Dell Data Protection Central 19.8

Getting Started Guide

Dell Inc.

December 2022
Rev. 01

Notes, cautions, and warnings

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

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

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

Contents

Preface

As part of an effort to improve product lines, periodic revisions of software and hardware are released. Therefore, all versions of the software or hardware currently in use might not support some functions that are described in this document. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

Purpose

This document includes information about how to deploy Data Protection Central, and then get started with Data Protection Central administration.

Audience

This document is intended for administrators of Data Protection Central.

Revision history

The following table presents the revision history of this document.

Table 1. Revision history

Revision	Date	Description
01	December 2022	Initial release of this document for Data Protection Central 19.8.

References to Data Domain systems in this guide, in the UI, and elsewhere in the product include PowerProtect DD systems and older Data Domain systems.

Related Documentation

For information about Data Protection Central compatibility, see the *Data Protection Central Release Notes*.

The Data Protection Central documentation set includes the following publications:

- *Data Protection Central Getting Started Guide*
- *Data Protection Central Security Configuration Guide*
- *Data Protection Central Release Notes*
- *Data Protection Central Administration Guide*

The documentation for the following products includes more information:

- Avamar
- Data Domain
- Search
- Data Protection Advisor
- NetWorker
- PowerProtect Data Manager

Typographical conventions

The following type style conventions are used in this document:

Table 2. Style conventions

Formatting	Description
Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
Italic	Used for full titles of publications that are referenced in text.
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, file names, file name extensions, prompts, and syntax • Commands and options
Monospace italic	Used for variables.
`Monospace bold`	Used for user input.
[ ]	Square brackets enclose optional values.
|	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate nonessential information that is omitted from the example.

You can use the following resources to find more information about this product, obtain support, and provide feedback.

Where to find product documentation

- https://www.dell.com/support
- https://www.dell.com/community

Where to get support

The Support website https://www.dell.com/support provides access to product licensing, documentation, advisories, downloads, and how-to and troubleshooting information. The information can enable you to resolve a product issue before you contact Support.

To access a product-specific page:

1. Go to https://www.dell.com/support.
2. In the search box, type a product name, and then from the list that appears, select the product.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Knowledge Base**.
3. In the search box, type either the solution number or keywords. Optionally, you can limit the search to specific products by typing a product name in the search box, and then selecting the product from the list that appears.

Live chat

To participate in a live interactive chat with a support agent:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Contact Support**.
3. On the **Contact Information** page, click the relevant support, and then proceed.

Service requests

To obtain in-depth help from Licensing, submit a service request. To submit a service request:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Service Requests**.

NOTE: To create a service request, you must have a valid support agreement. For details about either an account or obtaining a valid support agreement, contact a sales representative. To find the details of a service request, in the `Service Request Number` field, type the service request number, and then click the right arrow.

To review an open service request:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Service Requests**.
3. On the **Service Requests** page, under **Manage Your Service Requests**, click **View All Dell Service Requests**.

Online communities

For peer contacts, conversations, and content on product support and solutions, go to the Community Network https://www.dell.com/community. Interactively engage with customers, partners, and certified professionals online.

How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. Perform one of the following steps to provide feedback:

- Go tohttps://contentfeedback.dell.com/s, and submit a ticket.
- Send feedback to DPADDocFeedback@dell.com.

1

Overview

Learn about Data Protection Central.

This chapter contains the following sections:

Topics:

Data Protection Central overview

Data Protection Central is an active monitoring application with management capabilities. Data Protection Central provides a solution for data protection administrators who manage multiple independent data protection applications and storage devices.

When you work with multiple data protection applications, operational monitoring and management can be a complex, time consuming effort.

Data Protection Central enables administrators to monitor and manage the software products within the Data Protection Suite family from a single user interface, simplifying the entire data protection experience.

Data Protection Central includes the following features:

Comprehensive dashboards

Data Protection Central has a comprehensive and customizable dashboard for at-a-glance monitoring of systems and activities. Data Protection Central supports up to 20 dashboards per user.

PowerProtect Data Manager

When you add a PowerProtect Data Manager system to Data Protection Central, you can perform the following tasks:

- Launch PowerProtect Data Manager UI, using Single Sign-On (SSO), for supported versions.
- Monitor system health status and any alerts from the system.
- View and tag assets that are added to PowerProtect Data Manager.
- Monitor backup and replication activities at the asset and job level.

Avamar system monitoring and management

When you add an Avamar system to Data Protection Central, you can perform the following tasks:

- Launch AUI or Avamar Administrator, using Single Sign-On (SSO) for supported versions.
- Monitor system health status and any alerts from the system.
- Monitor storage capacity usage.
- Monitor backup and replication activities at the Avamar job level.
- Monitor backup and replication activities at the Avamar asset level. Assets are virtual machines or clients that you add to the Avamar system.
- Rerun failed backup and replication activities at the job or asset level.
- Manage and run Avamar protection policies.

- View and tag assets that are added to Avamar.

NetWorker system monitoring

When you add a NetWorker system to Data Protection Central, you can perform the following tasks:

- Launch NetWorker Management Console or the NetWorker Management Web UI, using Single-Sign On (SSO) for supported versions.
- Monitor system health status and any alerts from the system.
- Monitor backup and replication activities at the NetWorker action level.
- Monitor backup activities at the NetWorker asset level.
- View and tag assets that are added to NetWorker.

Data Domain system monitoring

When you add a Data Domain system to Data Protection Central, you can perform the following tasks:

- Launch Data Domain System Manager, using Single Sign-On (SSO) for supported versions.
- Monitor system health status and any alerts from the system.
- Monitor storage capacity usage.

NOTE: Any references to the Data Domain systems and the Data Domain devices in the document indicate PowerProtect DD appliances.

Search integration

When you integrate Search with Data Protection Central, you can launch Search Web User Interface, using Single Sign-On (SSO) for supported versions.

Data Protection Advisor integration

When you integrate Data Protection Advisor with Data Protection Central, you can perform the following tasks:

- Launch DPA Web Console, using Single Sign-On (SSO) for supported versions.
- Run 11 of the most used Data Protection Advisor reports on Avamar, NetWorker, PowerProtect Data Manager, and Data Domain systems.

