Dell EMC Data Protection Central

Version 18.2

Security Configuration Guide

302-005-213

REV 01

Published October 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
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.

Note

This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website https://www.dell.com/support.

Purpose

This document includes information about security features and capabilities of Data Protection Central.

Audience

This document is intended for individuals who are responsible for managing security for Data Protection Central.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
01	October 22, 2018	Beta release of the *Data Protection Central 18.2 Security Configuration 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
- Search
- Data Protection Advisor
- 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://www.dell.com/support
- https://community.emc.com

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 get 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://community.emc.com. 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. You can send feedback to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Security Quick Reference

Topics include:

Deployment models

You can deploy Data Protection Central as an OVA in VMware environments or with a .jar file on a Linux operating system in a physical or virtual server that is not hosted by VMware.

Open Virtualization Appliance deployment

If you have VMware vSphere virtual machine environment, it is recommended that you deploy Data Protection Central as an Open Virtualization Appliance (OVA).

The OVA deployment model includes a pre-configured bundle with the Data Protection Central software and the Linux operating system that the Data Protection Central software runs on.

The OVA environment also includes a pre-configured firewall that is tuned to the Data Protection Central communication needs with the monitored systems.

The OVA is deployed with an OVF template file. Refer to the VMware documentation for specific information regarding how to deploy an OVA or OVF template.

The *Data Protection Central Getting Started Guide* provides information on deploying Data Protection Central as an OVA.

Physical or virtual server deployment

Data Protection Central is also available as a self-extracting JAR file with a set of Linux RPM files.

This alternative deployment model is useful if you do not have access to a VMware vSphere virtual machine environment. You can deploy Data Protection Central with this method on a Linux server running a compatible version of SUSE Linux Enterprise Server.

The *Data Protection Central Getting Started Guide* provides information on deploying Data Protection Central on a physical or virtual machine that is not hosted by VMware.

Security profiles

Data Protection Central has a default security profile for secure http access. However, you can replace the security certificate.

CHAPTER 2

Product and Subsystem Security

Topics include:

Security controls map

Data Protection Central runs on virtual servers, supporting NetWorker and Avamar servers and Data Domain backup targets.

Each Avamar system uses a Data Protection Central adapter to send alerts and events to RabbitMQ, which is the message queue system.

For NetWorker, Data Protection Central connects to the RabbitMQ on the NetWorker server to receive job activity events information.

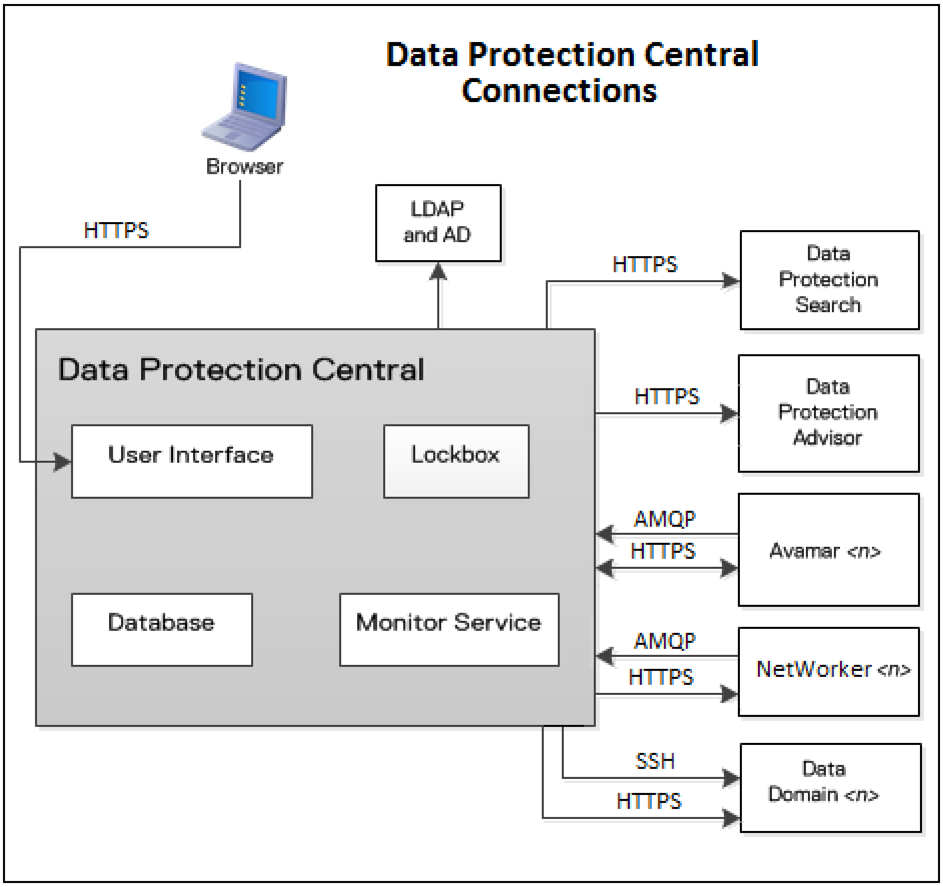
The Data Protection Central monitoring service saves the alert and event data from RabbitMQ to the MongoDB database.

