Dell EMC PowerProtect Cyber Recovery Product Guide

Version 19.2

302-005-890
REV 01
September 2019

DELL EMC

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Preface

As part of an effort to improve its product lines, Dell EMC 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 EMC 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 EMC Online Support.

Purpose

This guide describes how to install, upgrade, patch, and uninstall the Dell EMC PowerProtect Cyber Recovery software.

Audience

The information in this guide is primarily intended for administrators who are responsible for installing and upgrading the Cyber Recovery software.

Product Documentation

The Cyber Recovery product documentation set includes:

- Dell EMC PowerProtect Cyber Recovery Release Notes
- Dell EMC PowerProtect Cyber Recovery Installation Guide
- Dell EMC PowerProtect Cyber Recovery Product Guide
- Dell EMC PowerProtect Cyber Recovery Solutions Guide
- Dell EMC PowerProtect Cyber Recovery Security Configuration Guide
- Dell EMC PowerProtect Cyber Recovery Open Source License and Copyright Information

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

Where to get help

Go to Dell EMC Online Support to obtain Dell EMC support, and product and licensing information. You can also find documentation, release notes, software updates, or information about other Dell EMC products.

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

Comments and suggestions

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

Please include the following information:

- Product name and version

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

CHAPTER 1

Introduction

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

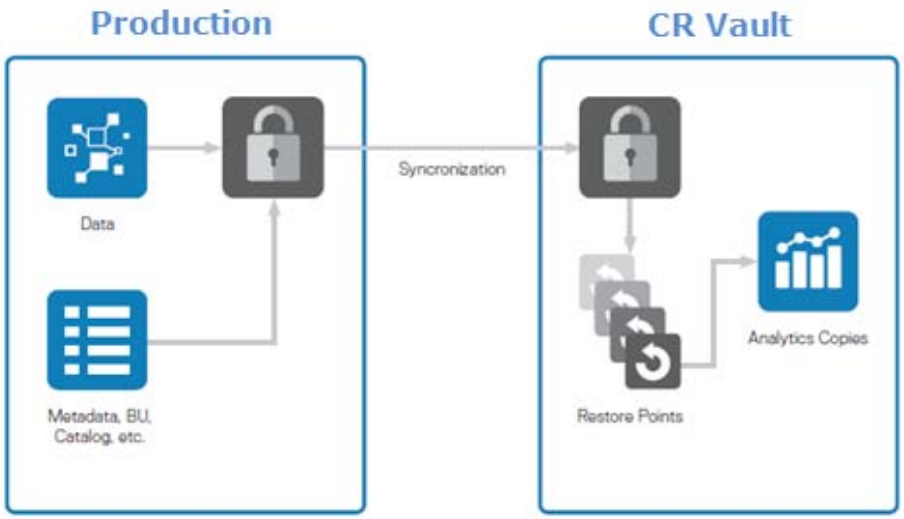
What is the Dell EMC PowerProtect Cyber Recovery solution?

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 (CR Vault) is physically isolated from an unsecure system or network.

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

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

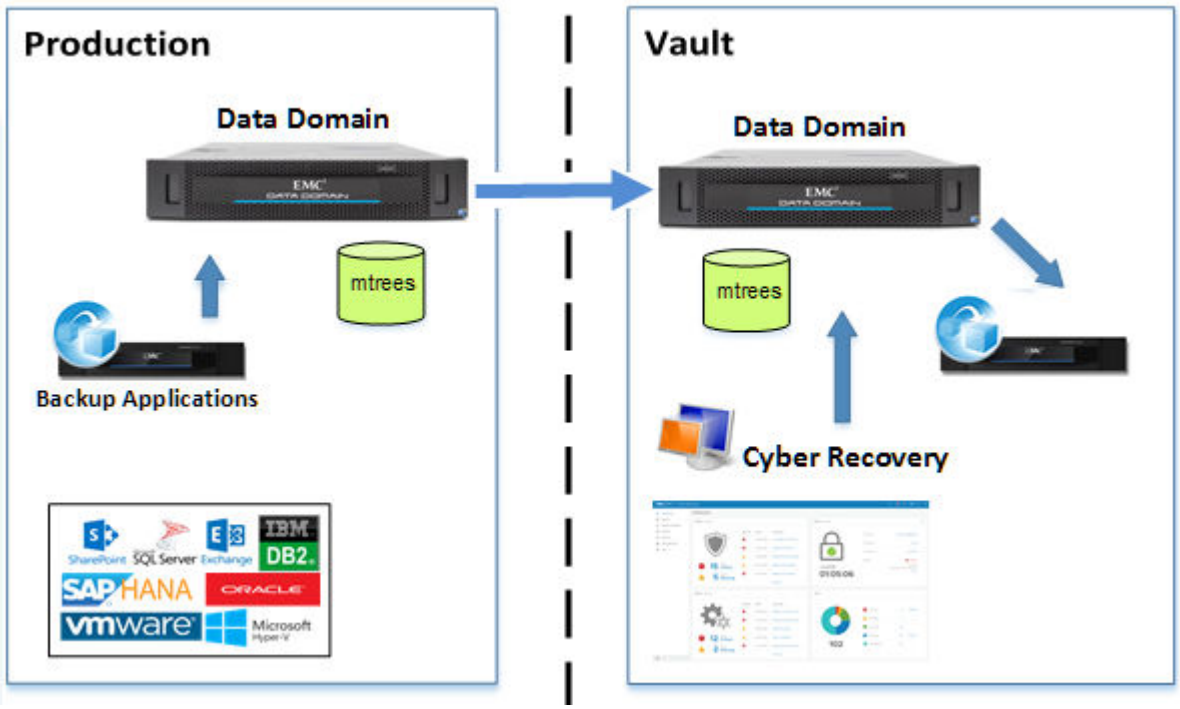
A policy, which can be scheduled, orchestrates the workflow between the production environment and the CR Vault. A policy is a combination of objects (such as Data Domain storage and applications) and jobs (such as synchronization, copy, and lock).

Note: References to Data Domain systems in this documentation, in the UI, and elsewhere in the product include Data Domain systems and the new PowerProtect DD systems.

Cyber Recovery architecture

As shown in the following diagram, the Cyber Recovery solution uses Data Domain systems to replicate data from the production system to the CR Vault through a dedicated replication data link:

Figure 2 Cyber Recovery architecture



Note: Unless otherwise specified, this document uses the term CR Vault to describe the vault environment, which includes the Data Domain system, the management host, and backup and analytics applications.

The CR Vault is a customer-provided secure location of the Data Domain MTree replication destination. It requires dedicated resources including a network, and though not required but strongly recommended, a name service such as DNS. The CR 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 Data Domain systems. The production Data Domain system is configured to replicate data to a corresponding Data Domain system in the CR Vault.

Vault environment

The CR Vault environment includes the Cyber Recovery management host, which runs the Cyber Recovery software and a Data Domain system. If required for application recoveries, the CR Vault can also include NetWorker, Avamar, PowerProtect Data Manager, and other applications. By installing Index Engines' CyberSense, an analytic and validation application, you can validate and analyze the data.

The Cyber Recovery software enables and disables the replication Ethernet interface on the Data Domain system in the CR Vault to control the flow of data from the production environment to the

vault environment. For short periods of time, the CR 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 CR Vault is secured.

Note: From the Data Domain command-line interface (CLI) and the Data Domain 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. Except for Avamar recovery, the Cyber Recovery software adds the `cr-` prefix to the name.

Cyber Recovery operations

Recovery managers can perform continuous and iterative operations that maintain recovery data in the CR Vault if it is 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.

Replication

Data Domain MTree replications are performed from the Data Domain production system to the Data Domain system in the CR Vault. Each replication uses Data Domain 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 Data Domain fast copy inside the CR 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 both:

- 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

For information about the governance and compliance archive data requirements and how to manage them, see the Data Domain documentation.

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.

Configuring Data Domain Compliance mode retention locking

Configure the CR Vault Data Domain system for Retention Lock Compliance.

Before you begin

The CR Vault Data Domain system must have a Retention Lock Compliance license.

For more comprehensive information about the procedures to configure Retention Lock Compliance on a Data Domain system, see the *Dell EMC Data Domain Operating System Administration Guide*.

About this task

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

Procedure

1. On the CR Vault Data Domain system, log in as an Admin user and then add a security account with the security role:

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

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

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

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

4. Log out as the Security Officer user and log in again as the Admin user.
5. Configure the CR Vault Data Domain 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 CR Vault Data Domain 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 CR Vault Data Domain system as an Admin user and provide the security officer credentials, when prompted.

Management tools

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

Cyber Recovery UI

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

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

Cyber Recovery REST API

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

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

Cyber Recovery Command Line Interface

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

CHAPTER 2

Getting Started

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

Logging in

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

About this task

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

Procedure

1. Open a supported browser and go to `https://<host>:14777`.

   where *<host>* is the hostname of the management host where the Cyber Recovery software is installed.

2. Enter your username and password.
3. Click **LOG IN**.

   The Cyber Recovery dashboard displays.

