Dell EMC Data Protection Central

Version 1.0.1

Getting Started Guide

302-004-505

REV 02

DELL EMC

Copyright © 2017-2018 Dell Inc. or its subsidiaries. All rights reserved.

Published February 2018

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.“ DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

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

CONTENTS

Preface

As part of an effort to improve 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
02	February 14, 2018	The following changes are included in this revision: • Added "Environment and system requirements" to the "Data Protection Central Overview" chapter. • Updated "Verify the deployment" to add a note about the browsers that are supported with Data Protection Central. • Added the "Adding Systems to Data Protection Central" chapter.
01	February 2, 2018	Initial release of the *Data Protection Central 1.0.1 Getting Started Guide*.

Related Documentation
For information about Data Protection Central compatibility, refer to 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
- Data Protection Advisor

- Data Protection Search
- NetWorker

Special notice conventions that are used in this document
The following conventions are used for special notices:

NOTICE

Identifies content that warns of potential business or data loss.

Note

Contains information that is incidental, but not essential, to the topic.

Typographical conventions
The following type style conventions are used in this document:

Table 2 Style conventions

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 non-essential 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://support.emc.com
- https://community.emc.com

Where to get support
The Support website at https://support.emc.com provides access to licensing information, product documentation, advisories, and downloads, as well as how-to and

troubleshooting information. This information may enable you to resolve a product issue before you contact Support.

To access a product specific Support page:

1. Go to https://support.emc.com/products.
2. In the **Find a Product by Name** box, type a product name, and then select the product from the list that appears.
3. Click  .
4. (Optional) To add the product to **My Saved Products**, in the product specific page, click **Add to My Saved Products**.

Knowledgebase
The Knowledgebase contains applicable solutions that you can search for by solution number, for example, 123456, or by keyword.

To search the Knowledgebase:

1. Go to https://support.emc.com.
2. Click **Advanced Search**.
   The screen refreshes and filter options appear.
3. In the **Search Support or Find Service Request by Number** box, type a solution number or keywords.
4. (Optional) To limit the search to specific products, type a product name in the **Scope by product** box, and then select the product from the list that appears.
5. In the **Scope by resource** list box, select **Knowledgebase**.
   The **Knowledgebase Advanced Search** panel appears.
6. (Optional) Specify other filters or advanced options.
7. Click  .

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

1. Go to https://support.emc.com.
2. Click **Chat with Support**.

Service requests
To obtain in-depth help from Support, submit a service request. To submit a service request:

1. Go to https://support.emc.com.
2. Click **Create a Service Request**.

Note

To create a service request, you must have a valid support agreement. Contact a sales representative for details about obtaining a valid support agreement or with questions about an account.

To review an open service request:

1. Go to https://support.emc.com.
2. Click **Manage service requests**.

Online communities

Go to the Community Network at https://community.emc.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all products.

How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Data Protection Central Overview

Learn about Data Protection Central.

Topics include:

Product overview

Data Protection Central provides a solution for data protection administrators who are challenged by having to manage independent and disconnected applications that are used to configure and manage one or more data protection and storage devices.

Working with multiple applications in this manner causes daily operational monitoring and management to be a complex, time consuming effort. Data Protection Central enables administrators to efficiently and effectively 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:

- Ability to launch the following software from a central location:
  - NetWorker
  - Avamar
  - Data Domain
  - Data Protection Search
  - Data Protection Advisor
- Comprehensive dashboards that include the following system information:
  - The following information for NetWorker, Avamar, and Data Domain systems:
    - Backup and replication activities
    - Health
    - Alerts
  - Capacity information for Avamar and Data Domain systems.
- Ability to monitor multiple systems capabilities including system health and activities.
- Ability to manage Avamar systems.
- Complex search and recover operations through integration with Data Protection Search.
- Reporting capabilities through integration with Data Protection Advisor.

Environment and system requirements

The following list includes information about environment and system requirements:

- To deploy the Data Protection Central OVA, you must use VMware vCenter with VMware ESX 5.5 or later. The Data Protection Central OVA does not deploy directly to the ESXi server.
- The Data Protection Central host must have 2 CPUs, 6 GB of RAM, and 550 GB of disk space available.
- The FQDN, IP, Netmask, Gateway, DNS, and time zone must be configured. The FQDN must resolve to the IP address.
- The environment must use static network settings.
- Data Protection Central requires a minimum browser window size of 1366x768.
- Ensure that the DNS is set up correctly. The correct DNS setup ensures that systems can resolve the Data Protection Central hostname and FQDN name.

- Data Protection Central is compatible with VMware vSphere Fault Tolerance (FT), VMware vSphere High Availability (HA), and VMware vSphere vMotion.