The Data Protection Central UI provides a centralized location for monitoring of alerts and events as well as providing management capabilities.

All system credentials are stored within the Data Protection Central secure storage.

The following figure displays the Data Protection Central security controls map.

Figure 1 Data Protection Central security controls map



Authentication

Learn about authentication in Data Protection Central.

Login security settings

Data Protection Central includes login security settings.

Access control

Access control settings provide protection of resources against unauthorized access.

Default user accounts

Data Protection Central includes three default user accounts.

Local user account

Data Protection Central provides a single default local administrative user account.

The username of this internal account is administrator@dpc.local.

The local administrator has access to all operations in the Data Protection Central web user interface and access to all external systems that can be launched from Data Protection Central.

The first time you log into Data Protection Central, you are prompted to change the password.

Operating system admin user account

The Linux system administrator can log into Data Protection Central using a secure shell (ssh) for system administration and maintenance.

This default account is only bundled with OVA deployments.

Operating system root account

After logging into Data Protection Central with ssh as the system administrator, switch to the root user to have administrative access to files and directories on the Data Protection Central operating system.

This default account is only bundled with OVA deployments.

External user accounts

When an LDAP or Active Directory (AD) server is connected to Data Protection Central, you can grant additional accounts the Data Protection Central administrator role by adding them to the Data Protection Central administrative group provided in the ldap.properties file.

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

Failed login behavior

Data Protection Central includes security settings for when there are multiple unsuccessful authentication occurrences.

Local user account lockout

After five consecutive failed attempts to login to the local user account, Data Protection Central temporarily locks out the user for a period of five minutes.

Any attempts to login during the lockout period causes the lockout timer to reset back to five minutes.

To end the temporary lockout, restart the ELG service.

To restart the ELG service, run the following commands:

1.
   ```
   service msm-elg stop
   ```

2.
   ```
   service msm-elg start
   ```

Operating system user account lockout

If you make three consecutive failed SSH login attempts for the operating system user account, that account is temporarily locked out of the Data Protection Central Linux operating system for a period of five minutes.

You are unable to log in to the Data Protection Central Linux operating system with this account during the lock-out period, even with the correct password. However, you can log in with a different user account.

Automatic session timeout

Each account has an automatic timeout setting

SSH and console session timeout

After 900 seconds of inactivity, connections to Data Protection Central made through SSH and the console, for OVA deployments, are automatically terminated.

This timeout does not apply to login sessions to the Data Protection Central web user interface, which has a different timeout interval and mechanism.

Idle browser session timeout

By default, after 20 minutes of inactivity, the Data Protection Central session times out and you are automatically logged out.

Modify the idle browser session timeout setting
Procedure

1. Open the application.properties file located in `/usr/local/dpc/lib/elg/` for editing.
2. Add the following entry to the application.properties file:

   ```
   server.session.timeout=X
   ```

   Where *X* is the idle timeout value in seconds.

   The minimum idle timeout value is 120 (2 minutes) and the maximum is 1800 (30 minutes).

3. Save and close the application.properties file.
4. Restart the msm-elg service using the following command:

   ```
   service msm-elg restart
   ```

Authentication types and setup considerations

Learn about Single-Sign ON (SSO) authentication and setup considerations in Data Protection Central.

Internal account SSO authentication

Data Protection Central uses Single-Sign On (SSO) authentication for the local user account.