Environment and system requirements

Learn about the environment and system requirements for the Data Protection Central.

Table 3. Environment and system requirements

Requirements	Description
Browser window size	Data Protection Central requires a minimum browser window size of 1366x768.
Data Protection Central host	• The Data Protection Central host requires a minimum of 4 CPUs, 8 GB of RAM, and 560 GB of disk space that is separated into two disks. Allocate a minimum of 500 GB for data (/data01) and 60 GB for service. • Data Protection Central 19.8 works only with SUSE Linux Enterprise Server (SLES) version 12 SP5. See Data Protection Central operating system updates, available on Dell Support site at https://www.dell.com/support/home/en-in/product-support/product/data-protection-central/, for upgrading from previous releases. • Do not use the underscore symbol in a hostname. This requirement is a standard practice for hostname configurations. For example, mars_jupiter.planets is not a valid hostname. When you deploy Data Protection Central to a server with a hostname that contains the underscore symbol

Table 3. Environment and system requirements (continued)

Requirements	Description
	(_), the deployment succeeds but Data Protection Central is unusable due to communication issues.
ESXi server	For Data Protection Central OVA deployment, use a supported VMware vCenter with VMware ESXi (see e-Lab-Navigator). To deploy the Data Protection Central OVA, you must use vCenter. Data Protection Central supports direct deployment of Data Protection Central OVA to the ESXi server.
FIPS mode	If you plan to operate Data Protection Central in FIPS mode, you must deploy Data Protection Central as an OVA.
Networking	• The environment must use static network settings. • The FQDN, IP, Netmask, NTP, Gateway, DNS, and time zone must be configured. The FQDN must have a domain information, and resolve to the IP address. The FQDN must not be configured to have a short name. • Ensure that the DNS is correctly configured. The correct DNS setup ensures that systems can resolve the Data Protection Central hostname and FQDN name. • If you are using only IPv4 in your environment, do not disable the IPv6 configuration. Some Data Protection Central components use the IPv6 loopback address. If you disable IPv6, those components do not start. • Configurations that use network address translation (NAT) are not supported.
Power	• Use an uninterrupted power supply device to protect the ESXi server for the VMware environment where Data Protection Central is deployed. • Do not use the **Power off the virtual machine** feature in vCenter to power off the Data Protection Central VM . Use the **Shut Down Guest OS** menu option to shut down the machine. Alternatively, log in to Data Protection Central using shell or SSH and type: **`shutdown -h now`**.
Support matrix	To review the simple support matrix for Data Protection Central, go to the e-Lab Navigator site (e-Lab-Navigator). The support matrix includes information about the minimum versions of products that Data Protection Central supports.
TLS protocol	OVA and JAR (software-only) deployments use TLS 1.2 protocol by default. Deployment disables the use of TLS 1.0 and 1.1 versions, which use less secure cipher suites. For more information, see the *Data Protection Central Security Configuration Guide*.
VMware compatibilities	Data Protection Central is compatible with VMware vSphere Fault Tolerance (FT), VMware vSphere High Availability (HA), and VMware vSphere vMotion.

Monitoring systems

Data Protection Central includes system monitoring features.

The systems monitoring features include:

- Job Activities: Monitor backup and replication activities at the job-level for Avamar, NetWorker, and PowerProtect Data Manager .
- Asset Activities: Monitor backup and replication activities at the asset-level within jobs for Avamar, NetWorker, and PowerProtect Data Manager systems.
- Health: Monitor the health status for Avamar, NetWorker, PowerProtect Data Manager, and Data Domain systems.
- Alerts: Monitor alerts originating from Avamar, NetWorker, PowerProtect Data Manager, and Data Domain systems.
- Capacity: Monitor capacity usage for Avamar, and Data Domain systems.

NOTE: Add NetWorker, Avamar, PowerProtect Data Manager, and Data Domain systems to enable Data Protection Central monitoring.

Managing Avamar systems

For Avamar systems, Data Protection Central includes policy management and client management capabilities.

Data Protection Central includes the following Policy Management capabilities:

- View, add, edit, and delete policies, retention, schedules, and dataset.

- Add clients and proxies to policies.
- Perform a backup of a policy.
- Rerun a backup or replication activity.

Data Protection Central includes the capability for you to view existing clients that are associated with Avamar system.

Search and recover capabilities

Data Protection Central integrates with Search to provide you with the ability to perform complex search and recover operations.

Data Protection Central launches Search in a new browser tab.

After launching Search, you can perform the following tasks:

- Perform a targeted full content index (FCI) search.
- Search for files by name, location, size, owner, file type, and date.
- Perform advanced search queries including symbols, wildcards, filters, and operators.
- From the **Search Results** page:
  - View a preview of the content.
  - Download content.
  - Recover content.
  - Review the size of files or directories.

For comprehensive information about Search, refer to the Search documentation set.

NOTE: To take full advantage of Data Protection Central capabilities, it is recommended that all systems that are configured in Search also be configured in Data Protection Central.

Report capabilities

Data Protection Central provides the capability for you to run Data Protection Advisor reports for supported systems.

Supported systems include:

- Avamar
- NetWorker
- Data Domain
- PowerProtect Data Manager

You can run, and then view these reports directly in the Data Protection Central user interface. You can also specify the reporting period for these reports within the Data Protection Central interface.

Data Protection Central reporting features require you to have Data Protection Advisor in the environment. For more information about Data Protection Advisor, see the Data Protection Advisor documentation set.

NOTE: To take full advantage of Data Protection Central capabilities, it is recommended that all systems that are configured in Data Protection Advisor be configured also in Data Protection Central.

2

Deployment and Configuration

Learn about how to deploy and configure Data Protection Central on premise or in cloud.

Topics include:

Topics:

Check the network setup with each system

Before deploying the Data Protection Central OVA, ensure that the network setup with each Avamar, NetWorker, Data Domain, Data Protection Advisor, and PowerProtect system is correct.

Steps

1. Ensure that the time on the system is set correctly.

   For successful activation of certificates, the time that appears on the system must be in synchronization with Data Protection Central.

