Dell Data Protection Advisor 19.12

Installation and Administration Guide

Dell Inc.

March 2025
Rev. 02

Notes, cautions, and warnings

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

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

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

Contents

Figures

Tables

Preface

As part of an effort to improve its product lines, Dell Technologies periodically releases revisions of its software and hardware. Therefore, some functions that are described in this document might not be supported by all versions of the software or hardware in use. The product release notes provide the most up-to-date information about product features.

Contact your Dell Technologies technical support professional if a product does not function properly or does not function as described in this document.

ⓘ **NOTE:** This document was accurate at publication time. Go to Dell Technologies Online Support (Dell Online Support) to ensure that you are using the latest version of this document.

Language use

This document might contain language that is not consistent with Dell Technologies current guidelines. Dell Technologies plans to update the document over subsequent future releases to revise the language accordingly.

This document might contain language from third-party content that is not under Dell Technologies control and is not consistent with the current guidelines for Dell Technologies own content. When such third-party content is updated by the relevant third parties, this document is revised accordingly.

Purpose

This document provides information about how to install Data Protection Advisor and set up Data Protection Advisor to monitor a data protection environment. This document also describes administrative functions such as creating users and roles, updating system settings, creating policies, and troubleshooting data collection.

ISO 9001 certification

The management system governing the design and development of this product is ISO 9001:2015 certified.

Audience

This document is intended for system administrators. Readers of this document must be familiar with the following tasks:

- Identifying the different hardware and software components that make up the backup and replication environment.
- Following procedures to configure backup and replication operations.
- Following guidelines to locate problems and implement solutions.

Revision history

The following table presents the revision history of this document.

Table 1. Revision history

Revision	Date	Description
02	March 2025	Updated the following sections: ● Installing Data Protection Advisor ● Administering Data Protection Advisor ● Self-Signed Certificate Generation ● Adding Application servers into setup with Database encryption ● Replace a self-signed certificate with a CA signed certificate

Table 1. Revision history (continued)

Revision	Date	Description
		- Data protection advisor post installation steps - for secure communication .
01	January, 2025	First release of this document for Data Protection Advisor 19.12.

Related documentation

The Data Protection Advisor documentation set includes the following publications:

- *Dell Data Protection Advisor 19.12 Release Notes*
- *Dell Data Protection Advisor 19.12 Installation and Administration Guide*
- *Dell Data Protection Advisor 19.12 Product Guide*
- *Dell Data Protection Advisor 19.12 Security Configuration Guide*
- *Dell Data Protection Advisor 19.12 Data Collection Reference Guide*
- *Dell Data Protection Advisor 19.12 Custom Report Guide*
- *Dell Data Protection Advisor 19.12 Report Reference Guide*
- *Dell Data Protection Advisor 19.12 REST API Guide*
- *Dell Data Protection Advisor 19.12 Online Help*

Typographical conventions

The following type style conventions are used in this document:

Table 2. Style conventions

Formatting	Description
Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
Italic	Used for full titles of publications that are referenced in the 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

- Dell Customer Support
- Dell Community Network

Where to get support

The Support website Dell Customer 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 Dell Customer 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 Dell Customer 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 Dell Customer 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 Dell Customer Support.
2. On the **Support** tab, click **Service Requests**.

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

To review an open service request:

1. Go to Dell Customer 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 Dell Community Network. Interactively engage with customers, partners, and certified professionals online.

How to provide feedback

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

- Go to Dell Content Feedback Platform, and submit a ticket.

- Send feedback to DPADDocFeedback.

Preparing to install Data Protection Advisor

This chapter includes the following sections:

Topics:

Overview

All Data Protection Advisor deployments include the following installations:

- Data Protection Advisor Datastore server and a Data Protection Advisor agent on one host
- Data Protection Advisor Application server and a Data Protection Advisor agent on another host

When you install Data Protection Advisor, the installation wizard takes you step by step through placement of these components.

Installing the Application and Datastore servers on a single host is not supported. You can connect multiple Application servers to the same Datastore server, where each additional Application server is on its own host. You can install additional Data Protection Advisor Agents for system monitoring and remote data collection. Data Protection Advisor supports Datastore Replication to enable continuous, safe, and reliable replication so that Data Protection Advisor can maintain a replica or secondary Datastore of the primary Datastore for resilience against a single point of failure.

System requirements

Data Protection Advisor has the following basic minimum system requirements. The *Data Protection Advisor Software Compatibility Guide* provides a comprehensive list of system requirements.

Data Protection Advisor Server platforms

Data Protection Advisor servers support for 64-bit operating systems only. Work with your Account Representative to determine appropriate sizing for your environment.

Memory requirements

- 16 GB RAM/4 cores for the Data Protection Advisor Datastore server
- 16 GB RAM/4 cores for the Data Protection Advisor Application Server
- 16 GB RAM/4 cores for the Data Protection Advisor Agent

Hard Disk Drive requirements:

- 18 GB of locally attached disk storage for the Application server
- 20 GB of locally attached disk storage for the Datastore Server
- 10 GB of locally attached disk storage for the Agent
- 5 GB of free space is required for database upgrade in the Data Protection Advisor installation directory

NOTE: Co-located Application and Datastore systems are not supported in production systems. Although the installer provides a co-located system option, when it is selected, a dialogue stating that it is not supported in a production systems displays.

- 5 GB of free space is required in the system temp directory for Server or Datastore installation
- 5 GB of free space is required in the system temp directory for Agent installation

> **NOTE:** Data Protection Advisor installer uses system temp directory (OS temp directory) to unpack the installation package. Conventional system temp folder location might vary depending on the OS used. Most OS allows to change temp directory with system environment variables. To find out where the temp folder is located in your environment and how to change it, refer to the OS documentation.

- The Data Protection Advisor Application server and Data Protection Advisor Datastore servers must not be used to run other applications. The Data Protection Advisor Application server host and Data Protection Advisor Datastore server host resources must be dedicated to Data Protection Advisor.
- If you are running Data Protection Advisor in a virtualized environment the allocated CPU and memory must be reserved for the Data Protection Advisor servers
- The Data Protection Advisor installer has a soft threshold of 7892 MB and a hard threshold of 5844 MB. The soft threshold allows the installation to continue, but the hard threshold does not.
- Automatic sizing and tuning of internal Data Protection Advisor resource usage takes place during installation. If resources (CPU, Memory) are taken away from the installation by other applications performance of Data Protection Advisor could be adversely affected.
- Storage size requirement for Datastore is highly dependent on the expected data collection and retention rates.
- Data Protection Advisor installations require Transport Layer Security (TLS) v 1.2 or later.
- Operating systems:

  The *Data Protection Advisor Software Compatibility Guide* provides information on the supported operating systems.

Datastore storage

For performance reasons, the installation of the Data Protection Advisor Datastore server on NAS-based file systems, such as CIFS or NFS shares is not recommended because these file systems might not have the bandwidth to manage the required I/O.

Although the standard datastore file system layout is adequate for most deployments, you can distribute different file systems across different file systems to optimize performance during installation under Advanced installation options.

Permissions

Ensure that you have the following permissions before you install the software to avoid installation failure:

- Windows:
  - Administrator privileges (domain or local with full access)
  - If User Account Control (UAC) is enabled, use Run As Administrator
  - Due to a known PostgreSQL issue, you must set additional permissions before product upgrade from previous releases to 19.1: "Authenticated Users" entity should have read and execute permissions set for Data Protection Advisor installation folder. After upgrade is completed you can remove this permission.
- UNIX / Linux:
  - Root user
  - If using security software to manage access to the root account, ensure the permissions allow the creation of new users after you become root. This must include the ability to create default home directories for the account to be created.

NTP time synchronization

It is a best practice to have Network Time Protocol (NTP) available to synchronize the Data Protection Advisor Server and the Data Protection Advisor Agent hosts. This ensures accurate and consistent data collection.

The Data Protection Advisor User Authentication process requires that the times on the system clock on the client machine and on the server be synchronized within one minute of one another.

Installation considerations

The Data Protection Advisor installation wizard provides advanced options to configure Datastore Replication with primary and secondary Datastores. If you use one or both of these options, ensure that you:

- Plan the final deployment topology before you start the installation.
- Have all hosts and IP addresses predetermined and available.

If you are planning an advanced installation, contact your Account Representative for help with advanced architecture solution design.

Configuring virtual infrastructure memory and CPU

If you plan to deploy Data Protection Advisor in a virtualized infrastructure, perform the following steps:

- Ensure that the memory allocated is reserved exclusively for each VM.
- Place theData Protection Advisor Application and Datastore VMs in a resource pool where the resource allocation shares are set to High. Alternatively, select High Share Allocation for each individual VM.
- Select Thick Provision Eager Zeroed for Datastore disks. Thick Provision Eager Zeroed disk allocation causes all space to be allocated upfront, and the full disk file is zeroed before the system is made available for usage.

OS resource optimization

General tuning

During installation, the installer tunes the Data Protection Advisor Datastore Service for the host environment on which it is being deployed. This tuning assumes that the host is dedicated to Data Protection Advisor and considers the resources such as Disk Space, Total Memory, and CPU cores. If during the lifetime of the Data Protection Advisor Datastore Service any of these physical resources are increased or decreased, run the `dpa datastore tune` command on the Datastore host. dpa datastore tune provides more information.

Hardware issues with tuning

For deployments where optimal performance is a concern, the type and quality of the hardware you use for your Datastore host server drastically impacts the performance of the Datastore Service.

Usually, the performance is better when you have more RAM and disk spindles in your system. This is because with the extra RAM you will access your disks less. And the extra spindles help spread the reads and writes over multiple disks to increase throughput and to reduce drive head congestion.

For production purposes the Data Protection Advisor Application Service and the Data Protection Advisor Datastore Service should be placed onto different hardware. Not only does this provide more hardware dedicated to the Datastore Service, but the operating system's disk cache will contain more Datastore data and not any other application or system data.

Communications settings in Data Protection Advisor

To ensure communication between the Data Protection Advisor Server and Data Protection Advisor Agents, configure the firewalls in the network to allow communication on these ports, as shown in the following figure. Extra firewall configuration is required for other ports depending on what you plan to monitor. For example, if you monitor Avamar, open port 5555 between the Avamar server and the Data Protection Advisor Agent. "Environment discovery in Data Protection Advisor" provides more information.

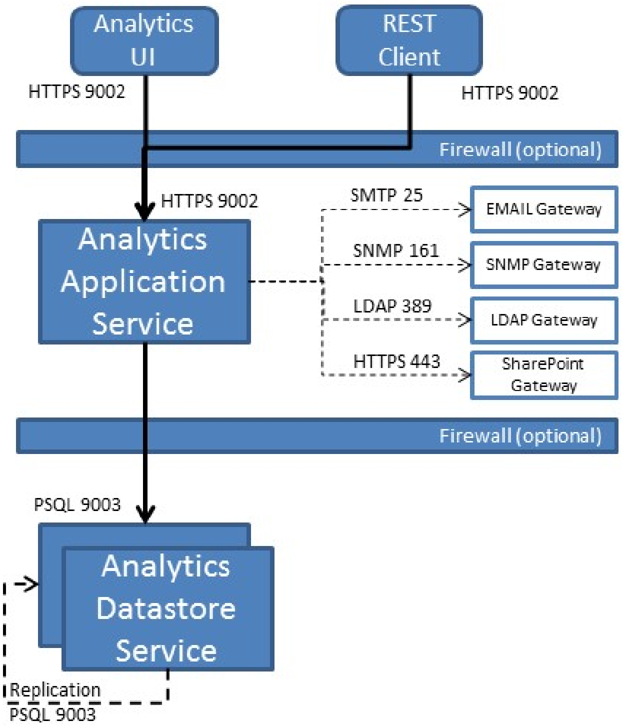


Figure 1. Data Protection Advisor ports and protocols

Data Protection Advisor port settings

The following tables provide the ports needed by Data Protection Advisor to function correctly. Additional ports can be required for the Data Protection Advisor Agents depending on the systems being monitored. The *Data Protection Advisor Installation and Administration Guide* provides information on installation requirements.

Table 3. Data Protection Advisor Application ports settings

Port	Description	Traffic direction
25	TCP port used for the SMTP service	Outbound connection to SMTP server.
80	TCP port used for the SharePoint service	Outbound connection to SharePoint server.
22	TCP port used for SSH	Bidirectional connection to SSH server.
161	UDP port used for SNMP service	Bidirectional connection to SNMP devices.
389/636 (over SSL)	TCP port used for LDAP integration	Outbound connection to LDAP server.
3741	TCP port used for Data Protection Advisor Agents communications.	Outbound connection to Data Protection Advisor agents

Table 3. Data Protection Advisor Application ports settings (continued)

Port	Description	Traffic direction
4447	TCP port used for intra-service communication	Inbound connection
4712	TCP port used for intra-service communication	Localhost connection
4713	TCP port used for intra-service communication	Localhost connection
5445	TCP port used for intra-service communication	Localhost connection
5455	TCP port used for intra-service communication	Localhost connection
8090	TCP port used for intra-service communication	Localhost connection
9002	TCP port used for the HTTPS service.	Inbound connection over SSL from UI, CLI and REST API clients.
9003	TCP port used for Data Protection Advisor Datastore communications.	Outbound connection to Data Protection Advisor Datastore.
9005	TCP port used for Jboss Management	Localhost connection
9999	TCP port used for Jboss Management	Localhost connection
31000 - 32000	TCP port used for local communication	Localhost connection

Table 4. Data Protection Advisor Datastore port settings

Port	Description	Traffic direction
3741	TCP port used for Data Protection Advisor Agents communications.	Inbound connection from Data Protection Advisor Application server.
9002	TCP port used for the HTTPS service.	Outbound connection over SSL to Data Protection Advisor Application server.
9003	TCP port used for Data Protection Advisor Datastore communications.	Inbound connection from Data Protection Advisor Application server.

Table 5. Data Protection Advisor Agent port settings

Port	Description	Traffic direction
3741	TCP port used for Data Protection Advisor Agents communications.	Inbound connection from Data Protection Advisor Application server.
9002	TCP port used for the HTTPS service.	Outbound connection over SSL to Data Protection Advisor Application server.

Installation and configuration overview

The Data Protection Advisor installation workflow provides a high-level workflow of tasks for installing Data Protection Advisor with various configurations.

Figure 2. Data Protection Advisor installation workflow

The Installation and configuration overview lists the tasks that you need to perform for installing Data Protection Advisor and configuring data monitoring.

Table 6. Installation and configuration overview

Action	Comments
Set up host system	
Provide at least two hosts for Data Protection Advisor server installation: One for the initial Data Protection Advisor Application server, and one for the Datastore. A separate host is required for the Datastore and Application server so that the operating system on each server can successfully and properly manage the I/O performance needs of one service and the RAM and caching requirements of the other service, without the two services competing with each other for resources.	Data Protection Advisor must not be installed on servers already running other applications. For installation in a production environment, you need one host for the Application Service and a separate host for the Datastore Service. recommends that you use a dedicated server with at least 2 GB of temporary space. The Compatibility Guide provides more information.
Provide a host for Data Protection Advisor Agent installation (optional).	If the Data Protection Advisor server is running on Windows and one or more discovered hosts are also Windows, you need not install an Agent on the discovered host. However, it is recommend that you use the Agent that is installed on the Data Protection Advisor Server hosts for Data Protection Advisor Server monitoring only. If the Data Protection Advisor server resides on a Linux host and you are performing client discovery of Windows hosts, at least one Data Protection Advisor agent must be installed on a Windows Agent.
Ensure that Data Protection Advisor and all its components are configured as exceptions in any anti-virus software.	If not defined as exceptions, Data Protection Advisor components are shut down, or the anti-virus software quarantines the associated files occasionally.
Provision networking infrastructure and a shared directory if installing multiple Application servers (Data Protection Advisor clustering).	● Allocate a dedicated VLAN for use by the Data Protection Advisor Application servers. If a dedicated VLAN is not available, ask your network administrator for a UDP Multicast group address that can be used for the Data Protection Advisor cluster. ● To increase resiliency and quality of service, provision a hardware load-balancing switch as a gateway to the Data Protection Advisor Application servers. ● Configure a shared directory that is accessible by all Application Servers. Data Protection Advisor uses this shared directory for writing scheduled reports and other temporary files that all Application Servers must access.
Check VMware or Hyper-V requirements.	Data Protection Advisor has been certified to work on a Linux or Windows virtual machine in a VMware or Hyper-V environment. The Software Compatibility Guide provides more information.
Configure virtual infrastructure memory and CPU.	Configuring virtual infrastructure memory and CPU provides more information.
Open or disable firewalls for communication between the Data Protection Advisor servers.	If you want to use, secure communication for connecting to the Application server on port 9002, ensure that Transport Layer Security (TLS) settings are enabled for secure communication in your browser settings. When installing on Data Protection Advisor Servers, the operating system/software– based firewalls can be disabled or have ports opened for communication between the Data Protection Advisor Application server, the Data Protection Advisor Datastore server, and the Data Protection Advisor Agents before installing the Data Protection Advisor components.

Table 6. Installation and configuration overview (continued)

Action	Comments
	Typically, the network in which the Data Protection Advisor servers and Data Protection Advisor Agents reside are secure and behind a network firewall. It means that you could choose to disable operating system/software-based firewalls. If you choose to leave the operating system/software based in effect, you must open/unblock the required ports. Communications settings in Data Protection Advisor provides information. If on Linux and you choose to disable the firewall, run the following commands to disable and ensure that the firewall remains disabled after startup or reboot: ● Run **`iptables stop`**. ● Set the `chkconfig` utility to **`iptables off`**.
Install the host operating system on the Data Protection Advisor Server(s) and Agent host and install all required patches.	The Software Compatibility Guide lists the required architectures and patches.
Install all required software on the agent host after the Data Protection Advisor latest release Application Server is ready.	When monitoring applications or devices remotely, you must install additional software on the Agent host. For example, the NetWorker client must be installed on the Agent host if the Agent is used to monitor NetWorker remotely. For more information, see Environment discovery in Data Protection Advisor
If DNS is not enabled in the environment, add the IP address and FQDN of the SharePoint server on the hosts file of the Data Protection Advisor Application server.	Data Protection Advisor and SharePoint integration requires the IP address and FQDN to enable you to publish reports to SharePoint and to configure the SharePoint port. The SharePoint port is configurable. The default port, if no port is specified, is 80. You can set the port by using a standard URL in the existing URL field in the SharePoint settings dialog. System Settings, SharePoint settings table, provides information.
If you are going to use LDAP User Authentication on your Data Protection Advisor server, gather the information that is needed for configuration.	You need the following information for LDAP User Authentication configuration: ● LDAP Server Name/IP ● Use SSL? ● LDAP Server Port ● LDAP Version ● Distinguished Name of Base Directory ● Identification Attribute
Download and save the binaries.	To download the Data Protection Advisor Server and Agent binaries, go to the Data Protection Advisor downloads section of https://www.dell.com/support Save the Data Protection Advisor Server and Agent binaries locally.
Obtain and save Licenses.	
Save the required license files on your local machine for quick access during installation. The Data Protection Advisor installation wizard prompts you to browse for the license file at license installation.	You must know the IP address of the primary Datastore server. For more information about obtaining Data Protection Advisor licenses or types of Data Protection Advisor licenses available and required, contact your Account Representative.

Table 6. Installation and configuration overview (continued)

Action	Comments
● For new nonmigrated installations - Obtain Data Protection Advisor licenses for all components that must be monitored. ● For migrated 5.x installations - Existing licenses is migrated. ● The CLP license is required for new Data Protection Advisor functionality and increased capacity on a Data Protection Advisor instance. If you are not adding capacity or changing to new Data Protection Advisor latest release functionality, import of CLP licenses is not required. If you are migrating from Data Protection Advisor version 5.x to Data Protection Advisor, the existing licenses are migrated with your configuration and data. When not increasing capacity or changing functionality on existing WLS licenses, WLS licenses can only co-exist with CLP license types if they are imported before CLP licenses. CLP and WLS license coexistence in Data Protection Advisor provides more information.	A Data Protection Advisor license is required to administer Data Protection Advisor after installation. Data Protection Advisor is bundled with a 90-day evaluation license. The evaluation license is created from the time of Data Protection Advisor installation, is valid for up to 90 days, and allows access to all features. If you import a license during 90-day evaluation license period, the evaluation license is removed and you have access to Data Protection Advisor features according to license you imported. For information about required Data Protection Advisor licenses or on purchasing licenses for your Data Protection Advisor installation, contact your Sales Representative.
Install Data Protection Advisor	
Install the Data Protection Advisor software.	Install the Data Protection Advisor server and agent according to the installation instructions. Installing the Datastore Service, Installing the Application Service, and Installing the Data Protection Advisor Agent provide more information.
Configure the environment for data protection monitoring.	
Ensure that the required ports between the Data Protection Advisor Agent host and the monitored server or devices are open and communication is possible over the protocol.	Communications settings in Data Protection Advisor lists the protocols and default Data Protection Advisor ports that are required for communication between the agent and the monitored device or server.
Ensure that the Data Protection Advisor credential used to connect to the monitored device or server is sufficient, or have the new credential details ready.	Permissions lists the default settings for the Data Protection Advisor credentials that are installed with Data Protection Advisor.
Set up monitoring of RecoverPoint (if applicable).	RecoverPoint agent host and application host requirements are listed in Monitoring of RecoverPoint
Discover and configure Application Host import (if monitoring Microsoft Exchange or a database).	● If a remote agent is being used to import hosts, the Data Protection Advisor server must be able to resolve the agent host. ● If application discovery is being performed without an agent, Configuring for Replication Analysis provides more information.
Define the data protection policies.	
Prepare the details of the policies that Data Protection Advisor monitors for compliance.	For replication analysis, the Data protection policy details consist of: ● The type or replication. ● Whether the replication is Point-in-Time or continuous. ● The replication target destination. For data protection reporting, the policies are ● Chargeback Policies - For financial cost analysis of data protection operations. ● Protection Policies - To analyze compliance with recovery time objective (RTO) and recovery point objective (RPO) data protection targets. Policies provides more information.

Installing Data Protection Advisor

This chapter includes the following sections:

Topics:

Data Protection Advisor server installation

The Data Protection Advisor server installation involves two stages:

1. Installing the Datastore service
2. Installing the Application service

Datastore Replication provides information on installing with Datastore Replication.

Installation of the Application service before the Datastore service results in failure of Application service installation. If you encounter issues during the installation, Troubleshooting provides information.

The procedures in this section are applicable to new installations. For upgrades from previously supported Data Protection Advisor versions to the latest version of Data Protection Advisor, and to install the latest version of version of 19.12, see Upgrades. The Data Protection Advisor Release Notes provides information on supported upgrades.

The Data Protection Advisor installer runs on Windows and Linux, provided that your Linux installation supports running a UI. The following procedures describe installation in a Windows 64-bit environment.

Note on Linux UI installations:

- The advanced installation options are different for Linux from those of Windows installations, due to security reasons.
- Per DPA-57626, the **Configure existing unix user account** option is available in the Linux UI installation only.

Installing the Datastore Service

This procedure includes implementation for a normal Datastore installation without clustering and Datastore Replication.

- Ensure that you log in as a local administrator or a Domain administrator with full local access.
- If UAC is enabled on a Windows host, start the installer by Run as Administrator.
- Copy the installation binary to the server or to your local machine.
- If installing on UNIX/Linux, ensure that you are logged in as root. You could experience problems with the Datastore server if you install after becoming root through certain SU-type security software; for example, using the `sesu` command.
- Ensure that ports are opened or disabled for communication between the Data Protection Advisor servers. Installation and configuration overview provides information.
- Ensure that you have the IP Address of the Application server for the Agent to communicate with. If installing on Linux IPv6, ensure that you also have the IPv6 Interface ID of the Datastore server. You are prompted for this in the **Configure Agent** window of the Datastore installation. To get the IPv6 Interface ID, run the `ip addr show` command on the Linux Agent machine and use the output to find the IPv6 Interface ID. For example:

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

Where the values before the % refer to the IPv6 of the Application server (in this example, `fe80::9c9b:36f:2ab:d7a2`) and those after refer to the interface Id (in this example, `2`).

1. Double-click the Data Protection Advisor server binary to start the installation.

   For Linux, provide execute permission to the Linux binary and execute it as `./DPA-Server-Linux-x86_64****.bin`.
2. Click **Next**.
3. Read and accept End User License Agreement. Scroll to the end of the agreement to activate the option to accept the terms of the License Agreement. Click **Next.**
4. In the Installation Options screen, select to install Datastore service, click **Next**.
5. If you do not perform an advanced installation, click **Next** and follow the installation wizard.

   To perform an advanced installation, select the Show Advanced Installation Options checkbox in the Advanced Installation screen, click Next, and follow the installation wizard.

   The Advanced Options are:

   - **Do not register Data Protection Advisor services**: Prevent the registration of the Datastore service with the operating system manager. This will prevent the Datastore service from being started after host reboot. You must use the Data Protection Advisor Command Line Interface to install the service with the operating system.
   - **Do not start Data Protection Advisor services**: Prevent the starting of the Datastore services after installation. Use of the Data Protection Advisor Command Line Interface will be required to start the service.
   - **Install with advanced datastore layout**: Configure the Datastore service with the required filesystems distributed across different disks to optimize performance.
   - **Install services under specified account**: Run datastore and agent services under a specified account.
6. When prompted, choose the installation folder.

   Choose the default location or browse to another folder location.
7. Review the Pre-Installation Summary, the disk space information in particular, click **Install**.

   The installation proceeds.

   If there is not enough disk space, cancel the installation or choose a different drive on which to install Data Protection Advisor.
8. When prompted, select the IP addresses that the Datastore should listen on for connections from the Data Protection Advisor Application Server(s).
9. On Linux, when prompted for Datastore Replication Option, select either Y or N.

   ```
   By default the DPA datastore service is installed not configured for
   replication.
   If replication is required please enter 'Y' and then the role of this
   datastore installation.
   Do you wish to configure for replication (Y/N):
   ```
10. When prompted, enter the IP address of the Data Protection Advisor Application Server that will use the Datastore from step 8 and then click **Add** and **Next**. On Linux, select option **Add an Application Client Address** and **Review and Complete**.

    ```
    Please enter the IP addresses for all DPA application service hosts that will
    connect to and use this datastore.


    At least one IP address must be provided.
     Additional clients can be added to the datastore access using the DPA command
    line interface.
        1- Add an Application Client Address
        2- Remove an Application Client Address

        3- Review and Complete
    Select action:
    ```
11. When prompted, specify the Datastore password.

    Note the following regarding the Datastore password:

    - Blank passwords are not supported.
    - Minimum length is 9 characters.

- The following are required:
  - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
  - A minimum of 1 numeric symbol
  - A minimum of 1 special character
- The dpa datastore dspassword command can be used to reset the Data Protection Advisor Datastore password . dpa datastore dspassword provides more information.

12. When prompted, specify the Data Protection Advisor Agent password:

    Note the following regarding the Agent password:

    - Blank passwords are not supported.
    - Minimum length is 9 characters.
    - The following are required:
      - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
      - A minimum of 1 numeric symbol
      - A minimum of 1 special character
    - The dpaagent --set-credentials command can be used to reset the Data Protection Advisor Agent password . dpaagent --set-credentials provides more information.

13. When the Data Protection Advisor Datastore Server installation is complete, click **Done**.

Installing the Application Service

This procedure includes implementation for a normal Application service installation without clustering and Datastore Replication.

- To ensure secure communication between the Data Protection Advisor Server and Agent, set the Agent registration password using the `dpa app agentpwd`CLI command on the Data Protection Advisor Application Server host. You must also set this password on all Data Protection Advisor Agent hosts.dpa application agentpwd provides information. Then restart the Application service. Ensure that you set this password for each Agent.
- Copy the Agent installation binary to the server or to your local machine.
- Ensure that ports are opened or disabled for communication between the Data Protection Advisor servers. Installation and configuration overview provides information.
- Ensure that the Datastore service option is checked, and that the Datastore service is running.
- If you plan to use SRS-VE for remote troubleshooting (recommended), ensure that you have the SRS-VE environment installed and configured before Data Protection Advisor installation. The Secure Remote Services Virtual Edition on Dell Technologies Online Support provides information about SRS-VE installations.

The Application service installation process is similar to installing the Datastore service.

1. Double-click the Data Protection Advisor server binary to start the installation.

   For Linux, provide run permission to the Linux binary and run it as `./DPA-Server-Linux-x86_64****.bin`.
2. Click **Next.**
3. Read and accept End User License Agreement. Scroll to the end of the agreement to enable the option to accept the terms of the License Agreement. Click **Next.**
4. In the Installation Options screen, select to install Application service, click **Next**.
5. If you do not perform an advanced installation, click **Next** and follow the installation wizard.

   The Advanced Options are:

   - **Do not register Data Protection Advisor services**: Prevents the registration of the service with the operating system service manager. This option prevents the Data Protection Advisor services from being started after a host reboot.

   - **Do not start Data Protection Advisor services**: Prevents the Data Protection Advisor services from being started after installation. Use of the command-line interface is required to start the service.

   - **Install services under specified account**: Run application and agent services under a specified account. Not applicable for clusters.

     The rest of the installation is similar to the Datastore installation.

6. In Linux, specify the user account.

```
Specify user
------------

Please enter a user account to run services.

Please enter the user name (Default: root):
```

7. For Linux, when prompted for a security warning, select the appropriate option.

```
Are you sure you want to install services under root account?

  ->1- OK
    2- Cancel

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE
   DEFAULT:
```

8. Review the Pre-Installation Summary, the disk space information in particular, click **Install**. The installation proceeds.

   If there is not enough disk space, cancel the installation or choose a different drive to install Data Protection Advisor on.

   > ⓘ **NOTE:** If the relevant firewall required to communicate between Application Server and the Datastore are not open, a datastore connection failure error might occur. Communications settings in Data Protection Advisor provides information.

9. In the **Connect to Remote Data Protection Advisor Datastore** step, enter the IP address for the Data Protection Advisor Datastore server previously installed.

   The installation resumes.

10. When prompted, specify the name or IP address of the Data Protection Advisor Application server host with which the Data Protection Advisor Agent communicates. By default the Agent communicates with the local Application server with IP address 127.0.0.1. Click **Next**.

    The Data Protection Advisor Application service installation is now complete.

11. When prompted, specify the Datastore password.

    Note the following regarding the Datastore password:

    - Blank passwords are not supported.
    - Minimum length is nine characters.
    - The following are required:
      - A minimum of one uppercase and one lowercase alphabetic symbol
      - A minimum of one numeric symbol
      - A minimum of one special character
    - The `dpa application dspassword` configures the Data Protection Advisor Datastore password. dpa application dspassword provides more information.

12. When prompted, specify the Administrator password.

    Note the following regarding the Administrator password:

    - Blank passwords are not supported.
    - Minimum length is nine characters.
    - The following are required:
      - A minimum of one uppercase and one lowercase alphabetic symbol
      - A minimum of one numeric symbol
      - A minimum of one special character
    - The `dpa app adminpassword` command can be used to reset the Data Protection Advisor administrator password and enable the Data Protection Advisor Administrator account when the Data Protection Advisor Datastore service is up and running. dpa application adminpassword provides more information.

13. When prompted, specify the Data Protection Advisor Agent password.

    Note the following regarding the Agent password:

    - Blank passwords are not supported.

- Minimum length is nine characters.
- The following are required:
  - A minimum of one uppercase and one lowercase alphabetic symbol
  - A minimum of one numeric symbol
  - A minimum of one special character
- The `dpaagent --set-credentials` command can be used to reset the Data Protection Advisor Agent password. dpaagent --set-credentials provides more information.

14. Click **Done**.

    After the installation is complete, start the Data Protection Advisor Server and license the Server. Data Protection Advisor post installation steps for secure communication provides more information.