Activating the Cyber Recovery license

Upload the Cyber Recovery license file to activate the license.

Before you begin

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

When Dell EMC emails you the license file, save it to a directory of your choice. If you must bring the license file into the CR Vault, you must enable a connection from your desktop to the CR Vault or use a USB flash drive.

About this task

After Cyber Recovery installation, the Cyber Recovery deployment state is **Unlicensed** by default. You can perform some perfunctory Cyber Recovery tasks, however you cannot access full Cyber Recovery capabilities.

Procedure

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

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

   - Expires On
   - State
   - Type
   - Software Instance ID

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.

Completing initial setup with the Getting Started wizard

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

About this task

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

Procedure

1. Under **Checklist**, click **REVIEW** to verify that you have performed the required deployment steps.

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

2. Under **Users**, click **ADD** to create an Admin user. Complete the following fields in the **Add User** dialog box and click **SAVE**:

Field	Description
Name fields	Specify the user's first name and last name.
Role	Select either: • Admin—Enables users to perform tasks in the Cyber Recovery software. • Dashboard—Enables users to view the Cyber Recovery dashboard but not perform tasks. The dashboard role does not time out.
User Name (required)	Specify a username.
Phone	Specify the user's telephone number.
Email (required)	Specify an email address for alert notifications if the user is configured to receive them.
Password/Confirm New Password (required)	Specify and confirm the password. 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 (~!@#$%^&*()+={}|:";<>?[]-_.,^') When you change a password, enter and confirm both the new and existing passwords.
Session Timeout	Select the amount of idle time after which the user is logged out of the Cyber Recovery UI.

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

Field	Description
Nickname	Enter a name for the storage object.
FQDN or IP Address	Specify the Data Domain host by using one of the following: • Fully qualified domain name (FQDN)

Field	Description
	• IP address
Storage Username	Specify a dedicated Cyber Recovery Data Domain administration account (for example, `cradmin`), which the Cyber Recovery software uses to perform operations with the Data Domain system. This Data Domain account must be an admin role and on the DD boost users list. **Note:** You cannot use the sysadmin account.
Storage Password	Enter the password of the Data Domain administrator.
SSH Port Number	Enter a storage SSH port number.
Tags	Optionally, add a tag that provides useful information about the storage object. The tag is displayed in the details description for the vault storage in the **Assets** content pane in the Cyber Recovery UI. Click **Add Tag**, enter the tag, and then click **Add**. **Note:** If a tag exceeds 24 characters, the details description displays the first 21 characters followed by an ellipsis (...).

4. Under **Policies**, click **ADD** to define a policy. Complete the following fields in the **Add Policy** dialog box and click **SAVE**:

Field	Description
Name	Specify a policy name.
Storage	Select the storage object containing the replication context that the policy will protect.
Context	Select the MTree replication context to protect. **Note:** There can be only one policy per replication context.
Replication Ethernet	Select the interface on the storage instance that is configured for replications. **Note:** Do not select the data are management Ethernet interfaces.
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.
Retention Lock Type	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. • **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.
Storage SO Username/Password	Required when you select **Compliance**. Enter the username and password of the storage instance Security Officer. **Note:** This username was created on the Data Domain system.
Retention Lock Minimum	Specify the minimum retention duration that this policy can apply to PIT copies. This value cannot be less than 12 hours. **Note:** If the retention lock type is set to **Compliance** and you edit this value, you are prompted to enter the Storage SO Username/Password.

Field	Description
Retention Lock Maximum	Specify the maximum retention duration that this policy can apply to PIT copies. This value cannot be greater than 1,827 days. **Note:** If the retention lock type is set to **Compliance** and you edit this value, you are prompted to enter the Storage SO Username/Password.
Retention Lock Duration	Specify the default retention duration that this policy applies to PIT copies.
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 (...).

When you complete these steps, the Cyber Recovery dashboard is displayed.

Note: You can recall the wizard at any time by selecting **System Settings > Getting Started** from the Masthead Navigation.

5. To run the policy immediately, do the following:
   a. Select **Policies** in the Main Menu.
   b. On the **Policies** content pane, select the policy checkbox. Then click **ACTIONS** and select the action that you want the policy to perform.

      Note: If you have not installed the Cyber Recovery license, you cannot run any Sync (replication) operations.

Cyber Recovery runs the policy and displays progress messages on the **Jobs** content pane and the dashboard.

Cyber Recovery UI

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

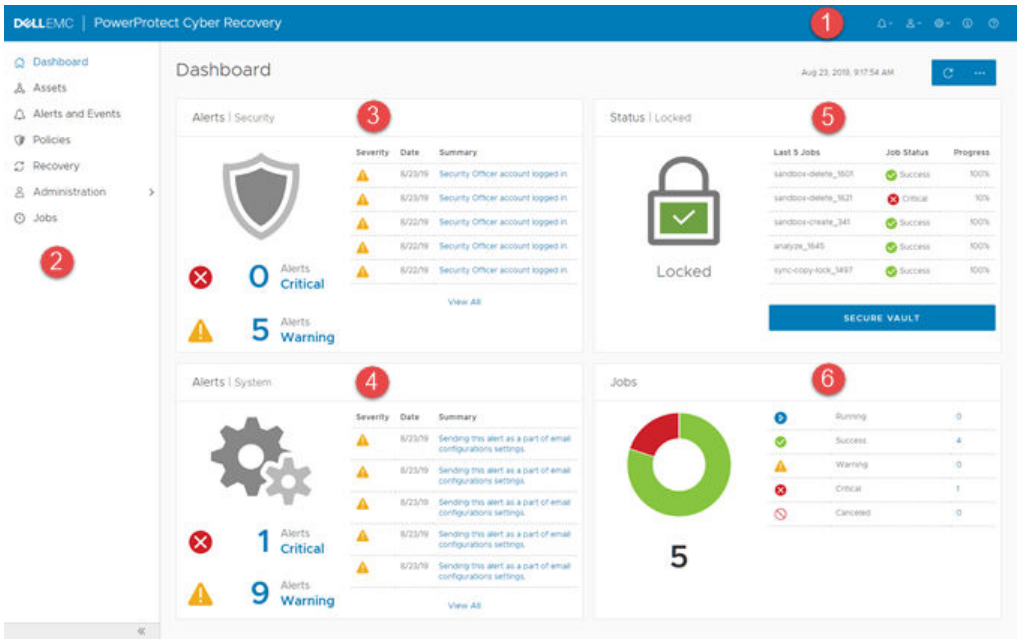
Note: If you log in to the Cyber Recovery UI as a dashboard user, your view of the dashboard is limited and you cannot perform tasks. However, the dashboard does not time out.

The 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.
- A dashboard that provides comprehensive alerts and events notifications that facilitate troubleshooting and error correction.

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

Figure 3 PowerProtect Cyber Recovery dashboard



1. The Masthead Navigation provides icons that enable you to view notifications and additional information, set system settings, and access the Getting Started wizard and online help. A dashboard user can only log out of the Cyber Recovery UI.
2. The Main Menu provides access to content panes from which you can perform operations. It is not available to a dashboard user.
3. **Alerts|Security** provides details about unacknowledged alerts that identify anomalies in vault activity.
4. **Alerts|System** provides details about unacknowledged system events.
5. **Status** shows the current state of the CR Vault and enables you to secure it manually if a network event occurs when the CR Vault is open and stop all replication operations. It also displays the five most recent jobs and their progress. For information about monitoring the CR Vault and about manually securing the CR Vault, see Monitoring the CR Vault status on page 38 and Manually securing and releasing the CR Vault on page 64.
   Note: A dashboard user cannot secure the vault.
6. **Jobs** shows the jobs that are created when a policy is triggered and the overall status of all jobs in the Cyber Recovery environment.

Note: Links in **Alerts** and **Jobs** enable you to access content panes that display more information about the specific details on the dashboard.

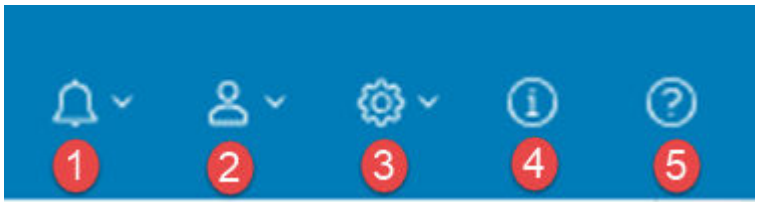
Your assigned role determines the functions that you can perform in the Cyber Recovery UI. For more information, see User roles on page 64.

Masthead Navigation

The Cyber Recovery UI includes Masthead Navigation.

The icons in the masthead of the Cyber Recovery UI provide information or enable you to perform administrative tasks. A dashboard user can only log out of the Cyber Recovery UI and has no access to the other icons.

Figure 4 Masthead navigation icons



1. Provides a drop-down list of unacknowledged alerts
2. Enables you to log out and identifies your username
3. Provides a drop-down list to access the Getting Started wizard, set clean-up and log settings, and enable license activation. The Security Officer can also manage the number of simultaneous login sessions.
4. Displays the Cyber Recovery version and Software Instance ID
5. Displays the Cyber Recovery online help

CHAPTER 3

Storage and Applications

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

Assets overview

Assets in the CR Vault are represented as storage and application objects.

