

Dell EMC PowerProtect Cyber Recovery

Installation Guide

Version 19.5

Notes, cautions, and warnings

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

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

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

Contents

Preface.....	4
Chapter 1: Getting Started.....	5
Production system requirements.....	5
Production storage requirements.....	5
Production backup and recovery applications.....	6
CR Vault system requirements.....	6
Enabling or disabling the firewall.....	6
Docker containers.....	7
Cyber Recovery management host.....	7
Cyber Recovery virtual appliance	8
CR Vault storage requirements.....	8
CR Vault backup and recovery applications.....	9
CyberSense feature.....	9
Chapter 2: Installing the Cyber Recovery Software.....	11
Obtaining the Cyber Recovery software.....	11
Installing the Cyber Recovery software.....	11
Installing the Cyber Recovery virtual appliance.....	13
Logging in initially.....	14
Chapter 3: Upgrading the Cyber Recovery deployment	15
Preparing to upgrade the Cyber Recovery software.....	15
Cyber Recovery software upgrade paths.....	15
Upgrading the Cyber Recovery software and the Cyber Recovery virtual appliance.....	16
Migrating data to a Cyber Recovery virtual appliance.....	17
Chapter 4: Patching or Removing the Cyber Recovery Software.....	18
Using the Cyber Recovery software to apply a secure software patch in the CR Vault.....	18
Applying Cyber Recovery virtual appliance security patches.....	19
Uninstalling the Cyber Recovery software.....	20

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](#)

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

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 Cyber Recovery UI, and elsewhere in the product include Data Domain systems and the new PowerProtect DD systems.

Topics:

- [Production system requirements](#)
- [CR Vault system requirements](#)

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.

The following table lists the supported storage systems:

Table 1. Cyber Recovery-supported storage systems

Storage system	Notes
Dell EMC Data Domain systems running DD OS Version 6.0.2.20 and later NOTE: The Cyber Recovery software does not support <ul style="list-style-type: none"> • High availability (HA) on a Data Domain system in the CR Vault • Data Domain with Cloud DR and Cloud Tier in the CR Vault • Data Domain with Cloud Tier in the CR Vault 	Ensure that the Cyber Recovery Data Domain system has more space than the production Data Domain system. For information about sizing your Cyber Recovery environment, see the Dell EMC PowerProtect Cyber Recovery Solution Guide .
Dell EMC DP4400 Integrated Data Protection Appliances	The replication target can be a supported Data Domain system or a DP4400 Integrated Data Protection Appliance. If the replication target in the CR Vault is a DP4400 Integrated Data Protection Appliance, the production-side system must also be a DP4400 Integrated Data Protection Appliance. Other than DD OS and AVE, the Cyber Recovery software does not support other features on the Integrated Data Protection Appliance in the CR Vault. It is recommended that you disable them.
Dell EMC DP53/5800 Integrated Data Protection Appliances	DP53/5800 Integrated Data Protection Appliances are not supported as a replication target in the CR Vault; they have been qualified for production environment replication to a supported Data Domain system target in the CR Vault. For configuration details, contact your Dell Technologies service representative.

Table 1. Cyber Recovery-supported storage systems (continued)

Storage system	Notes
Dell EMC DP83/8800 Integrated Data Protection Appliances	The DP83/8800 Integrated Data Protection Appliances are not supported in the production or the CR Vault environment due to Avamar Grid support limitations. However, replication through a single node or Virtual Edition is supported. For configuration details, contact your Dell Technologies service representative.

When multiple Data Domain systems are deployed in the production environment, they can be configured to replicate to 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.