Datastore Replication

Data Protection Advisor Datastore Replication enables continuous, safe, and reliable replication so that Data Protection Advisor can maintain a replica or secondary Datastore of the primary Datastore for resilience against a single point of failure. You can add additional secondary Datastores in a cascading fashion to the standard Primary Secondary configuration if required.

If the primary Datastore fails, you can update the secondary Datastore to the primary role by using the manual failover command. You can then configure the Application servers to use this new primary Datastore. Reconfiguration generally takes the same amount of time to take effect as the Data Protection Advisor Application and Datastore services startup take. Carrying out Datastore server failover provides more information.

There can be only one primary Datastore per deployment. All Datastores are primary Datastores after installation. Replication is enabled once a secondary Datastore can communicate with the primary Datastore. Data starts being replicated when an Application server is started.

You can configure Datastore Replication:

- During a fresh installation; Installing the primary Datastore Service with Datastore Replicationand Installing the secondary Datastore Service with Datastore Replication provide information.
- During an upgrade; Upgrading with Datastore Replication enabled with Data Protection Advisor 6.3 and later provide information.
- After installation and deployment; Configuring Datastore Replication after deployment provides more information.

Ensure that all Datastore nodes are using the same IP type of IP addressing, either IPv4 addresses or IPv6 addresses.

Configuring Datastore Replication

1. Configure the secondary Datastore, either during or after installation.
2. Configure the primary Datastore, either during or after installation.
3. Install or, if already installed, start the Application server.

Installing the secondary Datastore Service with Datastore Replication

This procedure includes implementation for a secondary Datastore installation implementing Datastore Replication.

- Ensure that you log in as a local administrator or a Domain administrator with full local access.
- If UAC is enabled on a Windows host, start the installer by Run as Administrator.
- Copy the installation binary to the server or to your local machine.
- If installing on UNIX or Linux, ensure that you are logged in as root. You could experience problems with the Datastore server if you install after becoming root through certain SU-type security software; for example, using the `sesu` command.
- If installing on UNIX or Linux, ensure that the `unzip` command for InstallAnywhere is installed on your system.
- Ensure that ports are opened or disabled for communication between the Data Protection Advisor servers. Installation and configuration overview provides information.
- Ensure that you have the IP Address of the Application server for the Agent to communicate with. If installing on Linux IPv6, ensure that you also have the IPv6 Interface ID of the Datastore server. You are prompted for this in the **Configure Agent**

window of the Datastore installation. To get the IPv6 Interface ID, run the `ip addr show` command on the Linux Agent machine and use the output to find the IPv6 Interface ID. For example:

```
fe80::9c9b:36f:2ab:d7a2%2
```

Where the values before the % indicate the IPv6 of the Application server (in this example, `fe80::9c9b:36f:2ab:d7a2`) and the values after indicate to the interface Id (in this example, `2`).

- Plan the final Datastore Replication deployment topology before beginning installation. More resources are available on the Dell Community Network that provides guidance and best practice for planning your deployment.
- Have all hosts and IP addresses predetermined and available.
- Ensure that all Datastore server or Application server, are using the same IP type of IP addressing, either IPv4 addresses or IPv6 addresses.
- Ensure that the Application server chosen is the same server that the primary Datastore is using.

1. Double-click the Data Protection Advisor server binary to start the installation.
2. Click **Next**.
3. Read and accept End User License Agreement. Scroll to the end of the agreement to activate the option to accept the terms of the License Agreement. Click **Next.**
4. In the Installation Options screen, select to install the Datastore service, click **Next**.
5. Select the **Show Advanced Installation Options** checkbox in the **Advanced Installation** screen, click **Next**.
6. Select **Install with advanced datastore layout** and click **Next**.
7. When prompted, choose the installation folder.

   Choose the default location or browse to another folder location.
8. Review the Pre-Installation Summary, the disk space information in particular, click **Install**.

   The installation proceeds.

   If there is not enough disk space, cancel the installation or choose a different drive on which to install Data Protection Advisor.
9. In the **Datastore Listening Addresses** window, specify the IP addresses that the Datastore service should listen on for connections from the Data Protection Advisor Application services.
10. In the **Configure Datastore Access** window, enter the IP addresses of the Data Protection Advisor Application Servers that uses the Datastore and then click **Add** and **Next**.
11. In the **Datastore Agent Address** window, specify the alternative address for the Datastore Agent to be the Load Balancer IP Address.
12. Select **Enable datastore replication** > **and select the replication role for this server** > **SLAVE**. Click **Next**.
    a. Provide the IP address or FQDN of the primary Datastore server.
    b. When prompted in the **Configure Agent** window, enter the FQDN or IP address of the Data Protection Advisor Application service that the installed Data Protection Advisor Agent must communicate with.

       By default, the Agent communicates with the Application server specified earlier in the wizard.
    c. Click **Next**.
13. When the Data Protection Advisor Datastore Server installation is complete, click **Done**.
14. On a command prompt, run the `dpa svc status` command to verify that the Datastore service is running.
15. Set the database connection pool size in all Datastore nodes. Run:

    `# dpa ds tune --connections xxx <RAM>GB` where *xxx* is approximately 250 per each Application server and *RAM* is the amount of RAM.

Installing the primary Datastore Service with Datastore Replication

This procedure includes implementation for a primary Datastore installation implementing Datastore Replication.

- Ensure that you log in as a local administrator or a Domain administrator with full local access.
- If UAC is enabled on a Windows host, start the installer by Run as Administrator.
- Copy the installation binary to the server or to your local machine.
- If installing on UNIX or Linux, ensure that you are logged in as root. You could experience problems with the Datastore server if you install after becoming root through certain SU-type security software; for example, using the `sesu` command.
- If installing on UNIX or Linux, ensure that the `unzip` command for InstallAnywhere is installed on your system.

- Ensure that ports are opened or disabled for communication between the Data Protection Advisor servers. Installation and configuration overview provides information.
- Ensure that you have the IP Address of the Application server for the Agent to communicate with. If installing on Linux IPv6, ensure that you also have the IPv6 Interface ID of the Datastore server. You are prompted for this ID in the **Configure Agent** window of the Datastore installation. To get the IPv6 Interface ID, run the `ip addr show` command on the Linux Agent machine and use the output to find the IPv6 Interface ID. For example:

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  Where the values before the % indicates the IPv6 of the Application server (in this example, `fe80::9c9b:36f:2ab:d7a2`) and the values after indicates the interface Id (in this example, `2`).
- Plan the final Datastore Replication deployment topology before beginning installation. More resources are available on the Dell Community that provides guidance and best practice for planning your deployment.
- Have all hosts and IP addresses predetermined and available.
- Ensure that all Datastore server or Application server, are using the same IP type of IP addressing, either IPv4 addresses or IPv6 addresses.
- Ensure that the Application server chosen is the same server that the primary Datastore is using.

1. Double-click the Data Protection Advisor server binary to start the installation.
2. Click **Next**.
3. Read and accept End User License Agreement. Scroll to the end of the agreement to activate the option to accept the terms of the License Agreement. Click **Next.**.
4. In the Installation Options screen, select to install the Datastore service, click **Next**.
5. Select the **Show Advanced Installation Options** checkbox in the **Advanced Installation** screen, click **Next**.
6. Select **Install with advanced datastore layout** and click **Next**.
7. When prompted, choose the installation folder.

   Choose the default location or browse to another folder location.
8. Review the Pre-Installation Summary, the disk space information in particular, click **Install**.

   The installation proceeds.

   If there is not enough disk space, cancel the installation or choose a different drive on which to install Data Protection Advisor.
9. In the **Datastore Listening Addresses** window, specify the IP addresses that the Datastore service should listen on for connections from the Data Protection Advisor Application services.
10. In the **Configure Datastore Access** window, enter the IP addresses of the Data Protection Advisor Application Servers that use the Datastore, and then click **Add** and **Next**.
11. In the **Datastore Agent Address** window, specify the alternative address for the Datastore Agent to be the Load Balancer IP Address.
12. Select **Enable datastore replication** > **and select the replication role for this server** > **MASTER**. Click **Next**.
    a. Provide the IP address or FQDN of the secondary Datastore server.
    b. When prompted in the **Configure Agent** window, enter the FQDN or IP address of the Data Protection Advisor Application service that the installed Data Protection Advisor Agent must communicate with.

       By default, the Agent communicates with the Application server specified earlier in the wizard.
    c. Click **Next**.
13. When prompted, specify the Datastore password.

    Note the following regarding the Datastore password:
    - Blank passwords are not supported.
    - Minimum length is nine characters.
    - The following are required:
      - A minimum of one uppercase and one lowercase alphabetic symbol
      - A minimum of one numeric symbol
      - A minimum of one special character
    - The `dpa datastore dspassword` command can be used to reset the Data Protection Advisor Datastore password . dpa datastore dspassword provides more information.
14. When the Data Protection Advisor Datastore Server installation is complete, click **Done**.
15. On a command prompt, run the `dpa svc status` command to verify that the Datastore service is running.
16. Set the database connection pool size in all Datastore nodes. Run:

`# dpa ds tune --connections xxx <RAM>GB`, where *xxx* is approximately 250 per each Application server and *RAM* is the amount of RAM.

Installing the Application Service with Datastore Replication

This procedure for installing for the Application service installation is included for completeness. There is no special Application service implementation for Datastore Replication.

- Copy the installation binary to the server or to your local machine.
- Ensure that ports are opened or disabled for communication between the Data Protection Advisor servers. Installation and configuration overview provides information.
- Ensure that the Datastore service option is checked, and that the Datastore service is running.
- If installing on UNIX/Linux, ensure that the `unzip` command for InstallAnywhere is installed on your system.
- If you plan to use SRS-VE for remote troubleshooting (recommended), ensure that you have the SRS-VE environment installed and configured before Data Protection Advisor installation. The Secure Remote Services Virtual Edition on Dell Technologies Online Support provides information about SRS-VE installations.

The Application service installation process is similar to installing the Datastore service.

1. Double-click the Data Protection Advisor server binary to start the installation.
2. Click **Next.**
3. Read and accept End User License Agreement. Scroll to the end of the agreement to enable the option to accept the terms of the License Agreement. Click **Next.**
4. In the **Installation Options** screen, select to install Application service and click **Next**.
5. If you do not perform an advanced installation, click **Next** and follow the installation wizard.
6. Review the Pre-Installation Summary, the disk space information in particular, click **Install**. The installation proceeds.

   If there is not enough disk space, cancel the installation or choose a different drive to install Data Protection Advisor on.

   NOTE: A Datastore connection failure error might occur if the relevant firewalls required to communicate between Application Server and the Datastore are not open. Communications settings in Data Protection Advisor provides information.

7. In the **Connect to Remote Data Protection Advisor Datastore** step, enter the IP address for the Data Protection Advisor primary Datastore server previously installed.

   The installation resumes.

8. When prompted, specify the name or IP address of the Data Protection Advisor Application server host with which the Data Protection Advisor Agent will communicate. By default the Agent communicates with the local Application server with IP address 127.0.0.1. Click **Next**.

   The Data Protection Advisor Application service installation is now complete.

9. When prompted, specify the Datastore password.

   Note the following regarding the Datastore password:

   - Blank passwords are not supported.
   - Minimum length is nine characters.
   - The following are required:
     - A minimum of one uppercase and one lowercase alphabetic symbol
     - A minimum of one numeric symbol
     - A minimum of one special character
   - The dpa datastore dspassword command can be used to reset the Data Protection Advisor Datastore password . dpa datastore dspassword provides more information.

10. Set the Administrator password.

    Note the following regarding the Administrator password:

    - Blank passwords are not supported.
    - Minimum length is nine characters.
    - The following are required:
      - A minimum of one uppercase and one lowercase alphabetic symbol
      - A minimum of one numeric symbol

    - A minimum of one special character
- The dpa app adminpassword command can be used to reset the Data Protection Advisor Administrator's password and enable the Data Protection Advisor Administrator account when the Data Protection Advisor Datastore service is up and running. dpa application adminpassword provides more information.

11. Click **Done**.

    After the installation is complete, start the Data Protection Advisor Server and license the Server. Data Protection Advisor post installation steps for secure communication provides more information.

Establish replication between the primary and secondary Datastores

To establish replication between the primary Datastore and the secondary Datastore, perform the following:

1. Run the `dpa_datastore_superuserpassword` command on the primary Datastore to change the superuser password on the primary Datastore.

   dpa datastore superpassword provides more information.
2. Run the `dpa_datastore_superuserpassword` command on the secondary Datastore to change the superuser password on the secondary Datastore.

   dpa datastore superpassword provides more information.

   The superuser password must be the same as the one set on the primary Datastore.
3. Run the following commands to create a new replication slot "standby1_slot" and verify it on the primary Datastore:

   `dpa ds query "select * from pg_create_physical_replication_slot ('standby1_slot');"`

   `dpa ds query "select slot_name, slot_type, active, wal_status from pg_replication_slots;"`.
4. Export the Datastore on primary Datastore by using the following command: `dpa ds rep -e <path of an empty folder>`.
5. Import the Datastore on the secondary Datastore by using the following command: `dpa ds rep -i <path>`.
6. Run the `dpa ds rep` command on the on primary and secondary Datastore.

   The output must show the replication status as streaming.

Datastore Replication best practices

Consider the following best practices for Datastore Replication:

- Install the Primary and secondary Datastores on the same version of Data Protection Advisor.
- Ensure that the primary and secondary Datastores have the same performance specifications.
- Restart the Datastore service when the role between the primary Datastore and the secondary Datastore changes.
- Run the replication configuration command **`dpa ds rep`** to check the status of replication. Running this command on the primary Datastore displays whether the replication is streaming and what the secondary Datastore is. Running the command on the secondary Datastore displays what the primary Datastore is.
- Before you export a Datastore, ensure that you create an empty directory on the Datastore, to which you want to export the Datastore file set. For example, `/tmp/export`.

Data Protection Advisor Agent installation

This section describes how to install the Data Protection Advisor Agent using the agent-only installation package. It is applicable to new installations.

An Agent is automatically installed on the Data Protection Advisor Application and Datastore servers. Therefore do not run this procedure on the Data Protection Advisor servers. For upgrades from previous Data Protection Advisor service packs to the latest version of Data Protection Advisor, and to install the latest version of Data Protection Advisor, see Upgrades.

Installing the Data Protection Advisor Agent

The following procedure explains installing the Data Protection Advisor Agent in a Windows or a Linux environment.

- Ensure that ports are opened or disabled for communication between the Data Protection Advisor servers. Installation and configuration overview provides information.
- Ensure that you have the IP Address of the Data Protection Advisor Application server for the Agent to communicate with. If installing on Linux IPv6, ensure that you also have the IPv6 Interface ID of the Agent. You are prompted for this in the **Configure Agent** window of the Agent installation. To get the IPv6 Interface ID, run the `ip addr show` command on the Linux Agent machine and use the output to find the IPv6 Interface ID. For example:

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  Where the values before the % refer to the IPv6 of the Data Protection Advisor Application server (in this example, `fe80::9c9b:36f:2ab:d7a2`) and those after refer to the interface ID of the Agent (in this example, `2`).

1. Double-click the Data Protection Advisor Agent binary to start the installation.

   For Linux, provide execute permission to the Linux binary and execute it as `./DPAServer- Linux-x86_64****.bin`.
2. Click **Next**.
3. Read and accept End User License Agreement. Click **Next.**
4. Choose an installation folder and click **Next**.
5. Select **Install services under non-default account** to change service user and click **Next**.

   If you do not want to install under a non-default account, leave the option unselected and click **Next**. The Data Protection Advisor Agent Service is installed under a Local System User.

   On Linux, select the appropriate option.

   ```
   Use non-default user
   --------------------

   Install services under non-default account
   Use non-default user (Y/N):
   ```

   NOTE: If the agent is installed with the named account, which is not a member of the local administrator's group, then the permissions for the named account must be modified to read, write, execute, and modify on the Data Protection Advisor Agent installation folder.
6. Enter the non-default account username and password.

   You must provide valid pair local_user|password or domain_user|password. You must enter the username in **`<DOMAIN>\<USERNAME>`** format.

   On Linux, select the appropriate option.

   ```
   Are you sure you want to install service under root account?

     ->1- OK
       2- Cancel

   ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE
      DEFAULT:
   ```
7. Verify the Pre-Installation Summary and click **Install**.
8. Choose the Agent installation options:
   - **Do not start Data Protection Advisor Agent service** - this option prevents starting of the Data Protection Advisor Agent service after installation.

     If you select this option, you must manually start the Data Protection Advisor Agent from the command line.

     If you select Do not start Data Protection Advisor Agent service, click **Next**.

     Type the fully qualified domain name or the IP address of the Data Protection Advisor Server that communicates with the Data Protection Advisor Agent.

- **Agent will be used to monitor Oracle Database:** Select this option to monitor an Oracle database with the Data Protection Advisor Agent.

  If you select this option, browse to the directory where the Data Protection Advisor Agent can find the Oracle Database device driver files.

9. Click **Next**.
10. In the **Configure Agent** window, enter the fully qualified domain name or the IP address of the Data Protection Advisor Application Server that communicates with the Data Protection Advisor Agent.

    If you are installing on Linux IPv6 and are installing Linux Agents, enter the IPv6 Interface ID of the Linux Agent.

    Click **Next**.
11. Set the same Agent password that you set during the Data Protection Advisor Datastore installation:

    Note the following regarding the Agent password:

    - Blank passwords are not supported.
    - Minimum length is 9 characters.
    - The following are required:
      - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
      - A minimum of 1 numeric symbol
      - A minimum of 1 special character
12. Click **Done** to complete the installation.
13. Restart the Agent service.

Follow the steps in Setting Data Protection Advisor Agent registration password.

Installing the Data Protection Advisor Agent on Solaris, AIX, and HP-UX

The following procedure explains installing the Data Protection Advisor Agent in a Solaris, AIX, and HP-UX environment.

- Ensure that ports are opened or disabled for communication between the Data Protection Advisor servers. Installation and configuration overview provides information.
- Ensure that you have the IP Address of the Data Protection Advisor Application server for the Agent to communicate with.

1. Double-click the Data Protection Advisor Agent binary to start the installation.
   - For Solaris, provide execute permission to the Solaris binary and execute it as `. /DPA-Agent-Solaris-x86_64****.bin`.
   - For Solaris-SPARC, provide execute permission to the Solaris-SPARC binary and execute it as `. / DPA-Agent-Solaris-SPARC64-****.bin`.
   - For AIX, provide execute permission to the AIX binary and execute it as `. /DPA-Agent-AIX-PPC64****.bin`.
   - For HP-UX, provide execute permission to the HP-UX binary and execute it as `./ DPA-Agent-HP-UX-IA64-xxxx.bin`.
2. Accept the terms of license agreement.
3. Specify the installation directory where you want to install the agent or proceed with the default installation directory.

```
Choose Install Folder
---------------------
Please choose a target folder for the installation of the DPA Agent service :
Where would you like to install?
  Default Install Folder: /opt/emc/dpa
ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

4. Verify the Pre-Installation Summary and click **ENTER** to continue.
5. Type **N** when prompted for Agent Installation Options.

```
Agent Installation Options
--------------------------
Advanced Application options are :
- Do not start DPA Agent service
- DPA Agent will monitor Oracle Databases
Do you want to select advanced options (Y/N): N
```

6. Type **Y** if you want to configure the Advanced Agent Installation options.
   - **Do not start Data Protection Advisor Agent service** - this option prevents starting of the Data Protection Advisor Agent service after installation.

     If you select this option, you must manually start the Data Protection Advisor Agent from the command line.
   - **Data Protection Advisor Agent will monitor Oracle Databases:** Select this option to monitor an Oracle database with the Data Protection Advisor Agent.

     If you select this option, specify the directory where the Solaris Agent can find the Oracle Database device driver files.
7. Set the Agent password by following the policy displayed on the console.

```
Set Agent Password
------------------
Please set the Agent password.
The password must have:
- at least 9 characters
- at least 1 uppercase letter
- at least 1 lowercase letter
- at least 1 special character
- at least 1 digit

Enter Password:
Re-enter Password:
```

8. Provide the IP address of the Data Protection Advisor Server (application node) that the installed Data Protection Advisor Agent must communicate with.

```
Configure Agent
---------------
Please enter the IP address of the DPA Server (application node) that the
installed DPA Agent needs to communicate with :
IP ADDRESS (Default: 127.0.0.1): xx.xx.xx.xx
```

9. Wait for the installation to complete.

```
PRESS <ENTER> TO EXIT THE INSTALLER:
```

10. Restart the Agent service.

```
Ex: cd  /opt/emc/dpa/agent/etc
./dpa restart
```

Setting Data Protection Advisor Agent registration password

After installation of the Data Protection Advisor Agent, set the Agent password.

Run **`dpaagent --set-credentials`** to set the Data Protection Advisor agent password.

dpaagent --set-credentials provides full command information.

Configure Data Protection Advisor Agent to go back and collect backup application data

By default, the newly installed Data Protection Advisor Agent starts collecting data from backup applications starting from the current date and time. If you would like to see alerts for failed backups within the previous days for auditing or other reasons, or if for any other reason you wish to collect days of backup application data, you can configure the newly installed Data Protection Advisor agent to collect data for user-defined number of hours.

You must have Data Protection Advisor 19.12 or later installed for this procedure.

For Linux

1. Install the Data Protection Advisor Agent. Do not start the Data Protection Advisor Agent.
2. Add the following two lines to the `dpa.config` file:

   `VARIABLE_NAME=NUMBER_OF_BACKUP_HOURS`

   `export VARIABLE_NAME`

   Where *VARIABLE_NAME* is the following for these backup applications:

   NetWorker: AGENT_NSR_JOB_STARTTIME

   Avamar: AGENT_AXION_JOB_STARTTIME

   TSM: AGENT_TSM_JOB_STARTTIME

   HPDP: AGENT_DP_JOB_STARTTIME

   CommVault: AGENT_CV_JOB_STARTTIME

   NetBackup: AGENT_NB_JOB_STARTTIME

   ArcServe: AGENT_AS_JOB_STARTTIME

   DB2: AGENT_DB2_JOB_STARTTIME

   SAP HANA: AGENT_SAP_HANA_JOB_STARTTIME

   RMAN: AGENT_RMAN_JOB_STARTTIME

   MSSQL: AGENT_MSSQLDB_JOB_STARTTIME

   The NUMBER_OF_BACKUP_HOURS is the number of backup hours before the current time.

   For example the following two lines in `dpa.config` should make the Data Protection Advisor Agent start collecting data from the 14 days previous:

   ```
   AGENT_AXION_JOB_STARTTIME=336
   export AGENT_AXION_JOB_STARTTIME
   ```

3. Start the Data Protection Advisor Agent.

For Windows

1. Export the key system registry to the registry path `HKEY_LOCAL_MACHINE\SOFTWARE\emc\DPA\AGENT` with the following information:

   `VARIABLE_NAME=NUMBER_OF_BACKUP_HOURS`

   Where *VARIABLE_NAME* is the following for these backup applications:

   NetWorker : NSR_JOB_STARTTIME

   Avamar : AXION_JOB_STARTTIME

   TSM : TSM_JOB_STARTTIME

   HPDP: DP_JOB_STARTTIME

   CommVault: CV_JOB_STARTTIME

   NetBackup: NB_JOB_STARTTIME

   ArcServe: AS_JOB_STARTTIME

   DB2: DB2_JOB_STARTTIME

   SAP HANA: SAP_HANA_JOB_STARTTIME

   RMAN: RMAN_JOB_STARTTIME

   MSSQL: MSSQLDB_JOB_STARTTIME

   The NUMBER_OF_BACKUP_HOURS is the number of backup hours before the current time.

   For example, add the following 3 lines as a contents of the `avamar.reg` file and start it from cmd to export to registry so that the Data Protection Advisor Agent collects data from NetWorker starting from 14 days previous:

   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\emc\DPA\AGENT]
   ```

```
NSR_JOB_STARTTIME="336"
```

2. Install and start the Data Protection Advisor Agent.

Configure Data Protection Advisor to show all VM Image Backups in Avamar

By default, the Backup Job Config and Backup Server Mapping data sources show the VM Image Backup clients that are being actively backed up in the last 30 days only in Data Protection Advisor for Avamar. Complete the procedure below to show all the VM clients configured in Avamar server.

1. Set the option `Show potentially disabled VM clients and HLE conatiners` to `True` on the Avamar Configuration request.
2. On the agent monitoring the Avamar server, set the environment variable *AGENT_AXION_DATASET_BACKUP_DAYS* to **`18000`**.

   This value can be used to override the default cut-off threshold of 30 days.
3. Depending on your OS on which you are running your Data Protection Advisor system, follow the steps outlined in the subtasks below.

For Linux

1. Edit the `<install_path>/dpa/agent/etc/dpa.config` file to add the following two lines:

   `AGENT_AXION_DATASET_BACKUP_DAYS=18000`

   `export AGENT_AXION_DATASET_BACKUP_DAYS`
2. Restart the Data Protection Advisor Agent service.

For Windows

1. Open regedit to create a registry key named *AXION_DATASET_BACKUP_DAYS* under the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\EMC\DPA\AGENT`.
2. Route to `HKEY_LOCAL_MACHINE\SOFTWARE\EMC\DPA\AGENT` .
3. Right-click to create **New** > **String Value** with name *AXION_DATASET_BACKUP_DAYS*.
4. Modify the registry key `AXION_DATASET_BACKUP_DAYS` with value **`18000`**.

Installing by using command line installation

Use the appropriate commands on the Data Protection Advisor agent and the server.

If you are installing Data Protection Advisor on any of the UNIX operating systems, run the `chmod755` command to change the binary execute permission.

- Linux

  ```
  DPA-<component>-Linux-<architecture>-<version>.xxx.install.bin [option]
  ```

  where *option* is one of the options listed for a silent or an interactive installation in Table 8.

  For example:

  - Data Protection Advisor agent : **`DPA-Agent-Linux-x86_64-<version>.bin -i silent -DUSER_INSTALL_DIR="/opt/custom/emc/dpa"`**
  - Data Protection Advisor server: **`DPA-Server-Linux-x86_64-<version>.exe -i silent -DCHOSEN_INSTALL_SET="APP" -DVAR_APPLICATION_DATASTORE_ADDRESS="<ip-`**

address of datastore>" -DVAR_ADMIN_PASSWORD="<admin-password>" -DVAR_APOLLO_USER_PASSWORD="<datastore-password>" -DVAR_AGENT_PASSWORD="<agent-password>"

- AIX

  ```
  ./DPA-<component>-AIX-<architecture>-<version>.bin
  ```

  For example: **./DPA-Agent-AIX-PPC64-<version>.bin**

- Windows

  ```
  DPA-<component>-Windows-<architecture>-<version>.xxx.install.exe [option]
  ```

  where *option* is one of the options listed for a silent or an interactive installation in Table 8.

  For example:

  - Data Protection Advisor agent: **DPA-Agent-Windows-x86_64-<version>.exe -i silent -DUSER_INSTALL_DIR="C:\custom\emc\dpa"**
  - Data Protection Advisor server: **DPA-Server-Windows-x86_64-<version>.exe -i silent -DCHOSEN_INSTALL_SET="<APP>" -DVAR_APPLICATION_DATASTORE_ADDRESS="<ip-address of datastore>" -DVAR_ADMIN_PASSWORD="<admin-password>" -DVAR_APOLLO_USER_PASSWORD="<datastore-password>" -DVAR_AGENT_PASSWORD="<agent-password>"**

ⓘ **NOTE:** This user account must have the Log on as a service Windows permission enabled.

Ensure that you carry out the steps provided in Data Protection Advisor post installation steps for secure communication.

Table 7. Installer command line options

Option	Description
-?	Displays help text
-i [swing | console | silent]	Specify the user interface mode for the installer: ● swing - Graphical interface ● console - console only ● silent - no user interaction
-D <name>="<value>"	Shows the installer name-value pairs that might be set on the command line (using the -D option) to override default installer values, or placed in a response file and used with the -*f* option. ⓘ **NOTE:** Quotes must be used around the value. Syntax: `-D<variable name>="<value>"` For example: `DPA-Agent-Windows-x86_64-<version>.exe -i silent -DUSER_INSTALL_DIR="C:\custom\emc\dpa"` *<variable name>* and *<value>* descriptions are included in the following tables.

-f <path of the response file>	Install Anywhere provides a way to silently install without user intervention using a response file with the -*f* option.
	Response files utilize a simple key=value format. It is a properties file with the .properties extension. You can specify all the options which is provided through the command line for silent installation in this response file.
	For example, create a file with the name installer.properties in the *C* drive and add the following details and run it:
	#This file was built for installing the Datastore silently.
	INSTALLER_UI=silent
	CHOSEN_INSTALL_SET="DS"

Table 7. Installer command line options (continued)

Option	Description
	VAR_DATASTORE_BIND_ADDRESSES="<Datastore_IP_address>" VAR_DATASTORE_CLIENTS_ADDRESSES="<Application_server_IP_address>" VAR_APOLLO_USER_PASSWORD="<Datastore_password>" For example: **`DPA-Server-Windows-x86_64-<version>.exe -f C:\installer.properties`** Where: INSTALLER_UI allows you to specify the installer mode in the properties file, negating the need to use the `-i` silent command-line switch. ⓘ **NOTE:** After you create the file with the installation details, it can be used again for later installations.