Storage objects

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

Application objects

Application objects represent applications, such as Avamar, NetWorker, PowerProtect Data Manager, or Index Engines' CyberSense.

Usually, you include Avamar, NetWorker, and PowerProtect Data Manager backup applications in the CR Vault when the Data Domain system is integrated with those applications in your production systems. The CR Vault does not require these applications to protect the data because MTree replications copy all the data to the CR Vault. However, running the applications in the CR Vault enables you to analyze, 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 Index Engines' CyberSense application, which analyzes backup data for the presence of malware or other anomalies. After you install Index Engines' CyberSense on a separate host in the CR Vault, define an application object for it. Then, Cyber Recovery policies can call Index Engines' CyberSense to analyze PIT copies.

Managing storage

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

Before you begin

Before you add a storage object, install the Data Domain instance in the CR Vault environment and perform an initial replication.

About this task

If you are defining the Data Domain system for the first time, see Completing initial setup with the Getting Started wizard on page 15.

Procedure

1. Select **Assets** from the Main Menu.
2. Do one of the following:
   - To add a storage object, click **ADD**.
   - To modify an existing object, select the object and click **EDIT**.
3. Complete the fields in the following dialog box:

Field	Description
Nickname	Enter a name for the storage object.
FQDN or IP Address	Specify the Data Domain host by using one of the following: • Fully qualified domain name (FQDN) • IP address
Storage Username	Specify a dedicated Cyber Recovery Data Domain administration account (for example, `cradmin`), which the Cyber Recovery software uses to perform operations with the Data Domain system. This Data Domain account must be an admin role and on the DD boost users list. **Note:** You cannot use the sysadmin account.
Storage Password	Enter the password of the Data Domain administrator.
SSH Port Number	Enter a storage SSH port number.
Tags	Optionally, add a tag that provides useful information about the storage object. The tag is displayed in the details description for the vault storage in the **Assets** content pane in the Cyber Recovery UI. Click **Add Tag**, enter the tag, and then click **Add**. **Note:** If a tag exceeds 24 characters, the details description displays the first 21 characters followed by an ellipsis (...).

4. Click **SAVE**.

   The **VAULT STORAGE** table lists the storage object.
5. Click in the row for the storage object to view more detailed information that is retrieved from the Data Domain system, such as the replication contexts and the Ethernet interface.
6. To remove a storage object, select the storage object, and then click **DELETE**.

Managing applications

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

Before you begin

The application must be installed and running at the CR Vault location before you can define it in the Cyber Recovery UI.

Procedure

1. Select **Assets** from the Main Menu and click **APPLICATIONS** at the top of the **Assets** content pane.
2. Do one of the following:
   - To add an application, click **ADD**.
   - To modify an existing application, select the application and click **EDIT**.
3. Complete the following fields in the dialog box:

Field	Description
Nickname	Enter a name for the application object.
FQDN or IP Address	Specify the Data Domain host by using one of the following: • Fully qualified domain name • IP address
Host Username	Specify the host administrator username. **Note:** This username is for the operating system host.
Host Password	Enter the password of the host administrator. **Note:** For PowerProtect Data Manager, enter the password for the user admin account, which is the default account.
SSH Port Number	Enter an application SSH port number.
Application Type	Selection an application type: • To represent an application in Cyber Recovery, select the following: ▪ **Avamar** ▪ **NetWorker** If you select the NetWorker application, complete the following 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. ▪ **PPDM** If you select the PowerProtect Data Manager application, complete the following fields:

Field	Description
	– In the **Application Username** field, enter the username of the application user. – In the **Application Password** field, enter the password of the application user. – In the **Host Root Password** field, enter the root password of the vault application. The root password is required to reboot the PowerProtect Data Manager appliance. ▪ **IndexEngines** • Select **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. • Select **Other** for other application types.
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 user name 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 (...).

4. Click **Save**.

   The **APPLICATIONS** table lists the application.
5. Click in the row for the application to view more detailed information.
6. To remove an application, select the application and click **DELETE**.

CHAPTER 4

Policies and Copies

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

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:

- One Cyber Recovery policy governs each Data Domain MTree that is being protected.
- 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.

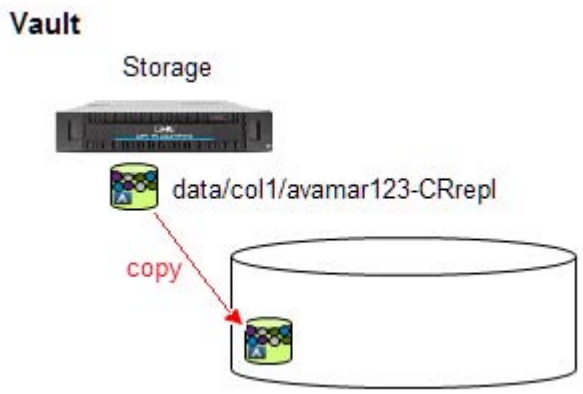
In the Cyber Recovery UI, you can retention lock a copy or analyze its data to detect the presence of malware or other anomalies. You can also delete unlocked copies.

Policy actions

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

Copy

A Copy action makes a point-in-time (PIT) copy of an Mtree's most recent replication in the CR Vault and stores it in the replication archive.

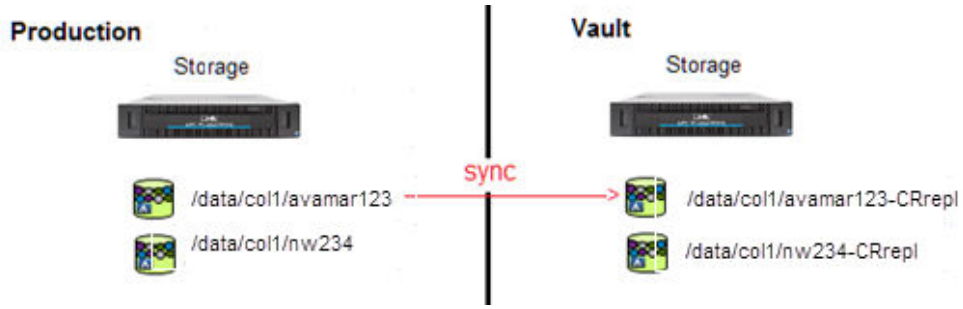


Copy Lock

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 CR 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 on page 33.

Managing policies

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

Before you begin

Ensure that a storage object is available to reference in the policy and that it has an unprotected replication context. Only one policy can protect a replication context. Policies that perform recovery or analysis operations require an application.

Procedure

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**.
   b. To modify a policy, select a policy and click **EDIT**.
3. Complete the fields in the following dialog box:

Field	Description
Name	Specify a policy name.
Storage	Select the storage object containing the replication context that the policy will protect.
Context	Select the MTree replication context to protect.

Field	Description
	Note: There can be only one policy per replication context.
Replication Ethernet	Select the interface on the storage instance that is configured for replications. **Note:** Do not select the data are management Ethernet interfaces.
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.
Retention Lock Type	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. • **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.
Storage SO Username/Password	Required when you select **Compliance**. Enter the username and password of the storage instance Security Officer. **Note:** This username was created on the Data Domain system.
Retention Lock Minimum	Specify the minimum retention duration that this policy can apply to PIT copies. This value cannot be less than 12 hours. **Note:** If the retention lock type is set to **Compliance** and you edit this value, you are prompted to enter the Storage SO Username/Password.
Retention Lock Maximum	Specify the maximum retention duration that this policy can apply to PIT copies. This value cannot be greater than 1,827 days. **Note:** If the retention lock type is set to **Compliance** and you edit this value, you are prompted to enter the Storage SO Username/Password.
Retention Lock Duration	Specify the default retention duration that this policy applies to PIT copies.
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. Click **SAVE** to complete creating or modifying the policy.

   For information about running policies, see Running policies on page 31.

5. To remove a policy, select the policy and then click **DELETE**.

   You cannot delete a policy if there are any active copies that are associated with the policy. Delete the copies before you try to delete the policy.

   Note:
   When you delete a policy, the Cyber Recovery software does not remove the MTree from the Data Domain system. The software does not delete unlocked PIT copies. Remove them manually.

   The data on the Data Domain system might be required until a retention lock expires or you might continue to want access to the data. Therefore, the data is retained.

Running policies

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

Procedure

1. Select **Policies** from the Main Menu.
2. Select the policy that you want to run.
3. Click **ACTIONS** and select one of the following:

Task	Description
Secure Copy	Performs a Sync, a Copy, and then a Lock action.
Sync Copy	Performs a Sync and then a Copy action.
Copy Lock	Retention locks the most recent point-in-time (PIT) copy. To retention lock an earlier PIT copy, see Managing copies.
Sync	Replicates the MTree from the production system to the CR Vault. This replication synchronizes with the previous replication of the MTree. Cyber Recovery unlocks the CR Vault to perform the replication. **Note:** When performing a Sync action, there might be a delay of up to 15 minutes, depending on the replication cycle on the production Data Domain system. The Cyber Recovery software itself does not initiate a replication. Instead, it waits for the production Data Domain system to synchronize its data over the replication interface and then validates the timestamp of the replicated data on the CR Vault Data Domain system.
Copy	Creates a PIT copy of the latest replication.

