Dell EMC PowerProtect Cyber Recovery

Version 19.2

Installation Guide

302-005-889

Rev 02

January 2020

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

Getting Started

Dell EMC PowerProtect Cyber Recovery software provides protection by replicating backup data from a production system to a secure air-gapped vault system.

This section describes the production system and Cyber Recovery Vault (CR Vault) prerequisites that are required to install the Cyber Recovery software.

ⓘ **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.

Production system requirements

Production storage requirements

The production environment must have at least one Data Domain system with at least one MTree replication context that is configured for replication to the Data Domain system in the CR Vault.

When multiple Data Domain systems are deployed in the production environment, they can be configured to replicate as many as five Data Domain systems in the CR Vault.

Production backup and recovery applications

The Cyber Recovery software supports Data Domain integrations with the NetWorker, Avamar, and PowerProtect Data Manager applications.

Supported Avamar versions:

- Version 7.4, 7.5, 18.1, 18.2, and 19.1
- Single-node physical appliance or Avamar Virtual Edition (AVE)-only server (Avamar grids are not supported)

ⓘ **Note:** Validated Avamar checkpoints are stored on the Data Domain system.

Supported NetWorker versions:

- Version 9.1, 9.2, 18.1, 18.2, and 19.1

ⓘ **Note:** The NetWorker server database and data devices are stored on the Data Domain system.

Supported PowerProtect Data Manager versions:

- Version 19.2
- DD OS must be Version 6.2 or 7.0
- The PowerProtect Data Manager server backups and policy data are stored on the Data Domain system.

CR Vault system requirements

Docker containers

The following Docker components are required to install Cyber Recovery software:

- Docker Version 18.09.7—Refer to Download Docker.

  ⓘ **Note:** RedHat Linux and SUSE Linux Enterprise Server only support Docker Enterprise Edition (EE). CentOS Linux also supports Docker Community Edition (CE).

- Docker Compose Version 1.24.0 or earlier—Refer to Install Docker Compose.

If you are using a firewall, install Docker after you set up the firewall. At installation, ensure that you enable Docker to restart and to configure firewall settings automatically when the management host reboots.

ⓘ **Note:** Ensure that you install the stable version of Docker.

Cyber Recovery management host

The management host is a physical or VM host with the following requirements:

- One of the following operating systems with the latest updates, patches, and security patches:
  - CentOS Linux Version 7.6
  - Red Hat Enterprise Linux Version 7.4, 7.5, and 7.6
  - SUSE Linux Enterprise Server Version 12 SP3 and 12 SP4
- 4 GB RAM
- 50 GB disk space
- 1.5 GB free space to extract the Cyber Recovery software
- 10 GB or more free space for installation of the Cyber Recovery software

TCP ports

A number of TCP ports on the management host must be reserved for use by the Cyber Recovery software.

The following table lists the required and optional network ports that Cyber Recovery functions require.

Port	Required	Service	Direction	Description
14777	Yes	Nginx	Inbound	Provides web browsers with HTTPS access to the Cyber Recovery UI.
14778	Yes	REST API	Inbound	Provides the HTTPS connection to the Cyber Recovery REST API.
14779	Yes	Cyber Recovery Docker Registry	Inbound	Used to upload or download Docker container images. The installation and upgrade scripts retrieve the images from the registry, if needed.
14780	No	Swagger	Inbound	Provides access to the Cyber Recovery REST API documentation.
27017	Yes	MongoDB	Inbound	Provides access to the database that holds Cyber Recovery configurations
22	Yes	SSH	Outbound	Provides SSH communication between systems in the CR Vault.
25	No	Notifications	Outbound	Used for SMTP email notifications about alerts and events.
2052	Yes	NFS Client	Outbound	Used for the NFS client to mount the Data Domain instance in the CR Vault and apply retention locking.

CR Vault storage requirements

The CR Vault storage environment includes a minimum of one and a maximum of five physical or virtual Data Domain systems on the same network as the Cyber Recovery software. Each Data Domain system has the following requirements:

- Version 6.0.2.20, 6.1, 6.2, and 7.0

  ⓘ **Note:** Deployments that use the PowerProtect Data Manager application for recoveries must run DD OS Version 6.2 or higher.