Table 8. Datastore installer variables

Variable Name	Description	Possible Values	Default Values
USER_INSTALL_DIR	Installation location	Valid Path	● Windows: `C:\Program Files\EMC\DPA`. ● Linux: `/opt/emc/dpa`
CHOSEN_INSTALL_SET	Installation set	DS	N/A
VAR_CUSTOM_SERVICE_USER	Linux silent installation under non-root user	TRUE/FALSE	
VAR_SERVICE_USER	Linux silent installation under non-root user	Username	
VAR_SERVICE_USER_SWITCHED	Linux silent upgrade installation if user changes	TRUE/FALSE	
VAR_CUSTOM_SERVICE_USER	Windows silent installation under non-root user		
VAR_SERVICE_USER	Windows silent installation under non-root user	Username	
VAR_SERVICE_USER_PASSWORD	Windows silent installation under non-root user		
VAR_SERVICE_USER_SWITCHED	Windows silent upgrade installation if user changes	TRUE/FALSE	
VAR_INSTALL_SERVICE	Advanced option to install the Datastore Service	TRUE/FALSE	TRUE
VAR_START_SERVICE	Advanced option to start/ stop the Datastore service	TRUE/FALSE	TRUE
VAR_DATASTORE_DATA_LOCATION	Advanced Datastore layout option to specify Datastore server data directory for optimizing performance	Valid Path	`$USER_INSTALL_DIR$\services\datastore\`
VAR_DATASTORE_XLOG_LOCATION	Advanced Datastore layout option to specify Datastore server Xlog directory for optimizing performance	Valid Path	`$USER_INSTALL_DIR$\services\datastore\data\`
VAR_USERNAME (LINUX only)	Advanced option to specify an existing UNIX user account to install the Datastore service	Existing username	N/A

Table 8. Datastore installer variables (continued)

Variable Name	Description	Possible Values	Default Values
VAR_DATASTORE_BIND_ADDRESSES	IPAddress for Postgres to listen on	Valid IP Address	N/A
VAR_DATASTORE_CLIENTS_ADDRESSES IPAddress of	IP Address of Application server(s) which will connect to the Datastore service	Valid IP Addresses separated by ", "	N/A
VAR_APOLLO_USER_PASSWORD	Data Protection Advisor Datastore password	[Set at installation or reset using Data Protection Advisor CLI.]	N/A

Table 9. Datastore Advanced options Replication variables

Variable Name	Description	Possible Values	Default Values
VAR_DATASTORE_REPLICATION	Role for Datastore replication	MASTER/SLAVE	N/A
VAR_DATASTORE_REPLICATION_	The IP address of primary Datastore or secondary Datastore. If VAR_DATASTORE_REPLICATION_ROLE is set as "MASTER", then the secondary Datastore's IP address must be entered, and vice versa when VAR_DATASTORE_REPLICATION_ROLE is set as "SLAVE "	Valid IP address of primary Datastore or secondary Datastore	N/A

Table 10. Datastore Agent variables

Variable Name	Description	Possible Values	Default Values
VAR_AGENT_APPLICATION_ADDRESS Data Protection Advisor Server FQDN or IP Address to manage the Datastore Agent	Data Protection Advisor Server FQDN or IP Address to manage the Datastore Agent In case of linux IPv6, <IPv6Address>%<Interface_Id_Of_Datastore_Agent>	Valid IP Address or hostname	For multiple application servers and for cases where the Datastore service is communicatong with linux IPv6 application server(s), this value will be empty. Otherwise the default value is the same as `VAR_DATASTORE_CLIENTS_ADDRESSES`
VAR_AGENT_START_SERVICE	Advanced option to start/ stop Datastore Agent after install	TRUE/FALSE	TRUE
VAR_AGENT_ORACLE_DIRECTORY	Advanced option used for monitoring Oracle by the Datastore Agent. Path where the Oracle Database device driver files can be found	Valid Path	N/A
VAR_AGENT_PASSWORD	Agent registration password		

Table 11. Application installer variables

Variable Name	Description	Possible Values	Default Values
USER_INSTALL_DIR	Installation location	Valid Path	• Windows: `C:\Program Files\EMC\DPA`

Table 11. Application installer variables (continued)

Variable Name	Description	Possible Values	Default Values
			- Linux: `/opt/emc/dpa`
CHOSEN_INSTALL_SET	Installation set	APP	N/A
VAR_CUSTOM_SERVICE_USER	Linux silent installation under non-root user	TRUE/FALSE	
VAR_SERVICE_USER	Linux silent installation under non-root user	Username	
VAR_SERVICE_USER_SWITCHED	Linux silent upgrade installation if user changes	TRUE/FALSE	
VAR_CUSTOM_SERVICE_USER	Windows silent installation under non-root user		
VAR_SERVICE_USER	Windows silent installation under non-root user	Username	
VAR_SERVICE_USER_PASSWORD	Windows silent installation under non-root user		
VAR_SERVICE_USER_SWITCHED	Windows silent upgrade installation if user changes	TRUE/FALSE	
VAR_INSTALL_SERVICE	Advanced option to Install the Application Service	TRUE/FALSE	TRUE
VAR_START_SERVICE	Advanced option to start/ stop the Application service after installation	TRUE/FALSE	TRUE
VAR_APPLICATION_DATASTORE_ADDRESS	IPAddress of the Datastore server	Valid IP Address where Datastore service is installed and running	N/A
VAR_ADMIN_PASSWORD	Data Protection Advisor Application administrator password	[Set at installation or reset using Data Protection Advisor CLI.]	N/A
VAR_APOLLO_USER_PASSWORD	Data Protection Advisor Datastore password	[Set at installation or reset using Data Protection Advisor CLI.]	N/A
VAR_AGENT_PASSWORD	Agent registration password		

Table 12. Application server Agent variables

Variable Name	Description	Possible Values	Default Values
VAR_AGENT_APPLICATION_ADDRESS	Data Protection Advisor Server FQDN or IP Address to manage the Application server's Agent	Valid IP Address or hostname	127.0.0.1
VAR_AGENT_START_SERVICE	Advanced option to start/ stop the Application server's Agent after install	TRUE/FALSE	TRUE
AVAR_AGENT_ORACLE_DIRECTORY	Advanced option used for monitoring Oracle by the Application server's Agent. Path where the Oracle Database device driver files can be found	Valid Path	N/A

Table 12. Application server Agent variables (continued)

Variable Name	Description	Possible Values	Default Values
VAR_AGENT_PASSWORD	Agent registration password		

Table 13. Standalone Agent Installer variables

Variable Name	Description	Possible Values	Default Values
USER_INSTALL_DIR	Installation location	Valid Path	● Windows: `C:\Program Files\EMC\DPA` ● Linux: `/opt/emc/dpa`
VAR_AGENT_APPLICATION_ADDRESS	Data Protection Advisor Server FQDN or IP Address to manage this Agent Valid IP Address or hostname.	In case of linux IPv6, <IPv6Address>%<Interface_Id_Of_Agent>	N/A
VAR_AGENT_START_SERVICE	Advanced Option to start/stop the Agent after install	TRUE/FALSE	TRUE
VAR_AGENT_ORACLE_DIRECTORY	Advanced option used for monitoring Oracle. Path where the Oracle Database device driver files can be found	Valid Path	N/A
VAR_CUSTOM_SERVICE_USER	Linux silent installation under non-root user	TRUE/FALSE	
VAR_SERVICE_USER	Linux silent installation under non-root user	Username	
VAR_SERVICE_USER_SWITCHED	Linux silent upgrade installation if user changes	TRUE/FALSE	
VAR_CUSTOM_SERVICE_USER	Windows silent installation under non-root user	TRUE/FALSE	
VAR_SERVICE_USER	Windows silent installation under non-root user	Username	
VAR_SERVICE_USER_PASSWORD	Windows silent installation under non-root user		
VAR_SERVICE_USER_SWITCHED	Windows silent upgrade installation if user changes	TRUE/FALSE	
VAR_AGENT_PASSWORD	Agent registration password		

Install Data Protection Advisor on SLES 15 and later

Perform the following steps to install Data Protection Advisor on SLES 15 and later:

1. Install the `insserv-compat` pre-requisite package. Type the following command to check if the `insserv-compat` package is installed or not:

   ```
   sudo rpm -q insserv-compat
   ```

   If it is not installed, type the following commands:

   - `sudo zypper insserv-compat` (if you have a valid SLES subscription with licensed repositories).
   - `sudo rpm -ivh insserv-compat` (if you do not have a valid SLES subscription, manually download the package, and run this command).

2. Type the following command to copy the `/etc/os-release` file content to `/etc/SuSE-release`:

   ```
   sudo cp /etc/os-release /etc/SuSE-release
   ```

3. Install Data Protection Advisor.

The following sections provide information:

- Data Protection Advisor server installation
- Data Protection Advisor Agent installation
- Installing by using command line installation

Install Data Protection Advisor on RHEL 9 and later

Data Protection Advisor installation considerations on RHEL 9 and later

Consider the following points when you install Data Protection Advisor on RHEL 9 and later:

- The `local/bin` directory must be present in the `/usr` directory.
- Data Protection Advisor 19.9 build 67 and later installation creates the Data Protection Advisor scripts in the `/etc/systemd/system` and `usr/local/bin` directories.

  > **NOTE:** On RHEL 8.x, Data Protection Advisor 19.9 build 67 and later installation creates the Data Protection Advisor scripts in the `/etc/init.d` and `usr/local/bin` directories.

- After the RHEL 9 OS upgrade, do not delete the Data Protection Advisor scripts from the `/etc/init.d` folder. You can delete the scripts only after you upgrade Data Protection Advisor to 19.9 build 67 or later.
- RHEL 9 and later must support the **systemd** service to auto-start services.
- Data Protection Advisor does not support its Health service on RHEL 9 and later.

Install Data Protection Advisor on RHEL 9 and later

The following sections provide information:

- Data Protection Advisor server installation
- Data Protection Advisor Agent installation
- Installing by using command line installation

Data Protection Advisor post installation steps for secure communication

After you install or upgrade Data Protection Advisor and access the Data Protection Advisor web console, a message is displayed that indicates the Data Protection Advisor Server the status of the initialization process. The initialization process can take approximately 10 minutes to complete.

During the initialization time, Data Protection Advisor is creating the database schemas, tables, views, and the Data Protection Advisor Datastore. It also creates the various system reports and dashboards templates, the default system users, Analysis Engine Rulesets, and various other default and initial objects. Your network connection time affects the speed at which all these actions are completed. Ensure that you perform the following steps after installing Data Protection Advisor.

1. If you have upgraded or migrated to the latest version of Data Protection Advisor, delete the browsing history or cache in your browser before using the latest version of Data Protection Advisor.
2. (Optional) Carry out the following steps to verify whether initialization is still in progress or completed:
   a. If you installed on Linux and the install is done to a nondefault location, log out and back in to the session. Alternatively, run from a new login window.

      A new shell is required for the executive command paths to be found before running dpa.sh svc status.

   b. On the Data Protection Advisor Application server, go to <install_dir>\services\applications.

   c. Check the *.rar ; *.ear, and *.war files for *.deployed, *.isdeploying, or .failed extensions.

      - If files have an extension of *.isdeploying, then server initialization is still in progress.
      - If files have an extension of *.deployed, then server initialization is complete and you can log in to the Data Protection Advisor web console.
      - If files have an extension of *.failed, then server initialization failed; contact Technical Support.

3. If you have Data Protection Central, and want to register Data Protection Advisor 19.8 for SSO, follow the substeps below. If not, go to step 4:
    a. In Data Protection Central, go to **System Management** and click **Add**.
    b. Follow the prompts to add Data Protection Advisor server credentials.
    c. Right-click to the left of **Data Protection Advisor** and select **Data Protection Advisor**.
    The Data Protection Advisor web console opens using SSO.
    d. [Optional] To verify that Data Protection Advisor is registered for SSO, go to **Administration** > **Users & Security** > **SSO Authentication**.
    A table appears which contains SSO configuration information.
4. Start the web console to verify successful Data Protection Advisor installation.

    All Data Protection Advisor services must be running when you launch the web console.

    a. Start a browser and connect to Data Protection Advisor Server over https on port 9002. Ensure that all pop-up blockers are disabled. For example:

    ```
    https://<server_name>:9002
    ```

    Where <*server_name*> is the name or IP address of the server or localhost.

    Alternatively, use

    ```
    https://<server_name>:9002/flexui url
    ```

    . If you choose to continue using the Flex-based Data Protection Advisor web console.
    b. Type the username and password. Username and password fields are case-sensitive.
    c. Click **Login**
5. Add licenses to the Data Protection Advisor server.

    The Data Protection Advisor server is installed with a 90-day temporary license.

    If you are upgrading and you are not adding capacity or changing to the latest version of Data Protection Advisor functionality, no licensing changes are needed.

    The CLP license is required for new Data Protection Advisor 19.12 functionality and increased capacity on a Data Protection Advisor instance. If you are migrating from Data Protection Advisor version 5.x to the latest version of Data Protection Advisor, the existing licenses are migrated with your configuration and data. CLP and WLS license coexistence in Data Protection Advisor provides more information.

    If you are adding CLP licenses, ensure that you select license files with the .lic file extension.

    If you are adding WLS licenses, select license files with the .wls file extension.

    After you install the license file, the Data Protection Advisor web console prompts you to close so it can register the license file.
6. Log back in to the Data Protection Advisor web console.
7. (Recommended) If you added CLP licenses in step 4, register the Data Protection Advisor Application server with the ESRS-VE. This registration process enables Customer Support to service the Data Protection Advisor instance.

    Observe the following:
    - If you are upgrading a previously registered Secure Remote Services, it is possible that Secure Remote Services shows that it is already registered with the following error:

      ```
      [ERROR] This node is already registered with a Secure Remote Support Service.
      ```

      Then, Secure Remote Services shows that host IP is not available anymore with the following errors:

      ```
      [ERROR] This node failed to delete with Secure Remote Support Service.
       Offline: Validation error
      ```

      This issue is an environment issue, and does not pertain to Data Protection Advisor. The KB article 000016196 on the Dell Support site provides information. For more information about, or any issues with the KB article, contact the Dell Support team.
    - Registering Secure Remote Services after a fresh installation requires that an SRS-VE be already installed and reachable from the Data Protection Advisor Application server. If you plan to use SRS-VE for remote troubleshooting (recommended), ensure that you have the SRS-VE environment installed and configured before Data Protection Advisor installation. The Secure Remote Services Virtual Edition on Dell Technologies Online Support provides information about

SRS-VE installations. The *Data Protection Advisor Software Compatibility Guide* provides supported SRS-VE module and version information.

- Register a single Application service. The registration includes both Data Protection Advisor Datastore and Application servers.
- If you are working in a clustered environment, register the Master Application server with Secure Remote Services. Use the `dpa app con` command to check if your Application server is Master or Slave server. The CLI section provides more information.
- When prompted for Secure Remote Support username and password, provide Dell online support credentials for registration. For example:

```
dpa app support --register 10.11.110.111
Dell Data Protection Advisor
Enter Data Protection Advisor Administrator username :
Enter Data Protection Advisor Administrator password :
Enter Secure Remote Support username :
Enter Secure Remote Support password :
```

- Note the following: In a clustered environment, do not use the Application server that is registered with Secure Remote Services for scheduled reports. Any problems with the scheduled reports or data collection on the listener are propagated across the Application servers in the cluster.

a. Log in to the Application server using Remote Desktop Connection for Windows or PuTTY for Linux.

b. Type the `dpa app support --register SRS_IP` command to register a Data Protection Advisor server.

   Where *SRS_IP* is the IP address of the Secure Remote Services Gateway.

   The Infrastructure Telemetry Notice appears.

c. When prompted, type the Secure Remote Support username and password.

The output that appears indicates that the request to register the Data Protection Advisor server with IP address that you typed is approved and the command is successful.

8. (Recommended) If you registered the Data Protection Advisor Application server with the SRS-VE in step 6, enable Health Service on the Data Protection Advisor Application server. On the Data Protection Advisor Application server, type:

   a. **`$ dpa health install`**

   b. **`$ dpa health start`**

9. (Optional) If you have upgraded from a previous 6.x version and you would like to display the **PowerProtect DD Overview** dashboard and the **PowerProtect DD Details** dashboard:

   a. Go to **Dashboard** > **+ icon** > **Open Existing Dashboard**.
   The **Open Existing Dashboard** window appears.

   b. Select **PowerProtect DD**, and then click **OK**.

10. (Optional) If you are monitoring a DD Operating System 5.7 and later and would like to ensure configuration of Physical Capacity Reporting data collection:

    a. Manually assign the request to any DDOS 5.7 boxes.

    b. Run the request so that the statistics are gathered on the PowerProtect DD and the schedule is created. Then, when you are ready to run the first report, data is returned.

Self-Signed Certificate Generation

This topic shows how Self-Signed Certificate is generated in SSL.

During the installation of Data Protection Advisor (DPA), self-signed certificates are generated for both the application and the datastore. These certificates are used to establish secure SSL/TLS connections. The Datastore contains the server.crt (public key) and server.key (private key) at the \EMC\DPA\services\datastore\data directory.

SSL/TLS Configuration: PostgreSQL, which is used by DPA for the datastore, uses these certificates to encrypt client connections. The configuration file postgresql.conf has the ssl = on attribute that is enabled by default, ensuring that SSL/TLS is used for secure communications. The application generates the apollo.keystore file that is stored in the \EMC\DPA\services\standalone\configuration\ directory.

TLS Configuration and Cipher Suites

The cipher suites have been updated in the standalone.xml file. The updated cipher suites are selected to provide a balance of security and performance, ensuring that data that is transmitted over the network is encrypted and protected against unauthorized access. Secure Communications: The SSL/TLS method involves the use of a public key and a private key to encrypt and decrypt data, ensuring that all communications between the client and the datastore are secure.

NOTE: Supports TLS 1.1 and TLS 1.2, with TLS 1.2 enabled by default.

Replace a self-signed certificate with a CA signed certificate

Perform the following to replace a self-signed certificate with a CA signed certificate. DPA also allows using CA-signed certificates. External CA-signed certificates provide a higher level of security, trust, and compliance for your applications and services.

1. To generate a keypair, type the following command:

   ```
   keytool -genkey -keyalg <ALGORITHM> -alias <ALIAS_NAME> -keysize <KEY_LENGTH> -dname
   <COMMON_NAME> -keystore <KEYSTORE_FILE> -storepass <KEYSTORE_PASSWORD> -storetype PKCS12
   ```

   NOTE: DPA supports up to 2048 key size.

2. To generate a CSR (Certificate Signing Request), type the following command:

   ```
   keytool -certreq -sigalg rsassa-pss -alias <ALIAS_NAME> -keystore <KEYSTORE_FILE>
   -v -file <CSR_FILE> -storepass <KEYSTORE_PASSWORD> -ext <SubjeCT_ALTERNATIVE_NAME>
   -storetype PKCS12
   ```

3. Get the CSR file signed by a CA.
4. Transfer the P7B file onto the machine where Data Protection Advisor is installed.
5. To import the signed certificate into the keystore, type the following command:

   ```
   keytool -import -trustcacerts -alias <ALIAS_NAME> -keystore <KEYSTORE_FILE> -file
   <P7B_CERTIFICATE_FILE> -storepass <KEYSTORE_PASSWORD> -storetype PKCS12
   ```

6. Stop the Application service.
7. Take a backup of the existing `apollo.keystore`, `standalone.xml`, and `application-service.conf` files.
8. Place the `<KEYSTORE_FILE>` file under the `<DPA_HOME>/services/standalone/configuration` folder.
9. Rename the `<KEYSTORE_FILE>` to `apollo.keystore`.
10. Change the key-alias value in the `standalone.xml` file from apollokey to `<ALIAS_NAME>`.
11. Change the wrapper.java.additional.34 = -Dapollo.keystore.alias value in the `application-service.conf` file from apollokey to `<ALIAS_NAME>`.
12. Start the Application service.

Configuring antivirus software with Data Protection Advisor

Configure the following antivirus configuration. Refer to your particular antivirus software documentation for information on how to configure the software so that there is no real-time monitoring of these processes or monitoring of the files that they read.

It is not necessary to have all Data Protection Advisor file systems monitored by antivirus software, and scanning certain file systems and processes can potentially degrade overall performance due to the impact of increased disk IO activity.

1. Exclude the following files and processes from antivirus monitoring.

   If you are configuring antivirus software on Linux, the following file names will not have a `.exe` extension.

   - Data Protection Advisor Application Server:
     - `<install_dir>services\executive\wrapper.exe`
     - `<install_dir>\agent\bin\dpaagent.exe`
     - `<install_dir>\services\_jre\bin\java.exe`
   - Data Protection Advisor Datastore Server:
     - `<install_dir>\services\datastore\engine\bin\postgres.exe`
     - `<install_dir>\agent\bin\dpaagent.exe`

2. Exclude the following specific directories form being monitored by your antivirus software.

   - Data Protection Advisor Application Server:
     - `<install_dir>\services\standalone\**`
     - `<install_dir>\services\tmp\**`

    - `<install_dir>\services\shared\**`
- File space on the Data Protection Advisor Datastore Server:

  > **NOTE:** If you selected advanced file system layout during Datastore installation, then alternative directories may be used instead of the following defaults.

    - `<install_dir>\services\datastore\data\**`
    - `<install_dir>\services\datastore\data\pg_log\**`

Upgrades

You can upgrade from previous Data Protection Advisor releases to the latest version of Data Protection Advisor and minor releases. The Dell Data Protection Advisor Release Notes provide information on supported upgrades.

Note that the Data Protection Advisor upgrade installer does not provide the option to use TLS protocol version v1.2 only. Additionally, Data Protection Advisor retains your existing TLS protocol version settings after upgrade. You can change the TLS protocol version to v1.2 only after upgrade. Setting TLS protocol version 1.2 only after installation or upgrade provides information.

> **NOTE:**
> - Starting from Data Protection Advisor 19.1 and later, the datastore password is not requested during an upgrade.
> - In the case of silent upgrades for versions earlier than Data Protection Advisor 19.2, specify the datastore password in the *VAR_APOLLO_USER_PASSWORD* variable of the upgrade configuration file.

Upgrade prerequisites

There are a set of recommended best practices before you carry out an upgrade of the Data Protection Advisor server.

- Back up the Data Protection Advisor Datastore by using the `dpa ds export` command. Backup of the Datastore provides information. The Data Protection Advisor Installer prompts you to do this.
- For Datastore and Application server upgrades, the Data Protection Advisor Agent on those servers is also upgraded as part of the server upgrade. You must carry out a separate upgrade for a Data Protection Advisor Agent in the case of standalone Data Protection Advisor Agents only.
- To install Datastore on Windows 19.5 and later, install the latest VC++ Redistributable for Visual Studio 2015.
- To ensure secure communication between the Data Protection Advisor Server and Agent, set the Agent registration password using the `dpa app agentpwd` CLI command on the Data Protection Advisor Application Server host. You must also set this password on all Data Protection Advisor Agent hosts,dpa application agentpwd provides information. Then restart the Application service. Ensure that you set this password for each Agent. The exception to this is if you are concurrently running Data Protection Advisor Agents previous to version 6.5 along with the upgrade to the latest version of Agents. Upgrading Data Protection Advisor Agents previous to version 6.5 alongside Data Protection Advisor version 6.5 Agents and version 6.5 Server provides information.
- Take note of the previous Data Protection Advisor 6.x build installed on your system by running dpa app ver and recording the output. This output is important when verifying package installation.
- Stop the Data Protection Advisor Application server. Good practice is to perform a complete backup of the host running Data Protection Advisor Application server.
- Stop the Data Protection Advisor Datastore. Good practice is to perform a complete backup of the host running Data Protection Advisor Datastore server.
- If your infrastructure is running on VM, stop the Data Protection Advisor Application and Datastore servers and take a snapshot of the Data Protection Advisor Application and Datastore servers to facilitate restoring them in case of upgrade problems.
- Clear the browser cache.
- Ensure that you have admin/root privileges.
- Due to a known PostgreSQL issue, you must set additional permissions before product upgrade from previous releases to 19.1 and later. The "Authenticated Users" entity must have read and execute permissions set for the Data Protection Advisor installation folder. After upgrade is completed, you can remove this permission.
- If upgrading on UNIX/Linux, ensure that the `unzip` command for InstallAnywhere is installed on your system.

- When upgrading or installing patches in clustered environments, stop the Data Protection Advisor Application service on all servers. Upgrade the Datastore first, and then upgrade the Application servers. You must stop the Application service because when the services are on separate machines, the installer cannot stop the services.

  Start the upgraded Data Protection Advisor Application. Confirm initialization completed and that you can login to the Data Protection Advisor web console before upgrading the remaining clustered Application servers.

- In relation to the database upgrade:
  - Ensure that you have 5GB of free space for the database upgrade.
  - Ensure that you are running a LINUX version with a minimum glibc version of 2.12. If your LINUX version is running a glibc version earlier than 2.12, use the procedure provided in Upgrading Data Protection Advisor with a LINUX version running glibc earlier than 2.12
- If you are currently using Data Protection Advisor for RMAN reporting through an existing Data Protection Advisor backup license, contact your Account Representative for the Data Protection Advisor for Enterprise Applications license. The Data Protection Advisor for Enterprise Applications license allows you to expand the number of RMAN servers being reported in Data Protection Advisor when you upgrade to Data Protection Advisor 6.3 and minor releases. Enter the DDBEA license into Data Protection Advisor 6.3 and minor releases after installation. The *Data Protection Advisor 6.2 Release Notes* provides more information on the license is for DDBEA.
- If you are upgrading from Data Protection Advisor 6.1, ensure that you review and edit the retention period on collection requests to match organizational policies before upgrading. Data collection requests contain a different default retention period in Data Protection Advisor 6.1.
- For federated groups:
  - Shut down the services of the primary (federated) and secondary (regional) Data Protection Advisor servers.
  - Restore the database of the primary Data Protection Advisor server using the `export` command.
  - Make the required updates in the `apollo.node` table such as renaming Symantec Netbackup to Veritas NetBackup, and so on. Also, update other affected groups and objects.
  - Start the primary server followed by the federated servers.

Upgrading Data Protection Advisor

Perform the following procedure to upgrade Data Protection Advisor if you do not have clusters or Datastore Replication configured, and if the LINUX version you are running has a minimum glibc version of 2.12, as applicable.

Add support for Upgrading installations where the database tablespaces have been configured to reside on different filesystems.

- Ensure that you carry out the prerequisites in Upgrade prerequisites.
- Ensure that you run the installer as admin or root user.

If you are running a LINUX version that has a glibc version earlier than 2.12, follow the procedure that is provided in Upgrading Data Protection Advisor with a LINUX version running glibc earlier than 2.12

1. If you have not already done so, shut down the Application Service.
2. Upgrade the Datastore. Follow the installation steps as directed in the Installer. Ensure that the existing Data Protection Advisor installation directory is specified correctly.

   You must install the Data Protection Advisor update package in the same installation directory as your existing Data Protection Advisor package.

   Data Protection Advisor provides the option `Change service user` with `Install services under non-default account .`

   On Windows:

   - **Yes** —You must specify the valid local or domain user with **Log on as a Service** Windows policy enabled.
   - **No** —Data Protection Advisor installs the services under the Local System User.

   NOTE: Per DPA-57610, it is possible to set an incorrect domain during installation if VM is not in the domain on Windows, resulting in failed services installation.

   On Linux:

   - **Yes**— You must specify the valid local or LDAP user.
   - **No**— Data Protection Advisor displays a warning and installs the services under root User.
3. Upgrade the Application server. Follow the installation steps as directed in the Installer. Ensure that the existing Data Protection Advisor installation directory is specified correctly on the installer.

   You must install the Data Protection Advisor update package in the same installation directory as your existing Data Protection Advisor package.

Data Protection Advisor provides the option `Change service user` with `Install services under non-default account .`

On Windows:

- **Yes**—You must specify the valid local or domain user with **Log on as a Service** Windows policy enabled.
- **No**—Data Protection Advisor installs the services under the Local System User.

ⓘ **NOTE:** Per DPA-57610, it is possible to set an incorrect domain during installation if VM is not in the domain on Windows, resulting in failed services installation.

On Linux:

- **Yes** — You must specify the valid local or LDAP user.
- **No** — Data Protection Advisor displays a warning and installs the services under root User.

4. Restart the Data Protection Advisor web console.
5. Wait for the files to be deployed under the installation folder.

   In Windows: `C:\Program Files\EMC\DPA\<install_dirservices\applications`

   In Linux: `/opt/emc/dpa/services/applications`

   The Data Protection Advisor web console UI splash page displays upgrade status.
6. Carry out the steps provided in Data Protection Advisor post installation steps for secure communication.

Upgrading Data Protection Advisor Agents

1. Shut down the Data Protection Advisor Agent service.
2. Upgrade the Agent using Agent Installer suitable for your OS. Follow the installation steps as directed in the Installer.

   You must install the Agent update package in the same installation directory as your existing Data Protection Advisor package.

   Data Protection Advisor provides the option `Change service user` with `Install services under non-default account .`

   On Windows:

   - **Yes**—You must specify the valid local or domain user with **Log on as a Service** Windows policy enabled.
   - **No**—Data Protection Advisor installs the services under the Local System User.

   ⓘ **NOTE:** Per DPA-57610, it is possible to set an incorrect domain during installation if VM isn't in the domain on Windows, resulting in failed services installation.

   On Linux:

   - **Yes** — You must specify the valid local or LDAP user.
   - **No** — Data Protection Advisor displays a warning and installs the services under root User.

   Consider that during the upgrade, the Agent is stopped and as such, requests that are holding during the upgrade can be failed. After upgrade finishes, the Data Protection Advisor Agent continues to work normally.

Upgrading Data Protection Advisor Agents previous to version 6.5 alongside Data Protection Advisor version 6.5 Agents and version 6.5 Server

You may be required to run versions of the Data Protection Advisor Agent previous to 6.5, which do not support the Agent password. In such situations, if you set the Agent registration password on the Data Protection Advisor Server then all the previous version Data Protection Advisor Agents which do not support the Agent password fail to connect. Follow the procedure below to avoid this situation.

You may be required to run Data Protection Advisor Agent versions previous to version 6.5 for collecting for systems which are no longer supported, or you may have so many agents that you cannot upgrade them all at once.

1. Upgrade the Data Protection Advisor server to version 6.5.

   Do not set the Agent registration password. 3. Do not uninstall the old version of agent then install 6.5.

2. Upgrade the Data Protection Advisor Agents which require an upgrade to version 6.5 following the normal upgrade process. When you upgrade the Data Protection Advisor Agent, it does not request that an Agent password is set. This process is different from a fresh installation, which would request that an Agent password is set.

Upgrading Data Protection Advisor with a LINUX version running glibc earlier than 2.12

- Ensure that you carry out the prerequisites in Upgrade prerequisites.
- Ensure that you run the installer as admin/root user.

1. Stop the Application Service.
2. Export the Datastore. Backup of the Datastore provides information.
3. Install a new Datastore with the latest version of Data Protection Advisor and a version of LINUX that is running glibc version 2.12.
4. Import the existing Datastore to the newly installed Datastore with the latest version of Data Protection Advisor and the supported version of LINUX with glibc version 2.12
5. Point the Data Protection Advisor Application server to the newly installed and imported Datastore. Run: **`dpa app configure --master <datastore_ip>`**
6. Upgrade the Datastore. Follow the procedure provided in Upgrading Data Protection Advisor.

Upgrading with Datastore Replication enabled with Data Protection Advisor 6.3 and later

Perform the following steps to upgrade with Datastore Replication enabled.

- Ensure that you have carried out all the steps that are provided in Upgrade prerequisites.
- If you are running UNIX machines, ensure that you are a root user.
- Before upgrading, check whether the replication slot is available or not, if it is not available, create it. To create a replication slot, run the following database query in Data Protection Advisor CLI on the primary Datastore: `dpa.sh ds query "select * from pg_create_physical_replication_slot('standby1_slot');"`
- Ensure that all processes in each step are complete before starting the process in the next step.

1. Stop all Data Protection Advisor services on all Data Protection Advisor nodes:
   a. Run the `dpa app stop` command on the Application Server.
   b. Run the `dpa ds stop` command on the primary Datastore.
   c. Run the `dpa ds stop` command on the secondary Datastore.
2. Upgrade the primary Datastore.
   a. Launch the Data Protection Advisor installer and follow the prompts.
   b. Run the `dpa ds status` command to verify that the primary Datastore is running.
3. Upgrade the Application servers.
   a. Launch the Data Protection Advisor installer and follow the prompts.
   b. Run the `dpa app status` command to verify that the Data Protection Advisor Application is running.
4. Update the secondary Datastore password :
   a. (For Data Protection Advisor 19.5 and later) Rename the `recovery.signal` file to `recovery_tmp.signal`.
   b. (For Data Protection Advisor 19.5 and later) Rename the `standby.signal` file to `standby_tmp.signal`.
   c. (For releases earlier than Data Protection Advisor 19.5) Rename the `recovery.conf` file to `recovery.done`
   d. Take a backup of pg_hba.conf file and change `hostssl` to `hostnossl` and `scram-sha-256` to trust in the `pg_hba.conf` file.
   e. Run the following commands:

```
C:\Program Files\EMC\DPA\services\datastore\engine\bin> dpa ds restart
(For Windows only)cmd.exe /c chcp 1252
psql -h <current datastore IP> -p 9003 -U apollosuperuser -d template1
ALTER USER apollosuperuser WITH PASSWORD 'Dpa@12345';
```

   f. Run the `dpa ds superpwd` to change the password.

g. After the password is changed successfully, rename `recovery_tmp.signal` to `recovery.signal` and `standby_tmp.signal` to `standby.signal`.

h. Replace the existing `pg_hba.conf` file.

5. Upgrade the secondary Datastore.
   a. Launch the Data Protection Advisor installer and follow the prompts.

      If you are implementing Cascading Replication, upgrade the Datastore at the end of the chain first.
   b. Run the `dpa ds status` command to verify that the secondary Datastore is running.
6. Run the `dpa ds rep -e <replication_export_directory>` command to create a Datastore Replication Export on the primary Datastore.
7. Run the `dpa ds stop` command to stop the secondary Datastore service.
8. Run `dpa ds rep -i <replication_export_directory>` command on the secondary Datastore to import the Datastore Replication export from the primary Datastore to the secondary Datastore.
9. Run the `dpa ds start` command to start the secondary Datastore service.
10. Verify that Datastore Replication is running. Run:

    `dpa ds rep status`

    Output should show STREAMING.