Results

The policy starts a job that you can monitor on the **Jobs** page.

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.

Scheduling policies

Schedule an action that you want the policy to perform.

Before you begin

- If you have not installed the Cyber Recovery license, you cannot create a schedule.
- 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 the Lock action.

About this task

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

Procedure

1. Select **Policies** from the Main Menu.
2. Click **SCHEDULES** at the top of the **Policies** content pane.
3. To add a schedule, click **ADD** and complete the following fields in the dialog box:

Field	Description
Schedule Name	Specify a schedule name.
Policy	Select the policy that you are scheduling.
Action	Select the action that the policy performs when it runs under this schedule. See Running policies on page 31 for a description of the actions.
Retention Lock Duration	Enter the duration of the retention lock that this policy applies to PIT copies.
Application Host	Only if you selected **Analyze** as the action, select the host for Index Engines' CyberSense
Data Type	Only if you selected **Analyze** as the action, select the application type.
Frequency	Enter the frequency in days and hours.
Start Date	Select the date to start running the policy under this schedule.
Start Time	Select the time to start running the policy under this schedule.

4. Click **APPLY**.

   The **Schedules** table lists the schedules.
5. To delete an existing schedule and remove it permanently, select the schedule and then click **DELETE**.
6. To disable an existing schedule but not delete it, select the schedule and then click **DISABLE**.

   The status column indicates that the schedule is disabled.
7. To enable a disabled schedule so that it runs again, select the schedule and then click **ENABLE**.

   The status column indicates that the schedule is enabled.

Managing copies

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

Procedure

1. Select **Policies** from the Main Menu.
2. Click **COPIES** at the top of the **Policies** content pane to display existing copies.

   Each row shows the copy name, policy name, size, expiration time, and indicates if the copy was analyzed.

3. To view details about a copy, click in the copy's row.

   The **Details** window displays the information and provides links to the policy and sandboxes (if any).

4. To retention lock a copy or extend the retention period of a locked copy, see Securing a copy.
5. To analyze a copy, see Analyzing a copy.
6. To delete an unlocked copy, select the copy and then click **DELETE**.

   Note: If a copy's **Expires On** column displays a date, the copy is retention locked and cannot be deleted.

   You can also view, lock, analyze, and delete copies by policy. Click the policy name in the **Name** column to display the **Details for Policy** page. Then click **COPIES**.

Securing a copy

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

Before you begin

A policy must create the PIT copy.

About this task

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

Procedure

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 Range** field displays the policy's minimum and maximum retention value. Specify a duration within this range.

Results

The retention lock is set and the **Expires On** column change from **Unlocked** and displays the expiration date.

Analyzing a PIT copy

Analyze a point-in-time (PIT) copy by using analytics tools that have been added to the CR Vault.

Before you begin

The following prerequisites must be satisfied:

- An analytics application must be installed at the CR Vault location and defined as a Cyber Recovery application asset.

  Note: Index Engines' CyberSense is an example of such a tool (for more information, go to the Index Engines website).

- A policy must create the PIT copy to analyze.

Procedure

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 to analyze and click **ANALYZE**.
   a. From the **Application Host** list box, select the application host name for Index Engines' CyberSense.
   b. From the **Data Type** list box, select the application type.

   Note: You cannot run an analysis concurrently on a copy. Otherwise, Cyber Recovery displays an informational message and does not create a job. When the initial job is completed, run the analysis on the copy.

   The policy starts a job that you can view on the **Jobs** page. If the analysis includes indicators of possible malware or other anomalies, the job status is listed as Critical. Otherwise, the job status is listed as Success.
4. When the analysis is complete, return to the list of copies and click in the copy's row.

   A **Details** panel displays the results in the **Last Analysis** fields.

Managing sandboxes

A sandbox is a unique location in the CR 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 CR Vault. Create sandboxes as needed to perform data analysis, recovery, or validation operations.

About this task

Cyber Recovery enables you to create custom sandboxes 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.

Procedure

1. From the Main Menu, click **Recovery**.
2. Select a PIT copy from the list.
3. Click **Sandbox**.
4. In the Sandbox dialog box:
   a. Select an application that is configured in the CR Vault.
   b. Enter a unique sandbox name.

   Note: The **cr** prefix is appended to the custom sandbox name. For example, if you enter **`MySandbox`**, the sandbox name displays as `cr-MySandbox`.

   c. Indicate if you want to mount the file system. Enter where you want to mount the data if you do not want to use the default.

   Note: Cyber Recovery supports mount operations for UNIX operating systems only. The host is available by using SSH.

   This step starts a job that you can view on the **Jobs** page.
5. From the **Recovery** content pane, click **Sandboxes** if you want to:

a. View the list of sandboxes and details.

b. Select a sandbox and then delete it.

CHAPTER 5

Monitoring

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

Monitoring the CR Vault status

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

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

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

If necessary, the Security Officer or an Admin user can manually lock the vault and close the connection. For more information, see Manually securing and releasing the CR Vault on page 64.

To view the CR Vault connection status, click **Dashboard** in the Main Menu. The state displays under **Status**.

The following table describes the three connection states:

Status	Icon	Description
Locked		All configured replication connections are closed because no replication is being performed. If a replication policy is run, the Cyber Recovery software opens the connection and changes the vault state to Unlocked.
Unlocked		One or more replication network connections are open because a replication is being performed. The state returns to Locked when the replication completes.
Secured		All replication network connections are secured because the Security Officer or an Admin user manually locked the connection due to a security breach. You cannot initiate any replication policy actions. When the CR Vault is released and returns to the Locked state, you can then run replication policies.

Monitoring alerts and events

The Cyber Recovery software generates notifications about alerts and events.

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

Alert categories include:

- System—Indicates a system issue that might compromise the Cyber Recovery system such as a failed component
- Storage—Indicates storage issues such as insufficient disk space
- Security—Indicates that a user cannot log in or malware might have been detected
  Note: By default, the alerts table includes the Security Officer login as a security alert. Use this account only when necessary.

Events indicate system events, such as the start of a job or completion of a retention lock.

You can view alerts and events from:

- The dashboard

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

The Alerts and Events content pane enables you to view details, acknowledge, and add notes for alerts. You can only view details for events.

Handling alerts

An alert indicates that you might have to take action.

Procedure

1. Select **Alerts and Events** from the Main Menu.

   The content pane lists the alerts.
2. To view details about an alert, click in the alert's row.

   The **Details** pane displays complete details about the alert.
3. Take any necessary actions to resolve the problem.
4. Select an alert or multiple alerts and click **ACKNOWLEDGE**.

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

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

   Note: The dashboard and the Navigation Masthead no longer show these alerts. Only the five most recent unacknowledged alerts are displayed on the dashboard and from the drop-down list on the Navigation Masthead.
5. Optionally, click **UNACKNOWLEDGE** to remove the acknowledgment from the alert.

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

   The note displays in the alert's **Details** pane.

Monitoring jobs

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

The **Jobs** content pane shows the job status, which indicates the job's progress. It lists jobs that are running, successfully completed, or canceled. When a job is completed, its status is either **Success**, **Warning**, or **Critical**. If a job's status is **Critical**, a critical alert is also associated with the job.

When you create or edit a policy, you can set an optional job window timeout value in hours for how long a job for a Sync action runs. If the duration of the job reaches the timeout limit, Cyber Recovery issues a warning alert. Cancel the job, if necessary.

In the **Jobs** content pane:

- For more information about a job, click in a job's row to bring up the **Details** window.
- To stop a running Sync, Sync Copy, or Secure Copy job, select the job and then click **CANCEL JOB**.
  The **Alerts and Events** content pane displays an alert for the cancel request.

- To refresh the content pane, click the refresh icon.
- To select how often the content pane refreshes, click the refresh icon and select the time from the list box.

CHAPTER 6

Performing a NetWorker recovery with Cyber Recovery

This section describes how to recover data from NetWorker point in time copies.

Recovering NetWorker data

Use a point-in-time (PIT) copy to rehydrate NetWorker data in the CR Vault.

The NetWorker application must be installed as the root user in the CR Vault.

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 CR Vault environment.

From the Cyber Recovery UI, initiate a recovery. The Cyber Recovery software creates a sandbox so that you can run the recovery from the NetWorker application.

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 CR Vault.