Application	Supported versions
Avamar	<ul style="list-style-type: none"> Version 7.5 and later Single-node physical appliance or Avamar Virtual Edition (AVE)-only server (Avamar grids are not supported) <p>NOTE: Validated Avamar checkpoints are stored on the Data Domain system.</p>
NetWorker	<ul style="list-style-type: none"> Version 9.1 and later <p>NOTE: The NetWorker server database and data devices are stored on the Data Domain system.</p>
PowerProtect Data Manager	<ul style="list-style-type: none"> Version 19.3 and later <p>NOTE: If you plan to use PowerProtect Data Manager for backup and recovery with Cyber Recovery Version 19.3 or later, upgrade to PowerProtect Data Manager Version 19.3 or later. Otherwise, you cannot use PowerProtect Data Manager with the Cyber Recovery software.</p> <ul style="list-style-type: none"> DD OS must be Version 6.2 or 7.0. <p>NOTE: The PowerProtect Data Manager server backups and policy data are stored on the Data Domain system.</p>

CR Vault system requirements

Enabling or disabling the firewall

Before you install the Cyber Recovery software and the Docker components, ensure that the firewall settings are configured appropriately for your environment.

Prerequisites

Determine if you want your CR Vault to be a firewall-enabled environment or a firewall-disabled environment.

About this task

Perform these steps on the Cyber Recovery host in the CR Vault.

Steps

- For a firewall-enabled environment, follow these steps:
 - Enable the firewall.

- b. Enable SELinux.
 - c. Install the Docker components.
 - d. Install the Cyber Recovery software (see [Installing the Cyber Recovery Software](#)).
2. For a firewall-disabled environment, follow these steps:
 - a. Disable the firewall.
 - b. Disable SELinux.
 - c. Reboot the Cyber Recovery management host.
 - d. Install the Docker components.
 - e. Install the Cyber Recovery software (see [Installing the Cyber Recovery Software](#)).

Docker containers

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

- Docker Version 17.06.0, 18.09.7, 19.03.5, and 19.03.8—See the [Download Docker](#).
- **NOTE:** Red Hat Linux and SUSE Linux Enterprise Server only support Docker Enterprise Edition (EE). CentOS Linux also supports Docker Community Edition (CE).
- Docker Compose Version 1.21, 1.24, 1.25.3, and 1.25.4 or earlier—See the [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 and 7.7
 - Red Hat Enterprise Linux Version 7.4, 7.5, 7.6, and 7.7
 - 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

Several 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:

Table 2. Network ports

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 for the user and UI REST interface.
14779	Yes	Cyber Recovery Docker Registry	Inbound	Used to upload or download the 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.

Table 2. Network ports (continued)

Port	Required	Service	Direction	Description
22	Yes	SSH	Outbound	Provides bi-directional communication between the SSH client and the remote systems in the CR Vault.
25	No	Notifications	Outbound	Used for SMTP email notifications about alerts and events.
111	Yes	NFS Client	Inbound/ Outbound	Used to perform NFS mounts between the Data Domain system and the Cyber Recovery management host.
123	No	NTP	Inbound	Controls the time synchronization of Cyber Recovery to another reference time source.
2049	Yes	NFS Client	Inbound/ Outbound	Used to perform NFS mounts between the Data Domain system and the Cyber Recovery management host.
2052	Yes	NFS Client	Outbound	Used to mount to the Data Domain system.
27017	Yes	MongoDB	Inbound	Provides access to the database that holds Cyber Recovery configurations. The installation process configures these ports.
5000	Yes	Cyber Recovery Docker Registry	Inbound	Used to upload or download the Docker container images. The installation process configures these ports. The installation and upgrade scripts retrieve the images from the registry, if needed.

NOTE: If you use NFSv4 on your Data Domain system, ensure that the **NFSv4 ID Map Out Numeric** option is set to **always**.

Cyber Recovery virtual appliance

The Cyber Recovery virtual appliance is a VM host with the following requirements:

- VMware vCenter/ESXi, Version 6.5 and 6.7
- Approximately 2 G for deploying the OVA file
- Approximately 195 GB for three disks that are partitioned as:
 - Disk 1 size: 48 GB
 - Disk 2 size: 48 GB
 - Disk 3 size: 97 GB

NOTE: A thin provisioned environment does not use all the space.

- 4 CPUs, single core per socket
- 8 GB memory

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 and later
- **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.

NOTE: If you are running DD OS 7.2, the Cyber Recovery software does not support the Indefinite Retention Hold capability of Retention Lock Governance or Retention Lock Compliance Modes.