Upgrading with Datastore Replication enabled with Data Protection Advisor versions earlier than 6.3

Upgrading with Datastore Replication is automated and does not require user interaction, except when upgrading the Replication secondary Datastore.

- Ensure that you have carried out all the steps that are provided in Upgrade prerequisites.
- If you are running UNIX machines, ensure that you are a root user.
- Ensure that all processes in each step are complete before starting the process in the next step.

1. Stop all services:
   a. Run `# dpa app stop` on the Application Server.
   b. Run `# dpa ds stop` on the primary Datastore.
   c. Run `# dpa ds stop` on the secondary Datastore.
2. Upgrade primary Datastore:
   a. Launch the Data Protection Advisor installer and follow the prompts.
   b. Verify that Datastore Replication is running. Run: **`# dpa ds rep`**
3. Create a copy of the primary Datastore. Type: **`dpa ds rep -e <empty_dir>`**
4. Uninstall the existing secondary Datastore.
5. Install a clean Datastore Server with the same install location as the primary Datastore, and configure the newly installed Datastore Server as a secondary Datastore. Type: **`dpa.sh ds rep --role Secondary <primary_datastore_IP_address>`**.

   Do not start or stop services.
6. Initialize the secondary Datastore from the primary Datastore copy. Type: **`dpa ds rep -i <primary_datastore_copy>`**
7. Start the secondary Datastore.
8. Upgrade the Application Server.

3

Administering Data Protection Advisor

This chapter includes the following sections:

Topics:

License management

This section describes license management in Data Protection Advisor.

Evaluation license bundled with Data Protection Advisor

Data Protection Advisor is bundled with a 90-day evaluation license.

The evaluation license is created from the time of Data Protection Advisor installation, is valid for up to 90 days, and allows access to all features. If you import a license during 90-day evaluation license period, the evaluation license is removed and you have access to Data Protection Advisor features according to license you imported.

Licensing types in Data Protection Advisor

Data Protection Advisor uses the *Common Licensing Platform* (*CLP*) license type.

The CLP license coexists with and, in certain circumstances, replaces the legacy *Wysdm Licensing System* (*WLS*) license type that was previously used with DPA before the product name was changed to Data Protection Advisor.

CLP and WLS license coexistence in Data Protection Advisor

The CLP license is required for Data Protection Advisor functionality.

If you are not adding capacity or changing to Data Protection Advisor functionality from a version of Data Protection Advisor later than Data Protection Advisor 6.2, import of CLP licenses is not required. However, if you are upgrading to the latest version of Data Protection Advisor from a version of Data Protection Advisor previous to Data Protection Advisor 6.2, contact mailto:licensing@dell.com after upgrade or migration to assist you with legacy license transition to CLP licenses of all your WLS licenses. If you are migrating from Data Protection Advisor version 5.x to the latest version of Data Protection Advisor, the existing licenses are migrated with your configuration and data. You must add CLP licenses only for the latest version of Data Protection Advisor functionality or for increasing current license capacity.

CLP licenses work on a replacement model. When you import a CLP license, the CLP license replaces all the existing licenses of the same type. Also, the base and Enterprise license functionality is moved into each CLP license. You must be aware of the existing license count when you order CLP licenses of the same type, then add on the new capacity that is required and order for the total. For information about purchasing licenses for your Data Protection Advisor installation, contact your Account Representative.

A system that has been migrated or upgraded from a former Data Protection Advisor contains WLS licenses. WLS and CLP can co-exist only where they are not for the same functionality.

Expired licenses

If a license expires, a license violation warning appears in the report title for reports run from all objects enabled by the expired license. In addition, new objects cannot be added in the web console for module components enabled by an expired license.

License removal

Removing a license causes a license violation warning to appear when running reports against objects for that license. New objects of that type cannot be added in the web console until you add a replacement license.

If you are using temporary licenses that have an expiration date, the License Expiration dialog appears to notify you of the expiration of your temporary licenses within 30 days of license expiration. Permanent licenses do not display.

To enable license expiration settings, go to **User Preferences** > **Show License Expiration**.

Adding new licenses

Go to **System Settings** > **Licenses** and then click **Manage Licenses**.

Disabling automatic temporary licence expiration pop-up

Go to **User Properties** > **Show License Expiration** and uncheck the box.

Users and security

User accounts

Four default users are supplied by default within Data Protection Advisor: Administrator, Application Owner, Engineer, and User.

The Administrator account is the only account active after Data Protection Advisor installation. The user sets the Administrator account password during the Data Protection Advisor installation process.

The Administrator must set passwords for the other default user accounts before they can be used to access Data Protection Advisor. If the Administrator does not set passwords for the other user accounts, they remain in a disabled state.

Managing users

The Data Protection Advisor Administrator can manage user accounts in the **Manage Users** section. Go to **Users & Security** > **Users** > **Manage Users**. In this section the Administrator is allowed to create, edit, view and delete user accounts.

Creating a new user account

1. Go to **Users & Security** > **Users** > **Manage Users**.
2. Click **CREATE USER**.

   Alternatively, select an existing user and click **SAVE AS** to create a copy of an existing user.
3. In the **Create User Properties** tab, update the information in the respective tabs:
   a. In the **User Properties** tab, specify the name, logon name, role, authentication type and password.
   b. If the user is to be authenticated by using LDAP, choose the LDAP authentication type.
   c. In the **Report Preferences**, **Preferences**, and **Appearance** tabs, assign preferences and appearance settings. Note that the role you assign to the user determines which areas of Data Protection Advisor they can access.
   d. Click **OK** to confirm the settings.

Editing and deleting user accounts

The Data Protection Advisor Administrator can edit or delete any Data Protection Advisor user account except the default Administrator account.

1. Go to **Users & Security** > **Users** > **Manage users**
2. Select the user you would like to edit or delete.
   - Click **EDIT** to customize desired items such as the user's name, role, password, or report and appearance preferences.
   - Click **DELETE** and **OK** to delete it.

Security settings

You can configure user security settings. Go to **Users & Security** > **Users**.

Table 14. Password policy

Setting	Description
Minimum number of characters	The minimum number of characters required for the password for the Data Protection Advisor web console. The minimum and default value is 9, and the maximum value is 256. Data Protection Advisor supports only Latin characters.
Must user uppercase characters	Requires uppercase characters in the password for the Data Protection Advisor web console. Enabled by default.
Must use lowercase characters	Requires lowercase characters in the password for the Data Protection Advisor web console. Enabled by default.
Must use special characters	Requires special characters in the password for the Data Protection Advisor web console. Enabled by default.
Must use numeric characters	Requires numeric characters in the password for the Data Protection Advisor web console. Enabled by default.

Table 15. Password history

Setting	Description
Password history	Enables the limiting of password history.
Limit of password history	The number of times that Data Protection Advisor allows the user to specify an identical password for that user from the previous password. The default value is 1. The maximum value is 10. Enabled by default. If **Limit of password history** is left at **1**, that user cannot change the password to the current one. If **Limit of password history** is set to greater than 1, that user cannot change password to the current one and to the previous one. Data Protection Advisor displays a message indicating that the previous password was already configured and that the user must specify a new password.

Table 16. Login limit

Setting	Description
Login limit	Enables the limit for number of attempts to log in to the Data Protection Advisor web console.
Limit of login attempts	The number of attempts that Data Protection Advisor allows the user to log in to the Data Protection Advisor web console. The default value is 5. The range is 1–10.
Lockout timeout	The amount of time that Data Protection Advisor temporarily locks the user out of the Data Protection Advisor web console

Table 16. Login limit (continued)

Setting	Description
	after exceeding the specified login limit. The default value is 3 minutes. The range is 1–60 minutes.

Table 17. Password expiration

Setting	Description
Password expiration	Enables password expiration. The default value is off.
Password expiration period (days)	The period in days that the Data Protection Advisor password is valid. The minimum and default value is 90, and the maximum value is 365.

Table 18. Session expiration

Setting	Description
Session expiration	Enables session expiration. The default value is off.
Session expiration period (minutes)	The period in minutes that the Data Protection Advisor session is valid. The default is 15 minutes. The minimum value is 1. The maximum is 1500.

Changing user account passwords

The Data Protection Advisor Administrator can change user account passwords in **Manage Users**. Non-Administrator users can change their password in **View User Properties** by clicking the gear icon on the top-right corner of the Data Protection Advisor web console.

1. Go to **Users and Security** > **Users** > **Manage Users**.
2. Select the user account for which you wish to change the password and click **EDIT**.
3. Go to **Edit User Properties** and set the **Authentication Type** to **Password**.
4. Type the new password in the **Password** field, and then retype the password in **Confirm Password** field.

   Note the following regarding Data Protection Advisor passwords:

   - Blank passwords are not supported.
   - Minimum length is 9 characters.
   - The following are required:
     - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
     - A minimum of 1 numeric symbol
     - A minimum of 1 special character
5. Click **OK**.

Unregister SSO

You must have permission to manage system settings for Data Protection Advisor to display the **Unregister** button.

1. Go to **Users & Security** > **SSO Authentication**.
   The **DPC SSO Client Configuration** table appears.
2. Click **Unregister**.
   A confirmation message appears to ask if you are sure that you would like to unregister your SSO client configuration.
3. Click **OK**.
   Data Protection Advisor logs you out, and the Data Protection Advisor log in page appears.
4. Log in to Data Protection Advisor.
5. [Optional] Verify that Data Protection Advisor is not registered as a DPC SSO client. Go to **Users & Security** > **SSO Authentication**.
   The **DPC SSO Client Configuration** window appears along with the text: `Data Protection Advisor is not registered as an SSO client.`

User roles and privileges

Roles are used to handle the privileges that are allowed for users. Users gain their privileges by being assigned to the appropriate role.

Four roles are supplied by default within Data Protection Advisor: Administrator, Application Owner, Engineer, and User. The default user roles are set and cannot be changed.

The following table lists the default role privileges.

Table 19. User roles

User roles	Privileges
Administrator	Can perform all configuration and reporting functions.
Application owner	Can perform all reporting functions and modify credential settings.
Engineer	● Can perform all reporting functions and most configuration functions. ● \Engineers cannot create or modify users or user roles, or modify system settings.
User	Can perform reporting functions only.

Data Protection Central Admin Local role for Single Sign On in Data Protection Central

As part of the Single Sign On (SSO) support into Data Protection Advisor as a Dell Data Protection Central user, when Data Protection Central logs you in to Data Protection Advisor UI for the first time, a new administrator user is created with OPENID authentication type in Data Protection Advisor.

NOTE: If there is no existing Data Protection Advisor Administrator role, the Data Protection Central Admin Local role is assigned read-only rights

Creating a new user role

The Data Protection Advisor Administrator can create a new custom user role with custom permissions and settings.

1. Go to **Users & Security** > **Roles** > **Manage Roles**.
2. Either click **CREATE ROLE**, or choose an existing role and click **SAVE AS**.

   Choose **SAVE AS** to create a copy.
3. In the **User Role Properties** window,
   a. Type a name and description for the new role in the **Name** and **Description** fields.
   b. Set the Privileges, Accessible Groups, Dashboards, and Menus.
   c. Click **OK** to confirm the settings.

Editing and deleting user roles

The Data Protection Advisor Administrator can edit or delete only custom user roles. Default user roles cannot be edited or deleted. It is not possible to delete a role unless the users within that role have first been assigned to alternative roles.

1. Go to **Users & Security** > **Roles** > **Manage Roles**.
2. Select the custom user role you would like to edit or delete:
   - Click **EDIT**to customize the privileges, accessible groups, dashboards, and menus.
   - Click **DELETE** and **OK** to delete the user role.

Viewing users within user roles

Go to **Users & Security** > **Roles** > **Manage Roles**. The Data Protection Advisor Administrator can review the users associated with a user role in the **Manage Roles** tab by selecting a specific user role name. A list of the default roles (administrator, application owner, engineer, user) is displayed, together with any new roles added since installation.

Limiting users to see only specific groups

You can configure a Data Protection Advisor user to be able to see specific groups or backup configuration items when running reports.

The groups must already exist.

By default, users can see the entire Data Protection Advisor object inventory. However, you may want to limit what certain users see of the Data Protection Advisor object inventory. For example, service providers may have groups configured in their Data Protection Advisor object inventory which correspond to their individual customers. The service providers may want to configure it so that the individual customers see and run reports against only the specific object inventory configured in their customer group when they log in to Data Protection Advisor.

1. Go to **Users & Security** > **Roles** > **Manage Roles**.
2. Create the custom role that you require, or select the custom user role you would like to edit and click **EDIT**.
3. Select the **Accessible Groups** tab.
   The list of all available groups is displayed
4. Select the group that will be accessible by the role and click **>** or **>>** to move all groups.
5. Click **OK** to confirm the settings.

Restricting user groups

You can restrict user groups so that certain user groups or roles can set values for custom attributes without the ability to update system attributes or create or change groups.

- Ensure that you log in to the Data Protection Advisor server as Administrator.

1. Create the Read Inventory role:
   a. Go to **Admin** > **Users & Security** > **Manage Roles** and click **Create Role**.

      The **User Role Properties** dialog appears.

   b. Populate the fields accordingly:

      In the **Name** field, type the name you would like to give to your role. For example, **Read Inventory**.

      In the **Description** field, type a description if you would like to do so.

   c. In the **Privilges** tab under **Inventory**, select **View existing objects and group management**.
   d. In the **Accessible Groups**, select the groups that you would like to view, click **Move selected groups** and then click **Close**.
2. Create the Read Inventory user:
   a. Go to **Admin** > **Users & Security** > **Manage Users** and click **Create Role**.

      The **Create User Properties** dialog appears.

   b. Populate the fields accordingly:

      In the **Name** field, type the name you would like to give to your user. For example, **Read**.

      In the **Logon** field, specify the logon the user should type. For example, `Read`.

      In the **Role** field, select the one that you created in step 1 for the Read Inventory role.

      In the **Authentication** field, select the desired authentication type from the dropdown. If you choose Password, specify and confirm a password.

   c. Click **OK**.
3. Create the Assign Attribute and Read Inventory Role:
   a. Go to **Admin** > **Users & Security** > **Manage Roles** and click **Create Role**.

      The **User Role Properties** dialog appears.

   b. Populate the fields accordingly:

In the **Name** field, type the name you would like to give to your role. For example, **Assign Attribute and Read Inventory Role**.

In the **Description** field, type a description if you would like to do so.

c. In the **Privileges** tab under **Inventory**, select **Assign/unassign attributes**.

The **View existing objects and group management** privilege is selected automatically.

d. In the **Accessible Groups** tab, select the groups that you would like to view, click **Move selected groups** and then click **Close**.

4. Create the Assign Attribute and Read Inventory user:

a. Go to **Admin** > **Users & Security** > **Manage Users** and click **Create Role**.

The **Create User Properties** dialog appears.

b. Populate the fields accordingly:

In the **Name** field, type the name you would like to give to your user. For example, **Assign**.

In the **Logon** field, specify the logon the user should type. For example, **`Assign`**.

In the **Role** field, select the one that you created in step 3 for the Assign Attribute and Read Inventory role.

In the **Authentication** field, select the desired authentication type from the dropdown. If you choose Password, specify and confirm a password.

c. Click **OK**.

External authentication, LDAP integration, and binding

Data Protection Advisor supports configuring an external authentication method via the Lightweight Directory Access Protocol (LDAP). Data Protection Advisor supports Microsoft Active Directory and OpenLDAP as LDAP servers

User account passwords are stored in the Data Protection Advisor Datastore only when the internal authentication method is configured. In the external authentication method the passwords are stored in the LDAP server. To enable LDAP authentication, select **Users & Security** > **External Authentication** > **Manage External Authentication**.

Data Protection Advisor supports two LDAP binding methods: anonymous bind and simple bind. To configure anonymous bind, ensure that the **Anonymous Bind** checkbox is checked in the **Manage External Authentication** tab. For simple bind, ensure that the **Anonymous Bind** checkbox is unchecked. Also, ensure that the username and password of a user with read base access is set.

LDAP authentication configuration

The following table lists the fields that you can use to configure the LDAP Authentication in Data Protection Advisor.

Table 20. LDAP Authentication configuration in Data Protection Advisor

Field	Description
Server	Hostname of the LDAP server. The hostname must be resolvable from the Data Protection Advisor server.
Use SSL	Select this option to connect to the LDAP server using an SSL connection.
Port	Port that the LDAP server listens on for requests: ● port 389 for non-SSL connections ● port 636 for SSL connections When you use Microsoft Active Directory configured as a Global Catalog server, specify the following in the Manage External Authentication dialog: ● port 3268 for non-SSL connections ● port 3269 for SSL connections
LDAP Version	Version of LDAP that is used on the server. Data Protection Advisor supports versions 2 and 3.

Table 20. LDAP Authentication configuration in Data Protection Advisor (continued)

Field	Description
Base Name	Location of all possible users. This location will be used as the starting point for all queries against the directory. The value entered must be the Distinguished Name of the base of the directory, for example, DC=eng,DC=company,DC=com.
Identification Attribute	The attribute in LDAP or Active Directory that is used to search for a user account, for example, sAMAccountName (Active Directory) or uid (OpenLDAP)
Anonymous Bind	Data Protection Advisor supports two different LDAP bindings: ● Anonymous Bind - Check the checkbox to connect to the LDAP server with Anonymous Bind ● Simple Bind - Leave the checkbox unchecked to use Simple Bind. This enables the Username and Password fields
Username	The bind DN of the user on the LDAP server permitted to search the LDAP directory within the defined search base.
Password	User password.
Validate	Click to test user authentication with the LDAP server. A message displays whether or not connection to the LDAP server successfully occurred.

Creating a new user account with LDAP authentication

As the Data Protection Advisor Administrator, once you have configured and tested the LDAP binding you can create or edit the user accounts that need to be authenticated by the LDAP server.

1. Go to **Users & Security** > **External Authentication** > **Manage External Authentication**
2. Set the **LDAP** value in the **Authentication type** field.
3. Provide the user's Distinguished Name (DN) or the Identification Attribute value in the **External Name** field.

   With the Active Directory integration, the Identification Attribute value is typically the sAMAccountName. With OpenLDAP, it is typically UID.

Multifactor authentication

Starting with Data Protection Advisor 19.7, you can enable multifactor authentication in Data Protection Advisor using RSA SecurID for Data Protection Advisor application users.

Multifactor authentication (MFA) is an authentication method that requires you to provide two or more forms of identity verification before you are allowed access to the Data Protection Advisor application. The main benefit of MFA is enhanced application security.

To use MFA, you must register on the RSA server and Data Protection Advisor and provide the RSA server details in the **RSA Authentication** page. After you are identified, enable RSA and provide the RSA token details to log in to the application.

Configure multifactor authentication using RSA SecurID

To enable multifactor authentication using RSA SecurID, perform the following:

- RSA Secure ID Authentication Manager must be configured.
- Data Protection Advisor users who are created on the local database or LDAP must have the same username in the RSA server also.
- Ensure that the required port is open and enabled. Port number 5555 is the default port.

1. Log in to Data Protection Advisor as administrator.
2. Go to **Users & Security** > **RSA Authentication**.
   The RSA Authentication Manager page appears.
3. Select **MFA Enabled** to enable multifactor authentication.
4. Enter the RSA client ID in the **`RSA Client Id`** field.
5. Enter the RSA base URL in the **`RSA Base Url`** field.
6. (Optional) Enter the RSA access ID in the **`RSA Access Id`** field.
7. Enter the RSA access key in the **`RSA Access Key`** field.
8. (Optional) Enter the RSA root certificate details in the **`RSA Root Cert`** text box.
9. Click **TEST** to verify RSA authentication.
10. Click **SAVE** to save the RSA authentication settings.

    ⓘ **NOTE:** The **Save** button is enabled only if the RSA verification is successful.

Automated user provisioning

Automated user provisioning is available in Data Protection Advisor when it is integrated with an LDAP server. Enabling the Auto Login feature makes it possible for Data Protection Advisor to automatically create a user account when a new user successfully logs in to Data Protection Advisor.

The user role assigned to the new user can be configured in the **Auto Login** tab. The Administrator can configure a default User Role or a role based on LDAP group mapping.

Auto-login—Default user role

When a default user role is set in the Auto login tab, this role is assigned to all new users automatically created by Data Protection Advisor. You can view the complete list of users created with the Auto login feature in the **Manage Users** tab. They will have the value *LDAPAUTO* in the Authentication type field.

1. Configure and test LDAP integration in Data Protection Advisor.
2. Go to **Users & Security** > **External Authentication** > **Manage External Authentication** > **Auto Login Properties** .
3. Select **Enable Auto Login**.
4. Select a role in the Default User Role drop-down list.
5. Click **OK** to confirm the settings.

   When you successfully authenticate using Auto-login, Data Protection Advisor automatically creates a user account for you within Data Protection Advisor.

Auto login—LDAP group mapping

As Data Protection Advisor Administrator, you can map specific LDAP groups to Data Protection Advisor user roles in the Auto Login settings.

1. Configure Auto login with a default user role.
2. Check the **Enable Group Mapping** checkbox to enable Group Mapping:
   - In the **Group Base** field, specify the Distinguished Name of the group. For example, **`cn=users,dc=eng,dc=company,dc=com`**
   - In the **Group Attribute** field, specify the LDAP attribute used for the group search. Typically this is either *CN* or *sAMAccountName* for Active Directory or *uid* for OpenLDAP.
   - In the **Group Member Attribute** field, specify the attribute that specifies members of the group. Typically this is either *member* for Active Directory or *memberUid* for OpenLDAP.
3. Click **Add** to add a new line to the **Group Mapping** section.
4. In the **LDAP Group Name**, set the name of the group to map with the user role.
5. In the **DPA User Role**, choose one of the available roles from the drop-down list.
6. Use **ADD**, **REMOVE**, **UP**, and **DOWN** to organize the Group Mapping.
7. Click **OK** to confirm the settings

Group Mapping

The group mapping feature allows Data Protection Advisor to map specified LDAP groups to Data Protection Advisor roles so that you can be assigned different Data Protection Advisor roles depending on the LDAP groups that you are in.

If you are a member of multiple LDAP groups, you are granted the Data Protection Advisor role that is mapped to the first group in the mapping table. Ensure that the LDAP group that maps to a Data Protection Advisor role with greater permissions is highest in the list. A user that is not a member of a group in the Group Mapping list is assigned the Default User Role. **Up** and **Down** buttons are provided to enable table entries to be moved to the desired positions in the table.

Configuring LDAP integration—scenario settings

The following table lists the LDAP integration scenarios and the corresponding example settings.

Table 21. Open LDAP server settings

Setting description	Setting
Server name	lab.emc.com
LDAP administrator	cn=admin dc=lab,dc=emc dc=com
Groups	Administrators: cn=administrators,ou=groups,dc=lab,dc=emc,dc=com
	Users: cn=users,ou=groups,dc=lab,dc=emc,dc=com
	Support: cn=support,ou=groups,dc=lab,dc=emc,dc=com
Users	Paul Abbey: uid=PAbbey,ou=people,dc=lab,dc=emc,dc=com (Users member)
	John Smith: uid=JSmith,ou=people,dc=lab,dc=emc,dc=com (Support member)
	Tom Baley: uid=TBaley,ou=people,dc=lab,dc=emc,dc=com (Marketing member)

Scenario: Configuring LDAP integration with Simple Bind

1. Go to **Users & Security** > **External Authentication** > **Manage External Authentication**.
2. Verify or type the following values in the User fields:
   - **Use LDAP Authentication**: selected
   - **Server**: `lab.emc.com`
   - **Use SSL**: selected (optional)
   - **Port**: `686`
   - **LDAP Version**: `3`
   - **Base Name**: `dc=lab,dc=emc,dc=com`
   - **Identification Attribute**: `uid (sAMAccountName for Active Directory integration)`
   - **Anonymous Bind**: Cleared
   - **Username**: `cn=admin,dc=lab,dc=emc,dc=com`
   - **Password**: `<admin_password>`
3. Click **Validate** to verify the LDAP binding.
   If the validation fails, check the LDAP connectivity from the Data Protection Advisor Application server and the LDAP server parameters.
4. Click **Test user** to verify the LDAP binding.

   Use the following username and password:

   Username: `PAbbey`

   Password: `<PAbbey_password>`
5. Click **TEST** to verify the LDAP user authentication.
   If the authentication fails, check if the username and password are correct in the LDAP server.

6. Click **OK** in the **Manage External Authentication** to confirm settings and close.
7. Go to **Users & Security** > **Users** > **Manage Users** and click **CREATE USER**.
8. Type the following values in the **User Properties** tab:
   - **Name**: `Paul Abbey`
   - **Logon**: `Pabbey`
   - **External Name**: `PAbbey`
   - Role: **User**
   - Authentication Type: **LDAP**
9. Click **OK** and verify that the account is in the user account list.

Scenario: Configuring automated user provisioning with group mapping

1. Go to **Users & Security** > **External Authentication** > **Manage External Authentication**.
2. Verify or type the following values in the User fields:
   - **Use LDAP Authentication**: selected
   - **Server**: `lab.emc.com`
   - **Use SSL**: selected (optional)
   - **Port**: `686`
   - **LDAP Version**: `3`
   - **Base Name**: `dc=lab,dc=emc,dc=com`
   - **Identification Attribute**: `uid (sAMAccountName for Active Directory integration)`
   - **Anonymous Bind**: Cleared
   - **Username**: `cn=admin,dc=lab,dc=emc,dc=com`
   - **Password**: `<admin_password>`
3. Click **Validate** to verify the LDAP binding.
   If the validation fails, check the LDAP connectivity from the Data Protection Advisor Application server and the LDAP server parameters.
4. Click **Test user** to verify the LDAP binding.

   Use the following username and password:

   Username: `PAbbey`

   Password: `<PAbbey_password>`
5. Click **TEST**.
6. Check **Enable Auto Login**, and ensure that the Default User Role selected is **User**.
7. Check **Enable Group Mapping** and verify or type the following values:
   - **Group Base**: `ou=groups,dc=lab,dc=emc,dc=com`
   - **Group Attribute**: `cn`
   - **Group Member Attribute**: **memberUid (member for Active Directory integration)**
8. Click **Add**:

   LDAP Group Name: Support

   Role: Engineer
9. Log in as John Smith.
   A new user account JSmith should be created with the Engineer role.
10. Log out.
11. Login as Tom Baley.
    A new user account TBaley should be created with the User role.

System settings

You can modify the default system settings for Data Protection Advisor agents, the server, and the datastore.

Configuring backup and restore resolution fields

Data Protection Advisor allows you to create up to five custom backup and restore resolution fields that allow you to add a resolution to a failed job, and then at a later date view the resolution to see what caused the failure.

For example, you can create a field as a reference to an external ticketing system that includes further resolution information for failed backups. Administrators can control the format of a custom field and make the field mandatory or optional.

1. Select **System Settings** > **Custom Resolutions** > **Manage Custom Resolutions**.
   The Manage Custom Resolutions dialog box appears.
2. Select an available row from the list and click **EDIT**.
   The **Resolution Custom Field** dialog box appears.
3. Select **Active** to enable the custom field.
4. Type a Label for the field.

   The field label will be used in the **Backup Resolution** and **Add Resolution** dialogs boxes.
5. Select the type of data that the custom field will hold from the **Input Cast** field.

   Data types include:
   - Flag (True or False)
   - Integer value
   - Decimal value
   - Text
6. (Optional) Select **Mandatory** to force administrators to complete a field of type Text when creating or adding resolutions. For other field types, the default value is used in the resolution if the user does not specify a value.
7. Click **OK**.

If desired, implement backup and restore resolutions in drilldown reports:

Add/View Backup Resolution actions can be used in all system reports that use the "Job Details Popup" drilldown menu.

1. Go to **Reports** > **Report Templates** > **Custom Report Templates**, select the report you wish to add the backup resolution to and click **EDIT**.
2. Select the **Preview** tab.
3. Click**DRILLDOWNS** to display the drilldown reports menu and select **Same drilldown menu for all columns**.
4. Edit or create the pop-up menu with the resolution options:
   a. Select **Action** and choose one of the backup and restore resolution options:
      - Add Backup Resolution
      - Add Restore Resolution
      - View Backup Resolution
      - View Restore Resolution

      Other options include Show selected alerts, exclude edit, gap details, show related alerts, and request history.

   b. Select **Automatic**.
   c. Click **OK**.

Viewing and editing settings

To view or edit system settings, select **System Settings**.

System Settings

The Data Protection Advisor system has settings for Data Collection Agents, Server, SharePoint, Replication Analysis, and Agentless Discovery. The following table describes each agent setting.

Table 22. Data Collection Agent settings

Setting	Description
Data Collection Agent Status	Enables collection of log files. Enabled by default.
Data Collection Agent Version	The version of the Data Protection Advisor data collection agent that is currently installed on the host.
Data Collection Agent Port	Port on which the data collection agent listens for requests.
Concurrency	Maximum number of threads the data collection agent uses to gather data. The default is five.
Log Level	Verbosity level when the data collection agent writes to the log file. For example, selecting Fatal writes only critical errors to the log file.
Log File	The location of the log file on the host.
Max Log File Size (MB)	Maximum size to which a log file can grow before the creation of a new log file (in MB). To set no limit for the size of the log file, set this value to 0.
Max Number of Log Files	Maximum number of log files maintained on the system. If a new file is created because the maximum file size of the current log file is exceeded, the oldest log file is removed.
Max Forward Queue Length	Maximum number of requests stored by the agent locally if the Server is offline. When the Server is offline, the agent processes and stores the request in the request queue only if the count of the number of requests that are stored in the queue is less than the "Max Forward Queue Length" configuration value and the total size of requests stored in the queue is less than the "Max Forward Queue Size" value. If the set value of "Max Forward Queue Length" or "Max Forward Queue Size" reaches its maximum, the agent stops further processing the request and discards it. For instance, consider the "Max Forward Queue Length" value is set to 5000 and the "Max Forward Queue Size" value is set to 500 MB. If the agent fills the 500 MB, but there is still 1000 left in the Max Forward Queue Length, the agent stops further processing the request and discards it because the total size of requests stored in the queue exceeds the set "Max Forward Queue Size" value of 500 MB.
Max Forward Queue Size (MB)	Maximum total size of all requests stored by the Data Protection Advisor data collection agent locally if the Server is offline (in MB). You can specify unlimited or specify a selected size.
Reload Data Collection Agent	Allows you to manually reload the data collection agent. This is done automatically when configuration changes are made in the Data Protection Advisor web console that affect a data collection Agent.
Remove Data Collection Agent	Removes the selected data collection agent.
Make Agent Default	Makes the selected data collection agent the default host.

Table 23. Server settings

Setting		Description
Global Data Collection Agent Settings	Binary Multiplier	Switching this global setting on, defaults all Agents to use the binary multiplier. Binary multiplier converts all incoming data as 1024 KB= 1MB. Applies to NetWorker agents only where the incoming data from Backup server is converted as 1000 KB = 1MB. Binary Multiplier is ignored when monitoring other applications.

