the generated report.

      For the following report:
      - **Capacity & Utilization**—This report lists the point-in-time (PIT) license utilization data for the CyberSense server or host. If a common license is used for multiple CyberSense servers by using the CyberSense License Server and Clients feature, the Cyber Recovery shows license use for individual CyberSense servers only.

        NOTE: The report details might include the PIT data outside of the specified data range because computed license use is based on current time (t) and previous (t-1) PIT data.

- **Jobs**—This report lists the jobs performed in the specified time range.

The **Generated Reports** page lists all the reports that were run again.

4. To delete a generated report:
   a. Select one report, multiple reports, or all reports on the current page or all pages.
   b. Click **Delete**.
   c. Click **Continue** to confirm that you want to delete the report or reports.
5. To capture information about all the generated reports in a `.csv` file, click **Export**.

   NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

   The Cyber Recovery software downloads the `generatedReports.csv` file.
6. To manage or see more information:
   a. At the upper right, click:
      - **All** to display all reports
      - **Scheduled** to display only reports that were scheduled
      - **On Demand** to display only reports that were run on demand
   b. Click to sort the information in each column.
   c. If you set filters, click **Clear Filters** above the **Report Name** column heading to remove all filters or click **X** next to a specific filter to remove that filter.
   d. To customize the columns in the table that lists the generated reports, click  and select the columns to show or hide.
   e. Click a row to open the **Details** pane on the right to view the creation date, creator, error message, checksum, delivery configuration, and so on. To close the details pane, click  .
   f. Click the report name for options to download, delete, or to display details for the report.
   g. Click the link in the **Schedule** column to view the report schedule that was used to generate a report.
   The **Scheduled Reports** page opens to display the appropriate report schedule. There are no links in the **Schedule** column for on-demand reports.

Managing scheduled reports

The **Scheduled Reports** page lists the report schedules.

Prerequisites

- You are logged in as the admin or operator user.
- A report schedule has been created using the Reports wizard.

About this task

The Scheduled Reports page lists the report name, the report type (Jobs or Capacity & Utilization), the frequency of the report, and the last and next scheduled run time.

NOTE: If a report is not complete, the software generates partial Cybersense reports that you can download or receive in an email message.

Steps

1. From the Main Menu, click **Reports** > **Scheduled Reports**.
   The page lists report schedules that you created using the wizard.
2. To run a scheduled report on demand:
   a. Select a report schedule.
      You can select only one report at a time.
   b. Click **Run Now**.
   c. Click **View Report** in the informational message to view the generated report.
3. To edit a report schedule:

a. Select a report schedule.
b. Click **Edit**.
The Scheduled Reports wizard opens.
c. Go through the wizard pages, making wanted changes and clicking **Next**, and then click **Finish** on the **Summary** page.
If the report schedule includes an email address with a restricted domain, an error message is displayed and you cannot proceed.
d. Click **View Report Schedule** in the informational message to see the edited report listed in the **Scheduled Reports** page.

4. To clone a report schedule:
a. Select a report schedule.
b. Click **Duplicate**.
The Scheduled Reports wizard opens.
c. Enter a different report name in the first wizard page, continue through the wizard pages optionally making any wanted changes and clicking **Next**, and then click **Generate** on the **Summary** page.

NOTE: If you do not use a different report name in the first wizard page, the operation fails.

d. Click **View Report Schedule** in the informational message to see the cloned schedule listed in the **Scheduled Reports** page.

5. To delete a report schedule:
a. Select one report schedule, multiple report schedules, or all report schedules on the current page or all pages.
b. Click **Delete**.
c. Click **Delete** to confirm that you want to delete the report.
An informational message confirms that the report schedule has been deleted.

6. To capture information about all the report schedules in a `.csv` file, click **Export**.

NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

The Cyber Recovery software downloads the `scheduledReports.csv` file.

7. To manage or see more information:
a. Click to sort the information in each column.
b. If you set filters, click **Clear Filters** above the **Report Name** column heading to remove all filters or click **X** next to a specific filter to remove that filter.
c. To customize the columns in the table that lists the report schedules, click  and select the columns to show or hide.
d. Click a row to display details about the report, such as the creation date, creator, modification date, delivery configuration and so on. To close the **Details** pane, click  .

8. To disable a report schedule so that it does not run a report, swipe left on the slider under the **Enabled** column.
An informational message confirms that the report schedule has been disabled.
The **Next Run** column no longer shows a date on which the report is scheduled to run. Swipe right on the slider to reenable the report schedule and to see on which date the report is scheduled to run. An informational message confirms that the report schedule has been enabled.

7

Monitoring Cyber Recovery Components

This section describes how to monitor the Cyber Recovery vault status, storage capacity, Cyber Recovery operations, and alerts and events.

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

Topics:

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, admin, or operator users can manually lock the Cyber Recovery vault and close the connection. Only the security officer can release the Cyber Recovery vault. 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 27. 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. **NOTE:** A timer indicates the length of time that the Cyber Recovery vault is unlocked.
Secured		All replication network connections are secured because a security officer or 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. **NOTE:** A timer indicates the length of time that the Cyber Recovery vault is secured. The Cyber Recovery software issues an alert that provides additional information and identifies which user secured the Cyber Recovery vault.

Table 27. Cyber Recovery connection states (continued)

Status	Icon	Description
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 storage capacity

Monitor the capacity of the vault storage and the details of the associated MTrees.

Prerequisites

- You are logged in as the admin or operator user.
- Vault storage is added to the deployment.

About this task

The **Storage** pane displays information about:

- The DD systems in your deployment
- The MTrees associated with those DD systems

> **NOTE:** Deleted MTrees are not counted towards the active MTree limit. This feature allows the Cyber Recovery software to support more policies running analyze and recovery check operations. The Cyber Recovery software sends an alert and prompts you to restart the DD system to enable this feature. If you enable this feature, you cannot disable it later. The maximum supported MTrees remain the same.

Steps

1. From the Main Menu, select **Infrastructure** > **Storage**.
   By default, the page displays information about the DD systems under the **Systems** tab.
2. Click the **Capacity** tab.
   The page displays alert information and physical and logical vault storage information for the DD systems.
3. To view more information about the critical or warning alerts:
   a. Click  on the top-left of the alerts pane to open the pane.
   The pane displays all critical and warning alerts for the DD systems and the MTrees in the deployment.
   b. Click a row under the **Systems** or the **MTrees** tab and click **View alert details** in the Details tab to view more information about that alert on the **Alerts** pane.
   c. Click to close the expanded pane; click **Capacity** to return to the initial view.
4. To capture information about the vault storage capacity in a `.csv` file, under either **Systems** or **MTrees**, click **Export**.
   For the system capacity, the Cyber Recovery software downloads the `capacitySystems.csv` file. For the MTree capacity, the Cyber Recovery software downloads the `capacityMtrees.csv` file,
5. To view detailed information about the percentage of physical storage used, under the bottom **Systems** link, hover over the status bar to open a pop-up window with the details.
   - If the storage capacity is between 80 and 89 percent, the status bar is yellow and is preceded by a warning icon ( ).
   - If the storage capacity is 90 percent or higher, the status bar is red and is preceded by a critical icon ( ).

NOTE: The warning and critical values are the default DD system settings. If you change the values of the filesys `warning-space-usage` or the `critical-space-usage` options on the DD system, the Cyber Recovery storage capacity monitoring displays the warning and critical icons using the values configured on the DD system.

6. Click a DD system's row to open the **Details** pane and view additional details about the DD system:
   a. Click the system FQDN or IP address to return to the **Systems Storage** page.
   b. Click the number next to **Active MTrees** or **Deleted MTrees** to view the applicable MTrees associated with the DD system.

      If the file count or number of active MTrees exceeds the threshold, the number is preceded by  or  to indicate either a warning or critical alert.
7. To customize the columns in the table that lists the DD systems, click  and select the columns to show or hide.
8. To view information about the MTrees in the deployment, click the **MTrees** tab.
   The FQDN or IP address of the DD systems is displayed.
9. Click a DD system's row to open the Details pane.
   The Details pane displays the FQDN or IP address of the DD system and a doughnut chart. The chart displays the consumers of the MTrees. It identifies the top four consumers, and all other consumers are in the All Others category.
10. In the Details pane, do the following:
    a. Click the FQDN or IP address of the DD system to return to the **Systems** tab.
    b. Click  next to **Purpose** to filter by MTree purpose for the chart.
       The chart is updated to reflect the new purpose.
    c. Click a specific section of the chart to view the associated MTree.
    d. Under the chart, click  next to **MTree** to filter the MTrees by logical capacity or file count.
    e. Under the MTree tab, click a specific MTree to display more details.
11. To display all the MTrees associated with a DD system, from the table, click  next to its FQDN or IP address.
    a. Click the link in the **Policy** column in an MTree's row to be redirected to the Policies page to view information about the associated policy.
    b. Click an MTree's row to open the details pane and view additional details.
       The link next to the **Policy** label redirects you to the **Policies** page.
    c. Click  to close the details pane.
    d. Click  to open the details pane again.

Monitoring alerts and events

The Cyber Recovery software generates notifications about alerts and events. Security officer, admin , and operator users can monitor these notifications.

Alert and event categories include:

- System—Indicates a system issue that might compromise the Cyber Recovery system such as a failed component.
- Storage—Indicates the status of or an issue with the DD system.
- Security—Indicates that a user cannot log in or malware might have been detected.

An alert indicates that an occurrence might require you to take action.

You can view alerts from:

- The dashboard.
- The **Alerts** tab of the **Alerts and Events** content pane, which also enables you to view additional details, acknowledge, and add notes for an alert.
- The Masthead Navigation by clicking  .

The security officer can configure a user's account to receive email messages with alert notifications.

Events indicate system events, such as the start of a job, completion of a retention lock, user login, and updates of user information. You can view events from the **Events** tab of the **Alerts and Events** content pane. An event log captures login and logout information for all user sessions.

To view more detailed information about events and alerts (including descriptions and remedies), click the row of an event or an alert.

- Click  to close the details pane.
- Click  to open the details pane again.

Handling alerts

View, acknowledge, annotate, and export all alerts.

Prerequisites

You are logged in as the security officer, admin, or operator user.

About this task

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, select the alert's row.

   The **Details** pane displays additional details about the alert.
3. Then, do the following:

   a. Click  to close the details pane.

   b. Click  to open the details pane again.
4. Take any necessary actions to resolve the problem.
5. Select an alert or multiple alerts and click **Acknowledge**.
   The **Acknowledge** column now displays

   for each selected alert.

   If you click the 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.
6. 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.
7. 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.
8. To capture information about all the alerts in a `.csv` file, click **Export**.

   NOTE: If you have applied column filters or search box filters, or selected a checkbox, the **Export** button is disabled. Clear the filter or the checkboxes to enable the **Export** button. When you hover over the **Export** button, a message indicates that the items will be exported or that you must remove the filters to enable the **Export** button.

   The Cyber Recovery software downloads the `alerts.csv` file.

   NOTE: The software exports all the alerts; you cannot filter for and export specific alerts.

Monitoring jobs

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

Only the admin or operator user can monitor jobs.

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, disaster recovery backup, and the multilink configuration.

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

- **Recovery Jobs**—Includes jobs for sandbox creation and deletion, recovery check, and application recovery and cleanup

The **Jobs** content pane shows 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** (a critical alert is also associated with the failed job). The Details pane for a **Completed w/Exceptions** or **Failed** job includes a Job Alert notification with a link to the **Alerts** content pane, which provides detailed information about the job's status.

NOTE: If you recover a DR backup, after the recovery, the DR backup job is displayed as a critical failed job. Ignore this status; you do not need to take any action.

The **Running** tab also includes the option to cancel a running job. Jobs in the **Canceling** state are displayed under the **Running** tab.

You can create report schedules or on-demand reports. The Jobs pages include an option to export the jobs into an Excel spreadsheet. For more information, see Creating a report.

Managing jobs

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

Prerequisites

- You must be logged in as the admin or operator user.
- 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 at the top of the pane.

   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  .

   To select how often the content pane refreshes, click the ellipsis (...) next to  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 running job, click the row for the job.

      In the **Details** pane, the **Details** tab provides job information and the **Step Log** tab shows the progress of each task in the job. The step log shows the steps that are completed, in process, and not yet started. Click the arrow on the right to close the window.

   c. For additional information about a completed job, click the row for the job.