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

NOTE: It is recommended 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:

Supported versions	Requirements
Avamar Version 7.5 and later	<ul style="list-style-type: none"> • 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 and later	<ul style="list-style-type: none"> • The same NetWorker version that is deployed on the production system • An uninitialized and correctly sized NetWorker instance that is used to perform an <code>nsrdx</code> operation by using data replicated from the production Data Domain system to the CR Vault Data Domain system
PowerProtect Data Manager 19.3 and later	<p>NOTE: The Cyber Recovery software enables you to perform a VM recovery or a file system recovery for a PowerProtect Data Manager deployment. For information about a file system recovery, see the PowerProtect Data Manager documentation.</p> <ul style="list-style-type: none"> • DD OS Version 6.2 and later • Credentials for the PowerProtect Data Manager host and the PowerProtect Data Manager application that match the production system • A UID that matches the production user UID

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.

CyberSense feature

Optionally, deploy the CyberSense feature, 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. To use the CyberSense feature, you must have a valid license.

For more information, see the [CyberSense website](#).

CyberSense feature must be installed at the same location as the CR Vault.

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

Requirements include:

- A valid CyberSense feature license. Contact your Dell Technologies sales representative to obtain a CyberSense feature license. You will be provided with access and instructions.
- CyberSense feature Version 7.1, 7.2, or 7.3. For the latest compatibility matrix, see the [CyberSense Support Matrix](#).
- A dedicated host running CentOS or Red Hat Enterprise Linux, on which the CyberSense feature is installed, that acts as the validation host. The validation host provides direct integration between the Cyber Recovery software and the CyberSense feature.

 **NOTE:** You can also install the CyberSense feature in an ESXi environment.

Installing the Cyber Recovery Software

This section provides instructions for installing the Cyber Recovery Version 19.5 software.

Topics:

- [Obtaining the Cyber Recovery software](#)
- [Installing the Cyber Recovery software](#)
- [Installing the Cyber Recovery virtual appliance](#)
- [Logging in initially](#)

Obtaining the Cyber Recovery software

Go to [Dell EMC Online Support](#) to obtain either:

- The Cyber Recovery installation package
- The Cyber Recovery virtual appliance file for an installation in a VMware ESXi environment

Installing the Cyber Recovery software

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

Prerequisites

Ensure that you satisfy all preinstallation requirements (see [Getting Started](#)).

About this task

The installation procedure takes approximately five minutes.

Steps

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 -xzf <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
19.08.30 13_45_20 : 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.

Next steps

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.

Installing the Cyber Recovery virtual appliance

Deploy the Cyber Recovery virtual appliance file to a VMware ESXi host in the CR Vault.

Prerequisites

Before you deploy the Cyber Recovery virtual appliance file:

- Obtain the DNS, default gateway, FQDN, and IP address of the VM. Adjust the time zone setting for your deployment so that logging times are accurate.
- Ensure that you satisfy all preinstallation requirements (see [Getting Started](#)).

About this task

The installation procedure takes approximately five minutes.

Steps

1. From the vSphere Client in the CR Vault, use the Deploy OVF Template wizard to deploy the Cyber Recovery virtual appliance file.
2. When the Cyber Recovery virtual appliance deployment is completed, open the vCenter console for the newly deployed appliance.
3. Log in as the root user using the default password `changeme`.
4. Run the `crsetup.sh` script with the `deploy` option to begin the installation:

```
# crsetup.sh --deploy
```

5. At the prompts, do the following:
 - a. Change the admin password of the Cyber Recovery VM.
 - b. Change the root password of the Cyber Recovery VM.

NOTE: You cannot use SSH to access the root user account. To access the root user account, use SSH to access the admin user account and then use the `su` command to change to the root account.

6. At the prompts, enter a unique passphrase or password for the Cyber Recovery Security Officer (crso), the Cyber Recovery lockbox, and MongoDB.

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: `~!@#$$%^&*()+={}|:~<>?[]-_,^'.`

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](#).

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.

Next steps

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.