Table 23. Server settings (continued)

Setting		Description
	Timeout(s)	Time out setting that the server uses when talking to the agent. The default is 120 seconds.
Global Email Settings	Mail Server Hostname	Mail server to which email messages are forwarded when sent from Data Protection Advisor.
	Mail From Address	E-mail address assigned to email messages sent from Data Protection Advisor.
	Mail Server Port	Mail server port number. Default value is 25 (for unauthenticated SMTP). Can also be: ● 465—for SSL/TLS security protocol ● 587—for encrypted StartTLS
	Security Protocol	Security protocol for message encryption. The default setting is None. Can also be: ● SSL/TLS ● Encrypted StartTLS ● Unauthenticated SMTP
	STARTTLS required	Option to enable encrypted StartTLS.
	Credentials	Option to select user/password credentials for SMTP configuration.
Global Logging Settings	Global Logging Settings	Global logging settings for the Analysis Engine, Configuration, Listener, Publisher, Recoverability Analysis, Reporter, and REST API. Settings can be INFO, DEBUG, DEBUG LOW, WARN, ERROR, and FATAL.
Data Deletion	Data Deletion	Schedule to delete data gathered from your environment. The default is 9 a.m. to 5 p.m. every day.
Root Cause Analysis	Root Cause Analysis Settings	Option to enable Root Cause Analysis Summary.
		Option to enable Root Cause Analysis Deletion. The default deletion setting deletes data that is older than 200 days. The period is not user-configurable.
Generate Support Bundle	Generate Support Bundle	Option to generate support zip file.
	Include all logs	Option to include all logs. If unselected, Data Protection Advisor collects only the latest log files. If selected, Data Protection Advisor collects all historical log files. Unselected by default.
DB Export	Database Export Age Notification	Option to set a time period that the Data Protection Advisor Database export is considered up to date. The default value is one week. The minimum is one day. When the time period expires and there is no fresh Data Protection Advisor Datastore export during this period, an alert is issued.
SNMP v3 Trap	SNMP version 3 Protocol Engine ID	This is a default setting auto-populated from the REST server. The parameter is user-editable in the REST server. The supported Engine ID value parameters are: ● No length restriction ● Can contain numbers ● Can contain alpha symbols: A-F

Table 24. SharePoint settings

Setting		Description
Name	Name	The user-defined name of the SharePoint site created in Data Protection Advisor SharePoint Server Settings.
Site	Site URL	The SharePoint destination URL for publications. HTTP protocol defaults to port 80, HTTPS defaults to 443. You can also specify the port explicitly. For example, to set to http port 24438 site URL, type: **`http://sharepoint-2013:24438/sites/demo2/`**.
User	Username	The username associated with the SharePoint account

Agentless Discovery

The Agentless Discovery settings are described in the following table.

Table 25. Agentless Discovery settings

Setting	Description
Sudo Program Path	The sudo program path for Agentless discovery settings. The default path is `/usr/local/bin/sudo`. The sudo command can also be located in either `/sbin` or `/usr/sbin`.
Agent Response Timeout	The time that Data Protection Advisor waits for response from the agent before timeout.
Telnet/SSH Login Prompt Timeout	The time that Data Protection Advisor waits for Telnet/SSH session to be created before timeout.
Telnet/SSH Handshake Timeout	The time that Data Protection Advisor waits for Telnet/SSH handshake before timeout.
Delete files created on the client during agentless discovery	Defines if temporary files will be deleted from the analyzed object at the end of the discovery. The default is that the files will be deleted.

Server data deletion

Data Protection Advisor implements a default data deletion schedule for collected data and system-generated data. Collected data is the data that the configured requests within Manage Data Collection Defaults gathers. System-generated data is the data that the system processes generates, such as log messages, histories of reports, and alerts.

When data exceeds the retention period, then the data is eligible for deletion. This data is then purged based on the data deletion schedule. Any unprocessed items remain in the queue until the next scheduled start time, at which point deletion of data continues.

You cannot delete a schedule that is currently used for scheduling a collected data deletion job. An error message is displayed if you attempt to do so.

The `server.log` contains the following logs:

```
Starting request history and datamine table cleanup
Checking for previous invocation by querying datamaine_cleanup_lock table.
Previous invocation is not running, so continuing current invocation..
Inserted record into datamaine_cleanup_lock table.
.
.
.
Starting Datamine Cleanup. Check Datastore Logs for more details.
.
.
```

```
.
Done with Datamine Cleanup. Check Datastore Logs for more details.
Deleted 0 rows from retentionjob
Deleted 0 rows from dpa_metric
Deleted 0 rows from reportlogentry
Deleted 0 rows from dpa_request_statistics
Deleted 0 rows from reporterjob
```

The `datastore.log` contains detailed information of the rows that are deleted from the table. The count of all the data that is deleted is tracked in the datastore logs. The deletion happens at the datastore side. For example:

```
Processing batch number 1
.
.
Deleting from request_history_datamine_type
.
.
Finished deleting from request_history_datamine_type. Deleted 10 records
.
.
.
```

Each batch deletes records from multiple tables and logs the batch result. For example:

```
Completed batch 28 in 28.162422895431519 seconds. Deleted 33891 request history rows and
27917 datamine table rows.
```

After you complete all the batches, the following message is logged:

```
Completed request history and datamine table cleanup. Total time: 8108.2374091148376
seconds, Total request history rows deleted: 3335770, Total datamine table rows deleted:
52970219, Total batches: 28
```

NOTE: If the datastore stops responding, the following server log message is displayed, if a deletion schedule is triggered: `Currently Datamine Cleanup Process is locked, Datamine Cleanup is already in progress so current invocation can not proceed`. In such a scenario, restart Data Protection Advisor using the CLI. On Windows, do not start the datastore application server from the Services window.

The default data deletion schedule is from 9:00 a.m. to 5:00 p.m daily.

Configuring Data Deletion Schedule

You can configure and specify a new schedule for use in Schedule Properties.

To configure data deletion, select **System Settings** > **Data Deletion**. The Data Protection Advisor Online Help provides more information.

Default retention periods

The following table provides information on default collected data retention periods.

Table 26. Default collected data retention periods

System information	Default retention period
Configuration data	365 days
Status data	90 days
Performance data	30 days
Job data	forever
Occupancy data	365 days

Default collected data retention periods are user-configurable within **Data Collection** > **Defaults** > **Manage Data Collection Defaults**.

The following table provides information on default system-generated data retention periods. Default system-generated data retention periods are not user-configurable.

Table 27. Default system-generated data retention periods

Policy	Default retention period
alerts (analysisalert table)	365 days
report history (reporterjob table)	365 days
agent error log entries (reportlogentry table)	14 days
request statistics (dpa_request_statistics table)	28 days

Root Cause Analysis Settings

You can set the Root Cause Analysis Summary to calculate potential root causes on a regular schedule from within the Systems Settings. You can also schedule the system to delete Root Cause Analysis results data. The Root Cause Analysis Deletion setting deletes data that is older than 200 days. The period is not user-configurable. Root Cause Analysis Summary and Deletion are enabled by default.

Disabling Root Cause Analysis Summary

Select **Support** > **Root Cause Analysis Settings**, and clear the **Enable Root Cause Analysis Summary** option.

Disabling Root Cause Analysis Deletion

Select **Support** > **Root Cause Analysis Settings**, and clear the **Enable Root Cause Analysis Deletion** option.

Gathering historical backup data using Data Protection Advisor web console

You can gather historical backup data on Avamar, BackupExec, DB2, Data Protector, NetWorker, NetBackup, Oracle RMAN, SAP HANA, and Spectrum Protect.

Consider the following when you gather historical backup data using Data Protection Advisor web console:

- You cannot gather historical backup data at the host level. You must go one level down in the configuration tree, to the application object. For example, to collect historical data from NetWorker, choose the Networker application object below the host level object.
- You can only gather historical backup from the JobMonitor requests.

1. In the web console, select **Inventory** > **Group Management**.
2. In the configuration tree, select the application object for which you'd like to gather historical backup data.

   The application object **Details** window opens.
3. In the host details window, select the **Data Collection** tab.
4. In **Data Collection**, select the JobMonitor request.
5. Right-click **Run** and select **Gather historical data**.
6. In the **Gather historical data** window, click **OK**.

   The same credentials and data options are available as for the request itself.
7. Click **Close** to the a dialog box that appears confirming that Data Protection Advisor is gathering the historical backup data.
8. Click **History** to view collected tests. The rows highlighted in orange indicate results from a historical backup gather.

Generate Support Bundle

The Generate Support Bundle option is a support tool. The Generate Support Bundle generates and saves a zip archive with provided resources in the file system directly from the Data Protection Advisor web console.

A Dell Technical Support Engineer might ask you to generate the Support Bundle and send it for analysis. The zip file is saved as the following local agent logs in the `support.zip` folder:

- dpaagent.log
- dpaagent.log.0
- dpaagent.log.1

The default location is user-configurable.

Generating the Support Bundle

1. Select **Support** > **Generate Support Bundle** and click **OK**.
2. When prompted, enter your Data Protection Advisor Administrator credentials.

Digital certificate

Data Protection Advisor uses a self-signed digital certificate for identification and encryption.

Time periods

When you run a report or create a scheduled report, you must decide the period of time over which the report is run, for example right now or last week. Several predefined time periods are provided by default and you can create custom time periods.

Creating custom time period for reports

To create a custom time period, select **System Settings** > **Time Periods** > **Manage Time Periods**.

Time zones in Data Protection Advisor

Data Protection Advisor gathers data from the environment and stores it in the Data Protection Advisor database it UTC format.

If the timestamp that the Data Protection Advisor database receives from a backup server, application, host, or switch is in a local time zone, such as EST, the Data Protection Advisor Agent converts it to UTC before sending it into the Data Protection Advisor Server. For reporting on that data, there are several settings that can be set. Time zone settings for reporting provides more information.

Time zone settings for reporting

You can set the following settings for time zones to ensure that the desired time zone displays in your Data Protection Advisor reports.

Discovered object details

After you discover an object using the Discovery Wizard, you can select the properties and choose to specify the time zone of where that object is located. In the discovered object **Details** window, select **Time zone** from the drop-down list.

User preferences

You can choose the time zone you wish data to be displayed in **User Preferences** > **View User Properties** > **Preferences**. Select the time zone from the Global Settings section, **Time zone** drop-down list.

Window properties

You can create a time period that is time-zone aware. In the **Window Properties** window, create a new time period and ensure that you select the **Adjust for time zone** option. If you select **Adjust for time zone** and the object is a backup client, Data Protection Advisor checks the parent backup server if the backup client doesn't have a time zone set explicitly on itself already, and creates a report that is time-zone aware.

Report Table Format

You can choose to configure a table style report to show the Time Zone object it was run on with the timestamp, by specifying which field to look at to find the name of the backup server. In the Report Editor, go to **Report Format** > **Table Format** > **Table Styles**. Under the Date Fields section ensure that the **Time Zone from Report Field** option is selected.

Example: Setting time zones for All Jobs report

This example shows how to set time zones on an All Jobs report for a NetWorker server that is located in the America/New York time zone for a database administrator that is located in the Europe/London time zone.

Before you change any settings, all report and display output is in UTC.

1. Go to **User Preferences** > **View User Properties** > **Preferences** and select **Europe/London** from the Global Settings section, **Time zone** drop-down list. Then click **OK**.
   When you run the All Jobs report on the NetWorker server, the Data Protection Advisor returns the report in UTC.
2. Update the time zone of the NetWorker server, which is located in New York:
   a. Go to **Inventory** > **Object Library** and navigate to the NetWorker host.
   b. Select the desired NetWorker host and in the **Details** window, select **America/New York** from the **Time zone** drop-down list.
   c. Click **OK**.

   The output remains in UTC because the user time zone setting or report setting are not yet changed. It does not change to America/New York time zone.
3. Create a custom time period that is time-zone aware. Go to **Window Properties** and create a custom time zone. Ensure that you select the `Adjust for time zone` option.
   This makes the report query for the time relative to the time zone of the object. So because the NetWorker server is in New York, Data Protection Advisor runs the query for the custom time period in the New York time zone.
4. Edit the report Table Format so that the date fields display in the time zone from your Server field and a desired date format for the time zone:
   a. In the Report Editor, go to **Report Format** > **Table Format** > **Table Styles**.
   b. Under the Date Fields section, select the desired date format from the **Date Format** drop down, and ensure that the `Time Zone from Report Field`option is selected .
   c. Click **OK**.

   Data Protection Advisor refreshes the report with the time stamps of the time zone of the NetWorker server, in this case, America/New York.

Automatic report prioritization

The default number of reports to run concurrently per Data Protection Advisor Application server is 10. You can configure the default settings. The maximum number of reports to run concurrently per Data Protection Advisor Application server is 50; the minimum number is 2.

Data Protection Advisor automatically queues reports that are scheduled to run concurrently or that are running concurrently, and automatically retries reports when the previously scheduled reports have been run. Additionally, any reports that you initiate from the web console take precedence over automated scheduled reports running from the server, including testing a scheduled alert.

In addition to giving priority to reports run from the web console, there is also a 30% minimum fixed concurrent space reserved for these reports on the server. For example, if the concurrency set is 10, three concurrent execution spaces on the server are reserved for web console reports. Hence, there can be three or more out of a maximum of 10 web console reports running at a particular instant. There can be only seven scheduled reports which can run concurrently.

Configuring concurrent report settings

To configure concurrent report settings, select **System Settings** > **Report** > **Configure Report Settings** > **Concurrency**.

After you change the concurrency setting in the Data Protection Advisor web console, ensure that you restart the Data Protection Advisor Application service. This is so that the report-engine service picks up the new concurrency value.

Schedules

Schedules are used to define when to run a scheduled report or generate a dashboard view block, or to define the backup window specified in the Protection Policy. Several predefined schedules are provided by default and you can also create custom schedules.

A schedule is made up of components that define when each schedule produces certain results or runs certain reports. The Schedule Editor provides two ways to create schedules:

- Basic editor - allows you to create schedules on a weekly basis only and edit the day and time of the schedule.
- Advanced editor - allows you to create more complex schedules by manually editing the schedule parameters.

Schedules created in the basic editor can be edited using the advanced editor. However, schedules created and saved in the advanced editor cannot be edited in the basic editor.

Creating schedules

To create a schedule, select **Admin** > **System** > **Manage Schedules**.

Manage Data Collection Defaults

A Data Protection Advisor request contains data on how and when to gather data from an object. Data collection defaults are the template that the Discovery Wizard uses to assign requests to objects. You can set the global default settings in **Data Collection** > **Defaults** > **Manage Data Collection Defaults** .

All requests have a default data-gathering frequency and a set of options that are associated with them. You can edit global data collection default values in a way that the Discovery Wizard can pick up for certain objects. The Data Protection Advisor online help provides information about editing requests.

You can gather certain types of data with Data Protection Advisor without deploying an agent on the monitored device. To do this, an agent on another computer (such as the Data Protection Advisor Server) gathers the data remotely. When you gather data remotely, the host of the agent is indicated as a proxy server. The agent uses a protocol to gather data from the remote computer and forwards it back to the Data Protection Advisor server. The protocol that is used depends on the type of data being collected.

For certain device types, such as IP switches and Fibre Channel switches, data must always be gathered remotely as it is impossible to install an agent directly on a switch.

To configure remote data collection within Data Protection Advisor, configure the details when assigning requests. If the Discovery Wizard created the objects, this configuration is already created. However, if proxy or credential details have changed, modify the details as required. Retention Periods on Requests are set on individual request using the Edit Request dialog box. Table 15 provides information about default retention periods for data collection policies.

Data collection request options by module

Data collection request options by module are described in the following table.

Table 28. Data collection request options by module

Module	Option name	Value	Description
ARCserve	dateformat	%d/%m/%Y %T which is day, month, year, and time.	The date format to be used. The `dateformat` option is present in the options for the following requests: ● Job Monitor ● Volume Status
Avamar	capacityfactor	1.075	Avamar decimal capacity factor. The `capacityfactor` option is present in the options for the following requests: ● Configuration ● Status
	dbname	mcdb	Database name. The `dbname` option is present in the options for the following requests: ● Configuration ● Job Monitor ● Status requests
	dbport	5555	Database port. The `dbport` option is present in the options for the following requests: ● Configuration ● Job Monitor ● Status requests
	amount of seconds in the job collection	86400	Changes the maximum amount of time the request gathers job data in one run of Jobmonitor. Default is 86400, which is one day in seconds. The value is configurable.
Backup Exec	dbserver	No default value	Database server\instance. The `dbserver` option is present in the options for the following requests: ● Configuration ● Job Monitor ● Status ● Volume Status
Celerra	port	No default value	HTTPS/HTTP port number in integers. The `port` option is present in the options for the following requests: ● Configuration ● Performance ● Status
	secure	True	Indicates to send requests using HTTPS instead of HTTP. The `secure` option is present in the options for the following requests: ● Configuration ● Status
	timeout	1800	HTTP request timeout, in seconds. The `timeout` option is present in the options for the following requests: ● Configuration ● Performance ● Status

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
CommVault	appversion	0	The version of CommVault to use. The `appversion` option is present in the options for the following requests: ● Configuration ● Client Occupancy ● Job Monitor ● Status ● Volume Status
	dbserver	No default value	DB server name. The `dbserver` option is present in the options for the following requests: ● Configuration ● Client Occupancy ● Job Monitor ● Status ● Volume Status
	setBackupJobsWithErrsToSuccess	False	If set to *True*, Data Protection Advisor reports commvault backup jobs' that were completed with *Completed w/one or more errors* status as successful jobs. The `setBackupJobsWithErrsToSuccess` option is present in the Job Monitor request.
PowerProtect DD	timeout	10	SSH Timeout value in seconds. The `timeout` option for SSH is present in the options for the following requests: ● Analysis ● Configuration SSH ● Performance SSH ● Status SSH ● SSH PCR
	timeout	10	SNMP Timeout value in seconds. The `timeout` option for SNMP is present in the options for the following requests: ● Configuration ● Performance ● Status
Data Protector	timeout	900	The timeout value in seconds for running commands for the Configuration request
	timeout	300	The timeout value in seconds for running commands. The `timeout` option is present in the options for the following requests: ● Internal Database ● Job Monitor ● Service Status ● Status ● Volume Status
	ignorefailedclones	False	Indicates not to collect information about source objects for failed clone jobs for the Job Monitor request
	nojobmedia	False	Indicates not to collect media information associated with each job for the Job Monitor request

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
	occupancy	False	Indicates to enable gathering of occupancy statistics for the Job Monitor request
	timeformat	No default value	omnidb time format for the Job Monitor request.
DB2	amount of seconds in the job collection	86400	Changes the maximum amount of time the request gathers job data in one run of Jobmonitor. Default is 86400, which is one day in seconds. The value is configurable.
	database port	50000	Database port. The `dbport` option is present in the options for the following requests: ● Job Monitor
	grace period for job	0	The grace period for the agent to look back and gather data for each request Job Monitor request, in seconds. The value is configurable. The minimum value is 0; the maximum value is 1000000.
EDL	timeout	10	SNMP timeout value in seconds. The `timeout` option is present in the options for the following requests: ● Configuration ● Performance ● Status
Fibre Channel Switch	timeout	10	SNMP timeout value in seconds. The `timeout` option is present in the options for the following requests: ● Configuration ● Performance ● Status
Host System Monitoring	disk	True	Indicates to include host disk information for the Configuration and Replication request
	ESXRequestParameters .ESX_CREDENTIALS	No default value	ESX server credentials for the Configuration and Replication request
	ESXRequestParameters .ESX_SERVER	No default value	Name of the ESXServer server to be used the Configuration and Replication request
	fchba	True	Include host FC HBA information. The `fchba` option is present in the options for the following requests: ● Configuration and Replication ● Performance ● Status
	fs	True	Include host filesystem information. The `fs` option is present in the options for the following requests: ● Configuration and Replication ● Performance ● Status
	host	True	Include basic host information. The `host` option is present in the options for the following requests: ● Configuration and Replication ● Status

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
	logical	False	Include logical network interfaces. The `logical` option is present in the options for the following requests: ● Configuration and Replication ● Performance ● Status
	memory	True	Include host memory information. The `memory` option is present in the options for the following requests: ● Configuration and Replication ● Performance ● Status
	netint	True	Include host network interface information. The `netint` option is present in the options for the following requests: ● Configuration and Replication ● Performance ● Status
	remote	False	Include remotely mounted filesystems. The `remote` option is present in the options for the following requests: ● Configuration and Replication ● Performance ● Status
	srm	True	Utilize srm libraries for disk/fs information for the Configuration and Replication request
	Time Offset(seconds)	0	Time Offset in seconds for the Configuration and Replication request
	disk	True	Include host disk information. The `disk` option is present in the options for the following requests: ● Performance ● Status
	fullpath	False	Include the full path of the process name for the Status request
	process	True	Include host running processes information for the Status request
	specific	No default value	Monitor the named process only for the Status request; Windows only.
Illuminator clarapi Engine Discovery	TIME_OFFSET_OPTION	0	Time offset in seconds for the illuminator clarapi engine discovery request
HP Disk Array	port	5989	CIM provider port for HP EVA disk arrays. The `port` option is present in the options for the following requests: ● Configuration ● Status
HP Virtual Library System	port	5989	Port to the HP VLS disk arrays. The `port` option is present in the options for the following requests: ● Configuration

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
			- Status
	SSLflag	True	SSL flag is enabled for HP VLS disk arrays. The `SSLflag` option is present in the options for the following requests: - Configuration - Status
	timeout	600	Timeout in seconds for HP VLS disk arrays. The `timeout` option is present in the options for the following requests: - Configuration - Status
Illuminator symapi Engine Discovery	Symapi Version	No default value	Indicates the SYMAPI version for the illuminator symapi engine discovery request
	TIME_OFFSET_OPTIO N	0	Time offset in seconds. The `TIME_OFFSET_OPTION` option is present in the options for the following request: - illuminator symapi engine discovery
	SYMAPI DB Path	No default value	Indicates the SYMAPI database path for the illuminator symapi engine discovery request
IP Switch	timeout	10	Timeout value in seconds for the Status, Performance, and Configuration requests
SQL Server Database	dbparams	No default value	XML specifying per database parameters/ credentials. The `dbparams` option is present in the options for the following requests: - Configuration - Job Monitor - Status
	dbport	1433	Database port. The `dbport` option is present in the options for the following requests: - Configuration - Job Monitor - Status
	HomeDir	No default value	Application home directory information for the mssql application discovery request
	Tools Director	No default value	Tools directory property information for the mssql application discovery request
	Virtual Computer Name	No default value	Virtual computer name property information for the mssql application discovery request
	Number of (rotated) error log files to check for failed backups	Default value is 6	Use this option to determine the number of log files to be read. A larger number allows you to read older logs. The value must be greater than 0.
NearStore	timeout	10	SNMP timeout value in seconds. The `timeout` option is present in the options for the following requests: - Configuration - Performance - Status

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
NetBackup	timeout	300	Command timeout in seconds. The `timeout` option is present in the options for the following requests: ● Client Occupancy ● Configuration ● Job Monitor ● Media Server Status ● Status ● Volume Status ● SLP Job Status
	EMMserver	No default value	Hostname of Enterprise Media Manager (EMM) server; required only if not the primary server host. The `EMMserver` option is present in the options for the following requests: ● Configuration ● Status
	timeformat	No default value	License expiration date time format for the Configuration request
	timeformat	No default value	bpdbjobs time format for the Job Monitor request
	partialasfailed	False	Mark partially successful jobs as failed for the Job Monitor request
	Whether to include container jobs	False	If set to `True` Data Protection Advisor also gathers the row for the parent/container job, in addition to the child jobs. Can be set for the Default request or on individual objects.
	Max data time range each request will gather	86400	Changes the maximum amount of time the request gathers job data in one run of SLP Job Status. Default is 86400, which is one day in seconds. The value is configurable.
NetWorker	command timeout	3600	The timeout in seconds, used for running external commands to gather data. The `command timeout` option is present in the options for the following requests: ● Configuration ● Status ● ClientStatus ● JobMonitor ● Occupancy ● Volume Status
	mminfo timeformat	No default value	The format that timestamps in the media database are returned in bpdbjobs time format. This is used to decode the start time/end time for a Job. By default, this option is disabled and the module attempts to automatically calculate this value. The `mminfo timeformat` option is present in the Job Monitor request.
	include jobs from media DB	True	Allows you to switch off the search for successful jobs from the NetWorker Media database. Data Protection Advisor searches the Media database in addition to the NetWorker

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
			Jobs database for completed jobs. If you are not using an external scheduler to initiate backups, then set this to `False` to speed up running the Job Monitor request The `include jobs from media DB` option is present in the Job Monitor request.
	max batch period of each request data poll	86400	Changes the maximum amount of time the request gathers job data in one run of Jobmonitor. Default is 86400, which is one day in seconds. The value is configurable.
NetWorker	individual ping timeout	10	The timeout in seconds, used for timing out ping responses from backup clients. The `individual ping timeout` option is present in the Client Status request.
	nsrexecd port	7937	The NetWorker client process listen port. The `nsrexecd port` option is present in the Client Status request.
	Number of concurrent pings	20	The number of clients to ping at any one time. The `Number of concurrent pings` option is present in the Client Status request.
	List of critical clients to ping	No default value	The name of the file that holds a comma separated list of critical clients to ping instead of all clients . The `List of critical clients to ping` option is present in the Client Status request.
	Path and name of file used to store temporary occupancy data before processing	No default value	Path and name of file used to store temporary occupancy data before processing. The value should be a valid path on the Agent host. For example, on Windows use `C:\temp` and on UNIX/Linux use `/tmp`. You may need to restart the Agent after enabling for the option to take effect. The `Path and name of file used to store temporary occupancy data before processing` option is present in the Occupancy request.
	Forces short client names	true,false	Whether to return the short version of the client name or not. The `Forces short client names` option is present in the options for the following requests: ● Configuration ● Status ● ClientStatus

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
			● JobMonitor ● ClientOccupancy
	time format used to determine bootstrap time	False	Specifies the time format used to decode timestamps returned in the results from NetWorker. By default, this option is not enabled and the module use a best-guess method to decode the time format. The `time format used to determine bootstrap time` option is present in the Status request.
	time format used to determine volume access time	False	Time format to use when decoding timestamps regarding the last time a volume was accessed. By default, this option is not set and the module attempts to calculate a time format automatically. The `time format used to determine volume access time` option is present in the Volume request.
	time format used to determine volume retention period	False	Time format to use when decoding timestamps regarding the retention time for a volume. By default, this option is not set and the module attempts to calculate a time format automatically. The `time format used to determine volume retention period` option is present in the Volume request.
	Whether to include failed jobs which are retried	False	The Data Protection Advisor Agent gathers only the final status of a backup job. If the job option is set to `False` and there is a long delay before the job runs, then the retry fails then this delays the reporting of the job failure. If the retry succeeds, the Data Protection Advisor Database has one entry for the job and that entry shows the job as a success. If the job option is set to `True`, the Data Protection Advisor Agent gathers all failed tries and the final status of the job and sends them to the Data Protection Advisor database. For example, if the job is retried once and succeeds, the Data Protection Advisor database records 2 entries for the job, 1 with a failure and 1 with a success. If both tries fail, then the Data Protection Advisor database records 2 job entries in the Data Protection Advisor database, both as failures.

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
			You can use the All Jobs - No Restarts report to filter out the failed attempts and show only the final status of the job.
Oracle	dbparams	No default value	XML specifying per schema parameters/ credentials. The `dbparams` option is present in the options for the following requests: ● Configuration ● Status
	dbport	1521	Database port integer. The `dbport` option is present in the options for the following requests: ● Configuration ● Status
	HomeDir	No default value	Application home directory information for the oracle application discovery request
	ArchivesPattern	No default value	Application archive pattern information for the oracle application discovery request
	LogPattern	No default value	Application log pattern information for the oracle application discovery request
	LogsDir	No default value	Application log directory information for the oracle application discovery request
PostgresSQL Database	dbparams	No default value	XML specifying per schema parameters/ credentials. The `dbparams` option is present in the options for the following requests: ● Configuration ● Status
	dbport	5432	Database port. The `dbport` option is present in the options for the following requests: ● Configuration ● Status
	initialdb	postgres	Initial database to connect to this port.. The `initialdb` option is present in the options for the following requests: ● Configuration ● Status
PowerProtect Data Manager	port	8443	HTTPS port used to connect to PowerProtect Data Manager instance REST API.
	connecttimeout	20	Timeout for network connect attempts (in seconds).
	timeout	60	Timeout for requests sent to REST API (in seconds).
RecoverPoint	scanforrecover	False	Scan for Recoverability for the configuration request
	Time Offset (in seconds)	0	Time offset in seconds for the configuration request
	timeout	300	SSH timeout value in seconds. The `timeout` option is present in the options for the following requests: ● Configuration

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
			- Performance cs - Performance
	filename	long_term_stats.tar.gz	Statistics filename for the performance cs request
	workdir	../tmp	Working directory for the performance cs request
RecoverPoint for VMs	Time Offset (in seconds)	0	Time offset in seconds for the configuration request
	timeout	300	REST API timeout value in seconds. The `timeout` option is present in the options for the following requests: - Configuration - Performance CS - Performance - Status
RMAN	dbport	1521	Oracle TNS listener port. The `dbport` option is present in the options for the following requests: - Job Monitor Control File - Job Monitor Recovery Catalog
	amount of seconds in the job collection	86400	Changes the maximum amount of time the request gathers job data in one run of Jobmonitor. Default is 86400, which is one day in seconds. The value is configurable.
	RMAN Schema	No default value	N/A
	Single DB Query	No default value	The Single DB Query option enables the collection of data for all Oracle databases at a time.
SAP HANA	database port	30115	Database port for the Job Monitor request
	amount of seconds in the job collection	86400	Changes the maximum amount of time the request gathers job data in one run of Jobmonitor. Default is 86400, which is one day in seconds. The value is configurable.
Tape Library	timeout	10	SNMP Timeout in seconds. The `timeout` option is present in the options for the following requests: - Configuration - Status
IBM Spectrum Protect (TSM)	timeout	No default value	Internal timeout for commands sent to Spectrum Protect server in seconds. The `timeout` option is present in the options for the following requests: - Client Occupancy - Job Monitor - Process Monitor - Volume Status
	timeout	3600	Internal timeout for commands sent to Spectrum Protect server in seconds for the Configuration request
	timeout	900	Internal timeout for commands sent to Spectrum Protect server in seconds for the Status request

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
	tsmhost	No default value	Hostname of the Spectrum Protect server. The `tsmhost` option is present in the options for the following requests: ● Client Occupancy ● Configuration ● Job Monitor ● Process Monitor ● Status ● Volume Status
	tsmport	1500	Port of the Spectrum Protect server. The `tsmhost` option is present in the options for the following requests: ● Client Occupancy ● Configuration ● Job Monitor ● Process Monitor ● status ● Volume Status
	disableprivatevolumes	False	Disable reporting of private volumes. The `disableprivatevolumes` option is present in the options for the following requests: ● Configuration ● Volume Status
	backupsets	True	Whether to gather backup sets for the Job Monitor request.
	filterbynoderegtime	True	Filter Missed Jobs before node registration for the Job Monitor request
	Whether to gather failed jbos from the activity log	False	If this is enabled and set to `True` any messages in the Spectrum Protect activity log that indicates a failed backup has taken place are also reported as a failed job in Data Protection Advisor. The `Whether to gather failed jbos from the activity log` option is present in the Job Monitor request.
	processingtype	No default value	The source of the processing jobs for the Job Monitor request. It can be either SUMMARY or ACTLOG.
	OPTION_LIB_MANAGER_CRED	OptionDefinition.Type.Credential	Library Manager Credentials for the Volume Status request
	ignorewarnings	No default value	Warning codes to treat Job Monitor request as successful. There are no character limitations.
VMware	port	443	Port of VMware server. The `port` option is present in the options for the following requests: ● Configuration ● Performance ● Status
	timeout	3600	Internal timeout for commands that are sent to VMware host in seconds. The `timeout` option is present in the options for the following requests:

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
			- Configuration - Performance - Status
	usessl	True	Use SSL over HTTP. The `usessl` option is present in the options for the following requests: - Configuration - Performance - Status
	vmwarehost	No default value	Hostname of VMware server. The `vmwarehost` option is present in the options for the following requests: - Configuration - Performance - Status
VMware vSphere Data Protection (VDP)	capacityfactor	1.075	Decimal capacity factor. The `capacityfactor` option is present in the options for the following requests: - Configuration - Status
	dbname	mcdb	Database name. The `dbname` option is present in the options for the following requests: - Configuration - Job Monitor - Status requests
	dbport	5555	Database port. The `dbport` option is present in the options for the following requests: - Configuration - Job Monitor - Status requests
Webserver	page	No default value	Web page to get for the Response request
	port	80	Web server port. The `port` option is present in the options for the following requests: - Configuration - Response
Xsigo	timeout	10	SNMP timeout value in seconds. The `timeout` option is present in the options for the following requests: - Configuration - Performance - Status
ⓘ **NOTE:** The following time formats are supported:	1.	- %c - Locale-specific - %x %X - Locale-specific - alternate format - %m/%d/%y %I:%M:%S %p - Hard-coded 12-hour US date format - %m/%d/%Y %I:%M:%S %p	he meaning of the elements in the time and date formats is: - %c - Date and time using the current locale format - %x - Date using the current locale format - %X - Time using the current locale format - %m - Month as an integer (1–12) - %d - Day of the month as an integer (00–31) - %y,%Y - Year without the century, as an integer (0–99)

Table 28. Data collection request options by module (continued)

Module	Option name	Value	Description
		- %d/%m/%y %I:%M:%S %p - Hard-coded 12-hour European date format - %d/%m/%Y %I:%M:%S %p - %m/%d/%y %r - %m/%d/%Y %r - Locale-specific - %d/%m/%y %r - %d/%m/%Y %r - %d/%m/%y %T - %d/%m/%Y %T - %m/%d/%y %T - %m/%d/%Y %T - %x - Locale-specific - %m/%d/%Y - %m/%d/%y - %d/%m/%y - %d/%m/%Y - %d.%m.%Y %T	- %I - Hour in 12-hour format (1–12) - %M - Minute as an integer (0 -59) - %S - Seconds as an integer (0–59) - %p - The equivalent of AM/PM of the local - %r - Time in 12 hr am/pm format - %T - Time - alias for hours:Minutes:Seconds. For example, if the time format is: Wednesday, July 05, 2017, 6:01:08 AM, then the following UNIX Standard STRPTIME format is used: **%A, %h %d, %Y, %I:%M:%S %p**
	2.	- %c - %x %X - %x, %X	

Manage Sites

You can set the Site attribute in the object property dialog, similar to other attributes, like Credentials and Schedule. You can assign the Site attribute to all top-level and component objects. Data Protection Advisor does not support assigning the Site attribute to group objects. Objects are searchable by the Site attribute.