The following table includes information about the versions of products that are supported with Data Protection Central:

Table 3 Compatibility

Product	Supported versions
NetWorker	9.2.1
Avamar	7.4.1-58_HF282217_6 hotfix
	7.5
	7.5.0-183_HF284113_2 hotfix
	7.5.1
Data Domain	6.0
	6.1
	6.1.1
Data Protection Advisor	6.4
	6.5
Data Protection Search	1.1 SP3
Mozilla Firefox	Latest version
Google Chrome	Latest version

Monitoring systems

Data Protection Central includes system monitoring features at the activity, system, and alert level.

The systems monitoring features include:

- Activities—Displays backup and replication (clone) activity information for Avamar and NetWorker systems.
- Alerts—Displays alerts information originating from Avamar, NetWorker, and Data Domain systems.
- Capacity—Displays capacity information at a system level for Avamar and Data Domain systems.

If a Data Domain system is configured in a monitored Avamar system, the Data Domain system is automatically added as a monitored system.

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, retentions, schedules, and datasets.

- 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 an Avamar system.

Search and recover capabilities

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

Data Protection Central launches Data Protection Search in a new browser tab.

After launching Data Protection 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 Data Protection Search, refer to the Data Protection Search documentation set.

Note

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

Report capabilities

Data Protection Central provides the capability for you to run 11 of the most used Data Protection Advisor reports for Avamar, NetWorker, and Data Domain systems.

Data Protection Central reporting features require you to have Data Protection Advisor in the environment. For more information about Data Protection Advisor, refer to 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 also be configured in Data Protection Central.

CHAPTER 2

Deployment and Configuration

Learn about how to deploy and configure Data Protection Central.

Topics include:

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, and Data Protection Advisor system is correct.

Procedure

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

   For successful activation certificates, the time that appears on the system must be in sync 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 in sync.