   It is recommended that Data Protection Central and all the systems that Data Protection Central monitors be configured with a Network Time Protocol (NTP) server. This configuration helps keep the system times synchronized. Configuring Network Time Protocol provides more information about configuring an NTP server.

2. Find out the Data Protection Central DNS hostname and domain name.
3. Check if the system is on the same domain as Data Protection Central.

   If the system is on the same domain, ensure that the DNS entry and search domain values are set.

   If the system is on a different domain, add the Data Protection Central DNS entry through the `yast2` command, or by editing the `/etc/resolv.conf` file on the system.
4. To check whether the system can resolve the Data Protection Central hostname and IP address, use the `nslookup` command.

   Type the following command:

   ```
   nslookup -query=any <dpc_hostname>
   ```

5. Check whether the hostname resolves correctly.

   If the hostname resolves correctly, the network setup is correctly configured. Otherwise, check all previously entered values.
6. If DNS cannot resolve the Data Protection Central hostname, add the short name entry in the `/etc/hosts` file. For example:

   `10.x.x.x dpc.domain.local dpc`

Deploy Data Protection Central as an OVA

Deploy the Data Protection Central Open Virtualization Appliance (OVA) using a VMware vSphere client. See the VMware documentation for specific information regarding how to deploy an OVF template.

Prerequisites

Observe the system requirements that are listed in Environment and system requirements .

NOTE: Ensure that the OS root password, UI admin password, and the lockbox password are different. If the passwords are the same, it compromises system security.

Steps

1. Log in to vCenter using the vSphere client.
2. Specify an ESXi server on which to deploy the OVF.
3. Begin deploying an OVF template.
4. Type the file or URL location.
5. Verify the OVF template details match the version of Data Protection Central that you are deploying.
6. Accept the user license agreement.
7. Specify the name and location of the Data Protection Central virtual machine.
8. Select the virtual drive format.

   The **Thick Provision Lazy Zeroed** option is recommended .
9. Configure the following settings in **Networking Properties** section:
   a. For the **Network IPv4 address**, specify the IPv4 address for the virtual appliance. This field is required if an IPv6 address is not provided.
   b. For the **IPv4 Default Gateway**, specify the default gateway IPv4 address that you want the virtual appliance to use. This field is required if an IPv4 address is provided.
   c. For the **IPv4 Network Netmask**, specify the netmask of the virtual appliance. This field is required if an IPv4 address is provided.
   d. For the **Network IPv6 address**, specify the IPv6 address for the virtual appliance. This field is required if an IPv4 address is not provided.
   e. For the **IPv6 Default Gateway**, specify the default gateway IPv4 address that you want the virtual appliance to use. This field is required if IPv6 is provided.
   f. For the **IPv6 Network Prefix**, specify the prefix length. This field is required if IPv6 is provided.
10. Configure the following settings in **DNS Settings** section:
    a. For the **DNS**, specify up to three domain name servers for this virtual appliance.

       IPv4 and IPv6 addresses may be included. Separate entries with commas.
    b. For the **FQDN [e.g. hostname.domain]**, specify the FQDN for the virtual appliance.

       NOTE: Ensure that you correctly configure hostname resolution for the name of the appliance. Forward and reverse lookups must succeed.
11. Configure the **NTP Server** settings in the **NTP Settings** section.

    Specify up to three Network Time Protocol (NTP) servers. Separate server IP addresses with commas.
12. Configure the following passwords in the **Operation System User Passwords** section:
    a. Specify the password for the Linux OS root account in the **Configure OS root password** field.

       The operating system root account is for OVA deployment only.
    b. Specify the password for the Linux OS admin in the **Configure OS admin password** field.

       The operating system admin account is the default user for Data Protection Central operating system administration.
    c. Specify the admin password for the Data Protection Central user interface in the **Configure UI admin password** field.

       This password must contain a minimum of nine characters including one uppercase, one lower case, one number, and one special character: `! @ # $ % ^ & * ( ) - _ .`

       NOTE: If the password requirements are not met, a warning is displayed.

    The operating system root and admin password length must have 8 to 256 characters.

13. Configure the primary lockbox password in the **Configure lockbox password** field in the **Lockbox Settings** section, specify a primary password for the Data Protection Central lockbox.

    The lockbox password length must be 8 to 256 characters.

    NOTE: For FIPS-compliant deployments, the minimum password length is 14 characters.

    The password creates an internal encryption key, which is used to encrypt credentials of systems that Data Protection Central monitors. System Stable Values (SSVs) are used to guard access to the lockbox.

    WARNING: Make note of this password. The lockbox password cannot be reset without the lockbox primary password. If the lockbox primary password is unavailable, the lockbox cannot be reset and the lockbox has to be re-created.

14. Configure the IAM admin password in the **Configure IAM Provider admin password** field in the **IAM Provider Settings** section.

    The IAM admin password must contain minimum nine characters including one lower case character, one upper case character, one numeral, and one special character: `! @ # $ . % ^ & * ( ) - _`

15. Under **Location Settings**, select the time zone of the Data Protection Central virtual machine.
16. Validate the information that you specified, and then complete the deployment of the Data Protection Central OVF.

Next steps

If you plan to operate Data Protection Central in FIPS mode, see *Data Protection Central Security Configuration Guide* for instructions.

Deploy Data Protection Central as a JAR

A Data Protection Central software-only installation can be deployed on a server or virtual machine using a self-extracting .jar file. The customer owns and configures the operating system to support the installation. This method of deployment is hardware-independent (and verified in limited hardware environments).

Prerequisites

Review the requirements listed in Environment and system requirements .