Go to **System Settings** > **Sites** > **Manage Sites** to add, edit, and delete sites.

Creating, editing, and deleting Sites

1. Go to**System Settings** > **Sites** > **Manage Sites**
   The **Manage Sites** window appears.
2. If you would like to:
   - Create a site:
     a. Click **CREATE**.

        The **Create Site** dialog appears.
     b. In the **Name** field, type a name for your site.
     c. In the **Location** field, type three or more characters for the geographical location that is closest to your site, then select the location that is the best geographical match to your site.
     d. Click **SELECT LOCATION** and **OK**.
   - Edit a site:
     a. Select the site that you would like to edit from the list of sites. The **Edit Site** dialog appears.
     b. Edit the desired field and click **OK**.
   - Delete a site:
     a. Select the site that you would like to delete from the list of sites. The **Delete Site** dialog appears.
     b. Confirm or cancel deletion of the site, as applicable.

Telemetry data collection in Data Protection Advisor

Telemetry data collection helps Dell Technologies to gain powerful insights into how users navigate through the applications. It enables precise pinpointing of areas for improvement by analyzing the usage patterns. This data-driven approach empowers Dell Technologies to streamline user interfaces, prioritize features, and optimize system performance.

Enable telemetry data collection

By default, the telemetry data collection is disabled. You can opt in or opt out of the telemetry data collection by using one of the following ways:

- After you log in to the Data Protection Advisor UI, a notification banner allows you to **ACCEPT** or **DECLINE** the telemetry data collection. Click the **For more details click here** link to read the **Telemetry Notice** and get more information about the data collection process. The notification appears every time you log in to the Data Protection Advisor UI until you accept or decline it.
- Another way to opt in or opt out of the telemetry data collection is to click the user icon and then click **User Preferences**.
    - In the **Preference** tab, click the **Enable Telemetry** toggle to the on position.
    - If you want to disable the telemetry data collection, click the **Enable Telemetry** toggle to the off position.

Application service administration

Running Linux Data Protection Advisor Application as non-root user

By default the Data Protection Advisor Application runs under root user on Linux. Carry out this procedure on the Data Protection Advisor Application Server to configure the Data Protection Advisor Application to run as a non-root user.

1. Stop the Data Protection Advisor Application service. Type: **`dpa app stop`**
2. Create an OS user to be used for running Data Protection Advisor Application.

   Alternatively, select the OS username `apollosuperuser` to be used for running the Data Protection AdvisorApplication from the `dpaservices` group.

   The `apollosuperuser` user is created during Data Protection Advisor Installation.
3. Transfer ownership of Data Protection Advisor services installation directory to the OS user, which will run the Data Protection Advisor Application. Type: **`chown --dereference -LR <user_to_run_dpa>:<group_of_user> <dpa_install_dir>/services`**
4. Modify the `<dpa_install_dir>/services/executive/applnsvc.sh` file. Change the line **`RUN_AS_USER=`** to **`RUN_AS_USER=<user_to_run_dpa>`**.
5. If performing an upgrade, repeat steps 3 and 4 above to restore the required FS permissions and owners.
6. Start Data Protection Advisor Application service. Type: **`dpa app start`**
7. Optional: If you configured any third-party scripts, for example, pre-processing script for scheduled reports or post-processing script in publish settings or scripts for Analysis Policies, modify the scripts for the OS user to `<user_to_run_dpa>` as indicated in step 4.

   The Data Protection Advisor Application may receive a permissions denial to run scripts under a new OS user that previously ran under the root user.

Setting TLS protocol version 1.2 only after installation or upgrade

You can set the TLS protocol version to 1.2 only after Data Protection Advisor installation or upgrade by using the `dpa application tlslevel` command.

1. Stop the Data Protection Advisor Application server. Type:

   dpa app stop
2. Run the `dpa application tlslevel` command to set the TLS protocol version to version 1.2 only. Type: **`dpa app tls 1.2`**

3. Start the Data Protection Advisor Application server. Type:
   dpa app start

Customization of service information

This section provides information on the types of Data Protection Advisor service customization which only an administrator can do. You must have physical access to the host on which Data Protection Advisor is running.

The *Data Protection Advisor Product Guide* provides information on customizing viewlets, dashboards, and reports. Users can carry out these customizations.

Create and register Data Protection Advisor message source in Windows OS

Configure an alert to write the Event Data to the Windows message field in the correct form in Windows OS.

You must have Visual Studio installed on your system.

If you have a Data Protection Advisor analysis policy configured to generate an event log for a certain event, configure Data Protection Advisor to populate the error under the Windows **<message>** section.

1. Open the Visual Studio command prompt.
2. Run the commands:

```
mc.exe dpa.mc
rc.exe /r dpa.rc
link -dll -noentry -out:dpa_msgfile.dll dpa.res /MACHINE:X64
```

   The `dpa_msgfile.dll` file is created. The `dpa.mc` has the following contents:

```
MessageIdTypedef=DWORD

MessageId=4096
Language=English
%1
.
```

3. Create the folder `C:\Program Files\EMC\DPA\services\dll`

   You can place the folder in any location.
4. Place the `dpa_msgfile.dll` file within `C:\Program Files\EMC\DPA\services\dll`.
5. Create the file `register_msgfile.reg` with the following contents:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\DPA]
"TypesSupported"=dword:00000007
"CategoryCount"=dword:00000006
"CategoryMessageFile"="C:\\Program Files\\EMC\\DPA\\services\\dll\\dpa_msgfile.dll"
"EventMessageFile"="C:\\Program Files\\EMC\\DPA\\services\\dll\\dpa_msgfile.dll"
```

VTL templates

When the Publisher process creates reports when publishing to HTML, it uses VTL templates located in the `vtltemplates` directory on the Data Protection Advisor Server to determine the report's default layout and style. By default, the Data Protection Advisor Server process uses the following template files: `reportcard.vtl`, `chart.vtl`, and `table.vtl` however, you can use another template file. You can create template files to change the appearance of reports that are published by the Data Protection Advisor Server process.

The template types are:

- Default uses the default VTL for the renderer.
- pivot is for generating pivot tables.
- pivot.css is for generating pivot tables using CSS.
- pivot.controlpanel.css is for generating pivot tables in control panels using CSS.

The following table lists the VTL templates.

Table 29. VTL templates

VTL template	Description	Template type
chart.vtl	Used by chart renderers that produces an image for the HTML output such as Area, Column, Line, Pie, Topology	Default
chart.controlpanel.css.vtl	Same as chart.vtl except this uses CSS.	N/A
chart.css.vtl	Same as chart.vtl except this uses CSS	css
email.attach.vtl	Used when sending the report as an attachment to the email	N/A
email.image.embed.vtl	Used for embedding the report inside of the email	N/A
email.notification.vtl	Used for creating the notification that can be sent out after a report was published	N/A
healthstatus.vtl	Used for Health Status	Default
healthstatus.controlpanel.css.vtl	Same as healthstatus.vtl except this uses CSS. Also does not contain the date and version at the bottom	N/A
healthstatus.css.vtl	Same as healthstatus.vtl except this uses CSS	css
reportcard.vtl	Used for ReportCard	Default
reportcard.controlpanel.css.vtl	Same as reportcard.vtl except this uses CSS. Also does not contain the date and version at the bottom	N/A
reportcard.css.vtl	Same as reportcard.vtl except this uses CSS	css
table.controlpanel.css.vtl	Same as table.vtl except this uses CSS. Also does not contain the date and version at the bottom	N/A
table.vtl	Used for Table	Default
table.css.vtl	Same as table.vtl except this uses CSS	css
table.pivot.controlpanel.css.vtl	Same as table.pivot.vtl except this uses CSS. Also does not contain the date and version at the bottom	pivot.controlpanel.css
table.pivot.css.vtl	Same as table.pivot.vtl except this uses CSS	pivot.css
table.pivot.vtl	Used for Pivot Table	pivot
timeline.vtl	Used for timeline charts. HTML gets embedded in the VTL	Default
timeline.controlpanel.css.vtl	Same as timeline.vtl except this uses CSS. Also does not contain the date and version at the bottom	N/A
timeline.css.vtl	Same as timeline.vtl except this uses CSS	css

Example - Part 1: Adding a message and company details to the table VTL template

If you are required to send daily or weekly reports in HTML format to customer using scheduled reports, then you can add custom text (such as a message or company contact information) to the scheduled report by creating a custom VTL template. The custom text displays for all HTML reports using this template.

1. In the `styles` or `vtltemplates` directory on the Data Protection Advisor Server, copy the table template, `table.vtl`, and rename it. For example, if you are creating a VTL template for table reports for the company Dell, use the naming standard of `table.<companyName>.vtl` then rename the table template to `table.dell.vtl`
2. Open the VTL in a text editor.
3. Using HTML tags, add text similar to the following within the body.

```
<body bgcolor="$background"><font face="Arial, Verdana,
                Helvetica, Sans-serif" color="$foreground">

<body>
Dear customer,
<p>
Your daily system status report is below.
<p>
Thank you,<br>
Dell Technologies
<p>
US Phone:1-800-555-5555<br>
Email:support@dell.com<br>
Website: www.dell.com
<p>
<table>
...
</table>
</body>
```

4. Save the VTL.

Example - Part 2: Using a custom VTL template in a scheduled report

Now that you have a custom VTL template, select this VTL in the Scheduled Report Wizard.

1. In the Data Protection Advisor web console, create a new or update an existing scheduled report.
2. In **Publish Settings**, select the Web Page (.html) report format and complete the remaining fields.
3. In **Advanced**, select the Dell template and then click **OK**. The template named Default is the unedited table.vtl.
4. Click the test icon to send the scheduled report to the Publisher. If you publish to file, go to the default directory to view the report, and then make any necessary updates to the VTL template. The default directory of the report is `<install-dir\services\shared\report-results\scheduled`.
5. If no further updates are required for the VTL template, save and close the Scheduled Report Editor.

Custom templates import and export

You can import and export custom report templates and custom dashboards from Data Protection Advisor 5.5.1 and later into Data Protection Advisor from a WDS file through the Custom Templates section. Importing and exporting to XML is not supported. You cannot import or export system templates. The imported reports must be supported on Data Protection Advisor.

You can import and export custom report templates and custom dashboards to fulfill the following needs:

- Import custom reports from Data Protection Advisor 5.x.
- Import custom reports that Dell Professional Services creates.
- Export custom reports to back them up.
- Export a custom report that is not working to send it to Dell Customer Support for troubleshooting.

The Dell Data Protection Advisor Online Help provides more information about how to import and export custom report templates.

Backing up the application

Backing up important application configuration and lockbox files

If Data Protection Advisor has been set up in a two-site failover disaster recovery configuration, then ensure that the lockbox files on the current primary site application are also copied to the secondary site application, so that they match. This must be done before any failover is performed.

Table 30. Data Protection Advisor application files

Item	Location	Purpose	Frequency	Required
application.lb	<install>/executive	Lockbox	One time only	Required
application.FCD	<install>/executive	Lockbox	One time only	Required
lockbox.conf	<install>/executive	Lockbox	One time only	Required
standalone.xml	<install>/standalone/configuration	Base JVM configuration	One time only or after any application configuration modification	Recommended
application-service.conf	<install>/executive	Runtime JVM configuration	One time only or after any application configuration modification	Recommended
apollo.keystore	<install>/standalone/configuration	Keystore for Data Protection Advisor certificates	After any certificate modification	Recommended

NOTE: Ensure that you back up important application configuration and lockbox files to a remote location, and not on the Data Protection Advisor server. This is because you might lose these files, if there is a disaster event, such as a disk failure. If there is a disaster event, it might not help even if you save the files to a directory outside of the Data Protection Advisor installation directory.

Datastore service administration

Note the following limitations for Datastore Replication:

- In busy environments, the best practice is to stop the Application servers for a Datastore Replication export so that the export can complete and import to the secondary Datastore, and resync with the primary Datastore.
- Data Protection Advisor supports Datastore Replication exports from the primary Datastore only. Data Protection Advisor does not support Datastore Replication exports run from the secondary Datastore.

Backup of the Datastore

It is a best practice to back up the Data Protection Advisor Datastore regularly and particularly prior to making any major change to Data Protection Advisor such as upgrading to a newer version or migrating to new hardware. An export of the Datastore contents is part of an overall backup of the Data Protection Advisor instance.

Exporting and importing a Data Protection Advisor Datastore is supported only on the same version of the Data Protection Advisor Datastore.

Exporting the Data Protection Advisor Datastore

With this export command, a complete and consistent copy of the Datastore is exported to the local file system, in a location that can optionally be specified.

The default folder/subdirectory of the export is: datastore-<*version*> <*date and time*>.

For example, datastore-6_3_0_90597-2017-10-01-1135.

Type the following command from a system prompt. **dpa datastore export [options]**

By default, the exported Datastore folder is saved to the same directory where the export command was run.

To save the exported Datastore folder to a specific directory, specify the location at the end of the command line.

The datastore export command also creates copies of the datastore.lb file and the lockbox.conf file in the same directory as the datastore export. For a Data Protection Advisor all-in-one stand-alone system, it creates a copy of the application.lb file as well.

For example, the following command line exports the folder to C:\ because that is the location specified in **C:\Program Files\EMC\DPA\services\bin>dpa datastore export C:\**

Exporting the Data Protection Advisor Datastore to Pipe

With this export format, a complete and consistent copy of the Datastore is streamed to a named pipe from a location where Avamar can read the contents.

Type the following command from a command line prompt. **dpa datastore export --pipeline**

For example, **dpa datastore export --pipeline /mydir/mypipe**

Data Protection Advisor supports backup up to Avamar using the ds export command and piping it directly to Avamar. For more information, see the Avamar documentation on how to pipe a backup into Avamar using "named pipes."

After you export Datastore

The dpa ds export command produces a folder that contains all the export files for the Data Protection Advisor Datastore. Read about the recommended actions for the folder.

You should back up the folder that contains all the export files for the Data Protection Advisor Datastore with Avamar or NetWorker or any other backup application.

If you are using Avamar, you must restore the content first, and then carry out the import on Data Protection Advisor.

If you are using NetWorker, consider placing these Datastore export folders into a separate filesystem and use the NetWorker block-based backup method to backup this folder efficiently.

> **NOTE:** Some type of data in the Datastore is encrypted, and the encryption key is stored in the special store on the Data Protection Advisor application host. In order to use the exported Datastore with different Data Protection Advisor application installation, you must copy the files containing the encryption key.
>
> Copy the following files from the current Data Protection Advisor application:
>
> - <DPA_INSTALL_DIRECTORY>/services/executive/application.lb
> - <DPA_INSTALL_DIRECTORY>/services/executive/lockbox.conf
>
> Dell Technologies recommends that you copy the files on every Datastore export. Otherwise, some of the data in the Datastore might become unrecoverable and might require additional manual changes to fully restore the state of the Data Protection Advisor application.

Importing the Data Protection Advisor Datastore

The dpa datastore import command-line option is used to import the contents of a Datastore file to the Data Protection Advisor Datastore.

1. Stop the Data Protection Advisor Application service.
2. Import the Datastore.
3. Start the Data Protection Advisor Application service.
4. From the system prompt, type the following commands:
    a. **dpa app stop**
    b. **dpa datastore status**

       The status must be running.

c. **`dpa datastore import [options] <filename>`**
d. **`dpa app start`**

Where *<filename>* is the previously exported Datastore file. The `import` command replaces the existing Datastore contents with the contents that are contained in the Datastore export file.

ⓘ **NOTE:**

If you reinstall the Data Protection Advisor application, ensure that you place the previously copied `application.lb` and `lockbox.conf` files in the `<DPA_INSTALL_DIRECTORY>/services/executive` folder. If import is being performed with the same Data Protection Advisor application (not with the reinstalled version), copying the `application.lb` and `lockbox.conf` files is not required.

For a complete list of Data Protection Advisor CLI commands, type **`dpa --help`** from the system prompt. Data Protection Advisor command line operations provides more information.

Backing up important datastore security and configuration files

It is recommended to back up important datastore security and configuration files to a remote location, and not on the Data Protection Advisor server. If there is a disaster event such as disk failure, backing up to a remote location prevents the loss of these files. If there is a disaster event, it might not help even if you save the files to a directory outside of the Data Protection Advisor installation directory.

Table 31. Data Protection Advisor datastore configuration files

Item	Location	Purpose	Frequency	Required
datastore.lb	<install>/executive	Lockbox	One time only	Required
datastore.FCD	<install>/executive	Lockbox	One time only	Required
lockbox.conf	<install>/executive	Lockbox	One time only	Required
datastore-service.conf	<install>/executive	Datastore configuration	One time only or after any datastore configuration modification	Required
postgresql.conf	<install>/datastore/data	Base Postgres configuration	One time only or after any datastore configuration modification	Recommended
pg_hba.conf	<install>/datastore/data	Postgres client configuration	One time only or after any datastore modification	Recommended
datastore-layout.properties	<install>/datastore	Postgres file system configuration variables	One time only	Recommended
DS export	Not Applicable	Export of the Data Protection Advisor Datastore database. It is a copy of the entire contents of the database.	As frequent as possible.	Highly recommended

Datastore Replication administration

Configuring Datastore Replication after deployment

Perform the following steps to configure Datastore replication on a system that is already installed and operational. Note that the CLI commands in this section are formatted for Linux RHEL.

1. Confirm that the Datastore server is installed as a secondary Datastore. If it is not, configure the Datastore server as a secondary Datastore. Run **`dpa.sh ds rep --role SLAVE <primary_Datastore_IP_address>`** to make the Datastore server secondary.
2. Follow the procedure Integrating secondary Datastore after it has been offline.

Configuring cascading Datastore Replication

You can configure cascading Datastore Replication after installation only with the Data Protection Advisor CLI. With cascading Datastore Replication, the primary Datastore replicates to a chain of secondary Datastores, one of which can be remote. Note that the CLI commands in this section are formatted for Linux RHEL.

- Stop all Application Servers by running the following command:

  ```
  dpa.sh app stop
  ```

- Stop all Datastore Servers by running the following command:

  ```
  dpa.sh ds stop
  ```

- Set the same apollosuperuser password on all Datastore Servers. On each Datastore Server, run the following command:

  ```
  dpa.sh ds superpwd
  ```

- The install directory for the Datastore must be the same on each Datastore machine for the import/export functionality to work.

1. On the primary Datastore, run the following command:

   ```
   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --role master <DPA_HOME>/emc/dpa/
   services/bin/dpa.sh ds rep --addSlave <replicating_secondary_Datastore_IP_address>
   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start
   ```

2. On the replicating secondary Datastore, run the following command:

   ```
   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --role replicating_slave
   <primary_Datastore_IP_address> <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --addSlave
   <secondary_Datastore_IP_address> <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start
   ```

3. On the secondary Datastore, run the following command:

   ```
   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --role slave
   <replicating_secondary_Datastore_IP_address> <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds
   start
   ```

4. Synchronize the secondary Datastores with the latest Datastore copy from the primary Datastore:
   a. For each Datastore, create an empty directory on the primary Datastore, to which you want to export the primary Datastore file set.
      For example, `/tmp/export`.
   b. On the primary Datastore, run the following command, and concurrently ensure that the primary Datastore is running.

      ```
      dpa.sh ds rep --export /tmp/export
      ```

   c. Use the appropriate platform to command copy the files to the empty directory on the secondary Datastore.
   d. On the replicating secondary Datastore, run the following command:

      ```
      <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --import /tmp/export <DPA_HOME>/emc/dpa/
      services/bin/dpa.sh ds start
      ```

   e. On the secondary Datastore, run the following command:

      ```
      <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --import /tmp/export <DPA_HOME>/emc/dpa/
      services/bin/dpa.sh ds start
      ```

5. Verify whether the replication is working on the Datastores by running the following command:

   ```
   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep
   ```

The following similar output appears:

```
<DPA_HOME>/emc/dpa/services/logs # /binary/emc/dpa/services/bin/dpa.sh ds rep

Data Protection Advisor

[INFO] Replication State : REPLICATING_SLAVE (for 10.11.111.110)
[INFO] Defined Slaves
                         : 10.11.111.111/12

[INFO]                                    SLAVE       BYTES LAG      STATUS
[INFO]                            10.11.111.111               0      streaming

[INFO] SLAVE is behind the MASTER by 0 [HH:MM:SS]

Command completed successfully.
```

6. Start the Application Servers by running the following command:

   `dpa.sh app start`

If the primary Datastore fails, you can make the replicating secondary Datastore or secondary Datastore into a new primary so that Data Protection Advisor can continue functioning. Carrying out Datastore server failover provides more information.

Configuring Wal parameters

To reconfigure the postgress wal parameters for the available maximum slot wal keep size and wal keep size, run the following command:

```
dpa.sh ds reconfigureWal -help
Reconfigure the postgress wal parameters for the available
max_slot_wal_keep_size and wal_keep_size

Usage : dpa datastore reconfigureWal [options] <value>[MB|GB]
dpa ds reconfigureWal [options] <value>[MB|GB]

Command Options :
--quiet Display warnings and errors only
--version Display tool version information
--help (-h) Display help screen
```

This command is supported only for primary Datastore in DS Replication setup :

```
dpa.sh ds reconfigureWal 1024MB

Dell Data Protection Advisor

Datastore Service successfully tuned.

The new memory utilisation for the datastore will not
take effect until the datastore service is restarted.
```

Other Datastores display an error when you run this command :

```
dpa.sh ds reconfigureWal 1024MB

Dell Data Protection Advisor

[ERROR] reconfigureWal command supports only for replication enabled DPA Master datastore
Completed in : 21ms
```

Carrying out Datastore server failover

When the primary Datastore fails, carry out a failover to the secondary Datastore. If you are unable to query the secondary database, try changing the password and perform the failover steps.

Ensure that the secondary Datastore is running.

1. Update the secondary Datastore password:
   a. Rename the `recovery.signal` file to `recovery_tmp.signal`.
   b. Rename the `standby.signal` file to `standby_tmp.signal`.
   c. Take a backup of `pg_hba.conf` file and change `hostssl` to `hostnossl` and `scram-sha-256` to trust in the `pg_hba.conf` file.
   d. Run the following commands:

   ```
   C:\Program Files\EMC\DPA\services\datastore\engine\bin> dpa ds restart
   (For Windows only)cmd.exe /c chcp 1252
   psql -h <secondary_Datastore_IP_address> -p 9003 -U apollosuperuser -d template1
   ALTER USER apollosuperuser WITH PASSWORD 'Dpa@12345';
   ```

   e. Run the `dpa ds superpwd` to change the password.
2. On the secondary Datastore, run the following command:

   `dpa.sh ds rep --failover`
3. Stop the Application server. Run the following command:

   `dpa.sh app stop`
4. Reconfigure the Application server to point to the new primary Datastore. Run the following command:

   `dpa.sh app con -m <hostname/new_primary_Datastore_IP_address>`
5. Verify that the Datastore is running. Run the following command:

   `dpa.sh ds status`

   Output is `INSTALLED`, `STOPPED`, or `RUNNING`.
6. If it is not running, start it. Run the following command:

   `<DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start`
7. Start the Application server. Run the following command:

   `dpa.sh app start`
8. Run the following command to create a replication slot on the new primary Datastore:

   `dpa ds query "select * from pg_create_physical_replication_slot('standby1_slot');"`

Reconfiguring Datastores

Use this procedure if you failed over to your secondary Datastore and want to reconfigure the former primary Datastore as a secondary Datastore.

1. On the new primary Datastore, use the **addSlave** command with the IP of the new primary Datastore. Run the following command:

   `dpa.sh ds rep --addSlave <primary_Datastore_IP_address>`
2. Restart the new primary Datastore. Run the following command:

   `dpa.sh ds restart`
3. Export the new primary Datastore. Run the following command:

   `dpa.sh ds rep --export /export`
4. Configure the new secondary Datastore as SLAVE. Run the following command:

   `dpa.sh ds rep --role SLAVE <primary_Datastore_IP_address>`
5. Stop the secondary Datastore. Run the following command:

   `dpa.sh ds stop`
6. Import the primary Datastore to the secondary Datastore. Run the following command:

   `dpa.sh ds rep --import /import`
7. Start the secondary Datastore server. Run the following command:

   `dpa.sh ds start`

   NOTE: While reconfiguring the former primary Datastore as a secondary Datastore, delete the existing replication store on the former primary Datastore by executing: **`dpa.bat ds query "select pg_drop_replication_slot('standby1_slot');"`**

Integrating secondary Datastore after it has been offline

This procedure is applicable if Datastore Replication was previously configured and the secondary Datastore goes down. This procedure is also applicable if you are introducing Datastore Replication into an already operational deployment. You then reintegrate a secondary Datastore.

Datastore Replication automatically resumes after short amounts of time offline, for example, after a restart of the Application server. The Datastore is configured to allow approximately 6 hours of downtime before it needs reinitialization. However, this value is approximate and a heavily loaded server may require reinitialization if down for less time. We recommend that you carry out testing to determine the threshold for your deployment.

This procedure is also applicable to resynchronizing a standalone secondary Datastore after isolation. Examples of isolation could be a network outage or break down in communications between the primary and secondary Datastores.

1. Create an empty directory on the primary Datastore to which to export the primary Datastore file set. For example, `/tmp/export`
2. Export the primary Datastore file set from the running primary Datastore. Run the following command:

   `dpa.sh ds rep --export /tmp/export`
3. Create an empty directory on the secondary Datastore into which to copy the primary Datastore file set.
4. Use the appropriate platform to command copy the files to the empty directory on the secondary Datastore.
5. Import the secondary Datastore. Run the following command:

   `<DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --import /tmp/import`

   where `<DPA_Home>` is the location of the Data Protection Advisor installation.
6. Start the secondary Datastore server. Run the following command:

   `<DPA_HOME>/emc/dpa/services/bin/dpa.sh ds` start where <DPA_Home> is the location of the Data Protection Advisor installation. The status of the secondary Datastore at this point is STARTED.
7. Verify that replication is functioning. On the primary Datastore, run the following command:

   `bin/dpa.sh ds rep`

   Output such as the following on the secondary Datastore appears: `EMC Data Protection Advisor [INFO] Replication State : SLAVE (for 10.11.111.112) Command completed successfully.`

   If the secondary Datastore has been down and is restarted, output such as the following indicating the bytes lag and status of *catchup* on the primary Datastore appears:

```
EMC Data Protection Advisor

[INFO] Replication State : MASTER
[INFO] Defined Slaves
                         : 10.11.111.111/12

[INFO]                                    SLAVE      BYTES LAG      STATUS
[INFO]                            10.11.111.111       11245376      catchup

Command completed successfully.
```

   Once the lag is caught up, output such as the following, with the status showing as *streaming*, appears:

```
EMC Data Protection Advisor

[INFO] Replication State : MASTER
[INFO] Defined Slaves
                         : 10.11.111.111/12

[INFO]                                    SLAVE      BYTES LAG      STATUS
[INFO]                            10.11.111.111              0      streaming

Command completed successfully.
```

Stopping Datastore Replication

To stop Datastore Replication, stop the secondary Datastore by running the following command:

`dpa.sh ds stop`

Database encryption management

The following section describes encryption management.

Adding Application servers into setup with Database encryption

Set up the Datastore and Application servers for encryption. provides information.

1. Install the second Application server. Choose to install without starting the services. Installing the Application Service provides information.
2. On the Datastore server, stop the Datastore service.
3. On the Datastore server, run the following command to tell the Datastore server that the Application server exists:

   ```
   dpa ds con --add <App Server2 address>
   ```

4. On the newly installed Application server, run the following command to tell the Application server which Datastore server is pointing to it:

   ```
   dpa app con -m <DataStore address>
   ```

5. Start the DataStore server and the newly installed Application server.

Recreating the Data Protection Advisor Datastore

You can recreate the Data Protection Advisor Datastore by using the `dpa datastore recreate` command in the case that it has the been corrupted. The `dpa datastore recreate` command clears the content of the database and leaves its state as if you just performed a fresh installation, while preserving the Data Protection Advisor configuration parameters, database configuration, and any layout changes.

- Stop all Application Servers. Type:

  ```
  dpa.sh app stop
  ```

- Stop all Datastore Servers. Type:

  ```
  dpa.sh ds stop
  ```

1. On the corrupt Datastore, run the following commands:

   ```
   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rec
    <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start
   ```

2. Start the Application Servers. Type: `dpa.sh app start`
3. Set the Admin password. Type: `dpa.sh app pwd <password>`
4. Verify that the database has been cleared and that only the default installation items are present.

   The default installation items are the Application server and Datastore servers.
5. Stop the Application server. Type: `dpa.sh app stop`
6. Import the most up-to-date backup of your Datastore. Type: `dpa.sh ds import <filename to import>`. Importing the Data Protection Advisor Datastore provides more information.
7. Start the Application server. Type: `dpa.sh app start`

Data Protection Advisor Database superuser password

One Data Protection Advisor Database superuser account is supplied within Data Protection Advisor Datastore: apollosuperuser. apollosuperuser is actually the user who owns the Data Protection Advisor Database and who can override all access restrictions within the Data Protection Advisor Database.

By default, the Data Protection Advisor Database is accessible by using that account only from the local machine. The `dpa datastore superpassword` CLI command provides the ability to change the apollosuperuser password. The dpa datastore commands section of the *Data Protection Advisor Installation and Administration Guide* provides information.

Lockbox

Lockbox is a mechanism by which, sensitive data, for example, pass phrases, configuration keys, and so on, is encrypted and stored. This mechanism provides a stronger level of security for important data.

In Data Protection Advisor, lockbox is essentially a collection of files where an encryption key, which is used for encrypting sensitive data is stored.

The lockbox file containing the encryption key is secured with a password, which is encrypted and stored inside the file called `lockbox.conf`.

Data Protection Advisor has three lockbox-related files that are on the Data Protection Advisor application server. The files are:

- `/opt/emc/dpa/services/executive/application.lb`
- `/opt/emc/dpa/services/executive/application.lb.FCD`
- `/opt/emc/dpa/services/executive/lockbox.conf`

These files are created during Data Protection Advisor installation, and the encryption keys are randomly generated every time that they are created. These files are not modified during upgrades.

There are similar lockbox files on the datastore that stores the encryption key that is used to encrypt the datastore password the user sets during installation. It is also used when the datastore password is set using the `dpa ds` commands.

- `/opt/emc/dpa/services/executive/datastore.lb`
- `/opt/emc/dpa/services/executive/datastore.lb.FCD`
- `/opt/emc/dpa/services/executive/lockbox.conf`

After you encrypt the datastore password, the encrypted value is also stored inside the `<DPA_HOME>/services/executive/datastore-service.conf` file.

When Data Protection Advisor 19.1 or later is installed or an earlier version of Data Protection Advisor is upgraded to Data Protection Advisor 19.1 or later, the lockbox files are created. When credentials are configured in the Data Protection Advisor UI, the Data Protection Advisor application uses the lockbox encryption key to encrypt the set of credentials. The encrypted credential is then stored in the Datastore Postgres database. This encryption happens during discovery of new objects, and when credentials are changed.

When the Data Protection Advisor application requires the credentials again for some purpose (such as LDAP authentication), it reads these encrypted credentials from the datastore and then uses the lockbox encryption key to decrypt it.

Also, data is uniquely encrypted in each setup and environment. For example, a lockbox from environment A cannot not be used in environment B.

Lockbox backup

The risk that is associated with losing the lockbox files on the Data Protection Advisor application server is that the Data Protection Advisor application might not be able to decrypt the data (the passwords) in the Data Protection Advisor datastore.

Losing the lockbox files can occur from:

- Accidental deletion
- A reinstall of the Data Protection Advisor application or datastore server
- A migration to another Data Protection Advisor application or datastore server
- A failover to a DR Data Protection Advisor application or datastore server

Any of the mentioned scenarios can lead to the loss of the original lockbox files. If the files are lost, there is no way for the Data Protection Advisor application or administrators to recover or re-create the original lockbox files. A backed-up copy of the lockbox files must be restored to the Data Protection Advisor application.

If the application lockbox is lost and not recoverable (no copies of these files), the Data Protection Advisor application cannot read any of the mentioned passwords or credentials.

If the datastore lockbox files are lost and not recoverable, run the `dpa ds password` command to reset the datastore password. Then run the `dpa app dspassword` on the Data Protection Advisor application server to match. If the `datastore-service.conf` file is lost, it might further complicate the recovery of the database passwords sometimes.

Data Protection Advisor command line operations

Sourcing the Data Protection Advisor config file for UNIX users

A Technical Support Engineer may ask you to source the Data Protection Advisor config file before running any agent binaries (including Data Protection Advisor Agent request in debug mode and bkupjob) and any command line operations on UNIX.

1. Navigate to the `/etc` folder of the Data Protection Advisor installation directory.
2. Run the following command :

```
cd <DPA install dir>/agent/etc
. ./dpa.config
```

The Data Protection Advisor config file sets up various environment variables and paths that the Data Protection Advisor agent uses. Running it when instructed ensures that the shell the user is working and has these set correctly. Failure to carry out this procedure when directed by a Technical Support Engineer could result in CLI command failure.

dpa CLI command

In a default Data Protection Advisor installation, the dpa CLI command can be found in `<install_dir>/services/bin` on UNIX and Linux and in `<install_dir>\services\bin` on Windows.

Use the following syntax:

For Windows:

```
dpa <service_part> <command> [options]
```

For Linux/UNIX:

```
 dpa.sh <service_part> <command> [options]
```

Where <service_part> is Application, Datastore, Agent or service. The service component includes both the Application, Datastore, and Agent services.