Procedure

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

   ```
   # crcli policy show -n <policy_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 Data Domain system in the CR 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 user name.

   b. If you are running DDOS 6.1.2.10 or later, 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 Data Domain 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.

Before you begin

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

- You have obtained the credentials for the CR Vault host on which the NetWorker application is installed and for the NetWorker application.
- The NetWorker server host within the vault has the same IP address and hostname as the NetWorker production host.
- The NetWorker application is installed in the CR 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.
- Password authentication and SSH access are enabled for root on the NetWorker server.
  Note: For Networker Virtual Edition (NVE), modify the `/etc/ssh/sshd_config` file to enable both password authentication and SSH access for root.
- SSH client is installed on the NetWorker server for Windows 2016.
- 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 CR Vault Data Domain system.

Procedure

1. Select **Recovery** from the Main Menu.
2. On the **Recovery** content pane, select the copy, and then click **APPLICATION**.
3. In the **Application** dialog box, select an application host, and then click **APPLY**.

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

   The recovery sandbox is created for the NetWorker application.
5. Click the job `recoverapp_<ID>` name and view the status detail.

   The Status Detail provides the name of the newly created sandbox.

Results

The latest NetWorker configuration is recovered.

CHAPTER 7

Performing an Avamar recovery with Cyber Recovery

This section describes how to recover data from Avamar point in time copies.

Recovering Avamar data

Use a point-in-time (PIT) copy to rehydrate Avamar data in the CR Vault.

The Avamar application must be installed as the root user in the CR Vault.

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 CR Vault environment.

A recovery operation is a two-step process:

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

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

Preparing the production-side Avamar system

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

Procedure

1. Log in to the production Avamar server as root user and run a checkpoint operation. This step might take some time.

   a. Type **`su admin -c "mcserver.sh --flush"`**:

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

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

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

root@ave-03:~/#: mccli checkpoint show
0,23000,CLI command completed successfully.
Tag                Time                      Validated Deletable
------------------ ------------------------- --------- ---------
cp.20180316130025 2018-03-16 09:00:25 EDT Validated No
cp.20180316130301 2018-03-16 09:03:01 EDT           No
cp.20180316151143 2018-03-16 11:11:43 EDT           No
```

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

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

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

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

```
sysadmin@crmgmthost# mtree list
Name                                                  Pre-Comp (GiB)
Status
----------------------------------------------------  --------------
-------
/data/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 CR Vault:

Done	Task	Notes
	Add the Avamar application as the root user.	
	Obtain the credentials for the host on which the Avamar application is installed.	
	Enable password authentication and SSH access for root on the Avamar server.	Modify the `/etc/ssh/sshd_config` file to enable both password authentication and SSH access for root.
	Ensure that the Avamar version and build are identical to the production system.	
	Ensure that the Avamar fully qualified domain (FQDN) name is identical to the production system.	You can use a different IP address in the CR Vault. The FQDN must be identical.
	Ensure that all Avamar credentials such as MCUser/GSAN accounts have the same passwords.	For Avamar services to start properly, the Avamar credentials must be the same.
	Ensure that the DD Boost username and UID in the CR Vault match the credentials of the production system.	Make sure that DD Boost username and UID are configured in the CR Vault before performing the Cyber Recovery steps.
	Obtain Avamar licenses, if necessary.	
	Establish Avamar applications in the CR Vault.	This task enables rehydrating applications in the CR Vault
	Ensure that DD OS version in the CR Vault is compatible with the Avamar application.	Make sure that the DD OS version works with the Avamar application.
	Configure the Data Domain hostname in the Avamar application.	Set this hostname in the CR Vault for the Avamar application to perform its recovery.

Creating the Avamar DD Boost account and UID for Cyber Recovery

Before performing an Avamar recovery, create the DD Boost account that is associated with the copy in the CR Vault.

Procedure

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 show -n <policy name>
   ```

   For example:

   ```
   # crcli login -u User1
   # crcli policy show -n av4
   ```

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

   ```
   Source Storage UID:  505
   ```

   Where 505 is the UID that you associated with this policy.

2. To determine if the account exists for this UID, log in to the Data Domain system in the CR 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 user name.

   b. If you are running DDOS 6.1.2.10 or later, create the username and account by running the following command:

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

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

      For example:

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

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 9 `temp` accounts.

Note: The user `add command` on the Data Domain system starts at UID 500.

Initiating an Avamar recovery in the Cyber Recovery UI

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

Before you begin

This procedure assumes:

- The Avamar application is installed in the CR Vault and defined as an application asset in Cyber Recovery.
- A policy has created a point-in-time (PIT) copy to use for the recovery.
- The UID associated with this copy has been created in the CR Vault Data Domain system.

Procedure

1. Select **Recovery** from the Main Menu.
2. On the **Recovery** content pane, select the copy and click **APPLICATION**.
3. In the **Recovery** dialog box, select the Avamar application host and click **APPLY**.

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

   The recovery sandbox is created for the Avamar application.
5. Click the `avamar-<GUID>` name, as shown in the following example code, and view the status detail:

   ```
   avamar-1560177494
   ```

   The Status Detail provides the name of the newly created sandbox. Use this name for the following recovery steps.

Performing manual steps for Avamar recovery

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

About this task

This procedure assumes that you have performed the GUI steps initiating the recovery as described in Initiating an Avamar recovery in the Cyber Recovery UI on page 50.

Procedure

1. In the CR Vault, log in to the Avamar server as root.
2. Edit the `/etc/hosts` file to alias the Data Domain data IP as the production Data Domain name.

Note: This change ensures that the restore operation uses the required production Data Domain name.

In the following example, `ddve-05` is the name of the production Data Domain system:

```
/#: cat /etc/hosts
127.0.0.1 localhost.localdomain localhost
::1       localhost.localdomain localhost
192.168.2.83    ave-03.vcorp.local ave-03
192.168.2.106   ddve-05.vcorp.local ddve-05
```

3. Verify that the Data Domain hostname resolves correctly:

```
# ping ddve05.vcorp.local
```

4. Cyber Recovery creates the recovery sandbox with the same name that Avamar uses in production. The HFS creation time (hfsctime) value is after the `avamar_` prefix. For example, the recovery sandbox is created as `avamar_1491947551` and the hfsctime is 1491947551. Use this value for the following step.
5. Run a checkpoint restore operation from the recovery sandbox by using the `HFS Time` of the Avamar DD Boost storage unit and the DD Boost user that is associated with that storage unit (similar to the following example):

   Note: Before proceeding with this command, ensure that the `ddr-user` name matches the name on the production system, including the UID.

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

   a. When prompted, enter the DD Boost password.

      The script displays a list of restorable checkpoints and asks which one you want to restore (similar to the following code example):

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

There are 4 available checkpoints.
    cp.20180315171722
    cp.20180316130025
    cp.20180316151143
    cp.20180316151143_1521213451
Checkpoint to restore or 'quit' to stop?
```

      Note: The preceding values differ on all systems.

   b. Enter the checkpoint that you want to restore and, when prompted, type `yes` to confirm your entry.

      The restore procedure is performed from the recovery sandbox and the script terminates with messages that confirm the operation.

6. On the CR Vault Data Domain system, perform the following steps:

a. Create the checkpoint snapshot by using the same checkpoint name that you selected in step 5b:

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

For example:

```
snapshot create cp.20180315171722 mtree /data/col1/avamar-20180315171722
```

7. Log back in to the Avamar system as root and stop the Avamar services:

a. Stop the Avamar services on the Avamar server:

```
# dpnctl stop
```

Note: This step might take a long time.

b. When asked if you want to shut down the instance, enter `y`.

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

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


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

c. When the process is completed, use the `dpnctl status` command to verify the results, as shown in the following code example:

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

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

d. Stop the Avamar Agent service:

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

e. Clear out the Avamar client ID (CID):

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

f. Start a rollback recovery of the checkpoint:

```
# dpnctl start --force_rollback
```

Note: This step might take a long time.

g. When asked if you want to continue, enter `y`.

```
Have you contacted Avamar Technical Support to ensure that this
  is the right thing to do?

Answering y(es) proceeds with starting all;
          n(o) or q(uit) exits


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

A message indicates:

```
The choices are as follows:
  1   roll back to the most recent checkpoint, whether or not validated
  2   roll back to the most recent validated checkpoint
  3  select a specific checkpoint to which to roll back
  4   do not restart
  q   quit/exit
```

h. Enter `3` to select a specific checkpoint.

The script displays a list of available checkpoints.

i. Enter the number that corresponds to the exact checkpoint name that you selected in the previous steps and on which you created the snapshot. Then enter `y` when prompted to confirm the recovery.

j. Wait for the rollback recovery to complete and the Avamar Services to start up.

8. Validate that all required services are up and running:

```
# dpnctl status
```

9. Add the SSH key for the CR Vault Data Domain system to the newly restored Avamar server, as shown in the following code example:

```
# echo \"Username: ddboost@ddve-05.vcorp.local\"; cat ~admin/.ssh/ddr_key.pub | ssh
ddboost@ddve-05.vcorp.local adminaccess add ssh-key
```

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

a. Regenerate the security certificates:

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

Reloading GSAN certificates for new changes to take effect

Done
```

b. View the session security settings:

```
# enable_secure_config.sh --showconfig

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

Client and Server Communication set to Authenticated mode with Two-Way/Dual
Authentication.
Client Agent and Management Server Communication set to secure_only mode.
Secure Data Domain Feature is Enabled.
```

c. Run the `avsetup mccli` command and accept all the defaults except for the MCUser password (similar to the following code example). Do not use the default value for MCUser.