External LDAP or AD account SSO authentication

Data Protection Central supports lightweight directory access protocol (LDAP) and Active Directory (AD).

Data Protection Central can authenticate users against directory servers, such as Windows Active Directory, using LDAP or LDAPS. Authentication against an LDAP server simplifies management because you do not need a separate set of credentials for Data Protection Central administration.

After you configure LDAP authentication, you can log into the Data Protection Central web console with any LDAP or AD account. Data Protection Central performs SSO authentication for external users and internally validates credentials and user authority with the LDAP or AD server.

The *Data Protection Central Getting Started Guide* provides instructions on configuring LDAP or AD during or after deploying Data Protection Central.

Configuring LDAP

Learn about LDAP requirements and configuration procedures.

Data Protection Central supports OpenLDAP and Active Directory (AD) authentication.

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

The Troubleshooting chapter in the *Data Protection Central Administration Guide* provides detailed troubleshooting information on diagnosing and resolving common LDAP configuration issues.

Note

LDAP without TLS protocol communicates in clear text without encryption. Secure LDAP (LDAPS) does not support communication in clear text. When you configure LDAP without TLS, to improve security, it is recommended that you use a segmented network containing only the LDAP server and the Data Protection Central server.

Configure LDAP or AD user access

Before you configure Lightweight Directory Access Protocol (LDAP) or Windows Active Directory (AD), configure the users who will access Data Protection Central.

Perform this procedure on the server that hosts Lightweight Directory Access Protocol (LDAP) or Windows Active Directory (AD).

Procedure

1. Create an administrative user group that will contain the users who can access Data Protection Central.

   The following list describes the default containers, according to the configuration type:

   - For Lightweight Directory Access Protocol (LDAP), the default user group is the OU=People folder.
   - For Windows Active Directory (AD), the default user group is the OU=Users folder.

2. For AD accounts only, set the user group scope setting to **Global**.

   Note

   Users who are part of this group are granted administrative privileges to Data Protection Central and the system management applications for any systems added to Data Protection Central, including Single-Sign On access.

3. Add any users that require access to Data Protection Central to the user group.

Prepare to add LDAP or AD to the Data Protection Central system

Before you add LDAP or AD, you must access the Data Protection Central system and stop the services.

Procedure

1. Login to the Data Protection Central system using SSH.
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
   ```

After you finish

Create or edit the `ldap.properties` file in the `/var/lib/dpc/elg/` folder to specify the values that are specific to the environment.

Create an LDAP properties file

Learn how to create an LDAP properties file.

The LDAP properties file must match the exact file name of `ldap.properties` and be located in the `/var/lib/dpc/elg/` directory.

Note

To quickly create an LDAP properties file, it is recommended that you copy the LDAP properties template file located at `/usr/local/dpc/lib/elg/conf/ldap.properties.example` into `/var/lib/dpc/elg/ldap.properties`.

The following table describes the attributes that you can specify in the LDAP properties file.

Table 3 LDAP properties file attributes

Attribute	Description	Examples

elg.ldap.type	Required.
	Specifies the type of LDAP environment. Specify either LDAP or AD.
		`elg.ldap.type=LDAP`
		`elg.ldap.type=AD`

elg.ldap.server.urls	Required.
	Specifies the URL of the server where LDAP is hosted. Type the URL in the following format:
	`{ldap
		ldaps}://<hostname>:<port>`	`elg.ldap.server.urls=ldap://ldap.dpc.local:389/`
			`elg.ldap.server.urls=ldaps://ldap.dpc.local:636/`

elg.ldap.base.dn	Required. Specifies the domain base distinguished name of the LDAP server.	`elg.ldap.base.dn=dc=dpc,dc=local`

elg.ldap.admin.dn	Required.
	Specifies the administrative username in the base distinguished name format.
		For example, consider the following entry for LDAP:
		`uid=admin,ou=people,dc=dpc,dc=local`
		For example, consider the following entry for Active Directory:
		`cn=Administrator,dc=abc,dc=xyz,dc=com`

elg.ldap.admin.password	Required. Specifies the password for the administrative user. After you save the file and restart the Data Protection Central services, the password is stored in the lockbox and removed from the ldap.properties file.	`elg.ldap.admin.password=changeme1`
elg.ldap.group.search.name	Required. Specifies the user group name that contains the users who require access to Data Protection Central. If you do not specify this attribute, the default value of `dp_admin` is used.	For example, if the distinguished name of the group is `cn=backupadmins, ou=groups, dc=dpc, dc=local`, specify the group name with the following entry: `elg.ldap.group.search.name=backupadmins`
elg.ldap.group.search.base	Optional.	For example, consider the following scenario.

Table 3 LDAP properties file attributes (continued)

Attribute	Description	Examples
	Specifies the distinguished name of the administrator user group on the LDAP server. **NOTICE** Do not specify this attribute unless there are duplicate entries of the group name on the LDAP or AD server. If you specify this attribute when there is a single instance of a group, user authentication may fail. If the group name specified with `elg.ldap.group.search.name` is duplicated on the LDAP or AD server, then you must specify this attribute for Data Protection Central to identify the correct instance of the group name. When there is only one instance of the group name, Data Protection Central automatically locates the group on the LDAP or AD server.	The LDAP server has two BackupAdmins groups in different locations. The groups have the following distinguished names: • `cn=backupadmins,ou=groups,dc=dpc,dc=local` • `cn=backupadmins,ou=groupcontainer,dc=dpc,dc=local` You want to use the group located in the `groupcontainer` folder. Data Protection Central. In this scenario, specify: `elg.ldap.group.search.base=ou=groupcontainer`

Examples of the LDAP properties file

Consider the following examples of the LDAP property file.

Example 1 Example LDAP properties file