```
dpa application <command> [options]
```

```
dpa datastore <command> [options]
```

```
dpa agent <command>
```

```
dpa service <command> [options]
```

The Data Protection Advisor server `start/stop/restart` command applies to whichever services are installed on the current host only. For example, if you run **`dpa server stop`** on the Data Protection Advisor Datastore, it does not stop services that may be running on the Data Protection Advisor Application server.

Examples of command and option abbreviations

The dpa command supports abbreviations of the commands. The following table provides some of the abbreviations. Refer to the specific dpa command for available options for that command.

Table 32. Command and option abbreviations

Command and option	Abbreviation
--add	-a
--bind	-b
--cluster	-c
--delete	-d
--help	-h
--master	-m
--pipeline	-p
--platform	-p
tune	tun
dpa application	dpa app
dpa datastore	dpa ds
dpa service	dpa svc

dpa agent commands

Use the dpa agent commands to manage the Data Protection Advisor Agent service. The dpa agent commands can be applied only to the local agent.

```
dpa agent start
dpa agent stop
dpa agent status
dpa agent restart
dpa agent install
dpa agent uninstall

dpaagent --set-credentials
```

After you start, stop, or restart a service, it may take a number of minutes to complete and may not result in an immediate state change.

dpa agent start

Starts the Data Protection Advisor Agent. The Agent service must be installed and stopped for this command to operate.

```
dpa agent start
```

dpa agent stop

Stops the Data Protection Advisor Agent. The Agent service must be installed and running for this command to operate.

```
dpa agent stop
```

dpa agent status

Displays the status of agent service. For example, RUNNING, STOPPED.

```
dpa agent status
```

dpa agent restart

Restarts the agent service. This command first stops the agent service and then starts the service. The agent service must be running for this command to operate.

```
dpa agent restart
```

dpa agent install

Installs the agent service. The agent service operates as a system-managed service, which is manageable through normal operating system service commands. Management of the lifecycle of the service can also be managed through this command line tool. This command installs the service but does not start the service automatically. If the agent service is already installed this command fails.

```
dpa agent install
```

dpa agent uninstall

Uninstalls the agent service.

```
dpa agent uninstall
```

dpaagent --set-credentials

Sets the Data Protection Advisor Agent Registration password. This command can be found in the following file locations:

- On Unix and Linux: `<agent_install_dir>/agent/bin`
- On Windows: `<agent_install_dir>\agent\bin`

```
dpaagent --set-credentials
```

Note the following regarding Agent password:

- Blank passwords are not supported.
- Minimum length is 9 characters.
- The following are required:
  - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
  - A minimum of 1 numeric symbol
  - A minimum of 1 special character

Example

`C:\Program Files\EMC\DPA\agent\bin>dpaagent --set-credentials`

```
Data Protection Advisor
Enter new password for the agent connection.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit
```

```
Retype new password for the agent connection :
[INFO] Your new password has been applied to the configuration.
[INFO] For this new password to be used you must ensure that all agents use the same new
password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

Use the following command to reset the Data Protection Advisor Agent registration password in a non interactive mode:

`echo <password> | dpaagent --set-credentials noninteractive`

Where:

<password> is the password that you specify.

dpa application commands

Use the dpa application commands to manage the Data Protection Advisor Application service.

```
dpa application  [options]
dpa application agentpwd [options]
dpa application adminpassword [options]
dpa application configure [options]
dpa application configureDatastoreCertificates [options]
dpa application dspassword [options]
dpa application demote [options]
dpa application disablessldatastore [options]
dpa application install [options]
dpa application importcertificate [options]
dpa application mfa [options]
dpa application ping [options]
dpa application promote [options] [<Application Server_IP_Address>]
dpa application restart [options]
dpa application start [options]
dpa application status [options]
dpa application stop [options]
dpa application support [options] <ESRS_IP address>
dpa application tls [options]
dpa application tune <value>MB|GB [options]
dpa application uninstall [options]
dpa application version [options]
```

After you start, stop, or restart a service, it may take a number of minutes to complete and may not result in an immediate state change.

dpa application adminpassword

Resets the Data Protection Advisor Administrator password. You must run the command when the Datastore Service is running.

```
dpa application adminpassword [options]
dpa app pwd [options]
```

Command options

--help (-h) — Displays the help screen

--version — Displays the tool version information

--quiet — Suppresses all output except for warning and error messages

Note the following regarding the Administrator password:

- Blank passwords are not supported.
- Minimum length is 9 characters.
- The following are required:
    - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
    - A minimum of 1 numeric symbol

- A minimum of 1 special character

Example

C:\Program Files\EMC\DPA\services\bin>dpa app adminpassword

```
Data Protection Advisor
Enter new administrator password.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new admin password :
[INFO] Your new password has been set.
[INFO] You must restart all Data Protection Advisor application nodes for this new
password to be used.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa application agentpwd

Configures the Data Protection Advisor Agent Registration password on the Application side.

```
dpa application agentpassword [options]
dpa app agentpwd [options]
```

Command options

--help (-h) — Displays the help screen

--version — Displays the tool version information

--quiet — Suppresses all output except for warning and error messages

Note the following regarding Agent password:

- Blank passwords are not supported.
- Minimum length is 9 characters.
- The following are required:
  - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
  - A minimum of 1 numeric symbol
  - A minimum of 1 special character

Example

C:\Program Files\EMC\DPA\services\bin>dpa app agentpwd

```
Data Protection Advisor
Enter new password for the agent connection.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the agent connection :
[INFO] Your new password has been applied to the configuration.
[INFO] For this new password to be used you must ensure that all agents use the same new
password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa application configure

Configures the Application service, including specifying the Datastore to communicate with. The Application service must be stopped for this command to operate.

```
dpa application configure [options]
dpa app con [options]
```

Command options

--master (-m) <IP_address>—Identifies the datastore with which to communicate.

--bind (-b) <IP_address>—Sets the bind address for the application service.

If you run the command without any options, the output shows information regarding how the Application server is configured. The Operation Mode in the output identifies whether the application is within a stand-alone.

Examples

Output for stand-alone server:

```
C:\Program Files\EMC\DPA\services\bin>dpa app con
Data Protection Advisor
[INFO] Bind Address       : 0.0.0.0
[INFO] Datastore Service : 127.0.0.1
[INFO] Operation Mode     : STANDALONE
```

dpa application demote

Demotes the application service from a cluster environment. The application service will operate as a standalone object instance. The application service must be installed and stopped for this command to operate.

```
dpa application demote [options]
```

Command options

--help (-h) — Displays the help screen

--version — Displays the tool version information

--quiet — Suppresses all output except for warning and error messages

Examples

```
dpa application demote
dpa app demote
```

dpa application disablessldatastore

Configures the Data Protection Advisor Application server to not use SSL encryption while communicating with Data Protection Advisor Datastore server.

```
dpa application disablessldatastore [options]
dpa app disablesslds [options]
```

Command options

--platform (-p) — Includes platform version information

--help (-h) — Displays the help screen

--version — Displays the tool version information

--quiet — Suppresses all output except for warning and error messages

dpa application dspassword

Configures the Data Protection Advisor Datastore password.

```
dpa application dspassword [options]
dpa app dspwd [options]
```

Command options

--help (-h) — Displays the help screen

--version — Displays the tool version information

--quiet — Suppresses all output except for warning and error messages

Note the following regarding Datastore password:

- Blank passwords are not supported.
- Minimum length is 9 characters.
- The following are required:
    - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
    - A minimum of 1 numeric symbol
    - A minimum of 1 special character

Example

`C:\Program Files\EMC\DPA\services\bin>dpa app dspassword`

```
Data Protection Advisor
Enter new password for the datastore connection.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the datastore connection :
[INFO] Your new password has been applied to the configuration.
[INFO] For this new password to be used you must ensure that all datastore nodes use the
same new password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa app fipsmode

Allows you to enable or disable the FIPS compliance mode or get the current status.

```
dpa app fipsmode [enable | disable]
dpa app fm [enable | disable]
```

Command options

enable — Enable FIPS mode.

disable — Disable FIPS mode.

No options — Shows the current status.

NOTE: Ensure that you stop the application server before you run the command to enable or disable FIPS mode. To get the current status, you do not have to stop the application server. If `apollo.keystore` is not in PKCS12 format, you are prompted to convert it to PKCS12.

Examples

```
dpa app fipsmode enable
dpa app fm disable
dpa app fipsmode
```

dpa application install

Installs the application service. The application service will operate as a system managed service, manageable through normal operating system service commands. Management of the lifecycle of the service can also be managed through this command line tool. This command will install the service, but will not start it automatically. If the application service is already installed this command will fail.

```
dpa application install [options]
```

Command options

--user (-U) (DOMAIN\username) User account having read and write access to the shared path specified. The specified user must have *Log on as a service* Windows permission enabled.

--password (-pass) <password> Password for the user specified (Windows only). If the user has changed the password, they must uninstall and install the Application service again.

--help (-h) Display help screen

--version Display tool version information

--quiet Display warnings and warnings and errors only

dpa application importcertificate

Allows you import your own certificate into the Data Protection Advisor application to encrypt the data rather than using the certificate provided by Data Protection Advisor.

```
dpa application importcertificate [options]
dpa app impcert [options]
```

Command options

--certificatefile (-cf) <certificatefile> —Sets the path of the certificate (X.509 format) to import.

--keystorefile (-kf) <keystorefile> — Sets the path of the keystore that contains the certificate to import.

--alias (-al) <alias> — Sets the certificate alias to use when accessing the given keystore.

--password (-pw) <password> — Sets the password to use when accessing the given keystore.

--quiet — Suppresses all output except for warning and error messages

Examples

```
dpa app impcert -kf "C:\work\new.keystore" -al newkey -pw password
```

dpa application lockbox

Allows you to create or recreate an existing lockbox of the Data Protection Advisor application. A lockbox contains the encryption key of the sensitive information encrypted and stored in the Datastore.

```
dpa application lockbox
dpa app lb
```

Note the following regarding password:

- Blank passwords are not supported.
- Minimum length is 9 characters.
- The following are required:

  - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
  - A minimum of 1 numeric symbol
  - A minimum of 1 special character

Example

```
dpa application lockbox

Dell Data Protection Advisor

Recreating the lockbox. Are you sure you would like to continue? [Y/N]
Y
[INFO] Recreating lockbox
Enter new password for the lockbox.
The password must have:
    - at least 9 characters
    - at least 1 uppercase letter
    - at least 1 lowercase letter
    - at least 1 special character
    - at least 1 digit

Retype new password for the lockbox :

Command completed successfully.

Completed in : 10mins 20secs
```

dpa application managementpassword

Allows you to change the JBoss management password in Data Protection Advisor.

```
dpa application managementpassword
dpa app mgmtpwd
```

Command options

--quiet — Suppresses all output except for warning and error messages.

--version — Displays the tool version information.

--help (-h) — Displays the help screen.

Note the following regarding JBoss management password:

- Blank passwords are not supported.
- Minimum length is 9 characters.
- The following are required:
  - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
  - A minimum of 1 numeric symbol
  - A minimum of 1 special character

Example

```
C:\Program Files\EMC\DPA\services\bin>dpa app mgmtpwd
Dell Data Protection Advisor

Enter new JBoss management password.
The password must have:
    - at least 9 characters
    - at least 1 uppercase letter
    - at least 1 lowercase letter
    - at least 1 special character
    - at least 1 digit

Retype new JBoss management password:
[INFO] New JBoss Management user password has been set.

Command completed successfully.
```

```
Completed in : 10.6secs
```

dpa application mfa

Allows you to enable or disable the multifactor authentication configuration of the Data Protection Advisor application service.

```
dpa application mfa [enable | disable]
dpa app mfa [enable | disable]
```

Command options

--quiet — Suppresses all output except for warning and error messages.

--version — Displays the tool version information.

--help (-h) — Displays the help screen.

Example

```
C:\Program Files\EMC\DPA\services\bin>dpa app mfa disable
Dell Data Protection Advisor

[INFO]mfa has been disabled successfully

Command completed successfully.

Completed in : 5.9secs
```

```
C:\Program Files\EMC\DPA\services\bin>dpa app mfa enable
Dell Data Protection Advisor

[INFO]mfa has been enabled successfully

Command completed successfully.

Completed in : 5.9secs
```

dpa application ping

Tests the connection between the application object, from which it is sent and the defined primary Datastore service.

```
dpa application ping [options]
dpa app pin [options]
```

Command Options

--help (-h) Display help screen

--quiet Display warnings and errors only

dpa application promote

Promotes the application service to a cluster environment. The application service will operate as a object within a cluster of objects. Management of the lifecycle of the service can also be managed through this command line tool. The application service must be installed and stopped for this command to operate.

```
dpa application promote [options]
```

Command options

--bind (-b) <IP_address> — Sets the bind address for the Application service

--user (-u) <username> — For UNIX: (username) is the user account that has read and write access to the shared folder. If omitted root user is used. For windows: (DOMAIN\Username) is the user account that has read write access to the shared folder. If omitted the local system user is used. This user account must have the Log on as a Service Windows permissions enabled.

--path (-p) <path> — Path that is shared among the clusters

--multicast (-m) <multicast address> Sets the multicast address used by the cluster application nodes to communicate with each other. All the application nodes in the cluster must use the same multicast address

--help (-h) — Displays the help screen

--role (-r) <role> Define the role of the application in cluster. Possible values are MASTER or SLAVE <primary_Datastore_IP_address>

--quiet — Suppresses all output except for warning and error messages

Examples

```
dpa app promote --bind 192.168.1.0 --role MASTER --user user1 --path \\shared
```

dpa application restart

Restarts the application service. This command first stops the application service and then starts the service. The application service must be running for this command to operate.

```
dpa application restart [options]
```

Command options

-platform (-p) — Includes platform version information

--help (-h) — Displays the help screen

quiet — Suppresses all output except for warning and error messages

dpa application start

Starts the Application service. The Application service must be installed and stopped for this command to operate.

```
dpa application start [options]
```

Command options

--help (-h) — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

Delays when starting and stopping Data Protection Advisor services

You might experience delays in launching the web console when starting the Data Protection Advisor services. If the Data Protection Advisor services have just been installed, there is a delay of up to 10 minutes in launching the web console. Similarly, if the Data Protection Advisor services are restarted, there might be a delay of about 3 minutes in launching the web console.

NOTE: The Data Protection Advisor services must be running if you want to launch the Data Protection Advisor web console.

dpa application status

Displays the status of application service. For example, RUNNING (STARTING...), RUNNING, STOPPED

```
dpa application status [options]
```

Command options

--help (-h) — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

Examples

```
# dpa application status
Data Protection Advisor
The status of the Application Service is RUNNING
```

dpa application stop

Stops the Application service. The Application service must be installed and running for this command to operate.

```
dpa application stop [options]
```

Command options

--help (-h) — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa application support

Configures the Data Protection Advisor Application server with Secure Remote Support Gateway.

If you plan to use SRS-VE for remote troubleshooting (recommended), ensure that you have the SRS-VE environment installed and configured before Data Protection Advisor installation. The Secure Remote Services Virtual Edition on Dell Technologies Online Support provides information about SRS-VE installations. .

```
dpa application support [options]
```

```
dpa app support [options]
```

Command options

--register (-r) <SRS_IP address> — Registers the Data Protection Advisor Application with Secure Remote Services gateway.

--update (-u) <Data Protection Advisor_new_IP address> — Updates the Secure Remote Services gateway with a new Data Protection Advisor server IP address.

--deregister (-d) — Unregisters the Data Protection Advisor Application server from Secure Remote Services gateway.

--ping (-p) <SRS_IP address> — Pings to obtain the Data Protection Advisor Application server or node information.

--help (-h) — Displays the help screen.

`C:\Program Files\EMC\DPA\services\bin>dpa app support --register 10.11.110.111`

dpa application tlslevel

Sets the TLS protocol version for the Data Protection Advisor Application services. This command will install the service, but will not start it automatically. If the application service is already installed this command will fail.

```
dpa application tlslevel [options]
dpa app tls [options]
```

Command options

1.2 — Set the TLS protocol version for the Data Protection Advisor Application services to TLS version protocol 1.2 only

1.1 — Set the TLS protocol version for the Data Protection Advisor Application services to TLS version protocol 1.1 only.

--help (-h) — Display help screen

--version — Display tool version information

--quiet — Display warnings and warnings and errors only

Example

`dpa app tls 1.2`

dpa application tune

Configures tunable parameters of the Application service for the available host memory resources.

```
dpa application --tune <size> MB|GB
dpa app tune <size> MB|GB
```

Command options

--help (-h) — Displays the help screen.

--quiet — Suppresses all output except for warning and error messages

NOTE: Data Protection Advisor application service must be restarted for tune changes to take effect.

dpa application uninstall

Uninstalls the Application service.

```
dpa application uninstall [options]
```

Command options

--help (-h) — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa application version

Displays the version information for the various functional libraries that make up the application service. The functional libraries include Apollo, Controller, Data Protection Advisor, RemoteX, and UI.

```
dpa application version [options]
```

Command options

-platform (-p) — Includes platform version information

--help (-h) — Displays the help screen.

--quiet — Suppresses all output except for warning and error messages

Examples

```
# dpa application version
[INFO] Version for     Apollo EAR is 1.0.0.3304
[INFO] Version for Controller RAR is 18.1.xxx
[INFO] Version for Data Protection Advisor EAR is 18.1.xxx
[INFO] Version for    Remotex EAR is 1.0.0.3304
[INFO] Version for         UI WAR is 18.1.x.local
```

dpa datastore commands

Use the dpa datastore commands to manage the Data Protection Advisor Datastore service.

```
dpa datastore [options]
dpa datastore configure [options]
dpa datastore dspassword [options]
dpa datastore export [options]
dpa datastore import [options] <import_filename>
dpa datastore install [options]
dpa datastore installcertificate [options]
dpa datastore logtz <time zone>
dpa datastore recreate [options]
dpa datastore replicate [options]
dpa datastore restart [options]
dpa datastore start [options]
dpa datastore status [options]
dpa datastore stop [options]
dpa datastore superpassword [options]
dpa datastore tune <size>MB|GB [options]
dpa datastore uninstall [options]
dpa datastore uninstallcertificate [options]
dpa datastore supportbundle [options] <directory of output file>
dpa datastore version
```

After you start, stop, or restart a service, it may take a number of minutes to complete and may not result in an immediate state change.

dpa datastore configure

Configures the Datastore service, including adding or removing an application service to the list of allowed connections to the datastore service.

```
dpa datastore configure [options]
dpa ds configure [options]
```

Command options

--bind <IP_address> — Set the bind address for the Datastore service. The default is 127.0.0.1

ⓘ **NOTE:** --bind cannot be specified with --add or --delete.

-add <IP_address> — Add an application service node as a valid Datastore client

--delete <IP_address> — Remove an application service node as a valid Datastore client

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

Examples

```
dpa datastore con --add 111.111.1.1
```

dpa datastore dspassword

Resets the Data Protection Advisor Datastore password. You must run the command when the Datastore Service is running.

```
dpa datastore dspassword [options]
dpa ds pwd [options]
```

Command options

--help (-h) — Displays the help screen.

--version — Displays the tool version information

--quiet — Suppresses all output except for warning and error messages

Note the following regarding Datastore password:

- Blank passwords are not supported.
- Minimum length is 9 characters.
- The following are required:
  - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
  - A minimum of 1 numeric symbol
  - A minimum of 1 special character

Example

C:\Program Files\EMC\DPA\services\bin>dpa ds dspassword

```
Data Protection Advisor
Enter new password for the datastore connection from the application node.
```

```
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the datastore connection from the application node:
[INFO] Your new password has been applied to the datastore.
[INFO] For this new password to be used you must ensure that all Data Protection Advisor
application nodes use the same new password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa datastore export

Exports the contents of the Datastore to the filename or pipeline specified. The Datastore service must be installed and running for this command to operate. Any existing filename present will be overwritten.

```
dpa datastore export [options]
```

```
dpa datastore export [options] <directory>
```

Command options

--pipeline — Export to pipe

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

Examples

```
C:\Program Files\EMC\DPA\services\bin>dpa datastore export C:\
```

The default filename of the export is: datastore-<*version*> <*date and time*>.

For example, `datastore-6_2_0_90597-2014-10-01-1135`.

dpa datastore genssc

Generates a self-signed certificate. After you run the `dpa datastore genssc` command, configure SSL on the datastore.

```
dpa datastore genssc [options]
dpa ds genssc [options]
```

Command options

--help (-h) — Displays the help screen

Example

`C:\Program Files\EMC\DPA\services\bin>dpa ds genssc`

dpa datastore import

Imports the contents of the Datastore export file to the Datastore. The import files must be available on the local filesystem. You will be prompted to stop all Application servers that communicate with this Datastore prior running the command. The datastore service must be running for the import command to execute.

```
dpa datastore import [options] <filename>
```

Where <filename> is a previously exported datastore file. The import command replaces the existing Datastore contents with the contents contained in the Datastore export file.

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

<import_filename> — Filename of the exported file to import

Examples

```
# dpa datastore import datastore-2013-02-20-1205
Data Protection Advisor
Datatstore imported from file : datastore-2013-02-20-1205
Imported to the datastore successfully
```

dpa datastore install

Installs the datastore service. The datastore service will operate as a system managed service, manageable through normal operating system service commands. Management of the lifecycle of the service can also be managed through this command line tool. This command will install the service, but will not start it automatically. If the datastore service is already installed this command will fail.

```
dpa datastore install [options]
```

Command options

--help — Displays the help screen --version — Displays the tool version information --quiet — Suppresses all output except for warning and error messages

dpa datastore lockbox

Allows you to create or recreate an existing lockbox of the Data Protection Advisor datastore.

```
dpa datastore lockbox
dpa ds lb
```

Note the following regarding password:

- Blank passwords are not supported.
- Minimum length is 9 characters.
- The following are required:
  - A minimum of 1 uppercase and 1 lowercase alphabetic symbol
  - A minimum of 1 numeric symbol
  - A minimum of 1 special character

Example

```
dpa ds lockbox

Dell Data Protection Advisor

Recreating the lockbox. Are you sure you would like to continue? [Y/N]
Y
[INFO] Recreating lockbox
Enter new password for the lockbox.
The password must have:
    - at least 9 characters
    - at least 1 uppercase letter
    - at least 1 lowercase letter
    - at least 1 special character
    - at least 1 digit

Retype new password for the lockbox :

Command completed successfully.

Completed in : 28.0secs
```

dpa datastore logtz

Configures the Data Protection Advisor Database logs time zone

```
dpa datstore logtz <time zone>
```

```
dpa ds logstz <time zone>
```

Example

dpa datstore logtz 'Europe/Moscow' Configures the Data Protection Advisor Datastore logs time zone to Europe/ Moscow

dpa datstore logtz Data Protection Advisor Datastore logs time zone to GMT

dpa datastore recreate

Recreates the datastore, reverting its content to factory settings.

dpa datastore recreate [options]

```
dpa ds rec [options]
```

Command options

--force (-f) — Override prompt that the current Datastore data is going to be overwritten

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa datastore replicate

Configures the Datastore service to replicate to another instance.

```
dpa ds rep [options]
```

Command options

--addSlave (-a) <hostname/secondary_Datastore_IP_address> — Adds a secondary Datastore to a primary Datastore

-deleteSlave (-d) <hostname/secondary_Datastore_IP_address> — Deletes a secondary Datastore from a primary Datastore

--role (-r) MASTER — Redefines the role of the secondary Datastore to the primary Datastore

--role (-r) SLAVE <primary_Datastore_IP_address> — Redefines the role of the primary Datastore to the secondary Datastore

--failover — Initiates failover between the secondary Datastore and the primary Datastore

--import (-i) <import> — Initializes a secondary Datastore with replica located in specified directory

--export (-e) <export> — Produces a clone of the primary Datastore to specified directory

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa datastore restart

Restarts the Datastore service. This command first stops the Datastore service and then starts the service. The Datastore service must be running for this command to operate.

```
dpa datastore restart [options]
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa datastore start

Starts the datastore service. The Datastore service must be installed and stopped for this command to operate.

```
dpa datastore start [options]
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa datastore status

Displays the status of Datastore service. For example, RUNNING (STARTING...), RUNNING, STOPPED

```
dpa datastore status [options]
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

Examples

```
# dpa datastore status
Data Protection Advisor
```

```
The status of the Datastore Service is RUNNING
```

dpa datastore stop

Stops the Datastore service. The Datastore service must be installed and running for this command to operate.

```
dpa datastore stop [options]
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa datastore superpassword

Resets the Data Protection Advisor Datastore superuser password. The superuser is the user that owns the Data Protection Advisor Database. You must run the command when the Datastore Service is running.

If you use Datastore Replication, you must run this command on all Datastore nodes. Run the command on the primary node first, and only then on all other replication secondary nodes.

```
dpa datastore superpassword [options]
dpa ds superpwd  [options]
```

Command options

--help (-h) — Displays the help screen

--version — Displays the tool version information

--quiet — Suppresses all output except for warning and error messages

Note the following regarding Datastore password:

- Blank passwords are not supported.

Example

C:\Program Files\EMC\DPA\services\bin>dpa ds superpassword

```
Dell Data Protection Advisor
Enter new password for the superuser owning the database.


Retype new password for the superuser owning the database:
[INFO] Your new password has been applied to the superuser owning the database.

Command completed successfully.
```

dpa datastore supportbundle

Gathers support information and stores the DPADPAData Protection Advisor Datastore support bundle zip to the specified directory.

```
dpa datastore supportbundle [options] <directory of output file>
dpa ds supbd [options] <directory of output file>
```

Command options

--help (-h) — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa datastore tune

Configures tunable parameters of the datastore service for the available host memory resources and database connections.

```
dpa datastore tune <size>MB|GB [options]
dpa ds tune <size>MB|GB [options]
```

Command options

--connections (-c) <connections> — Maximum number of concurrent Datastore connections allowed

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

ⓘ **NOTE:** Data Protection Advisor datastore service must be restarted for tune changes to take effect.

dpa datastore uninstall

Uninstalls the Datastore service.

```
dpa datastore uninstall [options]
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa datastore uninstallcertificate

Uninstalls the certificate and disables SSL communication to Data Protection Advisor Datastore server.

```
dpa datastore uninstallcertificate [options]
dpa ds uninscert [options]
```

Command options

--help — Displays the help screen

--version — Displays the tool version information

--quiet — Suppresses all output except for warning and error messages

dpa datastore version

Queries the Datastore version and patch number

```
dpa datstore version [options]
```

```
dpa ds version [options]
```

Command options

--help (-h) — Displays the help screen

dpa service commands

Use the dpa service commands to manage the Data Protection Advisor Application, the Data Protection Advisor Datastore, and the Data Protection Advisor Agent services.

```
dpa service install [options]
dpa service restart [options]
dpa service start [options]
dpa service status [options]
dpa service stop [options]
dpa service uninstall [options]
```

dpa service install

Installs the Datastore service and then the Application service. The services operate as a system managed services, manageable through normal operating system service commands. Management of the lifecycle of the services can also be managed through this command line tool. This command installs the services but does not start them automatically. If the services are already installed, this command fails.

```
dpa service install [options]
dpa svc install [options]
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa service restart

Restarts the Application and Datastore services. This command stops the Application service, stops the Datastore service, and then starts the Datastore service and Application service. The services must be running for this command to operate.

```
dpa service restart [options]
dpa svc restart [options]
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa service start

Starts the Datastore service and then Application service. The services must be installed and stopped for this command to operate.

```
dpa service start [options]
dpa svc start [options]
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa service status

Displays the status of Application and Datastore services. For example, RUNNING (STARTING...), RUNNING, STOPPED

```
dpa service status [options]
dpa svc status [options]
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

Examples

```
# dpa service status
Data Protection Advisor
The status of the Datastore Service is RUNNING
The status of the Application Service is RUNNING (STARTING ...)
```

dpa service stop

Stops the Application service and then the Datastore service. The services must be installed and running for this command to operate.