- Two Ethernet interfaces:
  - A primary interface is for the Data Domain hostname.
  - A second dedicated interface, which is managed by the Cyber Recovery software, is for replication.
- A Data Domain account with the admin role for use by the Cyber Recovery software to manage Data Domain operations. We recommend that you name this account *cradmin*, however, you can provide a name of your choosing.

  ⓘ **Note:** You cannot use the sysadmin account for the Cyber Recovery Data Domain system.

- Valid licenses for DD Boost, Replication, Retention Lock Governance, and Retention Lock Compliance.

  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.

- For each Cyber Recovery policy in the vault, capacity for at least three MTrees to protect one production MTree.

ⓘ Note: Dell EMC recommends that you perform an initial replication between the production and vault systems for each replication context before you define Cyber Recovery policies.

CR Vault backup and recovery applications

Optionally, deploy applications in the Cyber Recovery environment.

The following supported applications can perform recoveries from the CR Vault:

- Avamar Version 7.4, 7.5, 18.1, 18.2, and 19.1, with the following requirements:
  - The same Avamar version that is deployed on the production system
  - A single-node or AVE server (Avamar grids are not supported)
  - An uninitialized and correctly sized Avamar instance that is equivalent to the size of the Avamar instance on the production system
  - A hostname that matches the production hostname
  - The Data Domain system has the same Avamar DD Boost account name and UID
- NetWorker Version 9.1, 9.2, 18.1, 18.2, and 19.1, with the following requirements:
  - The same NetWorker version that is deployed on the production system
  - An uninitialized and correctly sized NetWorker instance that is used to perform an `nsrdr` operation by using data replicated from the production Data Domain system to the CR Vault Data Domain system
- PowerProtect Data Manager Version 19.2, with the following requirements:
  - DD OS Version 6.0.2.20, 6.1, 6.2, and 7.0
  - Credentials for the PowerProtect Data Manager host and the PowerProtect Data Manager application that match the production system
  - A hostname and IP address that matches the production hostname

ⓘ Note:

- Follow the documented Avamar, NetWorker, and PowerProtect Data Manager procedures for deployment in the CR Vault environment. Go to Dell EMC Online Support to find the latest Avamar, NetWorker, and PowerProtect Data Manager documentation.
- Follow the Cyber Recovery documentation to run the recovery procedures.

Index Engines' CyberSense software

Optionally, deploy Index Engines' CyberSense software, which is a third-party tool that validates and analyzes point-in-time copies for the presence of malware or other anomalies. A report provides indication of compromise.

For more information, refer to the Index Engines website.

Index Engines' CyberSense must be installed in the CR Vault.

Requirements include:

- Index Engines' CyberSense 7.0. For the latest compatibility matrix from Index Engines, see CyberSense Support Matrix.
- A dedicated host running CentOs or Red Hat Enterprise Linux, on which the Index Engines software is installed, that acts as the validation host. The validation host provides direct integration between the Cyber Recovery software and the Index Engines software.

CHAPTER 2

Installing the Cyber Recovery Software

This section provides instructions for installing the Cyber Recovery Version 19.2 software.

ⓘ **Note:** If you are running Cyber Recovery Version 18.1 or Version 19.1.0.4, see Upgrading the Cyber Recovery software version on page 19.

Obtaining the Cyber Recovery software

Go to Dell EMC Online Support to obtain the Cyber Recovery installation package.

Installing the Cyber Recovery software

Use the `crsetup.sh` setup script to install the Cyber Recovery software.

Before you begin

Ensure that you satisfy all preinstallation requirements (see Getting Started on page 7).

About this task

The installation procedure takes approximately five minutes.