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 <dpc_hostname>
   ```

   Type the following command:

   ```
   nslookup <dpc_ip_address>
   ```

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. Verify that the Data Protection Central entry in the `/etc/hosts` file includes the short name, for example:

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

Deploy the OVA

Deploy the Data Protection Central OVA using a VMware vSphere client. Refer to the VMware documentation for specific information regarding how to deploy an OVF template.

Before you begin

Ensure that the following system requirements are met:

- The DNS is set up correctly. The correct DNS set up ensures that systems monitored by Data Protection Central can resolve the Data Protection Central hostname and Fully Qualified Domain Name (FQDN).
- VMware vCenter with VMware ESX 5.5 or later is deployed. To deploy the Data Protection Central OVA, you must use vCenter. The Data Protection Central OVA does not deploy directly to the ESXi server.
- 2 CPUs and 6 GB of RAM.
- 550 GB of disk space available.
- The FQDN, IP, Netmask, Gateway, DNS, and time zone are configured. The FQDN must resolve to the IP address.
- The environment is using static network settings.

Procedure

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 is to be deployed.
6. Accept the end user license agreement.
7. Specify the name and location of the Data Protection Central virtual machine.
8. Select the virtual disk format.

   When selecting the virtual disk format, the `Thick Provision Lazy Zeroed` option is recommended.

9. Specify network properties:
   a. For the Network IP address, specify the IPv4 address or IPv6 address for the virtual appliance.

   Note

   For IPv6 addresses, to resolve the hostname of the appliance to the IP address, use the `nslookup` command. Specify the IPv6 address in the format that appears in the `nslookup` output.

   b. For the Default Gateway, specify the default gateway IPv4 address or IPv6 address that you want the virtual appliance to use.
   c. For the Network Netmask/Prefix, when you use IPv4 addressing, specify the netmask of the virtual appliance. When you use IPv6 addressing specify the prefix length.

d. For the DNS, specify up to three domain name servers for this virtual appliance.

   Separate domain names with commas.

e. For the FQDN, 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.

10. Specify a Master password for the Data Protection Central lockbox.

    The lockbox password length must be between 8 and 256 characters.

    Data Protection Central uses a lockbox to encrypt and store the credentials of the systems it monitors. This password is used along with certain System Stable Values (SSVs) to create an encryption key.

11. Specify location settings.
12. (Optional) Configure LDAP.

    Add LDAP to Data Protection Central during deployment on page 19 provides the steps to configure LDAP while deploying the OVA.

13. (Optional) If the deployment location requires EMC branding, in the **Change branding to support EMC required locale** list box, select **Yes**.
14. Validate the information that you specified, and then complete the deployment of the Data Protection Central OVF.

Deploy Data Protection Central on a standalone server or virtual machine

Data Protection Central can be installed on a server or virtual machine using a self-extracting .bin file.

Before you begin

Ensure that the following minimum system requirements are met:

- Standalone server deployments require 1.5GHz processor.
- Virtual machine deployments require 2 CPUs with 1 core each.
- 6GB of RAM.
- 250 GB of disk space available.
- The environment is running SuSE Linux Enterprise Server 12 SP2.
- Java version 1.8.0_151 is installed.
- The DNS is set up correctly. The correct DNS set up ensures that systems monitored by Data Protection Central can resolve the Data Protection Central hostname and Fully Qualified Domain Name (FQDN).
- The FQDN, IP, Netmask, Gateway, DNS, and time zone are configured.
- The environment is using static network settings.

Prior to installing Data Protection Central, ensure that an administrative user exists on the host named 'admin' and is added to a group named 'admin' .

Procedure

1. Download and save the Data Protection Central .bin file.

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

   ```
   ./<FILENAME>.bin
   ```

Verify the deployment

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

Before you begin

Ensure that the virtual machine where the OVA file was deployed is powered on.

Note

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

Procedure

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, type:

   `secret`
4. Click **LOG IN**.

   The first time you log in you are required to change the password. The password requirements are as follows:

   - A minimum of 9 characters.
   - A maximum of 15 characters.
   - At least 1 lowercase character.
   - At least 1 uppercase character.
   - At least 1 number.
   - At least 1 of the following special characters:
     ! @ # $ % ^ & * ( ) - _
   - The password cannot include any white space.

The *Data Protection Central Security Configuration Guide* provides the steps to reset the `administrator@dpc.local` password.

Migrating from Multiple Systems Management to Data Protection Central

Data Protection Central does not support a direct upgrade from Multiple Systems Management (MSM) due to significant architectural changes that give Data Protection Central better stability and scalability.

Procedure

1. Identify the Avamar systems being monitored with MSM that are supported with Data Protection Central.

   Avamar versions 7.4.1 and later are supported with Data Protection Central.

2. Using the MSM user interface, remove the Avamar systems identified in step 1 from MSM.
3. Deploy the Data Protection Central OVA.

   Deploy the OVA on page 15 provides instructions.

4. Log into the Data Protection Central OVA, and then use **System Management** to add the Avamar systems.

   Each Avamar system remains in the **NotReporting** state for several minutes until adaptor activation is complete.

Results

Once the adaptor activation is complete, the migrated Avamar systems begin logging activities to Data Protection Central and are no longer monitored by MSM.

Note

Historical Avamar monitoring data is not transferred to Data Protection Central.

Data Protection Central will attempt to automatically add any Data Domain systems configured with monitored Avamar systems. If required, Data Domain systems can also be added manually through Data Protection Central **System Management**.

Configuring LDAP

Data Protection Central supports LDAP authentication. Learn about LDAP requirements and configuration procedures in this section.

Note

OpenLDAP and Active Directory (AD) are supported.

You can configure LDAP during or after deploying Data Protection Central.

Add LDAP to Data Protection Central during deployment

You can optionally configure LDAP during deployment.

Procedure

1. Create a `dp_admin` group on the LDAP server, and then add to the `dp_admin` group any users that require access to Data Protection Central.
2. While deploying the Data Protection Central OVA, specify the following settings:
   - **LDAP server URL**—Type the FQDN or IP address of the server where LDAP is hosted.
   - **Port number**—Type the LDAP server port.
   - **Query username**—Type the username for logging to the LDAP server.
   - **Search admin group name**—Type the admin group name `dp_admin`.
   - **Base domain name**—Type the domain of the LDAP server.
   - **LDAP Type**—Select the type of LDAP:
     - Windows Active Directory (AD)
     - Lightweight Directory Access Protocol (LDAP) server

Add LDAP to Data Protection Central after deployment

You can optionally configure LDAP after deployment.

Procedure

1. To access the DPC system, type the following command:

   ```
   ssh -l USERNAME DPCSERVER
   ```

2. To switch to the root user, type the following command:

   ```
   su -
   ```

3. To stop the Data Protection Central services, type the following command:

   ```
   /usr/local/dpc/bin/dpc stop
   ```

4. Edit the following file to specify the values that are specific to the environment:

   `/var/lib/dpc/elg/ldap.properties`
   If the file does not exist, create it with the template file format specified below.

   Note

   This file must match the exact file name and location.

For example, consider the following ldap.properties file template.