```
#: avsetup_mccli
setting linux default
Enter the location of your JRE (1.8) installation [/usr/java/latest]:
Enter the root directory of your Avamar installation [/usr/local/
avamar]:
Enter the user data directory of your Avamar installation
[~/.avamardata/var]:

Configuring default local mcsprofile in /usr/local/avamar/lib/
mcclimcs.xml

Enter default mcs host name (mcsaddr) [ldpda126]:
Enter default mcs port number on ldpda126 (mcsport) [7778]:
Enter default userid on ldpda126 (mcsuserid) [MCUser]:
Enter password for MCUser (mcspasswd):
**********************************************************************
************
* EMC Avamar Management Console
(MC).                                                  *
* MC Security Tool for Secret Key generation, encryption, decryption
and digest. *
**********************************************************************
************

All MCCLI config files have been encrypted successfully.
See MCCipher log for details.
```

```
? 2012 EMC Corporation. All rights reserved.


        Avamar CLI 19.1.0 has been configured correctly
        Type mccli command to use it
```

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

d. Restart the Avamar MCS services:

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

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

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

e. Edit the Data Domain system configuration (similar to the following example):

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

f. Confirm the Data Domain system properties (similar to the following example):

```
# mccli dd show-prop --name=ddve-05.vcorp.local
0,23000,CLI command completed successfully.
Attribute                                  Value
------------------------------------------ -------------------
IPv4 Hostname                              ddve-05.vcorp.local
IPv6 Hostname                              N/A
Total Capacity (post-comp size)            821.9 GiB
Server Utilization (post-comp use%)        1%
Bytes Protected                            9.6 GB
File System Available (post-comp avail)    812.9 GiB
File System Used (post-comp used)          9.1 GiB
```

```
User Name                                       ddboost
Default Replication Storage System              Yes
Target For Avamar Checkpoint Backups            Yes
Maximum Streams For Avamar Checkpoint Backups 1
Maximum Streams                                 16
Maximum Streams Limit                           16
Instant Access Limit                            32
DDOS Version                                    6.0.1.0-556307
Serial Number                                   AUDVEWUJ7TS3V1
Model Number                                    DD VE Version 3
Encryption Strength                             none
Authentication Mode                             none
Monitoring Status                               OK
```

g. From the Data Domain system, revoke token access for DD Boost (similar to the following example):

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

For example

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

h. Stop the Avamar Agent service:

```
# /etc/init.d/avagent stop
avagent Info: Client Agent not running.
```

i. Edit the client properties:

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

j. Start the Avamar Agent service:

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

11. Log in to the Avamar GUI on the host server.
    a. Verify that the Data Domain system is displayed in the main window.
    b. Verify that the data that is represented on the Data Domain system matches that of the Avamar Data Domain system.
    c. Verify that all the policies, clients, and other configuration items match those of the production system.

12. Refer to Avamar standard operating procedures to reactivate clients in the CR Vault and perform the required application recoveries.

CHAPTER 8

Performing a PowerProtect Data Manager recovery with Cyber Recovery

This section describes how to recover data from PowerProtect Data Manager point-in-time copies.

Recovering PowerProtect Data Manager data

Use a point-in-time (PIT) copy to rehydrate PowerProtect Data Manager data in the CR Vault.

Initiate a PowerProtect Data Manager recovery by using the CRCLI. The Cyber Recovery software prepares your environment to recover VMs that are crash-consistent. Then, complete the recovery from the PowerProtect Data Manager application in the CR Vault.

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

Before a recovery operation, run application and server backups in the PowerProtect Data Manager production environment. Then, perform a Secure Copy policy operation to copy data to the CR Vault environment.

The PowerProtect Data Manager application must be installed as the admin user in the CR Vault.

Initiating a PowerProtect Data Manager recovery in the Cyber Recovery CLI

Initiate a recovery from the CRCLI.

Before you begin

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

- The CR Vault Data Domain system must be running DD OS Version 6.2 or later.
- You have deployed the PowerProtect Data Manager OVA file in the CR Vault. The PowerProtect Data Manager application must be installed as the admin user.
- The UID's that are associated with the production PowerProtect Data Manager DD Boost users are configured in the CR Vault Data Domain system. These UID's must be available in the Data Domain system in the CR Vault.
- The PowerProtect Data Manager application in the CR Vault must be configured with the credentials of the PowerProtect Data Manager application on the production system.
- The PowerProtect Data Manager server host within the CR Vault uses the same IP address and hostname as the PowerProtect Data Manager production host.
- The PowerProtect Data Manager application is defined as an application asset in the Cyber Recovery software. Use either the Cyber Recovery UI or the CRCLI to add the application.
- You have performed a Secure Copy policy operation to copy data to the CR Vault environment.
- You have created a policy for the VM data and a policy for the server backup.

Procedure

1. Log in to the PowerProtect Data Manager application in the CR Vault.

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

2. Take a VM snapshot of the PowerProtect Data Manager appliance.

   You use this snapshot to revert the PowerProtect Data Manager software after you complete the recovery.

3. Log in to the CRCLI.

4. Run the `recovery run` command. Ensure that you specify the backup copy first and then the data copy, as shown in the following example:

```
# crcli recovery run --action <action> --backupcopyname <metadata backup copy> --
copyname <PPDM data copy> --appnickname <PPDM application>
```

> **Note:** The backup metadata and data copies must be in the correct order on the command line.

For example:

```
# crcli recovery run -a recoverapp -b cr-copy-Backup-P-20190812170227 -c cr-copy-Data-
Pol-20190812170232 -i app1-PPDM
```

5. At the prompt, enter the lock box passphrase of the production PowerProtect Data Manager appliance.

   The Cyber Recovery software prepares your environment so that you can run a VM recovery from the PowerProtect Data Manager application console. As part of this process, the software creates a production DD Boost username and password and reboots the PowerProtect Data Manager appliance.

Performing postrecovery steps for a PowerProtect Data Manager recovery

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

Procedure

1. From the Cyber Recovery UI or the CRCLI, delete the two sandboxes that were created when you initiated the PowerProtect Data Manager recovery.
2. Optionally, on the Data Domain system, run the `filesys clean` command.

   This step deletes the DD Boost storage unit. If you choose not to perform this step, the DD Boost storage unit is deleted during the next scheduled cleaning operation.
3. Run the `user unassign` and `user del` command to delete the DD Boost user.

   ```
   # user unassign <DD Boost user>
   # user del <DD Boost user>
   ```

4. Revert the PowerProtect Data Manager software to the snapshot that you created in step 2 of Initiating PowerProtect Data Manager recovery in the Cyber Recovery CLI.

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

CHAPTER 9

Administration

This section covers the following 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).

Manually securing and releasing the CR Vault

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

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

- To secure the CR Vault if you suspect a security breach, click **SECURE VAULT** so that the CR Vault status changes from **Locked** to **Secured**. All Sync policy operations stop immediately and no new Sync policy operations can be initiated. The Cyber Recovery software also issues an alert that the CR Vault is secured.
  Note: All non-Sync policies can be run in the CR Vault while it is secured.
- To unsecure the vault when you are confident that there is no longer a security threat, click **RELEASE VAULT**. The CR Vault status returns to **Locked**. Sync policy operations can now be initiated.

For more information about the CR Vault status, see Monitoring the CR Vault status on page 38.

User roles

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

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

Note: Do not confuse the Cyber Recovery Security Officer with the Data Domain Security Officer for Data Domain Compliance retention locking.

There are three Cyber Recovery user roles:

- Dashboard—This role enables the user to view the Cyber Recovery dashboard but not perform tasks.
- Admin—This role has the following permissions:
  - Create, modify, and disable dashboard users
  - Create, manage, and run policies and associated objects
  - Acknowledge and add notes to alerts
  - Change administrative settings
  - Modify own user account
  - Change own password
  - Manually secure and release (unsecure) the CR Vault
- Security Officer—This role has the following permissions:

- All Admin permissions
- Create, modify, and disable users
- Change and reset user passwords
- Change the Security Officer password

If as the Security Officer, you forget your password, use the `crsetup.sh` script to reset it. For instructions, see Resetting the Security Officer password.

Managing users

The Security Officer creates, modifies, and disables users.

About this task

The Security Officer can enable and disable users, but not delete them.

Procedure

1. Select **Administration** > **Users** from the Main Menu.
2. Do one of the following:
   - To create a user, click **ADD**.
   - To modify a user, select a user and click **Edit**.
3. Complete the following fields in the dialog box.

Field	Description
Name fields	Specify the user's first name and last name.
Role	Select either: • Admin—Enables users to perform tasks in the Cyber Recovery software. • Dashboard—Enables users to view the Cyber Recovery dashboard but not perform tasks. The dashboard role does not time out.
User Name (required)	Specify a username.
Phone	Specify the user's telephone number.
Email (required)	Specify an email address for alert notifications if the user is configured to receive them.
Password/Confirm New Password (required)	Specify and confirm the password. 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 (~!@#$%^&*()+={}|:";<>?[]-_.,^') When you change a password, enter and confirm both the new and existing passwords.
Session Timeout	Select the amount of idle time after which the user is logged out of the Cyber Recovery UI.

4. Click **SAVE**.
5. Enable and disable users:
   a. Select the user and click **DISABLE**.

b. Click **DISABLED USERS** at the top of the content pane and note that the table lists the newly disabled user.

c. Select the user and click **ENABLE**. Note that the table no longer lists the user.

d. Click **ENABLED USERS** at the top of the content pane and note that the table lists the newly enabled user.

Managing login sessions

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

Before you begin

You must be assigned the Security Officer role to change login session settings.

About this task

The login session count uses a first in, first out priority. If a specific user and role exceeds the number of simultaneous logins, that user's earliest session is longer a valid Cyber Recovery session and the session is logged out. The user must log in to the Cyber Recovery software again.

Procedure

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

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

   - Security Officer—one login session
   - Admin—three login sessions
   - Dashboard user—three login sessions

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

   The maximum number of login sessions for each user is 10.

Configuring email notifications

If your configuration is set up to allow email to leave the CR Vault, specify which users receive email notifications about alerts.

Specifying which users receive email

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** check boxes.
   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 if the email was received.

Connecting to an email server

After you have configured an SMTP server, use Postfix to route and deliver Cyber Recovery email notifications to Cyber Recovery users. Postfix is an open-source mail transfer agent that is included in most non-Windows systems.

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

To set up the Postfix configuration:

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

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

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

   a. Add the inet address:

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

Note: Ensure that you do not uncomment more than one inet_interface.

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

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

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
```