In the **Details** pane, the **Details** tab provides job information:

- If the job's status is **Completed w/Exceptions** or **Failed**, the Details tab includes a Job Alert notification with a link to the **Alerts** content pane, which provides alert details. If you ran an Analyze operation, there is also a link to the CyberSense host.
- The **Step Log** tab 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.

d. To customize the columns in the table that lists the jobs, click  and select the columns to show or hide.

e. To manage which jobs are displayed, click 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.

f. To clear a specific filter, click the **X** in the lozenge. To click all the filters, click **Clear Filters**.

g. To sort the jobs, click the column title.

5. To capture information about all the applications in a .csv file, click **Export**.
6. To download an Excel spreadsheet that contains job details for current filter content, click **Export** on either tab.

NOTE: If you apply a column filter or search box filter, the **Export** button is disabled. Clear the filters to enable the **Export** button.

The Cyber Recovery software downloads the `jobsList.csv` file.

7. 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** pane to see on which step the process was canceled.

   When the cancellation is completed, the job is no longer displayed in the Running pane.

   d. Click the **Completed** tab to verify that the job shows the Canceled status.

8

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. Only the admin and operator users can perform this task.

Also see the Dell Technologies PowerProtect Cyber Recovery Info Hub for white papers, blogs, and videos about performing recoveries.

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 19.19 do not support backup applications running on Windows or the addition of Windows applications to the Cyber Recovery environment.

Topics:

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.

NOTE: To recover a backup application from a Cyber Recovery copy properly, ensure that your replication window start time is after the application backup on the production system is completed, including the required metadata backup. For an intermediate replication on the production system, ensure that the intermediate replication start time is also after the production backup completion time.

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

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

   c. 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 are logged in as the admin or operator user.
- For a deployment running NetWorker version 19.8, ensure that the NetWorker server state is set to the **`disaster recovery`** state.
- 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 if the IP addresses are the same, you can avoid these issues.

- 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.

About this task

NOTE: The Cyber Recovery software does not support an automatic application recovery of a NetWorker server with more than one MTree. However, you can perform a recovery of a server with more than one MTree manually. Contact Dell Support for more information.

Steps

1. Select **Recovery** from the Main Menu.
2. On the **Recovery** content pane, 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. From the drop-down list, select the NetWorker application.

   NOTE: The drop-down list does not display a NetWorker application host for which a sandbox already exists.

4. Enter the DD Boost username and password.
5. 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.

6. Click **Apply**.

   The recovery status of the copy is marked as **In Progress**.

   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.
7. 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.
8. Click the job `recoverapp_<ID>` name and view the status detail.

   The Status Detail provides the name of the newly created sandbox.
9. 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** and confirm that you want 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**.
10. (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*.

Results

After a NetWorker recovery, the recovery status of a copy is marked as:

- **Recoverable** if the recovery is successful
- **Failed** if the recovery fails

Running a NetWorker recovery check

Run a scheduled or on-demand NetWorker recovery check to ensure that after a successful recovery, a copy can be recovered.

Prerequisites

- Your Cyber Recovery deployment is running NetWorker version 19.9 or higher on Linux or Windows.
- You are logged in as the admin or operator user.

About this task

When the Cyber Recovery software completes a recovery check action, the status of the copy is marked as recoverable or failed. The Cyber Recovery software reverts NetWorker 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. To schedule a recovery check:
   a. Select **Policies** from the Main Menu.
   b. Click **Schedules**.
   c. Click **Add** to open the Add Schedule wizard.
   d. On the **Schedule Information** page, complete the following fields and then click **Next**:

Table 28. Schedule information page

Field	Description
Schedule Name	Specify a schedule name.
Policy	Select the policy that you are scheduling.
Action	Select **Recovery Check**.
Application Host	Select the NetWorker host.
Storage User	Enter the username for the storage user.
Storage Password	Enter the password for the storage user.
Bootstrap Device Folder	Optionally, enter the name of the folder that includes the last bootstrap backups.

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

Table 29. Scheduling page

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

   f. 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.

   NOTE: If your deployment is running NetWorker on Windows or a NetWorker version earlier than version 19.9, the Cyber Recovery software generates an error message.

2. To run an on-demand recovery check.
   a. Select **Recovery** from the Main Menu.
   b. Under **Copies**, select a copy.
   c. Click **Recovery Check**.
   d. In the **Recovery Check** window, select the NetWorker host from the **Application Host** drop-down list.
   e. In the next **Recovery Check** window, complete the following fields and then click **Apply**.

Table 30. On-demand recovery check information page

Field	Description
Application Host	The NetWorker host that you selected in the previous substep is displayed.

Table 30. On-demand recovery check information page (continued)

Field	Description
Storage User	Enter the username.
Storage Password	Enter the password for the storage user.
Bootstrap Device Folder	Optionally, enter the name of the folder that includes the last bootstrap backups.

The recovery check runs immediately.

NOTE: If your deployment is running NetWorker on Windows version 19.18 or earlier or a NetWorker version earlier than version 19.9, the Cyber Recovery software generates an error message.

Results

The recovery check procedure does not provide the option to access the NetWorker UI. The procedure recovers the NetWorker 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.

9

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. Only the admin and operator users can perform this task.

Also see the Dell Technologies PowerProtect Cyber Recovery Info Hub for white papers, blogs, and videos about performing recoveries.

Topics:

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.

NOTE: To recover a backup application from a Cyber Recovery copy properly, ensure that your replication window start time is after the application backup on the production system is completed, including the required metadata backup. For an intermediate replication on the production system, ensure that the intermediate replication start time is also after the production backup completion time.

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, create a checkpoint before performing a Secure Copy policy operation.

About this task

If you have already created a checkpoint, there is no need to perform the following procedure.

CAUTION: Ensure that a checkpoint validation (hfscheck) has verified the integrity of the checkpoint.

Steps

1. Log in to the production Avamar server as root user.

2. Run a checkpoint operation. This step might take some time.
   a. Type the following command:

```
su admin -c "mcserver.sh --flush"
```

   The following example shows sample output:

```
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 the following command:

```
mccli checkpoint create
```

   The following example shows sample output:

```
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. To ensure that a checkpoint validation (hfscheck) has verified the integrity of the checkpoint, type the following command:

```
mccli checkpoint validate --cptag=<cp tag name>
```

   The following example shows sample output:

```
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
```

3. On the Cyber Recovery host, run a Secure Copy policy action for the DD MTree.
4. 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 (for example: `/data/col1/avamar-1560177494-repl`).
   a. Type the following command:

```
mtree list
```

   The following example shows sample output:

```
sysadmin@crmgmthost# mtree list
Name                                                Pre-Comp (GiB)   Status
--------------------------------------------------  --------------   -------
/data/col1/avamar-1560177494-repl                              4.2   RO/RD
```

```
/data/col1/backup                                                    0.0   RW
/data/col1/cr-policy-5d5ad66394422f0001ced229-repo                   0.0   RW/RLGE
/data/col1/cr-policy-5d5ad69994422f0001ced22a-repo                   4.2   RW/RLGE
/data/col1/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.

NOTE: The table refers to Knowledge Base articles. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell representative.

Table 31. Avamar prerequisites

Done	Task	Notes
-	Review the latest Knowledge Base articles.	In particular, ensure that you review the following KB articles: ● Knowledge Base Article Number 188334—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—If you encounter any issues restoring the MCS; applies to Avamar 19.3 and later. ● Knowledge Base Article Number 119875—For information about run levels. **NOTE:** Access to Knowledge Base Articles depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.
-	Deploy the production Avamar server using its FQDN.	MCS fails to start after a recovery if you deploy the production Avamar server using its IP address.
-	Ensure that your Avamar deployment is up to date.	The production Avamar system and the Cyber Recovery vault Avamar system must be running the same Avamar version and patch levels. See the latest Knowledge Base articles. **NOTE:** Access to Knowledge Base Articles depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.
-	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 name (FQDN) 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, including the operating system and admin passwords.
-	Ensure that the DD Boost username and UID in the Cyber Recovery vault match the credentials of the production system.	Ensure that the DD Boost username and UID are configured in the Cyber Recovery vault before performing the Cyber Recovery steps.
-	Obtain Avamar licenses, if necessary.	You must have a license for both the production-site Avamar application and the Cyber Recovery vault Avamar application.

Table 31. Avamar prerequisites (continued)

Done	Task	Notes
-	Establish Avamar applications in the Cyber Recovery vault.	This task enables rehydrating applications in the Cyber Recovery vault
-	Create a new checkpoint and then validate and lock it to create the baseline checkpoint.	Run the following commands: • `mccli checkpoint create` • `mccli checkpoint validate --cptag=cp.nnnnnnnnnnnnn` • `avmaint lockcp --lock cp.nnnnnnnnnnnnn --avamaronly` See Knowledge Base Article Number 188334 for more detailed information. **NOTE:** Access to Knowledge Base Articles depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.
-	As a best practice, ensure that the DDOS version in the Cyber Recovery vault is the same version as the DDOS version on the production site.	Ensure that the DDOS version works with the Avamar application.

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:
   a. Log in to the CRCLI by typing the following command:

      ```
      crcli login -u <Cyber Recovery user>
      ```

   b. Type the following command on the management host:

      ```
      crcli policy list-copy --policyname <policy name> -c <copy name>
      ```

      For example:

      ```
      # 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     : 65534
      ```

      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 type 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. Create the username and account by typing the following command:

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

      For example:

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

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

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 Avamar application server in the Cyber Recovery vault.

Prerequisites

Ensure that the following prerequisites are met before you initiate an Avamar recovery:

- You are logged in as the admin or operator user.
- The Avamar application is installed in the Cyber Recovery vault and defined as an application asset in Cyber Recovery.
- A known good Cyber Recovery policy is available to use as a recovery sandbox.
- Usernames and passwords are available.
- You have acquired the latest copy of the `lockbox_restore.pl` file from the Dell Online Support site (see Knowledge Base Article Number 000181972) and placed it in the `/home/admin` directory on the production Avamar server as an executable file. As of the date of this publication, the version of this file is 19.5.100-77.

  NOTE: Access to Knowledge Base Articles depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- Data Domain SCP is enabled. SCP might be disabled as part of security hardening, but it must be enabled for recovery.

Steps

1. Verify that SCP is enabled:
   a. Use PuTTY to log in to the vault DD system as `sysadmin`.
   b. Type **`adminaccess show`**.

      The SCP setting is displayed near the top of the output.
   c. If SCP is disabled, type **`adminaccess enable scp`**.
2. Log in to the Cyber Recovery UI as the admin user.
3. Select **Recovery** from the Main Menu.
4. From the drop-down list, select the Avamar application.

   NOTE: The drop-down list does not display an Avamar application host for which a sandbox already exists.

5. Select a last known good copy and click **Apply**.
   The Cyber Recovery software runs a job that creates a recovery sandbox on the DD system and populates it with the selected copy, which is available to the Avamar application host.
6. Wait for the recovery application job to complete before proceeding. From the Main Menu, click **Jobs** to monitor the progress of the job.
7. From the **Recovery** content pane, click **Recovery Sandboxes**.
   The `avamar-<SystemID>` name (for example, `avamar-1560177494`) is listed.

NOTE: Record the SystemID of the `avamar-<SystemID>` name, which the following steps require. The SystemID, also known as the `hfsctime`, is appended to the Avamar MTree name.

8. Optionally, to verify the SystemID, log in to the vault DD system as `sysadmin` and type **`ddboost storage-unit show`**. The output displays both the SystemID and the DD Boost user who is associated with the Avamar MTree. Record this information.

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 successfully created a Recovery Sandbox in Cyber Recovery.
- You have downloaded an executable copy of the `lockbox_restore.pl` script to the `/home/admin/` directory on the Avamar server in the Cyber Recovery vault by typing the following command:

```
curl -O ftp://avamar_ftp:anonymous@ftp.avamar.com/software/scripts/lockbox_restore.pl
```

NOTE: If the link in the command does not work, see Knowledge Base Article 181972 for up-to-date information. Access to this document depends on your login credentials. If you do not have access to the document, contact your Dell Technologies representative.

  The `admin` user must own the script.
- You have the required credentials:

Table 32. Required credentials for an Avamar recovery

Component	Description
Application	Login credentials for PuTTY and Avamar
Avamar	The admin and root user accounts, which might be stored on a specific system or in a document
DD Boost	Avamar DD Boost user id and password on the Cyber Recovery vault
Cyber Recovery username	**`cradmin`**

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 procedure.

Steps

1. Use PuTTY to log in to the Avamar server as the `admin` user.
2. Stop the Avamar services by typing the following command:

```
dpnctl stop all
```

   Answer **Yes** to the query about shutting down the local instance of EM Tomcat.
3. Confirm that the services are stopped properly by typing the following command:

```
dpnctl status
```

4. Switch to the Avamar `root` user by typing the following command:

```
su -
```

5. Verify that the IP address of the vault DD system resolves to the production DD name by typing the following command:

CAUTION: This step is critical for performing the recovery. This step ensures that the Avamar server can connect to the vault DD system and perceives it as the production DD system in the vault.