Procedure

1. Log in to the Cyber Recovery management host as **root**.
2. Download the Cyber Recovery installation package to a directory with approximately 1.5 GB of free space.
3. Untar the installation package:

   ```
    # tar -xzvf <installation package tar file>
   ```

   The file is untarred to the `staging` directory (within the current directory). The extraction includes the `crsetup.sh` setup script.
4. Go to the `staging` directory and make the `crsetup.sh` setup script an executable script:

   ```
   # cd staging
   # chmod +x ./crsetup.sh
   ```

5. Verify that the prerequisite software is installed:

   ```
   # ./crsetup.sh --check
   ```

The following shows sample output:

```
19.08.30 13_45_20 : ============================================================
19.08.30 13_45_20 : # Checking pre-requisite software requirements...
19.08.30 13_45_20 : ============================================================
19.08.30 13_45_20 :
19.08.30 13_45_20 : Verify OS support .................... PASSED (Installed CentOS version
7.5.1804 meets the minimum 7.4+ requirement)
19.08.30 13_45_20 : Verify Required OS Packages .......... PASSED (nfs-utils INSTALLED on the
Management Host)
19.08.30 13_45_20 : Verify Required OS Packages .......... PASSED (postfix INSTALLED on the
Management Host)
19.08.30 13_45_20 : Verify Required OS Binaries .......... PASSED (Required binary 'find' is
installed)
19.08.30 13_45_20 : Verify Required OS Binaries .......... PASSED (Required binary 'grep' is
installed)
19.08.30 13_45_20 : Verify Required OS Binaries .......... PASSED (Required binary 'sed' is
installed)
19.08.30 13_45_20 : Verify Required OS Binaries .......... PASSED (Required binary 'readlink' is
installed)
19.08.30 13_45_20 : Verify Required OS Binaries .......... PASSED (Required binary 'ifconfig' is
installed)
19.08.30 13_45_20 : Verify Required Third Party Binaries . PASSED (Required binary 'docker' is
installed)
19.08.30 13_45_20 : Verify Required Third Party Binaries . PASSED (Required binary 'docker-compose'
is installed)
19.08.30 13_45_20 : Docker Client & Server versions ...... PASSED (Installed Docker Server (Engine)
version 18.03.1 meets the minimum Docker 17.06 + requirement)
19.08.30 13_45_20 : Verify Docker System Restart Enabled . PASSED (Docker properly configured for
system restart)
19.08.30 13_45_20 : Verify Required Port ................ PASSED (14777 AVAILABLE on the
Management Host)
19.08.30 13_45_20 : Verify Required Port ................ PASSED (14778 AVAILABLE on the
Management Host)
19.08.30 13_45_20 : Verify Required Port ................ PASSED (14779 AVAILABLE on the
Management Host)
19.08.30 13_45_20 : Verify Required Port ................ PASSED (14780 AVAILABLE on the
Management Host)
```

If any prerequisites are not satisfied, do not proceed with the installation.

6. Use the `hostname -i` command to determine if there are multiple IP addresses that are associated with the management host. If the command returns multiple IP addresses, use the following command to specify the IP address for the Cyber Recovery software to use to communicate with the Data Domain storage in the CR Vault:

```
# export dockerHost=<IP address>
```

7. Begin the installation:

```
# ./crsetup.sh --install
```

8. When prompted, press Enter to view the End User License Agreement (EULA). Enter **q** to exit the EULA at any time, and then enter **y** to accept the EULA.

   If you decline the EULA, the installation stops. Otherwise, the installation continues.

   The installation procedure attempts to create a Linux user (cyber-recovery-admin) on the management host in the CR Vault. It assigns a reserved UID:GID of 14999 to the cyber-recovery-admin user. This user owns specific installation directories.

   If the reserved UID:GID 14999 is assigned to another user or the cyber-recovery-admin user exists but is not assigned the reserved UID:GID 14999, the installation procedure issues a warning message. Otherwise, the installation procedure continues.

9. If the installation procedure displays a warning about creating the cyber-recovery-admin user, indicate if you want to continue or cancel the installation.

   If you complete the installation, the Cyber Recovery software operates correctly, however, a non-cyber-recovery-admin user might own some installation directories.

10. When prompted, specify the directory where you want to install the Cyber Recovery software or press Enter to accept the default location.

11. When prompted, specify the directory where you want to install the database or press Enter to accept the default location.

    Output is displayed about creating directories, loading Docker containers, and starting the Docker registry and MongoDB database.