```
elg.ldap.type=LDAP
elg.ldap.server.urls=ldaps://dpc.local.domain.com:636/
elg.ldap.base.dn=dc=local,dc=domain,dc=com
elg.ldap.admin.dn=uid=Admin,ou=People,dc=local,dc=domain,dc=com
elg.ldap.admin.password=PgK17y5*
elg.ldap.group.search.name=dp_admin
```

Example 2 Example LDAP properties file for active directory

```
elg.ldap.type=AD
elg.ldap.server.urls=ldap://dpc.corp.domain.com:389/
elg.ldap.base.dn=dc=corp,dc=domain,dc=com
elg.ldap.admin.dn=cn=Administrator,cn=Users,dc=sddc,dc=local
elg.ldap.admin.password=4tHgI8fL
elg.ldap.group.search.name=dp_admin
```

Finish adding LDAP or AD and log in to the Data Protection Central user interface

After you add the ldap.properties file, perform the following steps to complete the LDAP configuration.

Procedure

1. To assign administrator ownership on the ldap.properties file, type the following command:

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

2. To set the protection of the ldap.properties file, type the following command:

   ```
   chmod 644 /var/lib/dpc/elg/ldap.properties
   ```

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

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

4. 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
   ```

5. Launch a web browser and navigate to the Data Protection Central address using the fully qualified domain name.

   For example:

   ```
    https://dpc.local.com
   ```

6. Log in to the Data Protection Central user interface with the credentials for the LDAP user account.

Add a secure LDAP (LDAPS) certificate

Learn how to add a secure LDAP (LDAPS) certificate.

Secure LDAP (LDAPs) uses TLS, and therefore requires certificate-based authentication.

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.

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

Procedure

1. To retrieve the certificate details from the LDAP server, type the following command:

   ```
   /usr/local/dpc/bin/dpc trust-ldaps <LDAPS server FQDN or IP>
   ```

   The certificate details are listed. The operation prompts you to continue with adding the certificate to the keystore.

2. To add the LDAP server's certificate to the Data Protection Central Java keystore, type **y** in response to the prompt.
3. After the certificate is added to the keystore, restart the Data Protection Central services using the following commands:

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

Verify the LDAP or AD connection status

You can verify the LDAP or AD connection status by looking for messages in the log file or on the **Audit** page.

Check the LDAP status in the log file
Check the `/var/log/dpc/elg/elg.log` log file for messages about the LDAP connection status.

Messages that appear during LDAP connection failure
If the following message appears, the LDAP client did not make a successful connection to the LDAP server:

```
2018-04-03 11:00:26,929 INFO localhost-startStop-1
c.e.c.c.SecurityConfig LDAP or AD Directory Service providers are not
available
```

There are multiple issues that can prevent the LDAP client from connecting to the LDAP server. Look for error messages in the log file that provide more information.