```
LDAP configuration file template
/var/lib/dpc/elg/ldap.properties
#
# Copyright (c) 2017 Dell EMC.
# All rights reserved.
# This software contains the intellectual property of Dell
EMC or is licensed to
#  Dell EMC from third parties. Use of this software and the
intellectual property
#  contained therein is expressly limited to the terms and
conditions of the License
#  Agreement under which it is provided by or on behalf of
Dell EMC.
#
#-----------------------------------------------------------
----------------
# LDAP Authentication Configuration
#-----------------------------------------------------------
----------------
#

# LDAP configuration - possible values are: AD or LDAP
# AD = Active Directory
# LDAP = LDAP server
elg.ldap.type=LDAP

# LDAP server URL in the form of ldap://hostname:port.
# ldap example  = elg.ldap.server.urls=ldap://{URL:389}
# ldaps example = elg.ldap.server.urls=ldaps://{URL:636}
#elg.ldap.server.urls=ldap://ldaps.sddc.local:389/
elg.ldap.server.urls=ldaps://ldaps.sddc.local:636/

# LDAP base DN
# For example dc=dpc,dc=local
elg.ldap.base.dn=dc=my-domain,dc=com

# LDAP group name
# The value below must be 'dp_admin'
elg.ldap.group.search.name=dp_admin

# LDAP admin credentials.
# Should be in base dn format, for example
cn=Manager,ou=people,dc=dpc,dc=local
#elg.ldap.admin.dn=cn=CISAdmin,ou=people,dc=my-domain,dc=com
elg.ldap.admin.dn=cn=Administrator,dc=my-domain,dc=com
elg.ldap.admin.password=changeme
```

5. Save, and then close the file.
6. To assign administrator ownership on the ldap.properties file, type the following command:

```
chown admin:admin /var/lib/dpc/elg/ldap.properties
```

7. To restart Data Protection Central and activate the change, type the following command:

```
/usr/local/dpc/bin/dpc start
```

8. Once Data Protection Central is started, type the following command to confirm that all of the services are active:

```
/usr/local/dpc/bin/dpc status
```

9. Log in to the Data Protection Central user interface with the username and password for the LDAP user account.

   For example:
   https://*DPC_fqdn*

   where *DPC_fqdn* is the Data Protection Central fully qualified domain name.

Restoring access to Data Protection Central after LDAP misconfiguration

When LDAP is configured incorrectly, you can be locked out of the Data Protection Central OVA.

If you cannot log into Data Protection Central after configuring LDAP, perform the following steps.

Procedure

1. To disable the ldap.properties file, rename it using the following command:

```
mv ldap.properties ldap.properties.old
```

2. To restart Data Protection Central and activate the change, type the following commands:

```
/usr/local/dpc/bin/dpc stop
/usr/local/dpc/bin/dpc start
```

Results

After Data Protection Central is restarted, LDAP is disabled and access to Data Protection Central is restored.

Remove LDAP from Data Protection Central

If required, you can remove LDAP from Data Protection Central.

Procedure

1. To access the DPC system, type the following command:

```
ssh -l USERNAME DPCSERVER
```

2. To switch to the root user, type the following command:

```
su -
```

3. To remove the `ldap.properties` file, type the following command:

```
rm var/lib/dpc/elg/ldap.properties
```

4. To restart Data Protection Central and activate the change, type the following command:

```
/usr/local/dpc/bin/dpc start
```

5. Once Data Protection Central is started, type the following command to confirm that all of the services are active:

```
/usr/local/dpc/bin/dpc status
```

6. Log in to the Data Protection Central user interface with the username and password for the non-LDAP user account.

   For example:
   https://*DPC_fqdn*

   where *DPC_fqdn* is the Data Protection Central fully qualified domain name.

Secure LDAP (LDAPS) Certificate

Secure LDAP (LDAPs) requires an SSL link, and therefore requires certificate-based authentication.

Data Protection Central automatically uses the certificate authorities available within the standard Java keystore.

If the LDAP server that authenticates Data Protection Central credentials uses a non-standard certificate authority, you must add the root certificate of the authority that signed the LDAP server certificate to the Data Protection Central keystore.

The following command imports a server certificate to the Data Protection Central keystore:

```
keytool -importcert -file <filename.pem> -v -keystore /var/lib/
cacertificates/java-cacerts
-storepass changeit -alias <unique_alias_for_the_certificate>
```

The following command lists the certificates in the keystore:

```
keytool -list -v -keystore /var/lib/ca-certificates/java-cacerts -
storepass changeit
```

After the certificate is added to the keystore, restart DPC services using the following commands:

```
/usr/local/dpc/bin/dpc stop
/usr/local/dpc/bin/dpc start
```

Access control

Access control settings provide protection of resources against unauthorized access.

Data Protection Central provides a single, default administrative account.

The username of this internal account is:

`administrator@dpc.local`

The `administrator@dpc.local` account has all rights within the Data Protection Central application.

On initial log in to Data Protection Central, the user is prompted to change the password.

When LDAP is connected to Data Protection Central, additional accounts can be enabled as Data Protection Central administrators by adding them to the LDAP dp_admin group.

Each of these administrator accounts added through LDAP will have full authorization and access to all Data Protection Central functions. Data Protection Central also supports custom dashboard settings for each administrator account.

Default accounts

The following table includes the Data Protection Central default accounts and passwords.

Table 4 Default accounts and passwords

User account	Password	Description
web and browser admin	The admin password is set when Data Protection Central is deployed. The default account is `administrator@dpc.local` and the default password is `secret`.	The default user for Data Protection Central web application administration.
Linux OS admin	The admin password is set when Data Protection Central is deployed. The account is admin and the default password is `changeme`. This user account is for an OVA deployment only.	The default user for Data Protection Central OS-level administration. Only admin can log in using secure shell. After three failed login tries, the admin account is locked out for a period of five minutes.
Linux OS root	The default password is `changeme`.	Root operation system account. This account is for an OVA deployment only.

NOTICE

After completing the Data Protection Central deployment, it is recommended that you change the default passwords.

To change the password for the admin and root accounts, use the UNIX `passwd` command.

Only the admin account can log in using a secure shell (ssh).

Certificate management

Consider the following when managing certificates:

- Certificates are used for secure http access (https).
- By default, Data Protection Central generates a default SSL self-signed certificate in the following location:

  `/var/lib/dpc/webcerts`
- The self-signed certificate is sufficient to establish an encrypted channel between web browsers and the server.
- The self-signed certificate cannot be used for authentication.
- Consider company policies when creating certificates.
- You can create a self-signed certificate.
- You can create a certificate that is signed by a trusted certificate authority (CA) vendor.

Generate a self-sign certificate

To enable a secure browser connection, create a private key and a self-sign certificate.

Procedure

1. To connect to the Data Protection Central server as an admin user, run the following command:

   ```
   ssh admin@SERVER
   ```

2. To change to the root user, run the following command:

   ```
   su -
   ```

3. To change the directory to `/var/lib/dpc/webcerts`, run the following command:

   ```
   cd /var/lib/dpc/webcerts
   ```

4. To generate a new certificate, run the following command:

   ```
   openssl req -newkey rsa:2048 -sha256 -x509  -keyout private-
   key.pem -out cert.pem -nodes -days 3650
   ```

5. Set the owner and group of the new certificate files to the following:

```
chown admin *.pem
```

6. Restart NGINX.

```
systemctl restart nginx
```

7. To verify the new self-sign certificate, browse Data Protection Central.

Generate a Certificate Signing Request

To enable a secure browser connection, generate a Certificate Signing Request (CSR).

Procedure

1. To connect to the Data Protection Central server as an admin user, type the following command:

```
ssh admin@SERVER
```

2. To change to the root user, type the following command:

```
su -
```

3. To change the directory to `/var/lib/dpc/webcerts`, type the following command:

```
cd /var/lib/dpc/webcerts
```

4. To generate a new certificate using the private key at the self-sign step, type the following command:

```
openssl req -newkey rsa:2048 -sha256 -key private-key.pem -
out cert.csr
```

5. Send the `cert.csr` to a certificate authority (CA) vendor.
6. Replace the current *cert.pem* file to the certificate received from the CA vendor.
7. Restart NGINX.