A software-only installation has additional requirements that are listed here:

Table 4. Requirements for software-only deployments

Requirements	Descriptions
Admin	Before installing Data Protection Central, ensure that an administrative user exists on the host named 'admin' and is added to a group named 'admin' .
AppArmor	Ensure that the AppArmor profiles do not block the applications that Data Protection Central uses.
Docker	• docker-compose-1.29.2-1.x86_64 • docker-20.10.14_ce-98.80.1.x86_64
FQDN	Ensure that the hostname on the virtual machine is set before Data Protection Central is installed .
JDK version	Java Platform Standard Edition Development Kit (JDK) version 8 update 345 or greater is installed, including the following packages: • JDK version 8 update 345 • java-1_8_0-openjdk-1.8.0.345-27.78.1.x86_64 • java-1_8_0-openjdk-headless-1.8.0.345-27.78.1.x86_64 **NOTE:** Java may require additional packages to install. If there is a firewall, ensure that the ports that Data Protection Central requires have inbound and outbound access. See the *Data Protection Central Security Configuration Guide* for a list of required ports.
Linux socat	Ensure that the Linux socat package is installed.
Processor	Software-only deployments require a 1.5 GHz processor.

Table 4. Requirements for software-only deployments (continued)

Requirements	Descriptions
SLES support	Ensure that the environment is running SUSE Linux Enterprise Server 12 SP5.

NOTE: To acquire and install docker-compose version 1.29.2 on the system, run the following commands:

- curl -L https://github.com/docker/compose/releases/download/1.29.1/docker-compose-Linux-x86_64
- chmod +x /usr/local/bin/docker-compose

Steps

1. Launch a terminal window.
2. Log in as the root user.
3. Download and save the Data Protection Central .jar file.
   Make note of the file name and directory where it is saved.
4. Change the directory to the location where the .jar file is saved.
5. Start the installation by typing the following command:

```
java -jar <dpc*>.jar
```

During the installation, you are prompted to create these passwords:

NOTE: Ensure that the UI admin password, and the lockbox password are different. If the passwords are the same, it compromises system security.

- Lockbox primary password - minimum of eight characters
- Admin password for the Data Protection Central user interface - minimum of nine characters including one lower case character, one upper case character, one number, and one special character: `! @ # $ % ^ & * ( ) - _ .`

  WARNING: Make note of this password. The lockbox password cannot be reset without the lockbox primary password. If the lockbox primary password is unavailable, the lockbox cannot be reset and the lockbox has to be re-created.
- The IAM admin password must contain minimum 9 characters with at least one lower case character, one upper case character, one numeral, and one of the following special character: `! @ # $ . % ^ & * ( ) - _`

Deploy Data Protection Central in cloud

You can deploy Data Protection Central in public cloud.

Prerequisites

A software-only installation has additional requirements that are listed here:

Table 5. Requirements for software-only deployments

Requirements	Descriptions
Admin	Before installing Data Protection Central, ensure that an administrative user exists on the host named 'admin' and is added to a group named 'admin' .
AppArmor	Ensure that the AppArmor profiles do not block the applications that Data Protection Central uses.
Docker	• docker-compose-1.29.2-1.x86_64 • docker-20.10.14_ce-98.80.1.x86_64
FQDN	Ensure that the hostname on the virtual machine is set before Data Protection Central is installed .
JDK version	Java Platform Standard Edition Development Kit (JDK) version 8 update 345 or greater is installed, including the following packages: • JDK version 8 update 345 • java-1_8_0-openjdk-1.8.0.345-27.78.1.x86_64

Table 5. Requirements for software-only deployments (continued)

Requirements	Descriptions
	• java-1_8_0-openjdk-headless-1.8.0.345-27.78.1.x86_64 **NOTE:** Java may require additional packages to install. If there is a firewall, ensure that the ports that Data Protection Central requires have inbound and outbound access. See the *Data Protection Central Security Configuration Guide* for a list of required ports.
Linux socat	Ensure that the Linux socat package is installed.
Processor	Software-only deployments require a 1.5 GHz processor.
SLES support	Ensure that the environment is running SUSE Linux Enterprise Server 12 SP5.

NOTE: To acquire and install docker-compose version 1.29.2 on the system, run the following commands:

- curl -L https://github.com/docker/compose/releases/download/1.29.1/docker-compose-Linux-x86_64
- chmod +x /usr/local/bin/docker-compose

NOTE: See Data Protection Central Support Matrix, available at https://elabnavigator.dell.com/eln/elnhome, for more information about the supported cloud platforms.

Steps

1. Launch a terminal window.
2. Log in as the root user.
3. Download and save the Data Protection Central .jar file.
   Make note of the file name and directory where it is saved.
4. Change the directory to the location where the .jar file is saved.
5. Start the installation by typing the following command:

```
java -jar <dpc*>.jar
```

Next steps

During the installation, you are prompted to create these passwords:

- Lockbox primary password - minimum of eight characters
- Admin password for the Data Protection Central user interface - minimum of nine characters including one lower case character, one upper case character, one number, and one special character: `! @ # $ % ^ & * ( ) - _ .`
- The IAM admin password must contain minimum 9 characters with at least one lower case character, one upper case character, one numeral, and one of the following special character: `! @ # $ . % ^ & * ( ) - _`

WARNING: Make note of this password. The lockbox password cannot be reset without the lockbox primary password. If the lockbox primary password is unavailable, the lockbox cannot be reset and the lockbox has to be re-created.

NOTE: Ensure that the UI admin password, and the lockbox password are different. If the passwords are the same, it compromises system security.

Verify the deployment

When the deployment is complete, to verify that Data Protection Central was deployed successfully, perform the following steps.

Prerequisites

Ensure that the virtual machine where the Data Protection Central OVA or JAR file was deployed is turned on.

NOTE: Data Protection Central is supported with Mozilla Firefox and Google Chrome.

Steps

1. Open a browser, and then type the following in the **Address** field:
   `https://<FQDN>`

   The Data Protection Central **Login** page appears.
2. In the **Username** field, type:
   `administrator@dpc.local`
3. In the **Password** field, enter the password that you configured during deployment.
4. Click **LOG IN**.

   NOTE: If required, the *Data Protection Central Security Configuration Guide* provides the steps to reset the **`administrator@dpc.local`** password.

Configuring Network Time Protocol

Data Protection Central utilizes a Network Time Protocol (NTP) server to update system time.

To ensure that Data Protection Central can use single sign-on (SSO) to launch system management applications, you must configure Data Protection Central and all monitored systems with the same NTP server and disable VMware time sync.