The following table describes various error messages that appear during LDAP connection failures and their causes.

Table 4 LDAP communication messages

Message	Cause
`INFO localhost-startStop-1 c.e.c.c.SecurityConfig LDAP or AD Directory Service providers are not available`	No LDAP or AD setting are provided or they are provided with incorrect information.
`.ADLdapAuthenticationProvider Ignoring AD authentication. Verification of ldap settings failed. Failed to connect`	Invalid AD configuration information.

Table 4 LDAP communication messages (continued)

Message	Cause
`.LdapAuthenticationProvider Ignoring LDAP authentication. Verification of ldap settings failed. Failed to connect`	Invalid LDAP configuration information.
`PKIX path building failed: java.security.cert.CertPathBuilderException: Could not build a validated path`	Validation of the LDAP server certificate could not be completed. One possible solution for this issue is to add the LDAP server certificate to the Data Protection Central Java keystore.

Messages that appear during LDAP connection success

Messages similar to the following appear when the LDAP client successfully connects to the LDAP server:

```
c.e.c.s.a.l.LDAPSecureStorage LDAP admin credentials are secured
c.e.c.s.a.l.ExternalAuthenticationProvider Type: LDAP
c.e.c.s.a.l.ExternalAuthenticationProvider Base DN: dc=mydomain,dc=com
c.e.c.s.a.l.ExternalAuthenticationProvider Admin user DN:
cn=Administrator,dc=my-domain,dc=com
c.e.c.s.a.l.ExternalAuthenticationProvider User Base: ou=people
c.e.c.s.a.l.ExternalAuthenticationProvider User Search DN: (|(uid={0})
(cn={0}))
c.e.c.s.a.l.ExternalAuthenticationProvider User Pattern DN: []
c.e.c.s.a.l.ExternalAuthenticationProvider Group Name: dp_admin
c.e.c.s.a.l.ExternalAuthenticationProvider Group Search Base: ou=group
c.e.c.s.a.l.ExternalAuthenticationProvider Group Search Filter:
(&(member={0})(cn=dp_admin))
o.s.s.l.DefaultSpringSecurityContextSource URL 'ldap://
12.3.104.150:546/dc=my-domain,dc=com', root DN is 'dc=mydomain,dc=com'
12.3.104.150:546/dc=my-domain,dc=com', root DN is 'dc=mydomain,dc=com'
```

Check the LDAP status on the Audit page

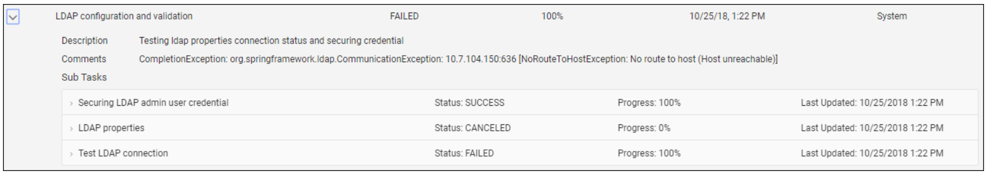
You can verify the success of the LDAP configuration on the Data Protection Central **Audit** page.

If LDAP configuration is successful, you can log into the Data Protection Central web user interface with an LDAP account. If configuration fails, login to Data Protection Central using the administrator@dpc.local account and browse to the **Audit** for details.

The **Audit** page shows the overall status of the operation and the status of each individual sub-task. You can use this information to locate the point in the operation that caused the LDAP configuration to fail.

The following figure shows an example of an LDAP configuration activity on the **Audit** page.

Figure 2 LDAP configuration activities on the Audit page



LDAP configuration and validation	FAILED	100%	10/25/18, 1:22 PM	System

Description Testing ldap properties connection status and securing credential

Comments CompletionException: org.springframework.ldap.CommunicationException: 10.7.104.150:636 [NoRouteToHostException: No route to host (Host unreachable)]

Sub Tasks

Securing LDAP admin user credential	Status: SUCCESS	Progress: 100%	Last Updated: 10/25/2018 1:22 PM
LDAP properties	Status: CANCELED	Progress: 0%	Last Updated: 10/25/2018 1:22 PM
Test LDAP connection	Status: FAILED	Progress: 100%	Last Updated: 10/25/2018 1:22 PM

User and credential management

Learn how to manage Data Protection Central users and credentials.