```
systemctl restart nginx
```

8. To verify the new certificate, browse Data Protection Central.

CHAPTER 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:

Log in to Data Protection Central

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

Procedure

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. The web browser account password is:

   `secret`
4. Click **LOG IN**.

   If this is the first time you are logging in to Data Protection Central, you are prompted to change the password.

User interface

The Data Protection Central user interface includes the following components.

Header

The header includes the following components:

- **System Filter** button—This button provides you with the ability to filter the information that appears on a page by one or more systems or groups. The **System Filter** button appears only on the **Health** information pages and the **Activities > Systems** page.
- **About** button—This button provides the ability to view Data Protection Central version information.
- **User** menu—This menu provides the ability to change the password or log out of Data Protection Central.

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:

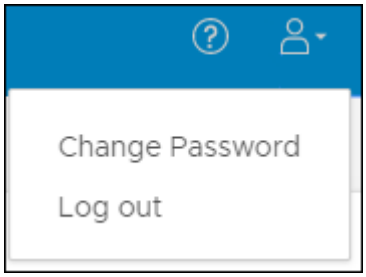
- Change a password.

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:

- **Dashboards**
- **Health**
  - Systems
  - Alerts
  - Capacity
- **Activities**
  - Systems
  - Audit
- **System Management**
- **Search and Recovery**

Note

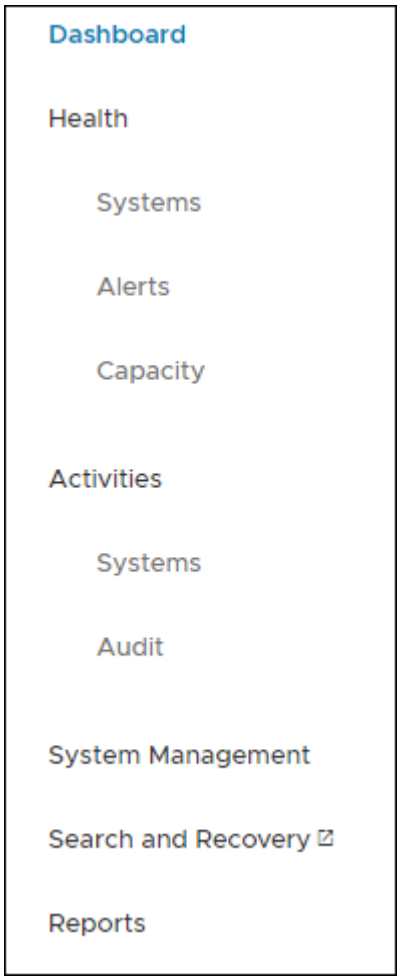
The **Search and Recovery** link is disabled when a Data Protection Search system is not successfully configured in Data Protection Central.

- **Reports**

Note

The **Reports** link is disabled when a Data Protection Advisor system is not successfully configured in Data Protection Central.

Figure 3 Left menu



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.

Master and Detail panes

Most Data Protection Central pages are composed of a **Master** and **Detail** pane.

The **Master** pane appears on the left side 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.

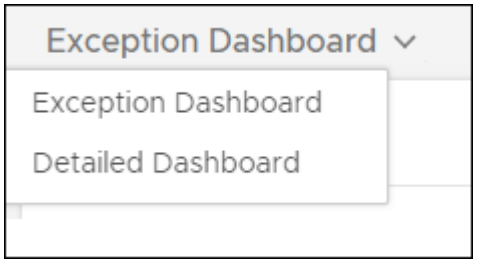
Choose another Dashboard menu

The **Choose another Dashboard** menu provides the capability for you to select a different dashboard to view.

Note

The **Choose another Dashboard** menu name is always the name of the dashboard that is selected.

Figure 4 Choose another Dashboard menu



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**—Appear in table headers.
- **Domain Filter**—Appears in the **Policies**, **Retentions**, **Schedules**, and **Datasets** pages.
- **System Filter**—Appears in the user interface header.
- **Widget filters**—Appears in widgets.

Column filters

Column filters can be used to filter the information that appears in tables.

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.

System Filter

The **System Filter** can be used to filter by one or more groups and systems.

The **System Filter** includes a tree that displays groups and systems. Systems must be part of a group to appear in the tree.

The **System Filter** appears in widgets and in the header on the following pages:

- **Health > Systems**
- **Health > Alerts**
- **Health > Capacity**
- **Activities > Systems**

When the **System Filter** is enabled, the icon appears bold and enclosed in a circle. A message appears in a bar across the top of the Data Protection Central interface with details about the applied filter.

Widget filters

Widget filters can be used to filter the information that appears in a widget.

All widgets include a **System Filter**.

Some widgets provide the ability for you to filter by reporting period. You can specify one of the following options:

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

When you use a dashboard widget to access a page, the information that is displayed is automatically filtered based on the widget settings. In contrast, when you use the **Left** menu to access a page, the information that is displayed is unfiltered or is filtered based on a previously set **System Filter**.

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

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.

To sort information, click a column heading.

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.

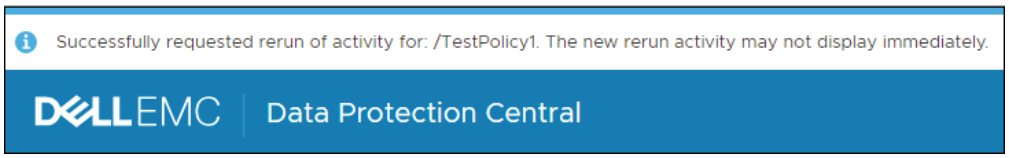
Dialog boxes

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 5 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 6 Overflow button

Dashboards overview

Data Protection Central dashboards provide at a glance insight into operational behavior.

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

- Backup Activities
- Replication Activities
- Capacity
- Health
- Alerts

From dashboard widgets, you can drill down in to specific areas of interest.

Dashboard widgets include a **System Filter** that provides the capability for you to filter by one or more systems or groups. Some widgets allow you to change the reporting period.

There are two default dashboards:

- **Exception Dashboard**
- **Detailed Dashboard**

You can add, edit, and delete dashboards as required.

A maximum of five dashboards are supported.

Health overview

Data Protection Central health includes information about system status, alerts, and capacity for systems that are configured in Data Protection Central.