Steps

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 that was created in the installation procedure and click **LOG IN**.
The Getting Started wizard displays in the Cyber Recovery UI.

Next steps

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](#).

Upgrading the Cyber Recovery deployment

This section provides upgrade paths and instructions for upgrading to a Cyber Recovery Version 19.5 deployment. Ensure that you review the upgrade path information.

Follow the instructions to upgrade from an earlier Cyber Recovery version to Version 19.5 or later.

This section also provides instructions for migrating data from a Cyber Recovery software deployment to a Cyber Recovery virtual appliance.

Topics:

- [Preparing to upgrade the Cyber Recovery software](#)
- [Cyber Recovery software upgrade paths](#)
- [Upgrading the Cyber Recovery software and the Cyber Recovery virtual appliance](#)
- [Migrating data to a Cyber Recovery virtual appliance](#)

Preparing to upgrade the Cyber Recovery software

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

Before you perform the upgrade procedure:


- Run the `crsetup.sh --save` command to back up data and save the backup copy outside of the Cyber Recovery server.
- Ensure that all Cyber Recovery users are logged out.
- Ensure that there are no jobs running.
- Ensure that there are no scheduled jobs about to start.
- If you plan to use PowerProtect Data Manager for backup and recovery with Cyber Recovery Version 19.3 or later, upgrade to PowerProtect Data Manager Version 19.3 and later. Otherwise, you cannot use PowerProtect Data Manager with the Cyber Recovery software.

NOTE:

- **Upgrades have no effect on existing assets, policies, and other Cyber Recovery objects.**
- **If you installed the Cyber Recovery software by using the Cyber Recovery virtual appliance file, follow the upgrade procedure that uses the `crsetup.sh` setup script to upgrade the Cyber Recovery software. See [Upgrading the Cyber Recovery software and the Cyber Recovery virtual appliance](#) on page 16.**

Cyber Recovery software upgrade paths

Follow these paths when you upgrade the Cyber Recovery software:

If you are running...	Then....
Cyber Recovery Version 18.1.1.6  NOTE: You can only upgrade to a later version from Version 18.1.1.6. If you are running an earlier 18.x version, upgrade to version 18.1.1.6 first and then perform the upgrade.	Upgrade to Version 19.1.0.8 and then upgrade to the latest Cyber Recovery version.
Cyber Recovery Version 19.1.0.8	Upgrade to Cyber Recovery Version 19.5.
Cyber Recovery Version 19.x or later	Upgrade directly to Cyber Recovery Version 19.5.

NOTE: If your current environment includes a version 19.3 Cyber Recovery virtual appliance deployment, it is highly recommended that you apply the optional Cyber Recovery virtual appliance security patches. Apply the patches before or after you upgrade to Cyber RecoveryVersion 19.5 or later. Ensure that you follow the instructions in [Dell EMC PowerProtect Cyber Recovery Installation Guide](#) .

Upgrading the Cyber Recovery software and the Cyber Recovery virtual appliance

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

Prerequisites

- Ensure that you satisfy all system requirements (see [Getting Started](#) on page 5 and [Preparing to upgrade the Cyber Recovery software](#) on page 15).

To verify that the prerequisite software is installed, run the following command:

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

- Ensure that you have saved a data backup copy outside of the Cyber Recovery server.

About this task

- Upgrades have no effect on existing assets, policies, and other Cyber Recovery objects.
- If your current environment includes a version 19.3 Cyber Recovery virtual appliance deployment, it is highly recommended that you apply the optional Cyber Recovery virtual appliance security patches. Apply the patches before or after you upgrade to Cyber Recovery version 19.4 or later.

Steps

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 -xzf <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:

If you are upgrading from Version 19.1 to Version 19.3, 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 you are upgrading from Version 19.1 to Version 19.3, and 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 MongoDB password.
9. When prompted, enter the lockbox passphrase.
The upgrade proceeds and starts the Cyber Recovery system.
10. If you are upgrading the version 19.3 Cyber Recovery virtual appliance, optionally and if you have not already done so, upgrade the security patches and base operating system components that are part of the version 19.3 Cyber Recovery virtual appliance. See [Applying Cyber Recovery virtual appliance security patches](#).