Pre-loaded accounts

The following table describes the pre-loaded Data Protection Central accounts.

Table 5 Pre-loaded 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. This account is for OVA deployments only. **Note** Only the Linux OS admin can log in using a secure shell (ssh).
Linux operating system root	The root operation system account. This account is for OVA deployments only.

Default credentials

The following table describes the default credentials for the pre-loaded Data Protection Central accounts.

Table 6 Default credentials

Account	User	Password
Data Protection Central administrator	administrator@dpc.local	secret
Linux operating system admin	admin	The admin password is set when Data Protection Central is deployed.
Linux operating system root	root	The OS root password is set when Data Protection Central is deployed.

Managing credentials

Learn how to manage user login credentials.

The default provider root password is stored in a configuration file. To reset the local and default account, edit the configuration file, and then restart the server.

The password that is entered during the OVA deployment is stored in a configuration file. On the first start up, the password is stored in an encrypted format in the Data Protection Central lockbox, and then the configuration file is deleted.

Reset the administrator password

If required, you can reset the **`administrator@dpc.local`** password to the default password. The default password is **`secret`**.

Procedure

1. Stop the ELG service by running the following command:

```
service msm-elg stop
```

2. To change the directory, type the following command:

```
cd /usr/local/dpc/lib/elg
```

3. To delete the account, type the following command:

```
bin/elgcli --deleteUserAccount
```

4. Start the ELG service by running the following command:

```
service msm-elg start
```

Results

The password is changed to the default password (**`secret`**). When you next log in to the Data Protection Central web user interface, Data Protection Central prompts you to change the password.

Modifying the Linux operating system user credentials

For OVA deployments of Data Protection Central, the Linux admin and root user passwords are configured when you deploy the OVA template. You can change these passwords using the standard Linux password change command.

From either an SSH session connected to the Data Protection Central system or using the Data Protection Central system console, run the following command to change the operating system admin or root password:

```
passwd {admin | root}
```

The Linux documentation provides more information on using the `passwd` command.

Password complexity

The following table describes the password complexity requirements.

Table 7 Password complexity requirements

Account	Password complexity requirements
Data Protection Central administrator	• 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.
Linux operating system admin	The password length must be between 8 and 256 characters.
Linux operating system root	The password length must be between 8 and 256 characters.

Authentication to external data protection systems

Data Protection Central includes features to monitor and manage external data protection systems, such as Avamar. Data Protection Central requires credentials to access the external system.

Configuring remote connections

Data Protection Central establishes a remote connection to external systems that you add from the **System Management** page.

When you add a system to Data Protection Central, you must provide connection information including the hostname and credentials for that system. Data Protection Central stores this connection information and uses it to access the remote system.

Credential security

Data Protection Central stores external credentials securely.

After you add a system to Data Protection Central, the external system credentials are stored in a secure lockbox.

Single Sign-On

Data Protection Central supports Single Sign-On (SSO) authentication for certain external systems.

SSO streamlines the process of managing systems by logging you into system management applications directly when you launch them from Data Protection Central.

Systems must meet the following version requirements to enable SSO:

Table 8 System version requirements for SSO

System type	User interface	Supported versions
Avamar	Avamar Administrator	7.5.1 and later
	AUI	18.1 and later
NetWorker	NetWorker Management Console (NMC)	18.1 and later
	NetWorker Management Web UI	18.1 and later
Search	Search Web User Interface	18.1 and later
Data Protection Advisor	DPA Web Console	18.2 and later

If systems do not meet these version requirements, SSO is not available. You can monitor the SSO health status on the **Health** page.

Note

The SSO health status reflects the Data Protection Central SSO connection status rather than the status of the remote system. Therefore, the SSO health may be reported as healthy when the monitored system is out of sync.

Authorization

Data Protection Central supports a single administrative role.

Both the default administrator@dpc.local account and any LDAP users added to the administrative group in the ldap.properties file are granted the administrator role in Data Protection Central.

When the Data Protection Central administrator logs in, they have access to all Data Protection Central features and functions.

The administrator also has administrative access to external system management applications, such as Avamar Administrator, for all systems added to Data Protection Central.

Network security

Learn about network security in Data Protection Central.