Configuring Network Time Protocol during Data Protection Central OVA deployment

To configure Network Time Protocol during Data Protection Central OVA deployment, use the **NTP Server** field to specify up to three Network Time Protocol (NTP) servers. Separate server IP addresses with commas.

If an NTP server is configured during deployment, VMware time sync is disabled by default.

Configuring Network Time Protocol after Data Protection Central deployment

If an NTP server was not configured during Data Protection Central deployment, configure an NTP server after deployment.

Prerequisites

Ensure that the following steps are done before configuring NTP server:

- Run the following command to block all the access:

```
restrict default ignore
restrict -6 default ignore
```

- Run the following command to allow access from the local host:

```
restrict 127.0.0.1
restrict -6 ::1
restrict \{ntp server\}
```

Steps

1. Add the NTP server to the `/etc/ntp.conf` file by adding the following command line:

```
server {ntp server}
```

2. Disable VMware time sync using the following command:

```
/usr/bin/vmware-toolbox-cmd timesync disable
```

3. Validate VMware time sync is disabled using the following command:

```
/usr/bin/vmware-toolbox-cmd timesync status
```

4. Enable automatic start of the *ntpd* service using the following command:

```
systemctl enable ntpd
```

5. Start the *ntpd* service using the following command:

```
systemctl start ntpd
```

Access control

Access control settings provide protection of resources against unauthorized access.

Preloaded accounts

The following table describes the preloaded Data Protection Central accounts.

Table 6. Preloaded accounts

User account	Description
Data Protection Central administrator	The default user for Data Protection Central web application administration.
Linux operating system admin	The default user for Data Protection Central operating system level administration. **NOTE:** Only the Linux operating system admin can log in using a secure shell (ssh).
Linux operating system root	The root operating system account.

3

Getting Started with Administration

Learn about how to get started with administering Data Protection Central.

NOTE: For comprehensive information about Data Protection Central administration, refer to the *Data Protection Central Administration Guide*.

Topics include:

Topics:

Log in to Data Protection Central

To use the Data Protection Central monitoring and management features, log in to the user interface.

Steps

1. In a browser address bar, type **`https://`**, and then the FQDN or IP address of the Data Protection Central server.
2. In the **Username** field, type a valid username. The default web browser account is: **`administrator@dpc.local`**.
3. In the **Password** field, type the password for the user.
4. Click **LOG IN**.

User interface

The Data Protection Central user interface includes the following components.

Header

The header includes the following components:

- **User** menu: This menu enables you to change the password or log out of Data Protection Central.
- **About** button: This button enables you to view Data Protection Central version information.
- **Help** button: This button opens the Data Protection Central online help.

Figure 1. Header

User menu

The **User** menu provides the capability for you to perform user tasks.

To perform the following user tasks, use the **User** menu:

- Change the password of the local Data Protection Central administrator user (administrator@dpc.local).
  NOTE: If an external LDAP or AD user is logged in to the Data Protection Central environment, change password is not supported.
- Log out of the user interface.

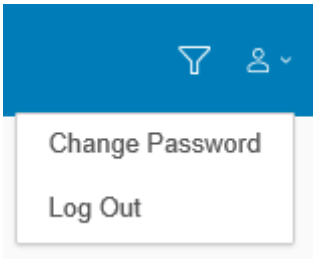

Figure 2. User menu

Left menu

The left menu provides the capability for you to browse the user interface.

From the left menu, you can access the following Data Protection Central features:

- **Dashboard**
- **Health**
- **Alerts**
- **Capacity**
- **Asset Activities**
- **Job Activities**
- **System Management**
- **Asset Inventory**
- **Reports**
- **Audit**
- **Search and Recovery**
- **Administration**

Pages

Data Protection Central presents information in dashboards and detail pages.

Dashboard pages provide at a glance insight into operational behavior.

Detail pages display focused information and provide the capability for you to perform Data Protection Central tasks.

Main and detail panes

Most Data Protection Central pages are composed of a main and detail pane.

The main pane appears in the middle of a page and displays information in a table format. The detail pane appears on the right side of a page and displays additional information for a selected row in a table. The detail pane may also include buttons that you can use to perform tasks that are specific to the selected row in the table. By default this detail pane is hidden. Users can either expand or collapse this detail pane by clicking on the elemental row list. Now users have the option to select number of display records per page at the bottom of grid as 25, 50 or 100 records.

Changing dashboards

Click the **Dashboard** drop-down list to select a different dashboard.

Filtering

Data Protection Central includes filtering capabilities. Filtering allows you to customize the information that appears.

The following filter types are available for you to use:

- **Column filters**: Appears in table headers
- **Domain Filter**: Appears in the **Policies**, **Retentions**, **Schedules**, and **Datasets** pages for Avamar only
- **Active Filter**: Appears in the user interface header of some pages
- **Asset Filter**: Appears as a search bar on the **Asset Inventory** page
- **Widget Filter**: Appears in widgets on the dashboard

Column filters

Column filters can be used to filter the information that appears in table columns. Depending on the table column, you can specify one of the following options:

- All Available
- Last Hour
- Last 24 hours
- Last 7 days
- Custom (specific date-and-time range)

Domain Filter

The **Domain Filter** can be used to select the domains that you want to view in the **Policies**, **Retentions**, **Schedules**, and **Datasets** pages for Avamar only. When you add a policy, retention, schedule, or dataset, the domain filter also determines which domain the policy, retention, schedule, or dataset is added in.

Asset Filter

The **Asset Filter** can be used to filter assets listed on the **Asset Inventory** page. The **Asset Filter** search bar enables you to filter assets using a search phrase such as an asset tag, operating system, plug-in, or asset name.

Active Filter

The **Active Filter** can be used to filter by system or system group (one or more). On the **Asset Inventory** and **Asset Activities** pages, you can use the **Active Filter** to filter by asset tags. The **Active Filter** appears in on the following pages:

- **Health**
- **Alerts**
- **Capacity**
- **Job Activities**
- **Asset Activities**
- **Asset Inventory**

To filter certain items with the **Active Filter**, move one or more systems or system groups to the **Filtered By** pane. When the **Active Filter** is enabled, a white filter icon appears in the header.