This information is used to determine the health state of the system.

Capacity information appears for Avamar and Data Domain systems only.

Activities overview

Data Protection Central Activities include system activity and audit information.

System activity includes information about backup and replication activities for Avamar and NetWorker systems connected to Data Protection Central.

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.

System Management overview

System Management provides the capability for you to add, edit, remove, and manage systems 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, Data Protection Advisor, and Data Protection Search systems.
- Organize systems in to 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.
  - View existing clients that are associated with an Avamar system.
  - View client backups.
- When an Avamar system is not reporting, you can reactivate messaging.

Search and recover overview

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

Data Protection Central launches Data Protection Search in a new browser window.

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

Note

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

Reports overview

Data Protection Central provides the capability for you to run 11 of the most used Data Protection Advisor reports for Avamar, NetWorker, and Data Domain systems.

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

For more information about Data Protection Advisor, refer to 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 also be configured in Data Protection Central.

CHAPTER 4

Adding Systems to Data Protection Central

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

Note

For information about editing systems and troubleshooting, refer to the *Data Protection Central Administration Guide*.

Topics include:

Add an Avamar system

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

Procedure

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

   The **Add System** dialog box appears.
3. In the **Type** list box, select **Avamar**.
4. Specify the following connection information:
   - **Name**—You can specify any name that helps identify the system.
   - **Hostname**—Specify the fully qualified domain name (FQDN) of the Avamar system.
   - **Avamar Username**—The username is MCUser.
   - **Avamar Password**—The password is the MCUser password.
   - **OS Root password**—The password is the OS root password.
5. (Optional) To specify optional fields, click **Show optional fields**, and then specify the following information, as required:
   - **Port**—The Avamar MCS port. The default value is 9443. To specify the default value, leave this field blank.
   - **Override MCGUI URL**—The default setting for the **AVAMAR ADMINISTRATOR** button is to open a new browser tab, and then direct the user to the Avamar Administrator log in screen. If you do not want to use the default setting, this field provides the capability for you to define the URL that the **AVAMAR ADMINISTRATOR** button directs a user to.
6. Click **SAVE**.

   The **Systems** page refreshes and displays the new system.

Add a NetWorker system

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

Procedure

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

   The **Add System** dialog box appears.
3. In the **Type** list box, select **NetWorker**.
4. Specify the following connection information:
   - **Name**—You can specify any name that helps identify the system.

- **Hostname**—The host name of the NetWorker server that is configured during NetWorker installation. You can specify either the short name or the fully qualified domain name (FQDN).
- **Username**—The username that is used to log in to NetWorker Management Console.
- **Password**—The password that is used to log in to NetWorker Management Console.

5. (Optional) To specify optional fields, click **Show optional fields**, and then specify the following information, as required:
   - **Port**—The REST API port. The default value is 9090.
   - **NMC URL**—The NMC URL when NMC is installed on a server that is separate from the NetWorker server. The value should be written in the following format, where the port is usually 9000:
     http://*<nmc-server-host-or-ip>*:*<port>*/gconsole.jnlp
   - **Override Element Manager Launch URL**—The default setting for the **NETWORKER MANAGEMENT CONSOLE** button is to open a new browser tab, and then direct you to the NetWorker Management Console log in screen.
     If you do not want to use the default setting, this field provides the capability for you to define the URL that the **NETWORKER MANAGEMENT CONSOLE** button leads to.
6. Click **SAVE**.

   The **Systems** page refreshes and displays the new system.

Perform manual activation of NetWorker system reporting

You must enable full communication between a NetWorker system and Data Protection Central. Perform the following procedure on the NetWorker server.

Procedure

1. Launch a command prompt.
2. For Linux systems only, install the NetWorker adaptor located in `/opt/nsr/nsrmq/bin`.

   This step applies only to NetWorker software running on Linux servers and is not required for NetWorker Virtual Edition environments.

   Note