Data Protection Central uses a firewall to enhance security by restricting inbound and outbound network traffic to the TCP and UDP ports. The tables in this section list the inbound and outbound ports that Data Protection Central uses.

Network exposure

Data Protection Central uses inbound and outbound ports when communicating with remote systems.

Outbound ports

Outbound ports can be used by Data Protection Central when connecting to a remote system.

The ports that are listed in the following table are the Data Protection Central outbound ports.

Table 9 Outbound ports

Port number	Layer 4 Protocol	Service
7	TCP, UDP	ECHO
22	TCP	SSH
25	TCP	SMTP
53	UDP, TCP	DNS
67,68	TCP	DHCP
80	TCP	HTTP
88	TCP, UDP	Kerberos
111	TCP, UDP	ONC RPC
123	TCP, UDP	NTP
161-163	TCP, UDP	SNMP
389	TCP, UDP	LDAP
443	TCP	HTTPS
448	TCP	Data Protection Search Admin REST API
464	TCP, UDP	Kerberos
514	TCP, UDP	rsh
587	TCP	SMTP
636	TCP, UDP	LDAPS
902	TCP	VMware ESXi
2049	TCP, UDP	NFS
2052	TCP, UDP	mountd, clearvisn
3009	TCP	Data Domain REST API
5672	TCP	RabbitMQ over amqp
8443	TCP	MCSDK 8443 is an alternative for 443

Table 9 Outbound ports (continued)

Port number	Layer 4 Protocol	Service
9000	TCP	NetWorker Management Console
9002	TCP	Data Protection Advisor REST API
9090	TCP	NetWorker Authentication Service and REST API
9443	TCP	Avamar Management Console web service

Inbound ports

Learn about the inbound ports that are available to be used by a remote system when connecting to Data Protection Central.

The ports that are listed in the following table are the Data Protection Central inbound ports.

Table 10 Inbound ports

Port number	Layer 4 Protocol	Service
22	TCP	SSH
80	TCP	HTTP
443	TCP	HTTPS
5671	TCP	RabbitMQ over amqp

Modify the Data Protection Central firewall to use a non-standard port

If you add a system to Data Protection Central that uses a non-standard port, you must modify the Data Protection Central firewall to allow communication with that port.

Procedure

1. To access the Data Protection Central system, run the following command:

   ```
   ssh -l <username> <dpc_fqdn>
   ```

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

   ```
   su -
   ```

3. To edit the Data Protection Central firewall rules file, open the following file with a Linux file editor:

```
/usr/local/dpc/lib/firewall/scripts/SuSEfirewall2-msm-custom
```

4. In the `fw_custom_before_denyall()` method, under production rules, modify the `--dport` entry to add the port you want Data Protection Central to access.

   For example:

```
# production rules
       exec_rule -A $chain -j ACCEPT -m multiport -p tcp --
dport 22,88,389,443,448,636,2049,2052,3009,9000,9002,9443
```

   It is recommended that you replace the default service port with the alternate port. The following table describes the ports that system services use by default:

Service	Port
Avamar Management Console	9443
NetWorker Authentication Service and REST API	9090
NetWorker Management Console	9000
Data Domain REST API	3009
Search Rest API	448
Search UI	443
Data Protection Advisor	9002

5. Save and close the file.
6. To restart the firewall and apply the changes, run the following commands:

```
service SuSEfirewall2 stop
```

```
service SuSEfirewall2_init stop
```

```
service SuSEfirewall2 start
```

```
service SuSEfirewall2_init start
```

Data security

The data that are held, managed, used, or operated on by Data Protection Central is stored and secured.

Data Protection Central does not encrypt event, or application data within MongoDB.

Data Protection Central prevents unauthorized access to the Data Protection Central system.

Lockbox

Data Protection Central uses a secure storage lockbox to encrypt and store both internal system credentials and credentials for external systems that Data Protection Central monitors and manages.

The lockbox is created when you deploy Data Protection Central. During deployment, you must specify a lockbox password. The password is encrypted and stored in the lockbox along with Stable System Values (SSVs), which uniquely identify the Data Protection Central host. The lockbox uses the SSVs to generate an encryption key to encrypt the system credentials.

Stable System Values (SSVs)

Stable System values (SSVs) validate access to the lockbox.