Widget Filter

The **Widget Filter** can be used to refine the information that appears in a widget. All types of widgets include a **Widget Filter** that enables you to filter the information reported in the widget. The filter organizes information by time range, system, system groups, or, for asset-specific widgets, by asset tags. Several widgets allow you to filter by time range. You can specify one of the following options:

- All Available
- Last Hour
- Last 24 hours
- Last 7 days

The **Activities Trend** widget enables you to view a historical 7-day trend of activities by using the **Days Ago** filter. For example, if you want to see the 7-day activity trend from 30 days ago, select **Days Ago**, and use the slider to select 30. To analyze to a data grid with more details, select a point in the graph.

The **Activities Count** and **Activities Trend** widgets allow you to pick whether to display backup activities, replication activities, or both.

When you use a dashboard widget to access a page, the information that is displayed is automatically filtered based on the widget filter settings.

Any active filters that are applied to a page, are listed in the filtered-by section that appears at the top of the table.

Monitoring data is stored for 90 days. The **All Available** option is limited to data stored within the last 90 days.

Sort information that is displayed in tables

Information that is displayed in tables can be sorted in ascending or descending order.

Steps

1. To sort information, click a column heading.
2. After you click the column heading, an arrow appears.

   An up-arrow indicates that the column data is sorted in ascending order. A down-arrow indicates that the column data is sorted in descending order.

Dialog boxes

Dialog boxes can appear with information about a specific task. Dialog boxes can also appear for questions that require a decision.

Notification bar

To inform you of completed events or to alert you of issues that may require attention, notifications may appear in a bar across the top of the Data Protection Central interface.

Figure 3. Example notification

Overflow button

Overflow buttons can appear within the user interface. When you click an **Overflow** button, a menu of available operations appears.

Figure 4. Overflow button

Dashboards overview

Data Protection Central dashboards provide at-a-glance insight into systems and activities.

Dashboard widgets include key performance indicators that display the following types of system information:

- Backup Activities
- Replication Activities
- Trends
- Assets
- Capacity
- Health
- Alerts

From dashboard widgets, you can examine specific areas of interest.

All dashboard widgets have customizable settings. The customizable settings vary based on each widget. Certain widgets enable you to change the activity type, widget type, and time range. All widgets include a widget filter that you can use to filter by systems and groups. The widget filter can also filter by asset tags when available for a widget.

You can customize dashboard widgets by changing the widget type, deleting the widget, or adding a widget. To change the title of the widget, click the title and change it to a different title. For example, if you applied a filter to show only grouped Avamar systems, you might change the Alerts Summary widget title to Avamar Alerts.

Individualized dashboard settings are stored for each user. You can add, edit, and delete custom dashboards. Each user can create and store up to 20 dashboards.

All the dashboards refreshes automatically every five minutes. The data is logged by Data Protection Central periodically.

Health overview

Data Protection Central tracks various criteria to determine system health status, including communication, alerts, SSO, and capacity for systems that are configured in Data Protection Central.

This information is used to determine the overall health state of the system. The health status is reported on the **Health** page.

Alerts overview

To view and manage alerts for Data Protection Central and all systems, visit the **Alerts** page.

Data Protection Central maps alerts from systems to three alert levels: Error, Warning, or Informational.

Capacity overview

Capacity monitoring can keep you aware of unexpected data growth that may cause downstream failures.

To view the capacity state of systems that are configured in Data Protection Central, visit the **Capacity** page.

Activities overview

Data Protection Central Activities include system activities at the job and asset level.

System activity includes information about backup and replication activities for PowerProtect Data Manager, Avamar, and NetWorker systems that are connected to Data Protection Central.

NOTE: NetWorker replication activities are not reported on the **Asset Activities** page because NetWorker does not replicate at the level of individual assets.

Audit overview

Audit information includes actions and tasks that Data Protection Central users have performed. The audit information can also be used to track the status of long running tasks.

View audit information on the **Audit** page.

System management overview

The **System Management** page provides the capability for you to add, edit, delete, and manage systems and groups in Data Protection Central.

The following list includes the system management capabilities that are available in Data Protection Central:

- Add, edit, and delete Avamar, NetWorker, Data Domain, PowerProtect Data Manager, Data Protection Advisor, and Search systems.
- Organize systems into groups, including the ability to add, edit, and delete groups.
- View system information.
- Launch the native management application for the system.
- For Avamar systems:

- View, add, edit, and delete policies, retentions, schedules, and datasets.
- Add clients and proxies to policies.
- Perform a backup of a policy.

- When an Avamar system is not reporting, Data Protection Central automatically attempts to reactivate the system every 15 minutes. Manually reactivating the Avamar system is possible, but if activation is already in progress, this operation does not work. It is recommended that you allow Data Protection Central to automatically reactivate the Avamar system.

NOTE: Use the filter option to filter the connected systems as per the *Type*, and *System Name*.

Search and recover overview

Data Protection Central integrates with Search to provide you with the ability to perform complex search and recover operations.

Data Protection Central launches Search in a new browser window.

For information about how to use Search, refer to the Search documentation set.

NOTE: To take full advantage of Data Protection Central capabilities, it is recommended that all systems that are configured in Search also be configured in Data Protection Central.

Reports overview

Data Protection Central provides the capability for you to run Data Protection Advisor reports for Avamar , NetWorker, PowerProtect Data Manager, and Data Domain systems.

Data Protection Central reporting features require you to have Data Protection Advisor system configured with Data Protection Central.

Add a Data Protection Advisor system provides instructions for adding a Data Protection Advisor system to Data Protection Central.

For more information about Data Protection Advisor, see the Data Protection Advisor documentation set.

You can run, and then view these reports directly in the Data Protection Central user interface. You can also specify the reporting period for these reports within the Data Protection Central interface.

NOTE: To take full advantage of Data Protection Central capabilities, it is recommended that all systems that are configured in Data Protection Advisor be configured in Data Protection Central.

Administration overview

The Data Protection Central administrator can change the idle timeout settings, and configure identity providers like LDAP, and Active Directory using the **Administration** option in the left pane.

The following capabilities are available in the **Administration** page.