   The *Backup & Recovery Manager 1.3 User Guide* provides instructions on how to install the adaptor on Linux systems.
3. Execute the `nsrmqctl` program using one of the following commands:
   - Linux:

     ```
     /opt/nsr/nsrmq/bin/nsrmqctl
     ```
   - Windows:

     ```
     C:\Program Files\EMC NetWorker\nsr\nsrmq\bin\nsrmqctl.exe
     ```

4. Check the `nsrmq.log` file and ensure that the nsrmq process is connected to NetWorker. The log file is located in the following directories:

   - Linux:

     ```
     /opt/nsr/nsrmq/logs/
     ```

   - Windows:

     ```
     C:\Program Files\EMC NetWorker\nsr\nsrmq\logs\
     ```

   Messages similar to the following appear when the nsrmq process is connected to NetWorker:

   ```
   2018-01-18 12:54:10-0700 [AMQP] Connecting to / on
   127.0.0.1:5672
   2018-01-18 12:54:10-0700 [AMQP] Connected to / on 127.0.0.1:5672
   2018-01-18 12:54:10-0700 [AMQP] Opening new channel to 127.0.0.1
   2018-01-18 12:54:10-0700 [AMQP] Checking for exchange
   'networker' on 127.0.0.1
   2018-01-18 12:54:10-0700 [AMQP] Declaring read queue on
   'networker' (127.0.0.1)
   2018-01-18 12:54:10-0700 [AMQP] Binding 'rpc:networker' to
   amq.gen-RjgSkAuRAiEAs4UqmFMjug on 'networker' (127.0.0.1)
   2018-01-18 12:54:10-0700 [AMQP] Setting up read task for
   'networker/rpc:networker' (127.0.0.1)
   2018-01-18 12:54:10-0700 [AMQP] Listening on 'networker/
   rpc:networker' (127.0.0.1)
   2018-01-18 12:54:10-0700 [NMMRA] Connecting to NetWorker at
   networker.sddc.local
   2018-01-18 12:54:11-0700 [NMMRA] Connected to
   networker.sddc.local (NetWorker)
   ```

5. At the `nsrmqctl` prompt, type the following command:

   ```
   monitor <DPC_hostname>
   ```

   Note

   The *Backup & Recovery Manager 1.3 User Guide* provides more information on `nsrmqctl` commands.

6. Check the `nsrmq.log` file again and ensure that the operation is successful.

   Messages similar to the following appear when the communication is successful:

   ```
   2017-12-19 11:16:40-0700 [MONITOR] Sending
   networkerRegistration message
   2017-12-19 11:16:41-0700 [MONITOR] Retrieving configuration
   information
   2017-12-19 11:16:41-0700 [MONITOR] Sending
   networkerConfiguration message
   ```

Note

If the NetWorker services are restarted or the NetWorker server is upgraded, you must perform this procedure again to reactivate full communication between the NetWorker server and Data Protection Central.

Add a Data Domain System

Procedure

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

   The **Add System** dialog box appears.
3. In the **Type** list box, select **Data Domain**.
4. Specify the following connection information:
   - Name—You can specify any name that helps identify the system.
   - Hostname—Specify the Fully Qualified Domain Name (FQDN) of the Data Domain system.
   - Username—The Data Domain username that is used to log in to System Manager.
   - Password—The Data Domain password that is used to log in to System Manager.
5. Click **SAVE**.

   The **Systems** page refreshes and displays the new system.

Add a Data Protection Advisor system

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

Procedure

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

   The **Add System** dialog box appears.
3. In the **Type** list box, select **Data Protection Advisor**.
4. Specify the following connection information:
   - Name—You can specify any name that helps identify the system.
   - Hostname—Specify the Fully Qualified Domain Name (FQDN) of the Data Protection Advisor system.
   - Username—The username that is used to log in to the Data Protection Advisor user interface.
   - Password—The password that is used to log in to the Data Protection Advisor user interface.

5. Click **SAVE**.

   The **Systems** page refreshes and displays the new system. Also, successfully adding a Data Protection Advisor system enables the **Reports** link in the **Left** menu. The **Reports** link can be used to launch Data Protection Advisor in a new browser tab.

Add a Data Protection Search system

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

Procedure

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

   The **Add System** dialog box appears.
3. In the **Type** list box, select **Data Protection Search**.
4. Specify the following connection information:
   - **Name**—You can specify any name that helps identify the system.
   - **Hostname**—Specify the fully qualified domain name (FQDN) of the Data Protection Search system.
   - **Username**—The username that is used to log in to the Data Protection Search user interface.
   - **Password**—The password that is used to log in to the Data Protection Search user interface.
5. (Optional) To specify optional fields, click **Show optional fields**, and then specify the following information, as required:
   - **Admin Rest API Port**—The default value is *448*. To specify the default value, leave this field blank.
   - **Search UI Port**—The default value is *443*. To specify the default value, leave this field blank.
6. Click **SAVE**.

   The **Systems** page refreshes and displays the new system. Also, successfully adding a Data Protection Search system enables the **Search and Recovery** link in the **Left** menu. The **Search and Recovery** link can be used to launch Data Protection Search in a new browser tab.