Changing the lockbox passphrase

For security purposes, use the `crsetup.sh` script to change the Cyber Recovery lockbox passphrase.

Before you begin

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

Note: This procedure is disruptive; it causes the Docker container services to be stopped.

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.

Note: Ensure that there are no jobs running before you change the lockbox password. Otherwise, the CR Vault might go to an unsecured state.

Procedure

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

```
# ./crsetup.sh --lockbox
```

3. When prompted to continue, enter **y**.

   The script stops the Docker container services.
4. When prompted, enter the current lockbox passphrase.
5. When prompted, enter and confirm the new lockbox passphrase.

   The script changes the passphrase and then restarts all Docker container services.

Changing the database password

For security purposes, use the `crsetup.sh` script to change the Cyber Recovery database password.

Before you begin

- You must provide the lockbox passphrase, which is created during the Cyber Recovery installation.
- Ensure that there are no jobs running before you change the database password.

Note: This procedure is disruptive; it causes the Docker container services to be stopped.

About this task

Cyber Recovery microservices communicate with the MongoDB database to access policies and other persisted data. The database is password-protected and only accessible by the microservices that run in the Cyber Recovery environment.

Procedure

1. Log in to the management host and go to the Cyber Recovery installation directory.

2. Enter the following command:

```
# ./crsetup.sh --mongodb
```

3. When prompted, enter `y` to continue.

   The script stops the Docker container services.

4. When prompted, enter and confirm the new database password.

   The script starts the Docker container services.

Resetting the Security Officer password from the management host

As the Security Officer (crso), use the `crsetup.sh` script to reset the crso password.

Before you begin

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

About this task

As the Security Officer, use the Cyber Recovery UI or Cyber Recovery CRCLI to change the crso password. However, if you forget the crso password or if there is a change in Security Officer, use the `crsetup.sh` script.

Procedure

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

```
# ./crsetup.sh --crso
```

3. When prompted, enter `y` to continue with the change.
4. When prompted, enter the lockbox passphrase.
5. Enter and confirm the new crso password.

   A message indicates that the change is successful.

Resetting the IP address on the management host

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

Before you begin

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

Procedure

1. Modify the IP address of the Cyber Recovery management host.
2. Restart the network service:

```
# service network restart
```

3. Restart Docker:

```
# service docker restart
```

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

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

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

```
# docker ps -a
```

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

Changing the log level

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

About this task

Cyber Recovery supports two log levels:

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

The default log level is Info.

Procedure

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

Collecting logs for upload

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

Procedure

1. From the Masthead Navigation, click the gear icon to access the **System Settings** list.
2. Click **Log Settings**.
3. In the **Service Log Level** dialog box, click **GENERATE LOG BUNDLE**.

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 associatedData Domain systems in the vault environment. To view these collections, click **Settings** (gear icon) in the PowerProtect DD Management Center and select **System** > **Support** > **Support Bundles**.

4. Click **OK** to dismiss the **Log Bundle** window and then close the **Service Log Level** dialog box.

Deleting unneeded Cyber Recovery objects

Delete alerts, events, expired and unlocked copies, and jobs when they are no longer needed. By setting a Cyber Recovery cleaning schedule, you can avoid system slowdown.

Procedure

1. From the Masthead Navigation, click the gear icon to access the **System Settings** list.
2. Select **Cleaning Schedule**.
3. In the dialog box, specify the frequency for when the schedule runs and the age of the objects to be deleted.
4. Optionally, change any of the default settings.
5. Click **Save** so that the data retention schedule runs at the specified time.

Cyber Recovery disaster recovery

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

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

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

See Cleaning up existing Cyber Recovery Docker containers on page 71.

After you clean up the existing Docker containers, follow the procedure to restore the Cyber Recovery software. For more information, see Restoring a Cyber Recovery installation after a disaster on page 73.

Cleaning up existing Cyber Recovery Docker containers

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

Procedure

1. Identify the Cyber Recovery containers that are running:

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

The output shows the running Cyber Recovery containers, which might be similar to the following example:

- cr_swagger
- cr_ui
- cr_edge
- cr_schedules
- cr_policies
- cr_mgmtdds
- cr_apps
- cr_notifications
- cr_vault
- cr_users
- cr_mongo-auth
- cr_registry

Note: Each container name includes a suffix, which differs depending on your version of Docker Compose.

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 clean up is complete.

8. Perform to the Cyber Recovery software restore procedure (see Restoring a Cyber Recovery installation after a disaster on page 73).

Restoring a Cyber Recovery installation after a disaster

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

Before you begin

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 on page 71.

About this task

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

Procedure

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

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

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

2. When the installation is complete, start the UI and validate that the configuration is empty.
3. Close the UI.
4. Start the Cyber Recovery software restore procedure:

   a. Run the `crsetup.sh` setup script:

   ```
   crsetup.sh --recover
   ```

   b. Type **y** to continue:

   ```
   Do you want to continue [y/n]:
   ```

   c. Type **y** to confirm and continue:

   ```
   Are you REALLY sure you want to continue [y/n]:
   ```

   d. Type the full path to the Cyber Recovery backup tar package location, for example:

   /tmp/cr_backups/cr.19.2.1.0-3.2019-09-19.08_02_09.tar.gz

e. Type the newly installed MongoDB password.

```
Please enter the newly installed MongoDB password:
```

Note: This password is the password that you created when you reinstalled the Cyber Recovery software in step 1.

f. Type the newly installed MongoDB password again to confirm:

```
 Enter newly installed MongoDB password:
```

g. 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.

CHAPTER 10

Troubleshooting

This section describes the following topics:

Troubleshooting suggestions

The following table lists possible Cyber Recovery problems and suggested remedies.

If you cannot	Do this

Install the Cyber Recovery software	• Ensure that the `crsetup.sh --check` command passed 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)
	  ▪ 14779 (for the Cyber Recovery Registry - local management host access)
	  ▪ 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)
	  ▪ 14779 (for the Cyber Recovery Registry - local management host access)
	  ▪ 14780 (for the Cyber Recovery API Documentation)

Run a job	Check the schedules, policies, or mgmtdds service logs.
Receive alert email messages	• If your system has an active firewall, ensure that port 25 is open on the firewall. • Verify your Postfix or email configuration and check that you added the email for alert notifications.
Secure the CR Vault	Check the vault service logs.
Recover or analyze	Check the policies and apps service logs.
Complete a NetWorker recovery operation cleanly. For example, if you encounter a problem during the automated recovery process.	Perform a manual cleanup: 1. Shutdown NetWorker For example: **`/etc/init.d/networker stop`** 2. For the resource database, complete the following steps:

If you cannot	Do this
	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: **`mv /nsr/mm.cr.155512814 /nsr/mm`** 4. Restart NetWorker. For example: **`/etc/init.d/networker start`**

Cyber Recovery logs

The Cyber Recovery software generates both a JSON and a text logfile for each service.

The logfiles are in the `/opt/dellemc/cr/var/log/<service>` directory, where *service* is one of the following services:

Services	Log message content
edge	The routing for all calls from REST clients, the Cyber Recovery CLI, and the Cyber Recovery UI, as well as the logic for setting system log levels, licensing, and dashboard. **Note:** This service is the entry point for all REST API calls.
apps	Anything that is related to applications that are associated with Cyber Recovery, including Index Engines' CyberSense used for copy analysis, NetWorker, Avamar, and PowerProtect Data Manager instances, and file system hosts.
mgmtdds	All communication with the CR Vault Data Domain.
notifications	All the system notifications (alerts and events) and SMTP email messages.
policies	Anything that is related to policies, jobs, copies, and sandboxes.
schedules	All the system schedules, cleaning schedules, and action endpoints.
users	Anything that is associated with users, including addition, modification, and authentication operations.