- Change application idle timeout settings.
- Add an identity source.
- Edit an identity source.
- Delete an identity source.

NOTE: Only make the changes mentioned above.

4

Adding Systems to Data Protection Central

Learn about how to add data protection systems to Data Protection Central.

Data Protection Central supports monitoring of the following systems that are deployed on premise or in cloud. Monitoring of the systems that are deployed over the cloud is same as the monitoring of the systems that are deployed on premises.

- Avamar
- Data Domain
- NetWorker
- PowerProtect Data Manager

NOTE:

- For information about editing systems and troubleshooting, see the *Data Protection Central Administration Guide*.
- For more information about supported cloud platforms, see Data Protection Central Support Matrix, available at https://elabnavigator.dell.com/eln/elnhome.

Topics include:

Topics:

Add Avamar system

Use Data Protection Central to add Avamar system.

Steps

1. In the **Left** menu, select **System Management**.
2. Click **ADD**.
   The **Add System** window is displayed.
3. On the **Select System Type** page, select **Avamar**, and then click **Next**.
4. On the **Connection Information** page, specify the following information:
   - **Name**: Specify a name that helps identify the system.
   - **Hostname**: Specify the fully qualified domain name (FQDN) of the Avamar system.
   - **Avamar Username**: Specify the username of the Avamar system. For Avamar Administrator, the username is MCUser.
   - **Avamar Password**: Specify the password for the Avamar system user interface.
5. (Optional) To specify optional fields, click **Show optional fields**, and then specify the following information, as required:
   a. **Port**: Specify the Avamar MCS port. The default value is 9443. To specify the default value, leave this field blank.

      NOTE: When you add a system to Data Protection Central that uses a nonstandard port, you must modify the Data Protection Central firewall to enable communication with that port. The *Data Protection Central Security Configuration Guide* provides instructions.

   b. **OS Root password**: Specify the OS root password.

      NOTE: OS root credentials are optional for Avamar 19.3 and later. If the Avamar version is 19.2 or earlier, click the toggle button to enable the field and specify the OS root password.

c. **Override MCGUI URL**: Specify an alternate URL destination for the **Avamar Administrator** button.

   To override the **Avamar Administrator** link to direct to the AUI, type **`https://<Avamar>_fqdn>/aui`**.

6. Click **Next**.
7. On the **Certificate Verification** page, to ensure that you are adding the right system, verify that the certificate information matches the exact certificate on the <Avamar> system.
8. Once you have confirmed that the certificate information is correct, select **Accept Certificate**, and then click **Save**.
   - Data Protection Central does not validate the certificate and uses the certificate that you verify to connect with the system. If the remote system certificate changes, Data Protection Central does not connect with the system.
   - In this scenario, edit the system on the Data Protection Central **System Management** page to verify the new certificate details.

Add a NetWorker system

To use Data Protection Central to monitor and manage NetWorker systems, add one or more NetWorker systems.

Steps

1. In the **Left** menu, select **System Management**.
2. Click **ADD**

   The **Add System** window is displayed.
3. On the **Select System Type** page, select **NetWorker**, and then click **Next**.
4. On the **Connection Information** page, specify the following information:
   - **Name**: Specify a name that helps identify the system.
   - **Hostname**: Specify the IP address or fully qualified domain name (FQDN) of the NetWorker server.
   - **Username**: Specify the local NetWorker Authentication Service administrator username.
   - **Password**: Specify the local NetWorker Authentication Service administrator password.
5. (Optional) To specify optional fields, click **Show optional fields**, and then specify the following information, as required:
   a. **Port**: Specify the REST API port number. The default value is 9090.

      NOTE: When you add a system to Data Protection Central that uses a nonstandard port, you must modify the Data Protection Central firewall to enable communication with that port. The *Data Protection Central Security Configuration Guide* provides instructions.

   b. **NMC URL**: Specify the NMC URL when NMC is installed on a server that is different from the NetWorker server. Type the URL in the following format:
   <http_or_https>://<nmc_server_host>:<port>/gconsole.jnlp

      Where:
      - *<http_or_https>* is either HTTP or HTTPS, depending on the connection type that is configured to access NMC.
      - *<nmc_server_host_or_ip>* is the NMC server hostname or IP address.
      - *<port>* is the port number for the HTTP or HTTPS service. The default port number is 9000 for HTTP and 9090 for HTTPS.

   c. **NWUI URL**: Specify the URL when the NetWorker Management Web UI software is installed in a location that is different from the default location. Type the URL in the following format:
   https://*<nwui_server_host>*:*<port>*/nwui

      Where:
      - *<nui_server_host_or_ip>* is the NetWorker Management Web UI server hostname or IP address.
      - *<port>* is the port number for the HTTPS service. The default port number is 9090.
6. Click **Next**.
7. On the **Certificate Verification** page, to ensure that you are adding the correct system, verify that the certificate information being displayed matches the certificate on the NetWorker system.
8. Once you have confirmed that the certificate information is correct, select **Accept Certificate**, and then click **SAVE**.
   - Data Protection Central does not validate the certificate and uses the certificate that you verify to connect with the system. If the remote system certificate changes, Data Protection Central does not connect with the system.
   - In this scenario, edit the system on the Data Protection Central **System Management** page to verify the new certificate details.

Next steps

If the NetWorker system is a NetWorker Virtual Edition system, you may be required to edit the NVE firewall settings to read jobs. To determine which versions of NVE require this operation, see the "Troubleshooting" chapter of the *Data Protection Central Administration Guide*.

Add a Data Domain System

Perform the following steps to add a Data Domain.

Steps

1. In the **Left** menu, select **System Management**.
2. Click **ADD**.
   The **Add System** window is displayed.
3. On the **Select System Type** page, select **Data Domain**, and then click **Next**.
4. On the **Connection Information** page, specify the following information:
   - **Name**: Specify a name that helps identify the system.
   - **Hostname**: Specify the Fully Qualified Domain Name (FQDN) of the Data Domain system.
   - **Username**: Specify the Data Domain administrator username.
     NOTE: The username for *SSO* authentication is **`sysadmin`** by default.
   - **Password**: Specify the Data Domain administrator password.
5. Click **Next**.
6. On the **Certificate Verification** page, to ensure that you are adding the right system, verify that the certificate information matches the certificate on the Data Domain system.
7. Once you have confirmed that the certificate information is correct, select **Accept Certificate**, and then click **SAVE**.