```
cat /etc/hosts
```

The following example shows sample output:

```
# 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
```

In the preceding example, `ddve-prod-05` is the name of the production DD system and 192.168.2.106 is the IP address of the vault DD system (also known as `ddve-cr-06`). Both the DD FQDNs and short names are assigned to the 192.168.2.106 IP address.

NOTE: The following FQDN names are used in examples throughout the rest of this document:

- *<Production_DD-FQDN>*: **ddve-prod-05.vcorp.local**
- *<Production_Stager_Avamar-FQDN>*: **ave-03.vcorp.local**

Modify the Avamar `/etc/hosts` file on the Cyber Recovery vault for both Avamar and Data Domain, as needed.

6. As the `root` user, run a checkpoint restore operation using the `hfsctime` noted during the recovery sandbox process and using the following syntax:

```
cprestore --hfsctime=<hfsctime> --ddr-server=<Production_DD-FQDN> --ddr-user=<ddboost user name>
```

For example:

```
# cprestore --hfsctime=1560177494 --ddr-server=ddve-05.vcorp.local --ddr-user=ddboost
```

7. When prompted, enter the DD Boost user password.
A list of available checkpoints that can be used to restore is displayed. The checkpoint at the bottom of the list is the most recent checkpoint.
8. Enter the name of the checkpoint that you want to restore, for example `cp.20211216090102`, ensuring that the name is exact. Press Enter and when prompted, type `yes` to confirm your entry.

NOTE: This step might take some time as it is copying data from the vault DD system to the staging Avamar server to perform the recovery steps. Press Enter every few minutes in the PuTTY window to avoid timing out.

9. When the checkpoint restore operation completes, enter the DD Boost user password when you are prompted for a password.
10. Switch to the Avamar `admin` user by typing the following command:

```
su - admin
```

11. Start the Avamar rollback procedure using the same checkpoint name as the checkpoint name that you selected for the checkpoint restore operation by typing the following command:

```
rollback.dpn --cptag=cp.20211216090102 --noddrollback --nogetserverlogs 2>&1 | tee -a
rollback.out
```

This step can take some time. When it is completed, it displays the output of the `status.dpn` command.

12. As the `admin` user, list the hostname of the Avamar server by typing the following command:

```
hostname -f
```

13. Begin the rollback of the MCS services by typing the following command:

```
mcserver.sh --restore --norestart --v 2>&1 |tee -a mcs_restore.out
```

When prompted, enter **Y** to proceed with the restore, enter the *<Production_Stager_Avamar-FQDN>* obtained from the `hostname -f` command; press Enter for port 27000.

14. Switch to the Avamar `root` user by typing the following command:

```
su -
```

15. Run the `lockbox_restore.pl` script by typing the following command and then answering **yes** to all the prompts:

```
/home/admin/lockbox_restore.pl
```

NOTE: If an error is displayed for the lockbox, type **yes** to proceed and then provide the correct operating system password for the `admin` user.

The following example shows sample output:

```
Sample run updating "admin": (Note - this run entered a BAD password the first time.
Second time was successful):

Your keystore contains 4 entries
Keystore certs: [mcectls, Nov 10, 2021] [mcrsatls, Nov 10, 2021] [mcecroot, Nov 10,
2021] [mcrsaroot, Nov 10, 2021]
DEBUG: Checking lockbox 'admin' key...
Sorry, try again.
Sorry, try again.
sudo: 3 incorrect password attempts
ERROR: 'sudo -A' failed. Error=256
        This indicates a problem with the 'admin' password stored in the lockbox.
        This will cause downstream problems with MCS startup.

Lockbox verification FAILED for admin. Proceed ?
  Enter `yes`<enter> to proceed, `q` to quit :yes
[LOCKBOX] Enter New lockbox entry for 'admin':*********
>>Backup lockbox file
>>Backup keystore files
>>Backup SSV files
>>Flush backup
>>Local backup dir: /usr/local/avamar/src/lockbox_backup/2022-05-24-20_33
>>Flush backup dir: /usr/local/avamar/var/mc/server_data/lockbox_backup
>>Updated with new value under name "admin".
>>Backup lockbox file
>>Backup keystore files
>>Backup SSV files
>>Flush backup
>>Local backup dir: /usr/local/avamar/src/lockbox_backup/2022-05-24-20_33
>>Flush backup dir: /usr/local/avamar/var/mc/server_data/lockbox_backup

Sorry, try again.
Sorry, try again.
sudo: 3 incorrect password attempts
ERROR: 'sudo -A' failed. Error=256
        This indicates a problem with the 'admin' password stored in the lockbox.
        This will cause downstream problems with MCS startup.

Lockbox verification FAILED for admin. Proceed ?
  Enter `yes`<enter> to proceed, `q` to quit :yes
[LOCKBOX] Enter New lockbox entry for 'admin':**************
>>Backup lockbox file
>>Backup keystore files
>>Backup SSV files
```

```
>>Flush backup
>>Local backup dir: /usr/local/avamar/src/lockbox_backup/2022-05-24-20_33
>>Flush backup dir: /usr/local/avamar/var/mc/server_data/lockbox_backup
>>Updated with new value under name "admin".
>>Backup lockbox file
>>Backup keystore files
>>Backup SSV files
>>Flush backup
>>Local backup dir: /usr/local/avamar/src/lockbox_backup/2022-05-24-20_33
>>Flush backup dir: /usr/local/avamar/var/mc/server_data/lockbox_backup

DEBUG: Avagent   version:     19.4.100-116
DEBUG: Avagent   OS version:  SLES-64
```

16. Switch to the Avamar `admin` user by typing the following command:

```
su - admin
```

17. Start the MCS by typing the following command:

```
mcserver.sh --start --v 2>&1 |tee -a mcs_start.out
```

18. Verify the services are up and running by typing the following command:

```
dpnctl status
```

19. Start any subsystems that are stopped by typing the following command:

```
dpnctl start <subsystem>
```

NOTE: Leave the scheduler and maintenance processes as `down`.

20. Do the following;
    a. Ensure that `emt` is started by typing the following command:

    ```
    dpnctl start emt
    ```

    b. Ensure that `ddrmaint-service` is started by typing the following command:

    ```
    dpnctl start ddrmaint-service
    ```

21. Switch to the Avamar `root` user by typing the following command:

```
su -
```

22. Add the SSH key for the Data Domain FQDN, using the following syntax:

```
cat ~admin/.ssh/ddr_key.pub | ssh <ddboost_user>@<Production_DD-FQDN> adminaccess add
ssh-key
```

For example:

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

When prompted, enter the password for the DD Boost username.

23. As the `root` user, regenerate the certificates by typing the following command:

```
enable_secure_config.sh --certs
```

24. Verify the security settings by typing the following command.

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

The following example shows sample output:

```
# 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"
```

NOTE: If the value for the first two options is `false`, type **`enable_secure_config.sh --enable-secure-all`** and then type **`enable_secure_config.sh --showconfig`** to check the security settings again.

25. Switch to the Avamar `admin` user by typing the following command:

```
su - admin
```

26. Restart the MCS by typing the following command:

```
mcserver.sh --restart --v  2>&1 |tee -a mcs_start.out
```

Enter **`Y`** to proceed.

27. Edit the DD properties by typing the following command:

```
mccli dd edit --name=<Production_DD-FQDN>
```

28. Confirm the DD properties by typing the following command:

```
mccli dd show-prop --name=<Production_DD-FQDN>
```

This step takes several minutes as it edits the DD name in the MCS. When the step is completed, the DD *<Production_DD-FQDN>* is displayed in several lines.

29. Switch to the Avamar `root` user by typing the following command:

```
su -
```

30. Revoke the token access using the following syntax:

```
ssh cradmin@<Production_DD-FQDN> "ddboost user revoke token-access <ddboost username>"
```

For example:

```
# ssh sysadmin@ddve-prod-05.vcorp.local"ddboost user revoke token-accessddboostuser"
```

Enter the password for the sysadmin.

NOTE: This command can use the sysadmin or cradmin user to revoke the token access. The command output displays the following message:

```
Revoked token access for user <ddboost username>
```

31. As the `root` user, stop the Avamar Agent service by typing the following command:

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

32. Delete the Avamar Client ID (`cid.bin`) by typing the following two commands:

```
cd /usr/local/avamar/var/client

rm -f cid.bin
```

33. Switch to the Avamar `admin` user by typing the following command:

```
su - admin
```

34. Edit the client properties by typing the following two commands: :

```
hostname -f

mccli client edit --domain=/MC_SYSTEM --name=<Production_Stager_Avamar-FQDN> --
activated=false
```

35. Switch to the Avamar `root` user by typing the following command:

```
su -
```

36. Start the Avamar Agent service by typing the following command:

```
/etc/init.d/avagent start
```

37. Switch to the Avamar `admin` user by typing the following command:

```
 su - admin
```

38. To take a checkpoint and validate it, type the following five commands:

```
dpnctl start ddrmaint-service

dpnctl stop maint

mcserver.sh --flush

avmaint checkpoint --ava <Wait a few minutes while the checkpoint is being created.>

cplist --lscp <A new checkpoint is displayed based on the current date.>
```

39. To view a status, type the following two commands:

```
avmaint hfscheck --ava --full

watch -d -n5 'avmaint hfscheckstatus'
```

40. Restart the maintenance service by typing the following command:

```
dpnctl start maint
```

41. Log in to the Avamar UI using the MCUser on the Avamar host server (https://*<avamar-host>*/aui). From the left navigation pane, go to **Administration** > **System** and then select **Data Domain** on the right pane.
    a. Verify that the DD system is displayed in the main window.
    b. Verify that the data represented on the DD properties matches the data of the Avamar DD system. The icons that precede the entry must be green or at least amber.
    c. From the Avamar navigation menu options, verify that all the policies, clients, and other configuration items match those items of the production system.

42. Return to PuTTY to ensure that the hfscheck procedure is completed and the status is `complete`. Press Ctrl-c to exit PuTTY.
43. See Avamar's standard operating procedures to reactivate clients in the Cyber Recovery vault and perform the required application recoveries.

Next steps

Delete the recovery sandbox. See Cleaning up after an Avamar recovery.

Cleaning up after an Avamar recovery

After the all Avamar recoveries have completed fully, delete the sandbox.

About this task

NOTE: Deleting the sandbox prevents the Avamar application in the Cyber Recovery vault from accessing the respective Avamar MTree from the Cyber Recovery vault Data Domain system. Therefore, delete the sandbox only after all required recoveries have been completed.

Steps

1. Log in to the system as the `admin` user.
2. To verify that the services are still running from the client recovery operations by typing the following command:

```
dpnctl status
```

3. If the services are up, type the following command to bring them all down:

```
dpnctl stop all
```

4. Delete the recovery sandbox created during this recovery steps. Do the following:
   a. From the Main Menu, click **Recovery** > **Recovery Sandboxes**.
   b. Select the recovery sandbox.
   c. Click **Cleanup.**
5. Perform an Avamar rollback to the baseline checkpoint.
   See Knowledge Base Article Number 19397 for more detailed information.

Results

The system is ready for another recovery operation.

10

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. Only the admin and operator users can perform this task.

Also see the Dell Technologies PowerProtect Cyber Recovery Info Hub for white papers, blogs, and videos about performing recoveries.

Topics:

Recovering PowerProtect Data Manager data

Use a point-in-time (PIT) copy to rehydrate PowerProtect Data Manager data in the Cyber Recovery vault on an on-premises or AWS deployment.

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

NOTE: If your configuration includes multiple DD systems in the Cyber Recovery vault, you can perform concurrent PowerProtect Data Manager recoveries. For information about this configuration, see Replication PowerProtect Data Manager Backups to the Cyber Recovery Vault - A User Journey on the PowerProtect Cyber Recovery Info Hub. Follow the steps in this chapter to perform a PowerProtect Data Manager recovery.

If you perform a PowerProtect Data Manager automated recovery in the Cyber Recovery vault, the following engines are not recovered:

- Protection engine (NAS protection engine and TSDM data movers)
- Search engine (Used for file search capability and restore)
- Reporting engine (For backup reports)

The engines are separate VMs that PowerProtect Data Manager deploys in the production system. Because the hostname/IP address for the vault PowerProtect Data Manager system is different, the Cyber Recovery software cannot deploy these engines during recovery.

When you initiate a recovery, the Cyber Recovery software prepares your environment so that you can run a PowerProtect Data Manager restore 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.

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 the prerequisites for a PowerProtect Data Manager recovery

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

- To use the linked recovery feature, your deployment must be running PowerProtect Data Manager version 19.19.
- Note that the Cyber Recovery software supports recovery for a production deployment that is running PowerProtect Data Manager version 19.14 or later with multifactor authentication enabled.
- If your Cyber Recovery deployment is on Amazon Web Services (AWS), a vCenter server is not required.

  NOTE: See the *Dell PowerProtect Cyber Recovery AWS Deployment Guide* and the *Dell PowerProtect Cyber Recovery Azure Deployment Guide* for information about deploying and using the Cyber Recovery solution on AWS and Azure deployments.

- If only NFS v4 is enabled on the DD system in the Cyber Recovery vault, a PowerProtect Data Manager recovery fails. The PowerProtect Data Manager server DR only supports NFS v3. Either use DD Boost for the server DR MTree, or enable NFS v3 and NFS v4 on the DD system to ensure PowerProtect Data Manager recoveries succeed.
- See the following documentation, which is available at Dell Online 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 DDOS version 7.10, 7.13, or 8.x.
- Deploy the PowerProtect Data Manager appliance in the Cyber Recovery vault:
  - Only use the PowerProtect Data Manager appliance in the Cyber Recovery vault to perform recoveries.
  - Ensure that the version is the same as the version of the production system.
  - Note that the hostname and IP address of the PowerProtect Data Manager server in the Cyber Recovery vault do not have to match the hostname and IP address of the production PowerProtect Data Manager server.
  - 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 on the PowerProtect Data Manager appliance in the Cyber Recovery vault.
  - Because the application username and the application password of the PowerProtect Data Manager appliance in the Cyber Recovery vault must match the application username and the application password on the production system, ensure that they are the same. If the application username and the application password on the production system have changed, for example, due to a rotation policy, change the application username and the application password for the PowerProtect Data Manager appliance in the Cyber Recovery vault.

    NOTE: If the credentials of the production system change, the recovery procedure of the new Cyber Recovery copies uses the new credentials and the recovery procedure of the old Cyber Recovery copies uses the former credentials.

  - The host username is the operating system host administrator username for the admin account of the PowerProtect Data Manager server in the Cyber Recovery vault. The password for the operating system host administrator username does not need to match the production account password. The password can be anything that you choose. These credentials are used for the second phase of the recovery procedure to protect the restored data against potential attacks. After recovery, the admin and root accounts on the host server will use this password.
  - 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.
- For on-premises deployments, 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:

  `%, &, *, $, #, @, !, \, /, :, *, ?, ", <, >, [, ], |, ;, '`

- For the UIDs that are associated with the production policy MTrees, UIDs for those policy MTrees must be 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.

- For on-premises deployments, 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.
- For on-premises deployments, 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.

  NOTE: To recover a backup application from a Cyber Recovery copy properly, ensure that your replication window start time is after the application backup on the production system is completed, including the required metadata backup. For an intermediate replication on the production system, ensure that the intermediate replication start time is also after the production backup completion time.

- If you recover from a DM 5500 appliance:
  - Create a Cyber Recovery policy with the `PPDM` type from the DM 5500 backup.
  - After you recover the PowerProtect Data Manager in the Cyber Recovery UI, use these credentials to log in to the PowerProtect Data Manager UI: `admin/Abcd!2345`.

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

- You are logged in as the admin or operator user.
- You have met all the prerequisites that are listed in Meeting prerequisites for a PowerProtect Data Manager recovery.
- If you want to use the linked recovery feature, the production server and the Cyber Recovery vault must be running PowerProtect Data Manager version 19.19.

About this task

You can recover a single copy, use the linked recovery feature to select multiple copies and recover all those copies simultaneously, or use the linked recovery feature to select additional copies to recover to a previously recovered PowerProtect Data Manager application.

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.
- 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.

Steps

1. Select **Recovery** from the Main Menu.
   The contents of the **Copies** tab are displayed, and the **Application** button is enabled.
2. Optionally, select either a hierarchical or list view by clicking:
   -  for a hierarchical view that shows the policies and their associated copies
   -  for a list view of the copies
3. If you want to enable the **Sandbox**, **Alternate Recovery**, and **Recovery Check** buttons that are disabled by default, select a copy.
   The **Application** button is disabled. To reenable the **Application** button, click **Clear Selected** next to the policy name.
4. To initiate the recovery, click **Application**.

The **Application Recovery** pane opens and provides a drop-down list of the PowerProtect Data Manager applications that you can use for a recovery.

5. Select a PowerProtect Data Manager application host from the **Application Host** drop-down list.
6. From the list of PowerProtect Data Manager production host names, click  to open the list of policies with the copies that you can recover to the production PowerProtect Data Manager system.
7. Click  to open the list of copies associated with each policy.
8. Start the recovery on an unrecovered PowerProtect Data Manager application by performing one of these steps:
   - Select a single copy and click **Apply**.

     This step initiates a full recovery job (`recoverappPPDM`). The job creates a sandbox, and then the full recovery is completed.

     NOTE: If this is the first copy selection using a PowerProtect Data Manager version 19.19 application in the Cyber Recovery vault, then only version 19.19 copies are available for selection. Copies that were created pre- Cyber Recovery version 19.19 do not have a copy version and are not available for selection with a PowerProtect Data Manager version 19.19 application in the Cyber Recovery vault.

   - Select multiple copies that you want to recover and click **Apply**.

     This step initiates a full recovery job (`recoverappPPDM`) using the latest copy that is associated with the policy and also associated linked recovery jobs (`linked-recoverapp`) using the latest copy available across all selected copies. The linked recovery jobs create corresponding sandboxes and then proceed after the full recovery is completed.

   - If there are multiple copies that are associated with various policies and you want to recover only the latest copies, swipe the **Select Latest Copies** slider to the left and click **Apply**. The linked recovery jobs create corresponding boxes and then proceed after the full recovery is completed.

   NOTE: A one-to-many configuration, in which the copies are replicated from one production DD system to two Cyber Recovery vault DD systems, is not supported. Therefore, when you select one copy on one Cyber Recovery vault DD system, the copy on the other Cyber Recovery vault DD system is disabled and cannot be selected for recovery. This event occurs because both copies have storage units that have the same DD source but a different DD destination. The **Select Latest Copies** option is also disabled. You can recover the copies that you cannot select by using a different PowerProtect Data Manager application in the Cyber Recovery vault.

   In the **Application Recovery** pane, the policy and the corresponding copy that was used for a full recovery show the **Recovery in Progress** status. The policies and corresponding copies that are used for a linked recovery show the **Linked Recovery in Progress** status. When the recovery is completed successfully and if the associated sandbox that was created during the recovery has not been deleted, the status is **In Active Recovery**.

   The recovery and linked recovery jobs create recovery sandboxes, populate them with the selected copies, and then make the sandboxes available to the application host.
9. Start additional recoveries on a previously recovered PowerProtect Data Manager vault application by selecting one or more additional copies for recovery.

   The additional copy selections are linked recoveries.

   NOTE: A one-to-many configuration, in which the copies are replicated from one production DD system to two Cyber Recovery vault DD systems, is not supported. Therefore, when you select one copy on one Cyber Recovery vault DD system, the copy on the other Cyber Recovery vault DD system is disabled and cannot be selected for recovery. This event occurs because both copies have storage units that have the same DD source but a different DD destination. The **Select Latest Copies** option is also disabled. You can recover the copies that you cannot select by using a different PowerProtect Data Manager application in the Cyber Recovery vault.

10. During the recovery process, note that if:
    - The full recovery is completed successfully, all the associated linked recovery jobs are also completed successfully.
    - The full recoveryfails, all the associated linked recovery jobs also fail. The sandboxes that were created remain.
    - If you cancel the full recovery, all the associated linked recovery jobs are also canceled. The sandboxes that were created are deleted. There is a sandbox delete job for each linked recovery job.
    - If you cancel the linked recovery job, the sandbox that was created is deleted.
    - If you start a linked recovery while the full recovery is canceling, the linked recovery job is canceled. The sandboxes are deleted.

11. 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. It then 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.
12. Wait for the recovery job to complete.
    A recovery sandbox is created for the PowerProtect Data Manager application.
13. 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** and confirm that you want 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.

Results

The latest PowerProtect Data Manager configuration is recovered.

NOTE: Before you can run another recovery job using PowerProtect Data Manager application *x*, clean up the application by running a delete operation on the recovery sandbox associated with PowerProtect Data Manager application *x*.

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.

Prerequisites

You are logged in as the admin or operator user.

About this task

When the Cyber Recovery software completes a recovery check action, the copy's status is marked as recoverable or failed. Also, the sandboxes and DD Boost storage units are deleted. The Cyber Recovery software reverts PowerProtect Data Manager back to its initial state from which you can run a recovery.

Steps

1. To schedule a recovery check:
    a. Select **Policies** from the Main Menu.
    b. Click **Schedules**.
    c. Click **Add** to open the Add Schedule wizard.
    d. On the **Schedule Information** page, complete the following fields and then click **Next**:

Table 33. Schedule Information page

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

Table 33. Schedule Information page (continued)

Field	Description
Action	Select the **Recovery Check**.
Application Host	Select the PowerProtect Data Manager host.

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

Table 34. Scheduling page

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

f. 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.

2. To 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, use the Cyber Recovery UI or the CRCLI to delete one sandbox, multiple sandboxes, or all sandboxes and the DD Boost storage unit. When all the sandboxes are deleted, the Cyber Recovery software reverts the PowerProtect Data Manager software to the snapshot that was created when you initiated the recovery.

Prerequisites

- You are logged in as the admin or operator user.
- To use the linked recovery feature, your deployment must be running PowerProtect Data Manager version 19.19.

Steps

1. Delete the recovery sandboxes that were 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. Optionally, select a view by clicking:
-  for a hierarchical view that shows the hosts and their associated sandboxes
-  for a list view of all the sandboxes

c. To delete a single sandbox that is associated with a host, select the sandbox and click **Cleanup** > **Continue**.
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.

d. To delete multiple sandboxes for a host with several associated sandboxes but not revert the system, select the sandboxes, ensure that one sandbox remains, and then click **Cleanup** > **Continue**.

   The selected sandboxes are deleted, and the system is not reverted. To confirm that the system remains the same, click  to access PowerProtect Data Manager.

   When you are ready to revert the system, select the remaining sandbox and click **Cleanup** > **Continue**.

e. To delete all sandboxes associated with a host simultaneously, select the host to select all the associated sandboxes and click **Cleanup** > **Continue**.

   The software uses one of the cleanup jobs to revert the system and simply deletes the remaining sandboxes.

   When a sandbox for a successfully completed full recovery is deleted, the status is **Recoverable**. If the sandbox cleanup fails, the status is **Unknown**.

2. Wait for approximately 10 minutes after the PowerProtect Data Manager recovery cleanup for the PowerProtect Data Manager VM rollback and PowerProtect Data Manager services to come up.

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. Do not click the alert to enable the services.

2. If the recovered PowerProtect Data Manager IP address or FQDN is the same as the production PowerProtect Data Manager system, you can perform centralized restore and recovery of an application directly without manual intervention.
3. If the recovered PowerProtect Data Manager IP address or FQDN is not the same as on the production PowerProtect Data Manager system, verify the recovery for SQL, Oracle, and file system workloads:
   - 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. Approve the host in PowerProtect Data Manager. From the PowerProtect Data Manager Main Menu, go to **Infrastructure** > **Application Agents**.
     f. Run a manual agent discovery.
     g. 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.sh` command to unregister the agent.
     c. If necessary, delete the ssl folder from the Agent Service folder.
     d. Run the `register.sh` 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 app aware system workloads:
  a. Remove the asset from the policy in the PowerProtect Data Manager system in the Cyber Recovery vault.

     The policy runs an **Unconfiguring** job.

  b. Uninstall the Microsoft application agent and the VM direct agent from the host, and delete the DPSAPPS and EMC folder from the host.
  c. Add the asset to the policy and wait for the configuration to complete.
  d. Run an on-demand asset source discovery.
  e. Perform a Restore operation.

11

Administration

This section describes Cyber Recovery administrative tasks.

Topics:

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). Your user role determines which tasks that you can perform.

Manually securing and releasing the Cyber Recovery vault

If you suspect a security breach, manually secure the Cyber Recovery vault.

Prerequisites

- To secure the Cyber Recovery vault, you are logged in as the security officer, admin, or operator user.
- To release (unsecure) the Cyber Recovery vault, you are logged in as the security officer.

About this task

When you secure the Cyber Recovery vault, the Cyber Recovery software performs no replication operations. Only when you are confident that there is no longer a security threat, a security officer can release the Cyber Recovery vault.

NOTE: For more information about the Cyber Recovery vault status, see Monitoring the CR Vault status.

Steps

1. From the dashboard, go to the **Status** tile.
2. 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. A timer indicates the length of time that the Cyber Recovery vault is secured. The Cyber Recovery software issues an alert that provides additional information and identifies which user secured the Cyber Recovery vault.
3. (Security officer only) If you are confident that there is no longer a security threat, click **Release Vault** to unsecure the vault.
   The Cyber Recovery vault status returns to **Locked**. Sync policy operations can now be initiated. The Cyber Recovery software issues an alert that provides additional information and identifies which user released the Cyber Recovery vault.

Configuring and managing users

Only a security officer manages other user's accounts.

The security officer can:

- View all users' account details.
- Create dashboard, admin, operator, and other security officer users.
- Modify dashboard, admin, operator, and other security officer users.
- Enable and disable users.
- Disable multifactor authentication for security officer, admin, and operator users, but not enable multifactor authentication.
- Delete dashboard, admin, operator, and other security officer users.
- Set the password policy for all users.