    Note: The installation procedure also creates internal IP addresses that enable communication between the Docker containers.

12. At the prompts that follow, enter and confirm a lockbox passphrase, database password, and Security Officer (crso) account password of your choosing.

    Note: Remember the lockbox passphrase. It is required to perform upgrades and reset the Security Officer's password. If you forget the lockbox passphrase, you must reinstall the Cyber Recovery software. If you have to change the lockbox passphrase, see the Dell EMC PowerProtect Cyber Recovery Product Guide.

    Enter a unique passphrase or password for the lockbox, the database, and the crso account.

    The passphrase and password requirements are:

    - Between 9-64 characters
    - At least one uppercase character
    - At least one lowercase character
    - At least one number
    - At least one special character: ~!@#$%^&*()+={}|:";<>?[]-_.,^'.

Results

The installation procedure starts Cyber Recovery services and then exits.

The installation procedure loads the `cyber-recovery.service` file. If the Cyber Recovery management host restarts after a shutdown, this file directs the management host to start the Cyber Recovery services automatically.

Note: At this time, the full system control options are not configured. If you run the `systemctl` command for `cyber-recovery.service`, the status is displayed as inactive.

After you finish

In your browser, go to the URL shown at the end of the installation script. Then, log in to the Cyber Recovery UI using the default Security Officer (crso) account and the password that you created.

Note: If your system has an active firewall, ensure that the ports that are listed at the end of the installation script are open on the firewall.

Logging in initially

The Cyber Recovery installation procedure adds the *crso* user to the database. This user has the Security Officer role and must perform the initial login and then create one or more admin users.

Procedure

1. In a supported browser, go to `https://<hostname>:14777`

   where <*hostname*> is the hostname of the management host.

2. In the **Username** field, enter `crso`.
3. In the **Password** field, enter the Security Officer (crso) password and click **LOG IN**.

   The Getting Started wizard displays in the Cyber Recovery UI.

After you finish

Do the following:

- Complete the Getting Started wizard to review requirements, add a user, add storage, and create a policy.
- Use the Cyber Recovery Software Instance ID to acquire the Cyber Recovery license file, and then activate the license.
- For information about how to perform these tasks and Cyber Recovery operations, see the Cyber Recovery online help or the Dell EMC PowerProtect Cyber Recovery Product Guide.

CHAPTER 3

Upgrading the Cyber Recovery software version

This section provides instructions for upgrading to a Cyber Recovery Version 19.2 deployment. Follow these procedures to upgrade from Version 19.1.0.4 to Version 19.2.

ⓘ **Note:** If you are running Cyber Recovery Version 18.1, upgrade to Version 19.1.0.4 first, and then upgrade to Version 19.2. For information about how to upgrade to Cyber Recovery Version 19.1.0.4, see the Dell EMC Cyber Recovery Version 19.1 Installation Guide on Dell EMC Online Support.

Preparing to upgrade the Cyber Recovery software

Before you upgrade the Cyber Recovery software, ensure that you meet the prerequisites.

Note: Upgrades have no effect on existing assets, policies, and other Cyber Recovery objects.

Before you perform the upgrade procedure:

- If your current deployment is running Cyber Recovery Version 18.1, upgrade to Version 19.1.0.4 first and then upgrade to Version 19.2. For information about how to upgrade to Cyber Recovery Version 19.1.0.4, see the Dell EMC Cyber Recovery Version 19.1 Installation Guide on Dell EMC Online Support.
- Ensure that all Cyber Recovery users are logged out.
- Ensure that there are no jobs running.

Upgrading the Cyber Recovery software

Use the `crsetup.sh` setup script to upgrade the Cyber Recovery software.

About this task

Upgrades have no effect on existing assets, policies, and other Cyber Recovery objects.