 **NOTE:** These upgrade patches are for the Cyber Recovery virtual appliance only.

Migrating data to a Cyber Recovery virtual appliance

Migrate data from a Cyber Recovery software deployment to a Cyber Recovery virtual appliance deployment.

Steps

1. Deploy the Cyber Recovery virtual appliance in the CR Vault.
For information about how to deploy the Cyber Recovery virtual appliance, see [Installing the Cyber Recovery virtual appliance](#) on page 13.
2. Upgrade the current Cyber Recovery software deployment to the same version as the Cyber Recovery virtual appliance.
For example, if you are upgrading from a Version 19.4 Cyber Recovery software deployment to a Version 19.5 Cyber Recovery virtual appliance deployment, you must first upgrade the current Cyber Recovery software to Cyber Recovery Version 19.5.
3. On the host that is running the Cyber Recovery software, run the `crsetup.sh --save` command to create a backup copy.
4. Copy the newly created backup file onto the Cyber Recovery virtual appliance.
5. On the Cyber Recovery virtual appliance, run the `crsetup.sh --recover` command to perform a recovery and restore the data.

Patching or Removing the Cyber Recovery Software

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

Topics:

- [Using the Cyber Recovery software to apply a secure software patch in the CR Vault](#)
- [Applying Cyber Recovery virtual appliance security patches](#)
- [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, PowerProtect Data Manager, CyberSense feature applications, and so on.

Prerequisites

- 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.

Steps

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 the CyberSense feature.
10. Apply the patch software.
11. Repeat step 9 through step 11 to apply additional software patches.

Applying Cyber Recovery virtual appliance security patches

Apply security patches to the Cyber Recovery virtual appliance.

About this task

Before you apply the security patches, back up data on and take a VM snapshot of the Cyber Recovery virtual appliance. Then, save the backup data and snapshot outside of the Cyber Recovery virtual appliance.

 **NOTE:** This procedure reboots the virtual appliance.

Steps

1. Go to [Dell EMC Online Support](#) to obtain the `cyber-recovery-osupdate-19.3.0.1-20200324.211700-1.jar` file.
2. Take a VM snapshot of the Cyber Recovery virtual appliance.
3. Run the `crsetup.sh --save` command to create a backup copy .
4. Save the backup data and snapshot outside of the Cyber Recovery virtual appliance.
5. Run the following command:

```
# java -jar cyber-recovery-osupdate-19.3.0.1-20200324.211700-1.jar
```

The following shows sample output:

```
Unpacking cyber-recovery-osupdate-1.4.0-1-SNAPSHOT.bin ...
Verifying archive integrity... 100% All good.
Uncompressing cyber-recovery-osupdate-makeself 100%
This update must only be executed on a Cyber Recovery system - exiting!
Note: after completing OS update, system will reboot
Removing all zypper repos ...
Adding repository
'osupdate' ..... [done]
Repository 'osupdate' successfully added
URI      : dir:///tmp/selfgz2021026536/repo
Enabled  : Yes
GPG Check : Yes
Autorefresh : No
Priority  : 99 (default priority)
Repository priorities are without effect. All enabled repositories share the same priority.
The following 5 packages are going to be upgraded:
  libvmtools0 open-vm-tools supportutils wicked wicked-service
The following 5 packages have no support information from their vendor:
  libvmtools0 open-vm-tools supportutils wicked wicked-service
5 packages to upgrade.
Overall download size: 1.9 MiB. Already cached: 0 B. After the operation, additional 28.1
KiB will be used.
Continue? [y/n/...? shows all options] (y): y
No processes using deleted files found.
Removing repository
'osupdate' ..... [done]
Repository 'osupdate' has been removed.
Rebooting in 10 seconds ...
  Enter ctrl-c to stop reboot
```

The procedure reboots the virtual appliance, even if there are no updates to apply.

Results

The security patch is applied to the Cyber Recovery virtual appliance.

Uninstalling 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 deletes 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.

Steps

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 uninstalled from your system.