NOTE: Security officer, admin, and operator users can click

on the Masthead Navigation and then click:

- **Change Password** to reset their password.

  NOTE: An admin or operator user cannot reset the password more than once every 24 hours. Contact the security officer to modify the password.

- **Multifactor Authentication** to enable multifactor authentication.

Admin and operator users can also click **User Details** to view their settings and test email.

Managing users

Add and modify all user accounts except the crso user.

Prerequisites

You are logged in as the security officer.

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 35. User fields

Field	Description
Name fields (optional)	Specify the user's first name and last name.
Role	Select either:

Table 35. User fields (continued)

Field	Description
	• Security officer—Enables users to create and manage user accounts, set the password policy, configure mail server settings, monitor alerts, secure and release the Cyber Recovery vault, manage support settings, and configure the number of login sessions. • Admin—Enables users to perform tasks and operations in the Cyber Recovery UI, monitor alerts, secure the Cyber Recovery vault, generate reports, and manage maintenance, disaster recovery backup, and support settings. • Operator—Enables users to view and export information, secure the Cyber Recovery vault, perform limited tasks and operation in the Cyber Recovery UI, and generate support bundles. • Dashboard—Enables users to view the Cyber Recovery dashboard but not perform tasks. The dashboard role does not time out.
User Name	Specify a username. **NOTE:** • The username is case insensitive. For example, if you add the username **admin**, you cannot add another username such as **ADMIN**, **Admin**, **ADMin**, or any other combination, The software displays an error message. Enter a unique username. • You cannot reuse the username of a deleted user.
Phone (optional)	Specify the user's telephone number.
Email	Specify an email address for alert notifications. If the Cyber Recovery software is configured to send email messages, configured recipients can receive the messages. **NOTE:** Later, if a user's email is modified, the 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	Specify and confirm the password. The default password requirements include: • 9–64 characters. • At least 1 numeric character. • At least 1 uppercase letter. • At least 1 lowercase letter. • At least 1 special character (**~!@#$%^&*()+={}|:";<>?[]-_.,^'**). **NOTE:** For this release, do not use the colon (:) in the Postgres database password. The password policy that the security officer sets defines the number of characters that are required. The password policy also checks if the new password matches previous passwords or if the password includes the username. While you enter the password, a tooltip is displayed and verifies that the entries follow password rules and policy. When you change a password, enter and confirm both the new and existing passwords.
Force Password Change (optional)	When adding a user only, select the checkbox to force the user to change the password when logging in for the first time.
Session Timeout	Change the amount of idle time after which the user is logged out of the Cyber Recovery UI. The default value is 10 minutes.

4. Click **Save**.
   The **Users** table lists the Cyber Recovery users.
5. Click a user's row to open the details pane and view additional details about the user, and then:
   a. Click  to close the details pane.
   b. Click  to open the details pane again.
6. To customize the columns in the table that lists the Cyber Recovery users, click  and select the columns to show or hide.

7. Disable or enable a user:
   a. To disable a user account so that a user cannot log in, swipe left on the slider under **Enabled**. An informational message confirms that the user has been disabled and the **Edit** button is inactive. Also, an event is created.
   b. To sort users by status, click **Enabled**.
   c. To filter on status, click and then click the **Enabled** or **Disabled** checkbox. Only the users with the selected status are displayed. If you select both checkboxes, all users are displayed.
   d. To reenable a user, swipe right on the slider under **Enabled**. An informational message confirms that the user has been reenabled and the **Edit** button is active. Also, an event is created.

   You cannot disable the crso, which is the security officer that the installation procedure created for the initial Cyber Recovery installation. The slider for the crso is disabled.

Disabling multifactor authentication

Disable multifactor authentication for any user account, except the crso user account.

Prerequisites

You must be logged in as the security officer.

About this task

Users must enable multifactor authentication for their own accounts; a security officer cannot enable multifactor authentication for other users. Multifactor authentication is not available to dashboard users.

NOTE: Security officer, admin, and operator users, if they can log in, can disable multifactor authentication for their own accounts by using the slider in the **Multifactor Authentication** window. See Enabling multifactor authentication.

Steps

1. Select **Administration** > **Users** from the Main Menu.
2. Select the user.
3. Click **Disable MFA**.
   The security officer, admin, or operator users, whose multifactor authentication is disabled, receive an email message that indicates that multifactor authentication is disabled. When any user whose multifactor authentication is disabled by the crso logs in, the slider in the **Setup Multifactor Authentication** window is set to the disabled position.

Deleting users

Delete dashboard, operator, admin, and other security officer user accounts.

Prerequisites

You are logged in as the security officer.

About this task

NOTE: The crso user account, which was created at initial installation, cannot be deleted.

Steps

1. Select **Administration** > **Users** from the Main Menu.
2. Select a user.
   The **Delete** button becomes active.
3. Click **Delete** and confirm that you want to delete the user.
   A message indicates that the user is deleted, and an alert is generated. The **Details** pane for the alert adds `zzz` to the username to indicate that the user has been deleted, for example, `zzz<username>`.

   NOTE: You cannot reuse the username of a deleted user when you add a new user.

Setting password policy

Manage and view the password requirements to enhance protection and prevent unauthorized access.

Prerequisites

You must be logged in as the security officer.

About this task

NOTE: The password policy applies to all users. You cannot set a password policy for an individual user.

Steps

1. Select **Administration** > **Users** from the Main Menu.
2. Click **Settings**.

   The **Password Policy** window opens.
3. If necessary, in the **Password Expiration** field, modify the number of days after which passwords expire and users must change their passwords. The default value is 60 days.

   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.

   If mail server support is enabled and a user's configuration allows alert notifications, the user also receives 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.
4. If necessary, in the **Password Length** field, modify the password length. The default value is the minimum value of 9 characters.
5. If necessary, in the **Password History Count** field, modify the number of previous passwords to check if the new password has already been used. The default value is 1 password, the minimum value is 1, and the maximum value is 24.

   For example, if you set the history password count to 4, the check compares the current password to the three prior passwords.
6. Optionally, enable the **Restrict the inclusion of username in the passwords** option.
   This option checks if the username includes the password.
7. Click **Save**.

Results

- An event indicates that the password policy has been modified.
- When the password policy changes and a user's existing password does not comply with the password policy, a warning message is displayed when the user logs in. The warning message provides a link to the **Change Password** window so that the user can change the password. Users cannot dismiss this warning message until they change their password to comply with the password policy.

  NOTE: The error message is displayed for dashboard users, but there is no link. Dashboard users must contact the security officer to change the password.

Resetting Cyber Recovery passwords

For security purposes, use the `crsetup.sh` command to change the Cyber Recovery lockbox passphrase and the Cyber Recovery database password. If you forget the crso password, you can also use the command to change the crso password.

Prerequisites

- You must provide the lockbox passphrase, which is created during the Cyber Recovery installation.

NOTE: If you forget the lockbox passphrase, it cannot be recovered. You must reinstall the Cyber Recovery software or redeploy the Cyber Recovery virtual appliance.

- 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.
- Use the `crsetup.sh` command if you forget the crso password. Otherwise, log in to the Cyber Recovery UI or CRCLI as the crso user and change the password.
- The password policy that the security officer set applies to this scenario.
- Cyber Recovery microservices communicate with the Postgres 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 crso, 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 crso, use the `crsetup.sh` command.

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**, go to the next step.
   - If you type **n**, go to step 6.
5. When prompted, enter the Postgres password.
   The Cyber Recovery software creates a DR backup.
6. When prompted, enter **y** to continue the procedure.
   The command 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 command then displays the prompt to change the Postgres password.
9. Optionally, enter and confirm the new database password when prompted.
   If you choose not to change the Postgres database password, the command 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 command 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 crso) had multifactor authentication enabled, it is disabled when the services start again. Re-enable multifactor authentication.

Managing login sessions

Set the number of maximum simultaneous login sessions.

Prerequisites

You are logged in as the security officer.

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, click  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
   - Operator—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, operator, and dashboard users are five sessions

Configuring mail server support

If your configuration allows email to leave the Cyber Recovery vault, enable and configure mail server support.

From the Cyber Recovery UI, configure the mail server settings for an external mail service or a Postfix email service.

For more information, see:

- Mail server certificates
- Configuring mail settings
- Configuring the Postfix email service

If you want to separate mail and management traffic on your Cyber Recovery virtual appliance deployment, you can add a second virtual Ethernet adapter to configure a separate IP address for SMTP communication. For more information, see the *Dell PowerProtect Cyber Recovery Installation Guide*.

Mail server certificates

For configurations with Transport Layer Security (TLS) enabled, mail server certificates provide an added level of security to your email messages.

If TLS is enabled, you must accept the mail server certificate to be able to send email messages. If you choose to disable TLS, acceptance of the mail server certificate is not required.

NOTE: Disabling TLS is not recommended as all email communication is in cleartext form.

The Cyber Recovery software retrieves the mail server certificate from the mail server that you identify when you configure mail settings. The **Mail Settings** window enables you to view and manage the mail server certificate that is in use. Options enable you to:

- Ensure that the Subject Alternative Name field in the mail server certificate includes either the IP address or DNS of the email server:

The Subject Alternative Name field must include the hostname or IP address of the email server that you used to configure the Cyber Recovery mail server settings.

- View the current mail server certificate information and determine specified field values
- Verify that the mail server certificate is available from the specified mail server and then add it to your configuration
- Renew a mail server certificate that is about to expire

If the mail server certificate is missing after an update, the Cyber Recovery software generates an alert and displays a red banner in the Cyber Recovery UI. You must then configure the mail settings to add it.

The behavior for a first-time software installation and a software update differs:

- When you perform a fresh Cyber Recovery software installation, TLS is enabled by default. From the **Mail Settings** window, you must verify and accept the mail server certificate to add it to your configuration.
- When you update your Cyber Recovery deployment that has TLS enabled, at login, a critical banner in the Cyber Recovery UI indicates that the mail server certificate is missing. Click the link in the banner to go to the **Mail Settings** window so that you can add the mail server certificate. The Cyber Recovery software also generates a critical alert, which is displayed every seven days until you add the mail server certificate.

NOTE: After an update, you can continue to send email messages without a mail server certificate. The software continues to display the critical banner and generates the critical alert until you add a certificate.

When a mail server certificate is about to expire:

- At 30 days before the mail server certificate expires, you receive a warning alert every seven days until you add a valid mail server certificate.
- At three days before the mail server certificate expires, you receive a critical alert.
- At 24 hours before the mail server certificate expires, you receive a critical alert.

NOTE: If you restart the Cyber Recovery services, the software resets the counter for the alerts. For example, if you received a warning alert and then restart services, you receive another warning alert even if seven days have not passed. The counter is reset to generate an alert every seven days.

When the certificate expires, you receive a final critical alert. You can no longer send email messages.

NOTE: If the mail server uses a certificate chain, the expiration of the root or intermediate certificate generates an alert. The monitoring service checks if the leaf certificate is expired or is nearing expiration and updates it automatically. However, if the mail server only uses a leaf certificate and there is no intermediate certificate, then an alert is generated when the leaf certificate expires.

Configure mail settings

After you have configured an email server in the Cyber Recovery vault, enable mail server support to route and deliver Cyber Recovery email notifications to Cyber Recovery users, and set restricted domains for email addresses for users and the reporting feature.

Prerequisites

You are logged in as the security officer.

About this task

The email service supports Transport Layer Security (TLS) 1.2 or TLS 1.3. If TLS is disabled, all email communication is sent in clear text. We recommend that you enable TLS, which also requires that you to use a mail server certificate, to prevent vulnerabilities. For more information, see Mail server certificates.

Steps

1. From the masthead navigation, click  to access the **System Settings** list.
2. Click **Support** > **Mail Settings**.

3. Under **Activate Mail Support**, swipe right on the slider to enable sending email notifications.

   If this option is disabled, you cannot modify the mail server configuration.

   NOTE: When you update to Cyber Recovery version 19.16 and later, the procedure checks if you are using an external mail service or Postfix. If neither is used, then the email option is disabled by default.

   The pane opens to display more options to activate mail support.
4. Under **Mail Server Settings**, swipe right on the slider to enable TLS, if necessary.

   NOTE: When you install the Cyber Recovery software, TLS is enabled by default.

   If you enable TLS for a relay server from the Cyber Recovery environment, only the inbound communication to the relay server is encrypted. To configure end-to-end encryption, ensure that you enable TLS for outbound connections from the relay server. For information about how to view message headers to verify TLS encryption, see Verifying TLS encryption.
5. Perform the tasks for each field that are described in the following table:

Table 36. Mail server settings fields

Field	Description
Mail/Relay Server (required)	Specify the hostname or IP address of the Cyber Recovery email server or the Postfix server.
Port (required)	Specify a port number. The default port number is 25.
Certificate (required if TLS is enabled)	Do one of the following: • If the mail server certificate is in place, click **View Certificate** to see general and detailed certificate information. From the **Details** tab, you can see the certificate hierarchy and view the certificate field details of all the certificates in the chain. From the **Certificate Fields** section under the **Details** tab, click the radio button next to a field to see the field value for the specified field. • If the mail server certificate is not in place, click **Verify** and then: a. Click the **Accept** check box at the bottom left. b. Click **Done**. c. Click **Save**. • To renew a mail certificate that is about to expire, click **Change**. Then, click **Verify** and: a. Click the **Accept** check box at the bottom left. b. Click **Done**. c. Click **Save**.
Sender's Email Address (required)	Specify the email address that delivers Cyber Recovery alert messages. The default value is `noreply@cyberrecovery`. **NOTE:** The delivered email displays the first part of the email address. For example, if the sender's email address is `CyberRecovery@acme.com`, the email message shows that it is from `CyberRecovery`.
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. **NOTE:** If a password is required for authentication and TLS is disabled, the email message is not sent and you receive an error message that indicates the connection is unencrypted.

6. Optionally, under **Domain Restrictions**, set restricted domains for user email and for the report feature:
   a. Swipe right on the slider to enable domain restrictions.
   b. In the **Allowed Domains** field, enter the allowed domains.

      You cannot add a duplicate domain name.
   c. To delete a domain, click the **X** next to the domain name.
   d. Click **Save**.

If domain restrictions are enabled, an error message is displayed if you enter an email address that is not allowed to add a user or for an analysis report. When a report schedule runs, a critical alert indicates that the report schedule includes email addresses with restricted domains.

7. Click **Save**.

Verifying TLS encryption

Verify that the mail/relay server is encrypted with Transport Layer Security (TLS).

About this task

To verify that delivered email messages have end-to-end encryption, see the email message headers.

NOTE: The following steps are for retrieving the message headers to verify TLS encryption using Outlook. The procedure for other applications differs. See the application documentation for information about how to retrieve message headers.

Steps

1. From Outlook, double-click an email message.
2. Click **File** > **Properties**.
3. See the **Internet headers** box.

   The information includes messages about the servers that delivered the email message. By looking at the `Received` header, you can see that the servers are enabled to use TLS encryption. The email messages from the sender's email server to the recipient's email server are protected during the transfer.

Message headers

The following examples show message headers that verify that TLS encryption was used:

```
 Received: from XXX.XXX.prod.outlook.com(2603:10b6:907::26) by XXX.XXX.prod.outlook.com
(2603:10b6:208:276::21) with Microsoft SMTP Server(version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6977.29; Mon, 13 Nov 2023
18:38:38
+0000
```

```
 Received: from XXX.XXX.prod.outlook.com
(2603:10b6:907:0:cafe::73) by XXX.XXX.outlook.office365.com
(2603:10b6:907::26) with Microsoft SMTP Server
(version=TLS1_2,cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6977.31 via
Frontend Transport; Mon, 13 Nov
2023 18:38:37 +0000
```

```
 Received: from XXX.XX.XX.com (XXX.XXX.XX.XX) by XXX.mail.protection.outlook.com
(XX.XXX.XXX.XXX) with Microsoft
SMTP Server (version=TLS1_2,cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7025.0
via Frontend Transport; Mon, 13 Nov
2023 18:38:37 +0000
```

Configuring the Postfix email service

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

Prerequisites

- You must be knowledgeable about Postfix.
- If you plan to add an extra virtual Ethernet adapter on the Cyber Recovery virtual appliance, see the *Dell PowerProtect Cyber Recovery Installation Guide*.

About this task

If you use Postfix, set up the Postfix service on a Linux host. The following steps are an example for a minimum configuration. For more information about your specific Linux deployment, see the Postfix Documentation.

Steps

1. If your system has an active firewall, ensure that port 25 is open on the firewall. 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 host running the Postfix service:

```
# 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 host running the Postfix service>
```

   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 deafult_transport parameter.
#
 relayhost = <mail server name>
#
```

   d. If you receive a Relay Access denied message when sending email messages, check the `mynetworks` property and set it appropriately:

```
# TRUST AND RELAY CONTROL

# The mynetworks parameter specifies the list of "trusted" SMTP
# clients that have more privileges than "strangers".
#
# In particular, "trusted" SMTP clients are allowed to relay mail
# through Postfix.  See the smtpd_recipient_restrictions parameter
# in postconf(5).
#
# You can specify the list of "trusted" network addresses by hand
# or you can let Postfix do it for you (which is the default).
#
# By default (mynetworks_style = subnet), Postfix "trusts" SMTP
# clients in the same IP subnetworks as the local machine.
```

```
# On Linux, this works correctly only with interfaces specified
# with the "ifconfig" command.
#
# Specify "mynetworks_style = class" when Postfix should "trust" SMTP
# clients in the same IP class A/B/C networks as the local machine.
# Don't do this with a dialup site - it would cause Postfix to "trust"
# your entire provider's network.  Instead, specify an explicit
# mynetworks list by hand, as described below.
#
# Specify "mynetworks_style = host" when Postfix should "trust"
# only the local machine.
#
# mynetworks_style = class
# mynetworks_style = subnet
# mynetworks_style = host
# Alternatively, you can specify the mynetworks list by hand, in
# which case Postfix ignores the mynetworks_style setting.
#
# Specify an explicit list of network/netmask patterns, where the
# mask specifies the number of bits in the network part of a host
# address.
#
# You can also specify the absolute pathname of a pattern file instead
# of listing the patterns here. Specify type:table for table-based lookups
# (the value on the table right-hand side is not used).
#
  mynetworks = 168.100.189.0/28, 127.0.0.0/8
# mynetworks = $config_directory/mynetworks
# mynetworks = hash:/etc/postfix/network_table
```

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
```

Enabling TLS on Postfix

Enable TLS on Postfix for incoming and outgoing connections.

Steps

1. If you do not have a self-signed certificate to use for the Postfix service, generate a self-signed certificate by using the `openssl` command:

```
openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out cert.pem
```

   Ensure that you save the `key.pem` and the `cert.pem` files in a secure location.

2. To enable TLS for incoming connections, add the following lines to the `/etc/postfix/main.cf` file:

```
smtpd_tls_security_level = encrypt
smtpd_tls_cert_file = cert.pem
smtpd_tls_key_file = $smtpd_tls_cert_file
```

   The incoming connections are from the Cyber Recovery notifications container to the relay server.

3. To enable TLS for outgoing connections, add the following lines to the `/etc/postfix/main.cf` file:

```
smtp_tls_security_level = encrypt
smtp_tls_cert_file = cert.pem
smtp_tls_key_file = $smtp_tls_cert_file
```

   The outgoing connections are from the relay server to the relay host (which you set in step 2c that is shown in Configuring the Postfix email service).

4. Reload the Postfix configuration file:

```
# postfix reload
```

5. Stop and start Postfix:

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

6. Optionally, check the Postfix status:

```
# postfix status
```

Specifying which users receive alert notification email

Specify which users receive email notifications about alerts.

Prerequisites

- You are logged in as the security officer.
- Email support is enabled

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.

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
```

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` command to ensure that the Cyber Recovery software runs properly.

Prerequisites

You must have the lockbox password to enter at the `crsetup.sh` command 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` command:

```
# ./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.

Changing the network gateway on the Cyber Recovery server

Modify the network gateway on the Cyber Recovery server and then restart the Docker daemon.

About this task

You must restart the Docker daemon to propagate the network information into the Docker containers correctly.

Steps

1. Stop the Cyber Recovery services:

```
crsetup.sh --stop
```

2. Modify the gateway on the Cyber Recovery server:
   - Use YaST for a SUSE Linux Enterprise Server deployment
   - Use nmtui for a Red Hat Enterprise Linux deployment
3. Restart the network services:

```
service network restart
```

4. Restart the Docker daemon:

```
service docker restart
```

5. Start the Cyber Recovery services:

```
crsetup.sh --start
```

Updating the TLS security certificate

Update a TLS 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 a TLS security certificate with your own security certificate. For example, replace the TLS 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` command.
   b. At each prompt, either enter the information for your deployment or press Enter to omit the information and go to the next prompt.

      NOTE: You can omit the IP address and URI in the certificate. As a result, the resulting script does not expose the IP address or the URI.

   c. When prompted, confirm the information that you provided.
   d. Enter the lockbox passphrase.

   The script lists the DNS name of the Cyber Recovery management host, which is essential for the certificate. The script also lists the IP address and URI if you chose to enter them in step 2b.

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

   The `crsetup.sh` command 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:
   a. Copy the *<certificatename>*`.crt` file (returned by the CA) into any directory on the Cyber Recovery management host.
   b. Run the `crsetup.sh --addcustcert` command.
   The command stops the Docker container services.
   c. At the prompt, enter the full path where the *<certificatename>*`.crt` files is located.
   For example:

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

   d. Enter the lockbox passphrase.

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

Using the auditing feature

The auditing feature captures actions to a log file.

NOTE: Optionally, you can choose to send the application audit logs to a third-party Security Information and Event Management (SIEM) server securely. For more information, see Sending audit logs to a SIEM server .

The captured actions include:

- Log in (successfully or unsuccessfully)
- Log out
- Secure and release the Cyber Recovery vault
- Manage user accounts, including:
  - Creating, modifying, and deleting user accounts
  - Changing passwords
  - Enabling and disabling multifactor authentication
  - Updating user alert notifications
- Change the PostgreSQL and crso passwords, and the lockbox passphrase.

The audit information is captured in the `audit.log` and `audit_json.log` files that are stored in the *<CR-install-dir>*`/var/log/audit/` directory. Only root OS users can access the audit logs.

Audit log format

The audit log captures information about specific actions.

NOTE: The audit log does not include secrets or passwords, or any other sensitive information.

The following figure shows an example of an audit log:

```
[2025-02-26 08:19:29.830] [AUDIT] [users] [users.go:198 Login]
: {user='crso'; source_ip='10.x.x.x'; destination_ip='10.x.x.x';
object='{"userId":"67bded5cc90958155a16b036"}'; status='200'; http_headers='{Content-
Type='application/json; charset=UTF-8',Content-Length='43',Accept-Encoding='gzip',User-
Agent='go-resty/2.15.3 (https://github.com/go-resty/resty)',Accept='application/json;
charset=UTF-8',}'; event_type='Login'; event_id='ebd8e0be-6e03-47cc-7f1b-de8e3f45982c';
session_id='N/A'; severity='1'; executed_cmd='N/A'; additional_data='{"Info":"User crso
logged in"}';}
```

Table 37. Audit log fields

Field	Description
Time	Timestamp of the event
User	User name
Source IP	IP address from which the request was originated
Destination IP	IP address on which the request was received
Object	ID of the object that was changed
Status	HTTP status code of the request
HTTP headers	HTTP headers with all sensitive information removed
Event type	Unique operation or event type such as authentication event, storage event, and so on
Event ID	A randomly generated ID of the audit log event
Session ID	Not applicable
Severity	Severity of the log entry
Executed command	Not applicable
Additional data	Optional information that changes with each event type

NOTE: All sensitive information is removed from the audit logs, including sensitive information in the HTTP headers.

Sending audit logs to a SIEM server

The Cyber Recovery software can send application audit logs to an external third-party Security Information and Event Management (SIEM) server. The audit logs are sent to the SIEM server using Transport Layer Security (TLS) 1.2 or TLS 1.3, which ensures that the audit logs are encrypted.

These audit entries are found in the `audit.log` and `audit_json.log` files. When you generate a support bundle, it includes both these files. Only OS root users can access the audit logs.

To use the rsyslog feature to send audit logs, your deployment must include the following packages:

- For deployments running on SUSE Linux Enterprise Server:
  - `rsyslog`—A high-performance log processing system for Linux and UNIX systems. It is used for collecting, processing, and forwarding log messages.
  - `rsyslog-module-gtls`—A module for rsyslog that enables secure log transmission using the GnuTLS library.
- For deployments running on Red Hat Enterprise Linux:
  - `rsyslog`—A high-performance log processing system for Linux and UNIX systems. It is used for collecting, processing, and forwarding log messages.
  - `rsyslog-gnutls`—A module for rsyslog that enables secure log transmission using the GnuTLS library.

For a Cyber Recovery virtual appliance deployment, run the Cyber Recovery OS update to acquire these packages. For a Cyber Recovery software installation, install these packages on your system. If these packages are not installed in your deployment when you perform an installation or update, the precheck step displays a warning. However, you can continue the installation or update successfully but you cannot use the auditing feature.

NOTE: Before you perform a software update, always run the OS update first.

To verify that these packages are installed in your deployment, run the following commands:

- `./crsetup.sh --check` for a configuration check that validates that you have the correct installation requirements
- `./crsetup.sh --upgcheck` for a preupdate readiness check that confirms that you have the required software

For a Cyber Recovery virtual appliance deployment only, when you install Cyber Recovery version 19.19 or perform a software update, the `forwardAuditLogs.conf` file configuration file is copied into the `/etc/rsyslog.d` directory on your system. For a Cyber Recovery software installation, you must add the file manually. For information about using the `forwardAuditLogs.conf` file as a guide to add a configuration file manually on a Cyber Recovery software installation, see the Knowledge Base article on Dell Online Support.

Configuring for SIEM integration

Edit the `forwardAuditLogs.conf` configuration file on the Cyber Recovery virtual appliance to enable integration with SIEM. This file forwards the audit logs to the SIEM server.

Prerequisites

NOTE: For a Cyber Recovery virtual appliance deployment only, when you install Cyber Recovery version 19.19 or perform a software update, the `forwardAuditLogs.conf` file configuration file is copied into the `/etc/rsyslog.d` directory on your system. For a Cyber Recovery software installation, you must add the file manually. For information about using the `forwardAuditLogs.conf` file as a guide to add a configuration file manually on a Cyber Recovery software installation, see the Knowledge Base article on Dell Online Support.

Ensure that:

- Before you update the Cyber Recovery software, run the OS update first.
- Ensure that the required packages `rsyslog` and `rsyslog-module-gtls` packages are present on the Cyber Recovery virtual appliance. You can run the `./crsetup.sh --check` command to verify.
- You have configured the SIEM server to accept the Cyber Recovery application audit logs.
- If your Cyber Recovery virtual appliance deployment is running on a cloud environment, update the network security rules (also referred to as security groups for firewall rules) that are provided by your cloud service provider.

About this task

When you install or update the Cyber Recovery software, the `forwardAuditLogs.conf` file configuration file is copied into the `/etc/rsyslog.d` directory. You must edit this file to set up the Cyber Recovery virtual appliance to enable the rsyslog service for SIEM integration for sending the audit logs.

NOTE: If you check the rsyslog status before you run this procedure, an error message is displayed. After you complete it, there are no error messages.

Rsyslog global parameters can only be set once and cannot be reset. If a parameter is set multiple times, the behavior is unpredictable. The software adds global parameters in the `forwardAuditLogs.conf` configuration file that manage sending audit logs to the SIEM server. These global parameters include:

- `module(load="imfile")`
- `global(workDirectory="/var/spool/rsyslog")`
- `DefaultNetstreamDriverCAFile`
- `ActionSendStreamDriver`
- `ActionSendStreamDriver`

If you have other configuration files with those directives, account for this rsyslog behavior.

Steps

1. Go to the `/etc/rsyslog.d` directory and verify that it includes the `forwardAuditLogs.conf` file.
2. Uncomment the `target` and `port` lines in the following action block:

```
action(type="omfwd"
       #target="x.x.x.x"
          #port="xxxx"
          protocol="tcp"
          StreamDriver="gtls"
          StreamDriverMode="1"
          Template="CRLogFormat")
```

3. Enter the appropriate values in the following fields:
   - `target="x.x.x.x"`—Enter the IP address of your SIEM server.
   - `port="xxxx"`—Enter the port number used by your SIEM server to receive logs.
4. Enable certificate verification.

   The following steps provide SIEM communication by using TLS and server-side certificate verification by specifying a certPath.

   NOTE: Ensure that the security certificate is not expired, otherwise, the audit logs are not sent to the SIEM server.

   If you want to disable server-side verification, go to step 13.

   NOTE: Though you can have SIEM communication without TLS, this configuration is not recommended.

   a. In the `forwardAuditLogs.conf` file, uncomment the following line:

   ```
   #$DefaultNetstreamDriverCAFile certPath
   ```

   This line specifies the path to the Certificate Authority (CA) certificate file.

   b. Replace `certPath` with the path of the `ca.pem` file.
5. Uncomment the following line:

```
#File="/var/log/dellemc/cr/var/log/audit/audit.log"
```

   This line specifies the path of the log file that rsyslog monitors.
6. Save the configuration file.
7. If necessary, add the port number that you added in the configuration file to the iptables rule.

a. List the current rules and check for the specific rule that uses the port number:

```
sudo iptables -L OUTPUT -v -n --line numbers
```

b. If the rule is not present, run the following command to add the port number to the rule:

```
sudo iptables -I OUTPUT -p tcp --dport xxxx -j ACCEPT
```

NOTE:

- By default, iptables rules do not persist after a reboot. Therefore, any rules that you set up are lost when the system restarts. You must add the rules to the iptables rule again manually.
- If your Cyber Recovery virtual appliance deployment is running on a cloud environment, update the network security rules (also referred to as security groups for firewall rules) that are provided by your cloud service provider.

8. Verify the configuration file by using either of the following commands:

```
sudo rsyslog -N1
```

```
rsyslogd -f /etc/rsyslog.conf -N1
```

If an error message is displayed, correct any errors in the configuration file.

9. Restart the rsyslog service to apply the changes:

```
sudo systemctl restart rsyslog
```

10. Check the status of the service:

```
sudo systemctl status rsyslog
```

11. Check the connectivity for TLS traffic between Cyber Recovery and the SIEM server:

```
openssl s_client -connect <siem_server_ip>:<port> -CAfile /etc/ssl/certs/audit/ca.pem
```

12. On the SIEM server, go to the directory that receives the audit logs and check to see if the SIEM server is receiving the logs.

    If the audit log file with content is present, the content is sent to the SIEM server when the configuration is completed.

    If you have updated the Cyber Recovery software and no actions were performed that cause the audit file to be created, no logs are sent to the SIEM server.

13. To disable the server-side verification, do the following:
    a. In the TLS setup section, add the new `$ActionSendStreamDriverAuthMode` parameter and set it to `anon`.

       The `anon` setting means that no server-side verification is required. Leave `$DefaultNetstreamDriverCAFile` commented because no certificate is required for no server-side verification.
    b. In the action section, add the `StreamDriverAuthMode` parameter and set it to `anon`.
    c. Uncomment the file to track the audit logs.
    d. Add the target port values for your configuration and ensure that you add the port number to the iptables rules, as described in step 7.
    e. Restart the rsyslog service to apply the changes and then check that status to ensure that your configuration is working as expected.

Cleaning up the initial SIEM server setup

If issues occur when you enable the SIEM server for the first time, perform cleanup steps.

About this task

NOTE: If you set up the SIEM server successfully and issues occur later, such as certificate expiration, do not perform these cleanup steps. Only perform the clean-up steps for the initial setup. Otherwise, unwanted behavior might occur.

After you edit the `forwardAuditLogs.conf` configuration file and restart the rsyslog service, you might see errors in the rsyslog service when you check the status. You might not see the logs on the SIEM server. When the rsyslog service is restarted, it reads the configuration file and creates a state file with the offsets in the `/var/spool/rsyslog` folder. When you restart the rsyslog service, it is enabled but might send logs from the saved offset. The expected behavior is to send the existing `audit.log` file and then keep sending the logs as they are added. To ensure that the existing logs are sent, you must perform the cleanup steps.

Steps

1. From the Cyber Recovery virtual appliance, do the following:
   a. Stop the rsyslog service:

      ```
      sudo systemctl stop rsyslog
      ```

   b. Go to the `/etc/rsyslog.d` folder and open the `forwardAuditLogs.conf` file.
   c. Comment the `File="/var/log/dellemc/cr/var/log/audit/audit.log` line.
   d. Restart the rsyslog service:

      ```
      sudo systemctl restart rsyslog
      ```

   e. Go to the `/var/spool/rsyslog` folder:

      ```
      cd /var/spool/rsyslog/
      ```

   f. Run the `ls -lrth` command to list the `imfil-state` files. The following example shows a sample `imfile` name:

      ```
      imfile-state: 100663435:2db6518a0f2cfe3a
      ```

   g. Delete the `imfile` file with the content that includes `audit.log` in the filename. For example:

      ```
      "filename": "\/var\/log\/dellemc\/cr\/var\/log\/audit\/audit.log", "prev_was_nl":
      0, "curr_offs": 9227, "strt_offs": 9227}
      ```

      If you are tracking other logs in other configuration files for which state files are created, ensure that you only delete the `imfile` that corresponds to the audit logs. Ensure that the `imfile` includes the entry with the `audit.log` file, as shown in the preceding example.

   h. Save the file state file.
   i. Restart the rsyslog service:

      ```
      sudo systemctl restart rsyslog
      ```

2. Uncomment the `#File="/var/log/dellemc/cr/var/log/audit/audit.log"` line and restart the rsyslog service.

   ```
   sudo systemctl restart rsyslog
   ```

3. Check the status:

   ```
   sudo systemctl status rsyslog
   ```

SIEM configuration limitations

Note the following limitations of the SIEM configuration:

- If TLS verification is enabled in the configuration and the TLS certificate expires, communication to the SIEM server is lost. Logs are still collected in the `audit.log` file but are not sent to the SIEM server.
- There is no mechanism to store logs on disk if the connection to the SIEM server fails. Logs that are generated during the downtime are not sent to the SIEM server.

  NOTE: Downtime includes:
  - Network connectivity issues—If the network connection between Cyber Recovery and the SIEM server is down, logs cannot be transmitted.
  - System outages—If the rsyslog service goes down, it does not report to the SIEM server. However, the logs are captured in the file.
  - Configuration settings—The system might be configured so that logs that are generated during downtime are not stored or forwarded.

Changing the log level

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

Prerequisites

You are logged in as the admin or operator user.

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  to access the **System Settings** list.
2. Click **Support** > **Log Settings**.
3. Do one of the following:
   - Click the **Set All** radio button to change the level for all logs.
   - Click a specific 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.

Prerequisites

You are logged in as the security officer, admin, or operator user.

Steps

1. From the masthead navigation, click  to access the **System Settings** list.
2. Click **Support** > **Support Bundles**.
3. Click **Generate Log Bundle**.

The operation status is displayed as `Generation in Progress`. When the operation is completed, the operation status is displayed as `Complete`.

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. Select the support bundle, which is displayed for a complete or partially complete generated support bundle.

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

   b. At the browser prompt, indicate that you want to download multiple files.

      The operation status is displayed as `Download in Progress`. When the operation is completed, the operation status is displayed as `Complete`.

      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 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.

Configuring a telemetry report

Enable the telemetry feature and schedule a telemetry report that is sent to Dell Technologies for troubleshooting purposes.

Prerequisites

- You are logged in as the security officer.
- You have a valid email address.
- The mail server is enabled to receive email messages.

About this task

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

- Count for each user role and each user role with multifactor authentication enabled
- Policies
- Applications
- Cyber Recovery versions for installations and updates
- Cyber Recovery services
- Vault DD storage
- Mail server
- Missing or expired Transportation Layer Security (TLS) certificates

The telemetry report sends telemetry information to `dataprotection-telemetry@emc.com`.

NOTE: If domain restrictions are enabled, the telemetry report is sent; restricted domains are ignored.

Steps

1. From the masthead navigation, click  to access the **System Settings** list.
2. Click **Support** > **Telemetry Reports**.
3. Swipe right on the slider to enable telemetry reporting.

4. Complete the **Frequency** and **Next Run** fields, and then click **Save**.
   The maximum number of days is 30, and the minimum is 1 day.
   NOTE: The Cyber Recovery UI uses the same time zone as the Cyber Recovery management host for the scheduled time.
5. Swipe left on the slider to disable telemetry reporting.

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

- You are logged in as an admin user.
- 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  to access the **System Settings** list.
2. Select **DR Backups**.
   The **Disaster Recovery Backups** pane is displayed.
3. Click **Configuration** and do the following:
   a. Swipe right on the slider to enable a DR backup.
      By default, DR backups are disabled.
   b. Click  and 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 date and 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 under the **Configuration** tab 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, go to the masthead navigation.

   a. Click  and then click **Maintenance**.

   b. Modify the **Delete DR Backups older than** field and click **Save**.

   Valid 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.

NOTE: If you recover a DR backup, after the recovery, the DR backup job is displayed as a critical failed job. Ignore this status; you do not need to take any action.

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/col1/drbackups <hostname>(no_root_squash)
   ```