Procedure

1. Log in to the management host as **root**.
2. Download the Cyber Recovery upgrade package to a directory with approximately 1.5 GB of free space.
3. Untar the file:

   ```
   # tar -xzvf <file name>
   ```

   The file is untarred to the `staging` directory (within the current directory). The extraction includes the `crsetup.sh` setup script.
4. Go to the `staging` directory and make the `crsetup.sh` setup script an executable file:

   ```
   # cd staging
   # chmod +x ./crsetup.sh
   ```

5. Begin the upgrade:

   ```
   # ./crsetup.sh --upgrade
   ```

6. At the prompt, indicate that you want to continue the upgrade.

   Note:
   The upgrade procedure attempts to create a Linux user (cyber-recovery-admin) on the management host in the CR Vault. It assigns a reserved UID:GID of 14999 to the cyber-recovery-admin user. This user owns specific installation directories.

> If the reserved UID:GID 14999 is assigned to another user or the cyber-recovery-admin user exists but is not assigned the reserved UID:GID 14999, the upgrade procedure issues a warning message. Otherwise, the upgrade procedure continues.

7. If the upgrade procedure displays a warning about creating the cyber-recovery-admin user, indicate if you want to continue or cancel the upgrade.

   If you complete the upgrade, the Cyber Recovery software operates correctly, however, a non-cyber-recovery-admin user might own some installation directories.

8. When prompted, enter the lockbox passphrase.

   The upgrade proceeds and asks if you want to remove the current Cyber Recovery service containers.

9. Enter `y` to verify removal of the containers.

   The upgrade proceeds and starts the Cyber Recovery system. When the procedure is complete, a message provides the URL to log in to the Cyber Recovery UI.

CHAPTER 4

Patching or Removing the Cyber Recovery Software

This section provides instructions for patching or uninstalling the Cyber Recovery software.

Using the Cyber Recovery software to apply a secure software patch in the CR Vault

If you do not want to take a laptop or external storage into the physical Cyber Recovery vault to upgrade vault components, you can move patch software from your production system into the CR Vault securely. You can then apply software patches to upgrade the Cyber Recovery management host and Data Domain systems, as well as applications such as the NetWorker, Avamar, Index Engines' CyberSense applications, and so on.

Before you begin

- On the production Data Domain system, create a dedicated MTree.
- On the production and CR Vault Data Domain systems, create and initialize a Data Domain replication.
- On the Cyber Recovery system, create a Cyber Recovery policy and select the replication context that is associated with the patch software.

Procedure

1. Place the patch software on the host.
2. On the production Data Domain system, export the dedicated MTree to a host.
3. NFS mount the production MTree to the host.
4. Download the patch software to the NFS location from the host.
5. Perform a checksum and run a scanner to ensure that the downloaded patch software is uncorrupted.
6. Optionally, test the software upgrade on a test system.
7. On the Cyber Recovery system, perform a Sync Copy operation to replicate the MTree on which the patch software resides.
8. After the Sync Copy job completes, create a Cyber Recovery sandbox of the copy and export it to the host on which you want to access the patch software.
9. Optionally, do either of the following:
   - Run a scanner to ensure that the downloaded copy of the software patch is uncorrupted.
   - Perform an analysis by using Index Engines' CyberSense.
10. Apply the patch software.
11. Repeat step 9 through step 11 to apply additional software patches.

Removing the Cyber Recovery software

Use the `crsetup.sh` setup script to uninstall the Cyber Recovery software.

About this task

When you uninstall the Cyber Recovery software, the procedure removes all Cyber Recovery components, including the database, user interfaces, and log files. You do not need to stop Cyber Recovery services before you uninstall the software.

You can also choose to save the entire Cyber Recovery configuration and, if required, use it to perform a recovery.

Procedure

1. Enter the following command:

```
# ./crsetup.sh --uninstall
```

2. When prompted to confirm that you want to uninstall, enter **`y`**.
3. When prompted, indicate if you want to save the configuration and then enter the MongoDB password. Otherwise, the uninstall procedure continues.

   If you confirm that you want to save the configuration, the uninstall procedure uses the tar program to save the MongoDB files, log files, and lockbox files as a compressed and zipped file (`.gz`) in the `/opt/dellemc/cr-configs` directory.

   > **Note:** You can save the configuration outside of the installation procedure by entering **`./crsetup.sh --save`** at the command prompt.

Results

The Cyber Recovery software is removed from your system.