Services	Log message content
vault	Anything that is related to the status of the vault, and opening and closing managed interfaces.

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.

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.	• Corrupted or truncated file • Policy 1 hour over the sync timeout period of 6 hours
INFO	Reports information about the progress of an operation or task.	• 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.

To stop or start the Docker container services, use the `crsetup.sh` script that is located in the Cyber Recovery installation directory.

Enter the following command to stop the Docker container services:

```
# ./crsetup.sh --stop
```

The following Cyber Recovery Docker container services stop in this order:

Service	Function
schedules	Manages Cyber Recovery schedule actions
edge	Acts as the gateway to the Cyber Recovery services
apps	Manages storage system and applications in the CR Vault actions
vault	Manages CR Vault actions
mgmtdds	Manages the Data Domain actions in the CR Vault
policies	Manages Cyber Recovery policy actions
ui	Manages Cyber Recovery UI actions
users	Manages the Cyber Recovery Admin users and the Security Officer user actions
notifications	Manages alert, event, email, and log actions
swagger	Provides access to the Cyber Recovery REST API documentation
Mongo-auth	Manages the database

Enter the following command to start the Docker container services:

```
# ./crsetup.sh --start
```

The Docker container services start again.

Note: At this time, you cannot stop and start an individual Docker container service.

Delete devices that are recovered onto your NetWorker server

After an automated NetWorker recovery using the Cyber Recovery software completes, manually delete devices that the procedure recovered onto your NetWorker server.

About this task

Your NetWorker server might include other devices that were there before the Cyber Recovery backup recovery job.

Note: Only delete devices that the Cyber Recovery software recovered onto your NetWorker server. Ensure that you do not delete devices that you must keep.

Procedure

1. Unmount the NetWorker sandbox from the Cyber Recovery management host:

   ```
   umount /opt/dellemc/cr/mnt/cr-rec-ldpda240_1604
   ```

2. Go to the NetWorker UI.
3. From the **Protection** tab, perform the following tasks:
   a. Delete newly added clients.
   b. Delete newly added policies.
   c. Delete newly added groups.
   d. Delete any other newly added protection types.
4. From the **Devices** tab, perform the following tasks:
   a. Delete newly added devices.
   b. Delete newly added Data Domain system.
   c. Delete newly added storage nodes (if necessary).
5. From the **Media** tab, perform the following tasks:
   a. Delete newly added disk volumes.
   b. Delete newly added media pools.
   c. Delete any other newly added media types.

Disabling SSH access to the replication interface

Disable SSH access to the replication interface on the CR Vault Data Domain system.

About this task

The Cyber Recovery software works with a replication data link between the vault-environment and production-environment Data Domain systems. The Cyber Recovery software communicates with all Data Domain systems by using SSH.

Optionally, use the following procedure on the Data Domain host to restrict SSH inbound access for the Cyber Recovery management host:

Procedure

1. On the management host, obtain the hostname.

2. Log in to the Data Domain host and enter the following command:

   ```
   adminaccess ssh add <hostname>
   ```

   where *<hostname>* is the hostname from step 1.

3. Use the Data Domain net filter functionality.

   For information about how to use the net filer functionality, see the Data Domain documentation.

Results

SSH is blocked on all interfaces except the management interface.

CHAPTER 11

Cyber Recovery Command Line Interface (CRCLI)

This chapter covers the Cyber Recovery command line interface (CRCLI).

CRCLI overview

The Cyber Recovery Command Line Interface (CRCLI) enables you to perform Cyber Recovery management tasks from a command line. The commands represent a subset of the functionality that is available in the Cyber Recovery UI.

The CRCLI is typically used by administrators. If the Cyber Recovery software is installed using the default locations, the CRCLI is located in the `/opt/dellemc/cr/bin` directory.

Functionality

The following table lists the Cyber Recovery operations that you can perform with the CRCLI.

Module	Functionality
login / logout	• Log in a user • Log out the current user
users	• Create users • Modify users • Disable and enable users • List users • Show user details • Change user passwords • Configure email notifications for users
dd **Note:** A storage object in the Cyber Recovery UI corresponds to dd in the CRCLI.	• Create a Data Domain • Modify a Data Domain • List Data Domains • Show Data Domain configuration
apps	• Create an application • Modify application • List applications • Show application details

policy	• Create a policy
	• List all policies
	• Run a policy with the following actions:
	  ▪ sync
	  ▪ sync-copy
	  ▪ secure copy
	  ▪ copy
	  ▪ copy-lock
	  ▪ lock

Module	Functionality
	▪ analyze • Show details about a policy • List jobs by policy • Get details about a specific job • Cancel a job • List PIT copies by policy • List sandboxes by policy
schedules	• Create schedules • List schedules • Modify schedules • Delete schedules
recovery	• Perform a recovery operation • List current recoveries
vault	• Secure (lock) the vault • Release (unlock) the vault • Show vault status
alerts	• List alerts • Show alert details • Acknowledge an alert • Add note to an alert
events	• List events • Show event details
system	• Initiate Cyber Recovery log collection and Data Domain support bundle. • Change log level settings • Change cleaning schedule settings
license	• Add a license • Show license information
version	Display the Cyber Recovery version and build number
help	Display help

CLI help system

The CRCLI help system provides reference documentation that gives detailed information about each command.

After you log in to the CRCLI, you can access help:

- To view the entire help system, enter:

```
# crcli help
```

- To view help for a specific module, include the module name in the command:

```
# crcli policy help
```

- To view help for a specific action, include the action name after the module name:

```
# crcli apps add help
```

The help system shows both required and optional parameters. In the following example, required parameters are listed first, followed by optional parameters that are enclosed within brackets ([ ]).

```
 # crcli users add help

  -a, --alertnotification string   (optional) ex. --alertnotification "critical"
  -e, --email string               (required) ex. --email user@sample.com
  -f, --firstname string           (optional) ex. --firstname "Mickey"
  -l, --lastname string            (optional) ex. --lastname "Mouse"
  -p, --phone string               (optional) ex. --phone 555-555-5555
  -r, --role string                (required) ex. --role admin
  -u, --username string            (required) ex. --username "admin1"

crcli users add   <Add a new user>

          --username <name of the user> --role <role of users> --email <email of user>
[ <options> ]
          -u "admin1" -r "admin" -e "admin1@local.com"
    Required:
                username             : Set the desired username
                role                 : Set the desired role for the user (Roles: admin,
dashboard)
                email                : Set the email address for the user
    Options:
                firstname            : Set the users first name
                lastname             : Set the users last name
                phone                : Set the users phone number
                alertnotification    : Define the type of alert the user will receive via
email (Alert Types: critical, warning)
    Examples:   crcli users add --username admin1 --role admin --email admin1@local.com
```

Using the CRCLI commands

All CRCLI commands have the same basic structure.

```
crcli <module> <operation> <parameters>
```

where:

- *<module>* is the module name, for example *users* or *policy*.
- *<operation>* is the operation name, for example *list*, *run*, or *show*.
- *<parameters>* are one or more required and optional parameters.

Parameters

CRCLI commands have both required and optional parameters.

To include a parameter, specify the parameter name or pflag followed by the parameter value. Two dashes precede the parameter names; a single dash precedes the pflags.

Use the CRCLI help system to view the parameters and pflags. For example, enter **crcli policy add** to view the parameters for adding a policy.

```
crcli policy add help
  -w, --jobwindow string                (optional) ex. --jobwindow 1h
  -h, --mgmtddid string                 (required) ex. --mgmtddid 5aec99e97f9d0732fcef00fb
  -c, --mgmtddreplctxname string        (required) ex. --mgmtddreplctxname "mtree://dd1/data/
col1/repl-1"
  -e, --mgmtddreplethinterface string   (required) ex. --mgmtddreplethinterface "ethV1"
  -n, --policyname string               (required) ex. --policyname "policy1"
  -d, --retlockduration string          (optional) ex. --retlockduration 1d (default "12h")
  -x, --retlockmax string               (optional) ex. --retlockmax 45d (default "45d")
  -m, --retlockmin string               (optional) ex. --retlockmin 12h (default "12h")
  -y, --retlocktype string              (optional) ex. --retlocktype compliance (default
"governance")
  -u, --securityuser string             (optional) ex. --securityuser ddso
  -t, --tags string                     (optional) ex. --tags "NW92,finance,daily"
```

Policy actions

When you run a policy, you can specify multiple **--action** parameters to define different actions.

Each **--action** parameter specifies a request operation:

- sync
- copy
- lock
- copy-lock
- sync-copy
- securecopy
- analyze

CRCLI password commands

For security purposes, do not specify passwords in CRCLI commands.

The CRCLI prompts you for passwords as needed. For example, an administrator name and password are required to create a storage object. However, when creating the object with the CRCLI, you specify the username, but not the password. After you issue the command, the CLI prompts you for the password value.