   Data Protection Central does not validate the certificate and uses the certificate that you verify to connect with the system. If the remote system certificate changes, Data Protection Central does not connect with the system.

   In this scenario, edit the system on the Data Protection Central **System Management** page to verify the new certificate details.

Role-based access control for Data Domain

Data Protection Central supports role-based access control for Data Domain using *SSO*.

The following prerequisites must be configured in Data Domain:

- Active Directory authentication, or LDAP authentication.
- Group role mapping
- Single sign-on user management mapping

Also configure the identity sources in Data Protection Central.

NOTE: Use **`domain\username`**, or **`username@domain`**, or **`username`** formats to log in to Data Protection Central.

Add a Data Protection Advisor system

To use the Data Protection Central reporting features, you must add a Data Protection Advisor system.

Steps

1. In the **Left** menu, select **System Management**.
2. Click **ADD**.
   The **Add System** dialog box is displayed.
3. On the **Select System Type** page, select **Data Protection Advisor**, and then click **Next**.
4. On the **Connection Information** page, specify the following information:

- **Name**: Specify a name that helps identify the system.
- **Hostname**: Specify the fully qualified domain name (FQDN) of the Data Protection Advisor system.
- **Username**: Specify the Data Protection Advisor Administrator username.
- **Password**: Specify the Data Protection Advisor Administrator password.

5. (Optional) To specify a nondefault Data Protection Advisor port number, click **Show optional fields**, and then type the port number in the **Port** field.

   NOTE: When you add a system to Data Protection Central that uses a nonstandard port, you must modify the Data Protection Central firewall to enable communication with that port. The *Data Protection Central Security Configuration Guide* provides instructions.

6. Click **Next**.
7. On the **Certificate Verification** page, to ensure that you are adding the correct system, verify that the certificate information being displayed matches the certificate on the Data Protection Advisor system.
8. Once you have confirmed that the certificate information is correct, select **Accept Certificate**, and then click **SAVE**.

   Data Protection Central does not validate the certificate and uses the certificate that you verify to connect with the system. If the remote system certificate changes, Data Protection Central does not connect with the system.

   In this scenario, edit the system on the Data Protection Central **System Management** page to verify the new certificate details.

Add a Search system

To perform advanced search and recover operations, you must add a Search system.

Steps

1. In the **Left** menu, select **System Management**.
2. Click **ADD**.

   The **Add System** window is displayed.
3. On the **Select System Type** page, select **Data Protection Search**, and then click **Next**.
4. On the **Connection Information** page, specify the following information:
   - **Name**: Specify a name that helps identify the Search system.
   - **Hostname**: Specify the fully qualified domain name (FQDN) of the Search system.
   - **Username**: Specify the Search Administrator username.
   - **Password**: Specify the Search Administrator password.
5. (Optional) To specify optional fields, click **Show optional fields**, and then specify the following information, as required:
   - **Admin Rest API Port**: Specify the Search REST API port. The default value is 448.
   - **Search UI Port**: Specify the Search UI port. The default value is 443.

   NOTE: When you add a system to Data Protection Central that uses a nonstandard port, you must modify the Data Protection Central firewall to enable communication with that port. The *Data Protection Central Security Configuration Guide* provides instructions.

6. Click **Next**.
7. On the **Certificate Verification** page, to ensure that you are adding the correct system, verify that the certificate information being displayed matches the certificate on the Search system.
8. Once you have confirmed that the certificate information is correct, select **Accept Certificate**, and then click **SAVE**.

   Data Protection Central does not validate the certificate and uses the certificate that you verify to connect with the system. If the remote system certificate changes, Data Protection Central does not connect with the system.

   In this scenario, edit the system on the Data Protection Central **System Management** page to verify the new certificate details.

Add a PowerProtect Data Manager system

To use Data Protection Central to monitor and manage PowerProtect Data Manager systems, add one or more PowerProtect Data Manager systems.

Prerequisites

NOTE: AD and LDAP users must observe these SSO requirements when launching PowerProtect Data Manager:

- PowerProtect Data Manager and Data Protection Central must connect to the same AD/LDAP server.
- Users must log in to Data Protection Central using UPN format.

For more details, see the *Data Protection Central Security Configuration Guide*.

Steps

1. In the **Left** menu, select **System Management**.
2. Click **ADD**.
   The **Add System** dialog box is displayed.
3. On the **Select System Type** page, select **PowerProtect Data Manager**, and click **Next**.
4. On the **Connection Information** page, specify the following information:
   - **Name**: Specify a name that helps identify the system.
   - **Hostname**: Specify the fully qualified domain name (FQDN) of the PowerProtect Data Manager system.
   - **Username**: Specify the PowerProtect Data Manager Administrator username.
   - **Password**: Specify the PowerProtect Data Manager Administrator password.
5. Click **Next**.
6. On the **Certificate Verification** page, to ensure that you are adding the correct system, verify that the certificate information being displayed matches the certificate on the PowerProtect Data Manager system.
7. Once you have confirmed that the certificate information is correct, select **Accept Certificate**, and then click **SAVE**.
   Data Protection Central does not validate the certificate and uses the certificate that you verify to connect with the system. If the remote system certificate changes, Data Protection Central does not connect with the system.
   In this scenario, edit the system on the Data Protection Central **System Management** page to verify the new certificate details.

Role-based access control for PowerProtect Data Manager

Data Protection Central supports role-based access control for PowerProtect Data Manager using *SSO*.

The following prerequisites must be met for role-based access control:

- The identity sources and group-role mapping must be configured in PowerProtect Data Manager.
- The identity sources must be configured in Data Protection Central.
  NOTE: Use **`username@domain`** or **`username`** to log in to Data Protection Central. PowerProtect Data Manager does not support the **`domain\username`** format.
- To enable the role based access control, the identity sources provided in Data Protection Central and PowerProtect Data Manager must match.