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

   ```
   mount <DD hostname>:/data/col1/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/col1/drbackups <hostname>
```

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

Setting up a maintenance schedule

Configure a cleaning schedule to delete alerts, events, expired and unlocked copies, DR backups, and jobs when they are no longer needed.

Prerequisites

- You are logged in as the admin user.

  NOTE: An operator can only view the maintenance schedule.

- To ensure that the DR backup is in the cleaning schedule, enable and configure a DR backup from the **DR Backups** 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  to access the **System Settings** list.
2. Select **Maintenance**.
3. To modify the default cleaning schedule, from the **Cleaning Schedule** tab:
   a. Specify the frequency for when the schedule runs, the date and 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 number 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, from the **Clean Now** tab, click **Run 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 command 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 command does not allow removal of the Cyber Recovery software.

For a Cyber Recovery software installation, follow these procedures in this order:

1. Cleaning up existing Cyber Recovery Docker containers
2. Restoring a Cyber Recovery software installation after a disaster

For a Cyber Recovery virtual appliance deployment, follow the procedure in 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_ --format '{{.Names}}'
   ```

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

   - cr_swagger_1
   - cr_ui_1
   - cr_edge_1
   - cr_clouds_1
   - cr_shelteredharbor_1
   - cr_system_1
   - cr_schedules_1
   - cr_reporting_1
   - cr_policies_1
   - cr_vcenter_1
   - cr_mgmtdds_1
   - cr_apps_1
   - cr_notifications_1
   - cr_vault_1
   - cr_users_1
   - cr_postgresql_1
   - 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 Microsoft Azure, Amazon Web Services (AWS), or Google Cloud Platform, the `cr_clouds_1` container is not displayed.
   - If the Cyber Recovery instance is not running in a Sheltered Harbor deployment, the cr_shelteredharbor container is not displayed.
   - If the Sheltered Harbor feature is not enabled, the Sheltered Harbor container will not be running.

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 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 command 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 and Update 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, the Postgres 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 command:

      ```
      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 Postgres database password.

      ```
      Please enter the newly installed Postgres 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 command 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.

About this task

For information about how to deploy the Cyber Recovery virtual appliance, see the Dell PowerProtect Cyber Recovery Installation and Update 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 command:

      ```
      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.

12

Troubleshooting

This section describes tasks that you can perform to troubleshoot Cyber Recovery issues.

Topics:

Using the crsetup.sh command

Run the `crsetup.sh` command 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 that are used in the procedures in this guide.

Syntax

```
./crsetup.sh <option>
```

NOTE:

- You have three chances to enter the correct password or passphrase for `crsetup.sh` commands before.
- When you run a `crsetup.sh` command, the Docker and Docker Compose versions that are used in the system container are updated to reflect the corresponding versions that are installed on the machine from which you run the `crsetup.sh` command.

Options

The following options, including the corresponding flags, determine the result of the `crsetup.sh` command.

`--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, Postgres database, and the 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 crso password.

`--check, -c`
: Run the configuration check to validate that you have the correct installation requirements.

`--deploy, -d`
: Configure the Cyber Recovery software (OVA only).

`--forcerecreate, -f`

Force re-creation 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.

--recover, -r

Recover the Cyber Recovery software.

--restart, -e

Stop and then start all services.

--save, -b

Save the Cyber Recovery software configurations.

--secureresset, -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.

--shenable, -m

Enable the Sheltered Harbor feature.

--start, -s

Start all services or a single device.

--stop, -p

Stop the Cyber Recovery software.

--uninstall, -x

Uninstall the Cyber Recovery software.

--upgcheck, -k

Run a preupdate readiness check. This check confirms that you are running a supported operating system, the deployment has an enabled admin user, no services are down that cause the update procedure to fail, and so on.

--upgrade, -u

Update the Cyber Recovery software.

--verifypassword, -v

Verify the lockbox passphrase and the Postgres database and crso passwords.

Troubleshooting suggestions

The following table lists possible Cyber Recovery problems and suggested remedies.

Table 38. Troubleshooting suggestions

If you cannot	Do the following

Install the Cyber Recovery software	• Ensure that the `crsetup.sh --check` command verifies all prerequisites before continuing.
	• Ensure that you are using a stable version of Docker.
	• Set Docker to start on reboot with the `systemctl enable docker` command.
	• Find the `crsetup.sh` logs in the directory from which you run `crsetup.sh`.
	• If your system has an active firewall, ensure that the following ports are open on the firewall:
	  ○ 14777 (for Cyber Recovery UI)
	  ○ 14778 (for the Cyber Recovery REST API)

Table 38. Troubleshooting suggestions (continued)

If you cannot	Do the following
	○ 14780 (for the Cyber Recovery API Documentation)
Log in to the Cyber Recovery UI	• 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: ○ 14777 (for Cyber Recovery UI) ○ 14778 (for the Cyber Recovery REST API) ○ 14780 (for the Cyber Recovery API Documentation)

Start the Cyber Recovery software after a reboot due to an unlabeled context type and custom policies.	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:
	1. Assuming that the Cyber Recovery software is installed in `/opt/dellemc/cr`, change the SElinux context, as shown in the following example:
	`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/crsshutil`
	2. Reboot the system.
	The following is an example of the SElinux context:
	`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`

Enable multifactor authentication	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. **NOTE:** If you modify the Cyber Recovery host time, stop and then restart the Cyber Recovery services. To avoid this scenario, internal NTP configuration is recommended.
(For crso only) Log in because multifactor authentication is enabled and you are unable to provide the security code	As the crso, type **`crsetup.sh --changepassword`** or **`crsetup.sh -w`** to change the crso password and disable multifactor authentication. Enable multifactor authentication again after you log in.
Change the application type	Delete the application and then add a new application and choose the appropriate application type.
Run a job	Check the schedules, policies, or mgmtdds service logs.
Complete a successful Sync job	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.
Receive alert email messages	• If your system has an active firewall, ensure that port 25 is open on the firewall.

Table 38. Troubleshooting suggestions (continued)

If you cannot	Do the following
	• Verify your Postfix or email configuration and check that you added the email for alert notifications.
Secure the Cyber Recovery vault	Check the vault service logs.
Recover or analyze	Check the apps, mgmtdds, and policies service logs.
Run a subsequent Analyze job after performing a DR backup while running an Analyze job	Wait for the currently running Analyze job to finish, delete the stale sandboxes, and then run the Analyze job again. **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.
Run an Analyze job due to an inactive or degraded multilink configuration	Ensure that: • The DD and CyberSense interfaces are enabled. • The cabling and switches between the interfaces are working correctly. • A DD Boost user is configured on the CyberSense host • There are no hardware issues. You can remove a link, but might encounter performance issues.
Run a policy, sandbox, or recovery due to mount errors from the DD system	Ensure that the NFSv4 and NFSv3 settings on the DD system are configured to run NFS operations: 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`**.
Perform a PowerProtect Data Manager successfully	If NFS v4 is enabled on the DD system in the Cyber Recovery vault, either disable it and use NFS v3 or use DD Boost for the server DR MTree.
See a successful DR backup job status after you recover a DR backup	If you recover a DR backup, after the recovery, the DR backup job is displayed as a critical failed job. Ignore this status; you do not need to take any action.

Complete a NetWorker recovery operation cleanly. For example, if you encounter a problem during the automated recovery process.	Perform a manual cleanup:
	1. Shut down NetWorker.
	For example:
	`/etc/init.d/networker stop`
	2. For the resource database, complete the following steps:
	a. Find the latest `resdb` (`/nsr/res.cr.<timestamp>`) directory.
	b. Remove the current `/nsr/res` directory.
	c. Restore the previous resource database by renaming the `res.cr.<timestamp>` directory to the following:
	`/nsr/res`
	For example:
	`mv /nsr/res.cr.1554828308 /nsr/res`
	3. For the media database, complete the following steps:
	a. Find the latest `mm` directory (`/nsr/mm.cr.<timestamp>`).
	b. Remove the current `/nsr/mm` directory.
	c. Restore the previous media database by renaming the `/nsr/mm.cr.<timestamp>` directory to the following:
	`/nsr/mm`
	For example:

Table 38. Troubleshooting suggestions (continued)

If you cannot	Do the following
	mv /nsr/mm.cr.*155512814* /nsr/mm 4. For the index database, complete the following steps: a. Find the latest `index` directory (`/nsr/index.cr.<timestamp>`). b. Remove the current `/nsr/index` directory. c. Restore the previous index directory by renaming the `/nsr/index.cr.<timestamp>` directory to the following: `/nsr/index` 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 39. Cyber Recovery component log directories

Cyber Recovery component	Log directories
apps service	Anything that is related to applications that are associated with Cyber Recovery, including CyberSense used for copy analysis, NetWorker, Avamar, and PowerProtect Data Manager instances, and file system hosts.
clouds service	Anything that is related to the Cyber Recovery vault on Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform.
cradmin	Anything that is related to lockbox activity.
crcli	Anything that is related to the CRCLI.
crsetup	Anything that is related to the `crsetup.sh` command.
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.
mgmtdds service	All communication with the Cyber Recovery vault DD.
nginx service	Anything that is related to the web server that runs the Cyber Recovery UI.
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.
reporting service	Anything that is related to reports
schedules service	All the system schedules, cleaning schedules, and action endpoints.
shelteredharbor	Anything that is associated with Sheltered Harbor financial institutions.
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.
telemetry	Telemetry report.

Table 39. Cyber Recovery component log directories (continued)

Cyber Recovery component	Log directories
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.
vcenter service	Anything that is associated with vCenter objects.

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 40. Log levels

Log Level	Purpose	Example
ERROR	Reports failures in the execution of some operation or task that usually requires manual intervention.	• 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.	• A Corrupted or truncated files. • A policy is one hour over the sync timeout period of 6 hours.
INFO	Reports information about the progress of an operation or task.	• 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` command 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 41. 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, which include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform
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
reporting	Manages Cyber Recovery reports
policies	Manages Cyber Recovery policy actions
vcenter	Manages the vCenter server objects that are required for PowerProtect Data Manager deployments
shelteredharbor	Manages the Sheltered Harbor feature
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
postgresql	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-<networker sandbox>_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 systems.
   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.

Disassociating DD storage from Cyber Recovery

You must disassociate DD storage from Cyber Recovery in a specific order.

Steps

1. First, delete copies by deleting all sandboxes that are associated with a copy.
2. Next, delete all policies by deleting all copies that are associated with each policy.
3. Finally, delete the vault storage by deleting all policies that are associated with the vault storage.

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 filer functionality, see the DD documentation.

Results

SSH is blocked on all interfaces except the management interface.