When data is written to or retrieved from the lockbox, the SSVs in the lockbox are compared against the SSVs generated from the host. If the SSVs match, the operation is permitted. If the SSVs do not match, the operation fails.

Cryptography

Learn about cryptography in Data Protection Central.

Data Protection Central uses cryptography for the following components:

- Access control
- Authentication
- Digital signatures

Certificate management

Data Protection Central uses certificates 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.

You can use the following types of certificates for Data Protection Central authentication:

- A self-signed certificate.
- A certificate that is signed by a trusted certificate authority (CA) vendor.

Note

Consider company policies when creating certificates.

Generate a self-signed certificate

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

Auditing and logging

Learn about auditing and logging in Data Protection Central.

The following list includes information about the Data Protection Central directory structure and log information:

- The `/var/log/dpc/install` directory hosts all logs generated from deploying or upgrading Data Protection Central.
- The `/var/lib/dpc` directory hosts all Data Protection Central generated data which consists of MongoDB and RabbitMQ.
- The `/var/log/dpc` directory hosts all Data Protection Central related logs including NGINX, MongoDB, and RabbitMQ.
- All Data Protection Central related logs are under:
  `/var/log/dpc/[module name]`

  `[module name].out` files contain console logging from starting and running the module process.

  `[module name].log` files contain logging from the module.
- All Elemental Gateway (ELG) logs are under:
  `/var/log/dpc/elg/`
- The Data Protection Central user interface (msm-ui-main service) log is under:
  `/var/log/dpc/msm-ui-main`

This log file is small and contains information from starting the Node.js server.

- The Data Protection Central Monitoring (dpc-monitor service) logs are under: `/var/log/dpc/monitor`

  This directory contains the rolling log files from the monitoring process.

Serviceability

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

There is no special login to Data Protection Central for service personnel.

Ensure that you install security patches and other updates when they are available, including the Data Protection Central OS update.

Security patches

A security update for Data Protection Central may be periodically provided.

The periodic updates are cumulative.

Each periodic update is announced through a security advisory. The security advisory provides details about the contents of the periodic update and installation instructions. To view these advisories or to register for email notifications, go to the Support website at:

https://support.emc.com

Data Protection Central OS update

Periodically, security patches and fixes are released for the Data Protection Central OS.

These fixes must be installed on OVA deployments of Data Protection Central. When available, it is highly recommended that you install these security patches and fixes on the Data Protection Central server.

The *Data Protection Central OS Update Release Notes* provides information about the security patches and fixes included in the Data Protection Central OS update. The Support KB article https://support.emc.com/kb/522157 provides instructions for installing the OS update.

Product code integrity

When the Data Protection Central software is uploaded to the online support website, a SHA-256 checksum is also provided. It is recommended that you use the checksum and to verify the authenticity of the Data Protection Central deployment file.

The Data Protection Central deployment files, both OVA and JAR objects, are digitally signed. You can verify the authenticity of the OVA file when you deploy the OVF template. When you deploy the JAR file, run the `jarsigner --verify -verbose` command to verify the authenticity.

CHAPTER 3

Miscellaneous Configuration and Management

Topics include:

Licensing

Data Protection Central does not require any special or additional product licensing.

Protect authenticity and integrity

To ensure product integrity, the Data Protection Central installation components are signed.

Enable external web access with SSL using a trusted certificate authority (CA).

Perform backups and restores of Data Protection Central

To protect Data Protection Central from a disaster scenario, It is recommended that you perform backups of Data Protection Central. If required, you can restore Data Protection Central from these backups.

Virtual machine based backups of Data Protection Central are recommended. Refer to the vCenter documentation for more information.

If you are not using vCenter to perform backup and restore operations, you can also perform the following steps to backup and restore Data Protection Central.

Procedure

1. Backup the `/var/lib/dpc` directory.
2. To shutdown the Data Protection Central software, type the following command:

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

3. Restore the `/var/lib/dpc` directory.
4. To start Data Protection Central, type the following command:

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

Embedded component usage

Learn about Data Protection Central embedded component usage.

To locate Data Protection Central OSS third party software, use the `/usr/local/dpc/licenses` folder. This folder contains the `oss-ship-manifest.xls` file, which specifies the license information. The End User License Agreement (EULA) is also in this folder.