```
dpa service stop [options]
dpa svc sop [options]
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

dpa service uninstall

Uninstalls the Application service and then the Datastore service.

```
dpa service uninstall [options] <certificate> <key>
dpa svc uninstall [options] <certificate> <key>
```

Command options

--help — Displays the help screen

--quiet — Suppresses all output except for warning and error messages

Loading historical backup job data

The preferred method to gather historical backup data is by using the Data Protection Advisor web console.

Gathering historical backup data using Data Protection Advisor web console provides more information.

After a backup application object is created and requests are assigned, the agent immediately begins gathering data on backup jobs to store in the datastore. However, the agent also can gather data on backup jobs that were run prior to object creation in Data Protection Advisor.

> ⓘ **NOTE:** To commit the data to the Data Protection Advisor server, the installed agent must have previously been started and successfully registered with the Data Protection Advisor Server. However, it need not be currently running in order to load the historical data.

Each backup module has an equivalent executable in the installed Agent's bin directory, `<DPA_HOME>/emc/dpa/agent/bin` directory, where <DPA_Home> is the location of the Data Protection Advisor installation.

The following example collects backup job data run on an NetWorker server:

Example

```
<install_dir>/agent/bin/dpaagent_modnetworker -c -f jobmonitor -t NetWorkerServer_IP -B
"01/01/2012 00:00:00" -E "01/01/2012 00:00:00"
```

Running the executable with the `-?` parameter shows the valid command-line options. Module options applicable to the request (for example, timeformat) may also be specified explicitly on the command line in order to ensure consistent behavior with "normal" data collection. In the case of the DataProtector jobmonitor request, the occupancy option must be specified explicitly if you want historic data to be included in occupancy calculations. The Dell Data Protection Advisor Data Collection Reference Guide provides more information about options.

To load historical backup data, run the agent binary from the command line. You must specifically use some options and parameters from the following table:

Table 33. Options and parameter table

Parameter with option (if required)	Description	Comments
-a	Target specified is the local host. The parameter indicates that the agent is used locally (unlike remotely working).	
-d *<debug_level>*	Debug level for module.	This option requires one of the following parameters: ● Off - no debug logging ● Fatal - log fatal errors only ● Error - log errors only ● Warn - log errors and warnings ● Info - log errors, warnings, and information messages ● Debug - log errors, warnings, information and debug messages ● Debug low - log all messages
-f *<function_name>*	(Mandatory) Name of data gathering function to execute.	This option requires a function name as a parameter. A list of function names can be obtained with the use of '-?' option. An example of the function name is: jobmonitor.
-g *<auth_protocol>*	Authentication protocol.[a]	This option requires one of the following parameters: ● 0 - no authentication ● 1 - for SHA1 ● 2 - for MD5
-i *<tsm_instance>*	Spectrum Protect (TSM) instance name (TSM only).	
-j *<privacy _ protocol>*	Privacy protocol.	This option requires one of the following parameters:

Table 33. Options and parameter table (continued)

Parameter with option (if required)	Description	Comments
		● 0 - no privacy protocol ● 1 - for AES ● 2 - for DES
-l *<log _ file _ name>*	Name and path of the log file to generate when running the command to load historical data. The default log file location is the location from which the command is run.		
-o *<option_name>*	Option name to pass to the module . Option -v can be used with -o.[b]	
-t *<target _ host>*	The host address of the backup application server. The default is localhost.	
-u *<node_uuid>*	Node uuid.	An example of the *node_uuid* parameter value: "123e4567-e89b-12d3-a456-426655440000" .
-v *<value>*	Value of the option. The option '-v' can follow after the option '-o'. [c]	
-B *<start_time>*	Start time from which to gather backup jobs. The format is dd/mm/yyyy hh:mm:dd or Unix epoch time format. [d]	Example of start_time parameter value: "01/01/2012 00:00:00" .
-C	(Gzip) compress output .	
-E *<end_time>*	The end time from which to gather backup jobs. The format is dd/mm/yyyy hh:mm:dd or UNIX epoch time format. [e]	Example of end_time parameter value: "01/01/2012 00:00:00" .
-F	FIPS mode.	
-G *<auth_key>*	Authentication key. [f]	
-I *<data_lifetime>*	Lifetime of data (in seconds, default: 3600).	
-J *<privacy_key>*	Privacy key. [g]	
-O *<output_file>*	The output file where the module stores the output.	
-P *<password_string>* or *<community_string>*	The password to connect to the backup application (apply if required for applications without SNMP) or community string. [h]	
-U *<user_name>*	The username to connect to the backup application. Apply where necessary, if required.	
-V	Shows version information.	

[a] If a module uses SNMP protocol to connect to overseeing object.

[b] An example of the string with one option and its parameter is: "-o pollbatch -v 86400".

[c] An example of the string with one option and its parameter is: "-o pollbatch -v 86400".

[d] If <start time> is specified and <end time> is not, <end time> is set to the current time. This includes all the backup jobs that ended after <start time>. If <end time> is specified and <start time> is not, <start time> is set to 0. This includes all the backup jobs that end before <end time>.

[e] If <start time> is specified and <end time> is not, <end time> is set to the current time. This includes all the backup jobs that ended after <start time>. If <end time> is specified and <start time> is not, <start time> is set to 0. This includes all the backup jobs that end before <end time>.

[f] If a module uses SNMP protocol to connect to overseeing object.

Table 33. Options and parameter table

[g] If a module uses SNMP protocol to connect to overseeing object.

[h] If a module uses SNMP protocol to connect to overseeing object.

The following example collects backup job data run on an Avamar server:

Example

```
dpaagent_modavamar.exe -f jobmonitor -t De-dup-muc.corp.emc.com -U viewuser -P viewuser1
-c -B "01/01/2012 00:00:00" -l /tmp/mod_avamar.log
```

Job summary reports

The job summary reports provide overviews of the totals of backup and maintenance jobs (such as all jobs, successful jobs, failed jobs) that have occurred on backup servers. The summary reports rely on the most up-to-date data in the datastore to produce accurate summary results.

While historical backup job data is loading using the agent command line options, summary reports might display inaccurate totals. It is best to wait until all historical job data is loaded before running summary reports for the loaded historical periods.

4

Environment discovery in Data Protection Advisor

This chapter includes the following sections:

Topics:

Creating, editing, or copying a credential

Credentials are used by the data collection agent to connect to hosts, applications, and devices for data collection. Once a credential is created, it can be assigned when configuring data collection for an object using the Discovery Wizard or from Inventory.

1. Go to **System Settings** > **Credentials** > **Manage Credentials**.
2. Perform one of the following:
   - To create a credential, click **CREATE CREDENTIAL**.
   - To edit a credential, select the credential and then click **EDIT**.
   - To copy a credential, select the credential and then click **SAVE AS**.
   - To delete a credential, select the credential and then click **DELETE**.
3. Type a name for the credential.
4. Select the type of credential.
5. Perform one of the following based on the type of credential:
   - If you select **SNMP**, specify the SNMP version, and do the following:

     If the SNMP version is 2:

     a. Specify the community string (the string with which to connect to the device).
     b. Confirm the community string, and click **OK**.

     If the SNMP version is 3:

     a. Specify the **Username**.
     b. (Optional) Specify the Authentication Protocol. The protocol can be MD5 or SHA1.
     c. Specify the Authentication Password, then confirm it.
     d. (Optional) Specify the Privacy Protocol. The protocol can be AES or DES.
     e. Specify the Privacy Password, then confirm it.
     f. Click **OK**.
   - If you select **Standard**, type the username and password.
   - If you select **UNIX**, type the username and password. Click **Advanced Options** to switch to root (su) after connecting or use sudo to become root after connecting.
   - If you select **Windows**, type the domain, username, and password.
6. Click **OK**.

Configuring the environment for discovery

Discovery overview

The diagram below shows the relationship between the Data Protection Advisor Application object and the Data Protection Advisor Agents that are deployed to monitor your data protection infrastructure.

Some types of devices must be monitored using a Data Protection Advisor Agent that is deployed as a proxy. A proxy is used typically where the object being monitored is hardware and access for agent installation is not possible.

An agent that is directly installed on the same host as the backup manager can monitor most types of backup managers. A proxy agent can remotely monitor the resource-constrained backup managers.

Data Protection Advisor is case insensitive regarding backup pool names. For example, if you define the pools as:

- test_name
- Test_name
- Test_Name

Data Protection Advisor creates one object in the configuration tree. When you run a report on the scope and select this object, you see only one set of numbers.

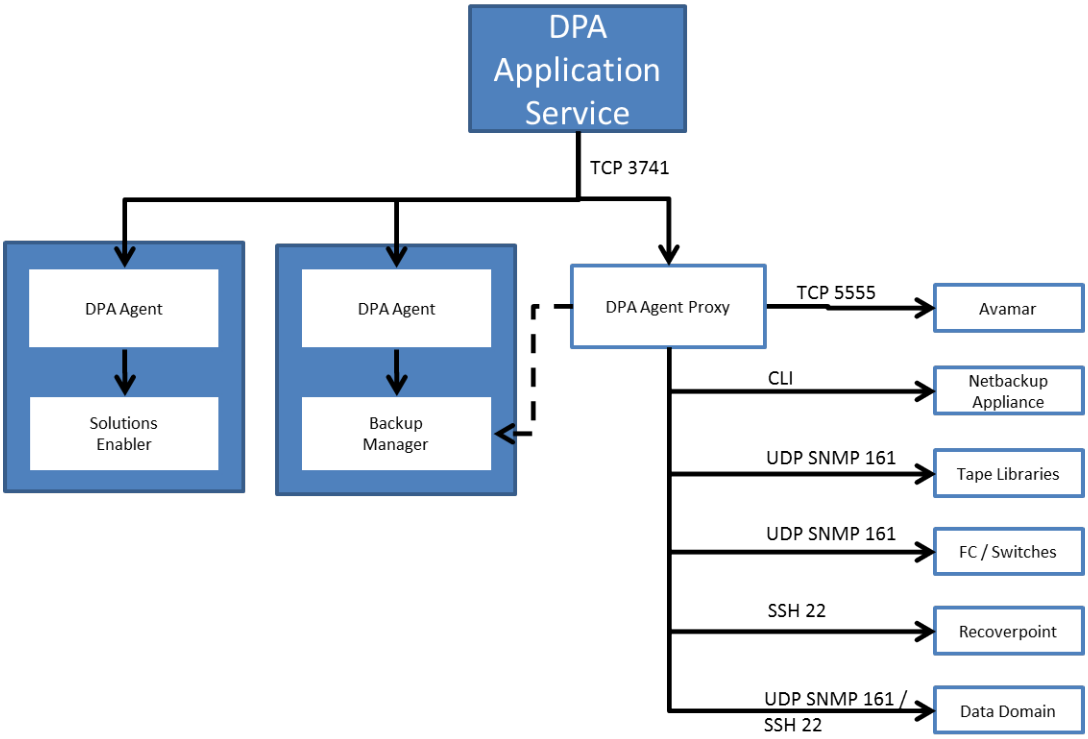


Figure 3. Relationship between Data Protection Advisor Application nodes and Data Protection Advisor Agents monitoring applications

Defining objects to be monitored

To define objects to be monitored in Data Protection Advisor, perform the steps that are described in the following table.

Table 34. Data monitoring setup summary

Step	Description
Check licenses	Check that the licenses to monitor your device, host, or environment have been purchased and installed.

Table 34. Data monitoring setup summary (continued)

Step	Description
Install the agent	If you are monitoring the object from a host other than the Data Protection Advisor server host, you need to install the Data Protection Advisor agent. See Data Protection Advisor Agent installation.
Install third-party binaries or define the object for monitoring	This step is required for remote or agentless (proxy) data collection. You might need to install binaries on the Data Protection Advisor host or the remote agent host to connect to the monitored object. You also might need to define an account or connection on the monitored object. The following sections describes the prerequisite configuration for all objects: ● Configuring for Replication Analysis ● Monitoring of backup applications ● Monitoring of Databases ● Monitoring of RecoverPoint ● Monitoring operating systems ● Monitoring of tape libraries ● Monitoring of switches and I/O devices ● Monitoring of file servers ● Monitoring of protection storage ● Monitoring of StorageTek ACSLS Manager ● Monitoring of disk management servers ● Monitoring of VMware environment
Create or modify the Data Protection Advisor credential	A credential stores the information used to connect to the monitored object. You might need to modify the default credential or create a new one with the account details from the previous step.
Run the Discovery Wizard	Use the Discovery Wizard to define objects to be monitored. Select **Inventory** > **Discovery Wizard**.
Modify data collection default settings	Review the default retention times for all requests and modify if required. Data collection requests are assigned to the object created by the Discovery Wizard. If you want to modify the default data collection, select **Data Collection** > **Defaults** > **Manage Data Collection Defaults** .
Test data collection	After at least 10 minutes of letting the request run, run a report from the object that should include data (for example, Backup Job Summary or a configuration report).

Before you run the Discovery Wizard

1. Check the installed licenses. In the Data Protection Advisor web console, go to **System Settings** > **Licenses**.

   The options that are available for configuration in the Discovery Wizard depend on the types of licenses that you have installed with Data Protection Advisor. If you do not have the correct license installed, the option to create that device or host is disabled in the wizard.

2. If you are performing discovery on a Linux host, ensure that the *libstdc++.so.6* library is installed on the host.
3. Ensure that you take note of the connectivity details outlined in the following table.

Table 35. Connectivity details for configuring data collection through the Discovery Wizard

Item	Value to note for input in Discovery Wizard
Network Configuration Information for Data Protection Advisor Server or agent if agent is remote to Data Protection Advisor server	
Hostname	Value:
IP Address	Value:
Network mask	Value:
Primary DNS server address	Value:
Secondary DNS server address	Value:
Gateway Address	Value:
Time zone	Value:
Credential Information Needed for Discovery of Virtual Disks through SSH	
IP Address of ESX Server	Value:
ESX Server Root Credential	Value:
Credential Information Needed for Discovery of Servers and Arrays	
Server Name/IP	
SSH Credentials	Value:
RPC Credentials	Value:
WMI Credentials	Value:
Solutions Enabler Host Credentials Requires root/administrator credentials	Value:
RPA Credentials	Value:
Credential Information Needed for Monitoring of Oracle Databases	
Oracle username and password required	Value:
Oracle Service Name and Port, specifically the Oracle SID and TNS port	Value:
Oracle Monitor RMAN An oracle user with catalog access to the RMAN schema and the username and password is required.	Value:
Oracle Host Name	Value:
Oracle Monitor Schema If multiple RMAN schemas are present on one Oracle SID, then each RMAN schema owner and username and password are required.	Value:
Credential information needed for SQL Server databases	
SQL Database User Account	Value:
SQL Server Instance	Value:
SQL Database Name	Value:
PostgreSQL Credentials	
PostgreSQL User Account (must be a super user)	Value:
Credential information for Backup Servers, Tape Libraries, I/O Devices	

Table 35. Connectivity details for configuring data collection through the Discovery Wizard (continued)

Item	Value to note for input in Discovery Wizard
CommVault User Account	Value:
Avamar User Account As of Avamar 7.1, Avamar no longer ships with a default password for the viewuser account, and the viewuser account password is set by the user during installation Avamar installation. If you are discovering Avamar 7.1 or later, and it was not upgraded from a previous version, you must create a new set of credentials within Data Protection Advisor. Go to **System Settings** > **Manage Credentials**.	Value:
Data Protector User Account	
IBM Spectrum Protect host, Spectrum Protect Instance Name, Spectrum Protect port, and Spectrum Protect username and password for each Spectrum Protect instance is required.	Value:
Veritas Backup Exec User Account	Value:
SNMP community string for PowerProtect DD SSH username and password for PowerProtect DD, preferably a separate username and password than the PowerProtect DD's system administrator default credentials. Both are required because data is collected using both of the mechanisms.	Value:
SNMP Community String for EDL	Value:
SNMP String for Fibre Channel Switch	Value:
SNMP Community String for Tape Libraries	Value:
SNMP Community String for IP Switch	Value:

Monitoring of backup applications

This section describes how to monitor backup applications.

Monitoring of CA BrightStor ARCserve

CA BrightStor ARCserve servers are monitored from an agent running on the CA BrightStor ARCserve server or from an agent running on any other Windows computer in the environment.

Before starting the Discovery Wizard for monitoring CA BrightStor ARCserve

- You must know the resolvable hostname or IP address of the ARCserve server.
- When running ARCserve 11.x, the hostname must be the host short name. You cannot use aliases.

1. Install the ARCserve Manager on the computer on which the agent is running.

   The agent credentials must match the existing ARCserve account.
2. If you would like Data Protection Advisor to collect job data from 14 days before, and for the reports show data straight away for ARCserve, enable the default historical data from the Job Monitor request. In the Data Protection Advisor web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Monitoring of CommVault

Monitoring CommVault servers with DPA agent running on the CommVault database is supported only on the Microsoft platform.

Before starting the Discovery Wizard for monitoring CommVault

The Data Protection Advisor Agent service must run with a named account if the CommVault SQL Server is using Windows authentication. The named account chosen for the Data Protection Advisor Agent service must have permission for execution of SQL queries on the CommVault SQLServer Database.

Alternatively, if SQL authentication is used, you must define Data Protection Advisor credentials for the CommVault requests; for example, username: cvadmin; password: password of cvadmin user.

You need to know:

- The resolvable hostname or IP address of the CommVault server.
- The database hostname and instance name if the CommVault database is remote to the server.

If you would like Data Protection Advisor to collect job data from 14 days before, and for the reports show data straight away for CommVault, enable the default historical data from the Job Monitor request. In the Data Protection Advisor web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Monitoring of Avamar

Monitor Avamar servers using a Data Protection Advisor agent installed on any remote computer in the environment, including the Data Protection Advisor Server. Do not install a Data Protection Advisor Agent on the Avamar server or storage object.

NOTE: The Avamar version, OS type, and encryption strength is collected when the Data Protection Advisor agent is installed locally on the Avamar Server. You must seek the required permissions from the Avamar administrator before you install the Data Protection Advisor agent locally on the Avamar Server.

To enable monitoring of basic Avamar grid on version 7.2 and later, by the supported Data Protection Advisor deployment, ensure that you select **Remote Data Collection Unit**.

To enable the Clone Operations report to display data when the source grid is selected as the scope for the report, you must monitor the source Avamar grid using the Job Monitor request from an Avamar replication setup.

Before starting the Discovery Wizard for monitoring Avamar

No additional software is required to monitor an Avamar server remotely.

Before you start the Discovery Wizard, you need to know the resolvable hostname or IP address of the Avamar server.

1. To gather data from Avamar, Data Protection Advisor connects directly to the Avamar database. It connects to the mcdb database on the default port for Avamar, which is 5555. If these parameters were modified, edit the Avamar Configuration, Avamar Job Monitor and Avamar Status request options to specify the database name and port in use. In the Data Protection AdvisorA web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.
2. If you would like Data Protection Advisor to collect job data from 14 days before, and for the reports show data straight away for Avamar, enable the default historical data from the Job Monitor request. In the Data Protection Advisor web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.
3. If you are discovering Avamar 7.1 or later, and it was not upgraded from a previous version, you must create a new set of credentials within Data Protection Advisor. Go to **System Settings** > **Credentials** > **Manage Credentials** > **Create Credential**.

   As of Avamar 7.1, Avamar no longer ships with a default password for the viewuser account, and the viewuser account password is set by the user during installation Avamar installation.
4. Create new credentials in the Default Avamar Credentials in the Data Protection Advisor web console from **System Settings** > **Credentials** > **Manage Credentials** as username / password get reset on upgrade.

   When Data Protection Advisor connects to the database, it uses the viewuser account to log in to the database.

About job data gathering after Avamar discovery

Read about Avamar job data gathering after you discover Avamar within Data Protection Advisor.

- When a new Avamar server is discovered, Data Protection Advisor gathers job data from 14 days before.
- Each time the Jobmonitor request is run Data Protection Advisor gathers at most a "batch period" amount of data. This value is configurable and defaults to one day's worth of data.
- After multiple Jobmonitor requests have been run, the time period of gathered jobs catches up to the present time and new backups are gathered.
- The default time between the end of the last Jobmonitor to when a new Jobmonitor request is run, is 5 minutes. This is configurable as with all requests.

Data Collection Request Options by Module provides more information.

Monitoring of NetWorker

Monitor NetWorker either from an agent running on the backup server or remotely using an agent running on the Data Protection Advisor Server or any other remote computer in the environment.

Before starting the Discovery Wizard for monitoring NetWorker

If monitoring NetWorker remotely, the NetWorker client package must be installed on the agent's host. The NetWorker module uses commands such as `jobquery` and `nsradmin` to communicate with the NetWorker server and requires access to the binaries within the NetWorker client package.

- Before you start the Discovery Wizard, you need to know the resolvable hostname or IP address of the NetWorker server.
- If you are monitoring NetWorker 9.0.0.4 and later, ensure that you have the NetWorker server credentials. You will be prompted to enter the NetWorker server credentials to allow the Data Protection Advisor Agent to issue an `nsrauth` and to run nsradmin.

1. If you are monitoring NetWorker 9.0.0.4 and later remotely, install NetWorker Client and NetWorker Extended Client. The NetWorker 9 Client and Extended Client must be installed on the Data Protection Advisor Agent host. If you have a previous version of the NetWorker Client, then you need to upgrade. If you are monitoring older versions of NetWorker, use the NetWorker9 Client and Extended Client to monitor those other versions if the Data Protection Advisor Agent is used to also monitor a NetWorker 9 server.
2. If you are monitoring NetWorker 7.6 or later remotely, the Data Protection Advisor user and the proxy host must be added to the Users list of the NetWorker Administrators User Group. For example, if you are monitoring NetWorker remotely from the host Data Protection Advisor Agent Host and the agent is running as the Windows user Data Protection AdvisorAgent, you must add the following line to the Users list of the properties for Administrators:

   ```
   user=Data Protection AdvisorAgent,host=Data Protection AdvisorAgentHost
   ```

3. If you Data Protection Advisor to collect job data from 14 days before, and for the reports show data straight away for NetWorker, enable the default historical data from the Job Monitor request. In the Data Protection Advisor web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

About job data gathering after NetWorker discovery

Read about NetWorker job data gathering after you discover NetWorker within Data Protection Advisor.

- When a new NetWorker server is discovered, Data Protection Advisor gathers job data from 14 days before.
- After you run multiple Jobmonitor requests the time period of gathered jobs catch up to the present time and new backups are gathered.

As a result of this operation, it will take 7 hours for the jobmonitor request to start gathering current job data. This is because each request is scheduled by default to run every 30 minutes and in each request a maximum of 1 day's data is gathered.Data Collection Request Options by Module provides more information.

Monitoring of Micro Focus Data Protector

An agent can monitor Micro Focus Data Protector servers running on the Data Protector Cell Manager or remotely from another computer.

Before starting the Discovery Wizard for monitoring Micro Focus Data Protector

If monitoring a Cell Manager remotely, follow the same instructions as documented in Monitoring Micro Focus Data Protector remotely.

ⓘ **NOTE:** You cannot assign the status request when monitoring the Data Protector server remotely because it relies on a the `omnisv` command. The command is only available on the Data Protector server.

If you are monitoring a Data Protector environment that uses the Manager of Managers option, you must configure Data Protection Advisor as if monitoring a remote Data Protector server.

To monitor Data Protector remotely, you must install the Data Protector client software on the agent's host and configure the client on the Data Protector Cell Manager so that it has permission to run reports. Monitoring Micro Focus Data Protector remotely provides information on testing connectivity from the agent host.

If you would like Data Protection Advisor to collect job data from 14 days before, and for the reports show data straight away for Data Protector, enable the default historical data from the Job Monitor request. In the Data Protection Advisor web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Gathering occupancy data

Gathering occupancy data is not enabled by default for Data Protector. To enable occupancy data gathering, you must enable the occupancy option for the Data Protector Jobmonitor request and assign the Data Protector Client Occupancy request to the Data Protector client in the **Edit Request** dialog.

You can use the *DP_OCCUPANCY_DB_PATH* environment variable for the Data Protection Advisor Agent to control where the occupancy data is stored when you run the jobmonitor request. If you do not use the *DP_OCCUPANCY_DB_PATH* environment variable, then the system stores the occupancy data in the temporary directory.

ⓘ **NOTE:** Gathering occupancy information for Data Protector can have a significant performance impact on the Data Protector server.

Changing the location of Occupancy database on Linux

1. Stop the Data Protection Advisor Agent.
2. Use the `cd` command to access the `/opt/emc/dpa/agent/etc` directory.
3. Edit the `dpa.custom` file. Add the following to the end of the file:

   ```
   COLLECTOR_DP_OCCUPANCY_DB_PATH=/your/absolute/path/
   export COLLECTOR_DP_OCCUPANCY_DB_PATH
   ```

   Ensure that you include the trailing backward slash (/) character in the path.

4. Restart the Data Protection Advisor Agent

Changing the location of Occupancy database on Windows

1. Stop the Data Protection Advisor Agent.
2. Run the regedit.exe as the administrator user.
3. Expand the HKEY_LOCAL_MACHINE registry key.
4. Expand the SOFTWARE registry key.
5. Create a Dell registry key if one does not already exist.
6. Create a Data Protection Advisor registry key if one does not already exist.
7. Ceate an Agent registry key if one does not already exist.
8. Create a new String registry value with name DP_OCCUPANCY_DB_PATH and set the value to the desired directory path.

For example: `C:\DPA\OccupancyData\` Ensure that you include the trailing slash (\) character in the path.

9. Restart the Data Protection Advisor Agent.

omnirpt patch

HP has released a patch for Data Protector 6.1 that must be installed on a Data Protector 6.1 installation before it can be supported by Data Protection Advisor.

The following table lists the required patch ID by platform.

Table 36. Data Protector 6.1 patch IDs

Platform	Patch ID
Windows	DPWIN_00417
HPUX PA-Risc	PHSS_39512
HPUX IA64	PHSS_39513
Linux	DPLNX_00077
Solaris	DPSOL_00371

The patch is available for General Release from HP from www.hp.com. Type the patch ID into the Search field of the HP home page. You are directed to the patch download page.

Configuring restore job data and updated occupancy retention times

Carry out the following procedure to obtain Jobmonitor function restore job data and updated occupancy retention times.

1. In the Data Protector Manager UI, go to **Internal Database** > **Global Options**.
2. Add the following options:

Option	Description
EnableRestoreReportStats	Enable extended restore session data
LogChangedProtection	Log occupancy changed retention

   Ensure that you set the Value for both options to **1** and select**In Use** for both.

3. Restart the Data Protector services with the `omnisv` command for the changes to take effect.

Monitoring Micro Focus Data Protector remotely

You must install the client software on the computer that monitors the Cell Manager:

1. Launch the Data Protector Manager administration UI to add a client.
2. When selecting the software components to install on the client, ensure that the **User Interface** option is selected.

   The Data Protection Advisor Data Protector module requires access to commands such as `omnirpt` and `omnicellinfo` to gather data from the Cell Manager. These components are only installed when the user interface component is installed, so it is essential to select this option.

3. Configure the client to have permissions to run reports on the Cell Manager. First determine the user for which the Agent process runs:
   - On UNIX systems, the Agent always runs as the root user.
   - On Windows systems, the Agent runs as the Data Protection Advisor Agent service user. To verify the user for the service on a Windows system, launch the Windows service control manager and view the details of the Data Protection Advisor Agent service.
4. Create a user on the Cell Manager that matches the username of the Agent. Type the name of the host in the **user definition** field.
5. Add the user to a Data Protector User Group that has **Reporting and Notifications** and **See Private Objects** permissions.

Typically, this means adding the user to the admin group. However, to restrict a user from inheriting other administrator privileges, create a new group with Reporting and Notification and See Private Objects permissions and add the user to that group.

6. Verify that remote authentication privileges are set up correctly by running the following command from the host of the Agent:

   ```
   omnirpt -tab -report list_sessions -timeframe 06/01/01 12:00
   06/01/30 12:00
   ```

   If successful, this command returns a list of all the sessions that have run on the Data Protector server during the time period specified. If an error indicating insufficient permission to run reports appears, review the configuration settings on the Data Protector server.

   > **NOTE:** Starting from Data Protector 10.x, it is necessary to exchange private authentication keys between the Data Protector Cell Manager and the remote Data Protection Advisor Agent host.

Exchange private authentication keys between Micro Focus Data Protector Cell Manager and the remote Data Protection Advisor Agent host

Perform the following steps:

1. Install DataProtector 10.x on the Collector or the Agent.
2. Create the Data Protection Advisor user with the required permissions.
3. Open TCP port 5555 bi-directionally between Cell Manager and the Collector or the Agent.
4. Use the following commands to exchange the certificate between the Data Protector Cell Manager host and the Data Protection Advisor Agent host:
   - On the Data Protection Advisor Agent host: `omnicc -secure_comm -configure_peer CellManager_Hostname`
   - On DataProtector Cell Manager: `omnicc -secure_comm -configure_peer DPA_Agent_Hostname`

Monitoring of IBM Spectrum Protect

Monitor a Spectrum Protect server from an agent running on the Spectrum Protect Server or remotely from an agent running on a different host, such as the Data Protection Advisor server. If you are monitoring Spectrum Protect remotely, follow the instructions in Monitoring Spectrum Protect remotely before configuring the server in Data Protection Advisor.

Before starting the Discovery Wizard for monitoring Spectrum Protect

The Spectrum Protect Credential must use the name and password of a Spectrum Protect Administrator. The Administrative user does not need full system privileges: Analyst or Operator privileges are sufficient.

1. If the Server being monitored is a shared Library Client, set the agent using the following Data Protection Advisor environment variables (UNIX) or registry settings (Windows) to query the Server's Library Manager to gather certain data:
   - AGENT_TSM_LIBMGRUSERNAME
   - AGENT_TSM_LIBMGRPASSWORD

   By default, the agent uses the same credentials used to query the Library Client to query the Library Manager.
2. If you want Data Protection Advisor to collect job data from 14 days before, and for the reports show data straight away for TSM, enable the default historical data from the Job Monitor request. In the Data Protection Advisor web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.
3. Select **System Settings** > **Manage Credentials** to modify the Spectrum Protect Credentials that are created after you have used the Discovery Wizard to create a Spectrum Protect object.

Gresham Clareti EDT

In Spectrum Protect environments that use Gresham Clareti EDT for device control, Data Protection Advisor communicates with EDT to gather device configuration information by reading information from two files:

- `elm.conf`

- `rc.edt`

Data Protection Advisor reads from `elm.conf` at the following location:

- On Windows, an environment variable called *EDT_DIR* is set by EDT. Data Protection Advisor looks up the location specified in *EDT_DIR*.
- On Unix, Data Protection Advisor looks first in `/opt/GESedt-acsls/bin` for `elm.conf`. If not found, on AIX Data Protection Advisor looks in `/usr/lpp/dtelm/bin`. On other flavours of UNIX/Linux, Data Protection Advisor looks in `/opt/OMIdtelm/bin`.

If the `elm.conf` file is not present in these directories, the registry variable (Windows) or environment variable (UNIX) `AGENT_TSM_ELMCONF_FILENAME` can be set to the location of `elm.conf` if required.

Data Protection Advisor reads from the `rc.edt` file at the following location:

- On Windows, Data Protection AdvisorA looks up the location specified in the environment variable *EDT_DIR*.
- On UNIX, Data Protection Advisor looks first in `/opt/GESedt-acsls/SSI` for `rc.edt`. If not found, on AIX Data Protection Advisor looks in `/usr/lpp/dtelm/bin`. On other flavours of UNIX/Linux, Data Protection Advisor looks in `/opt/OMIdtelm/bin`.

If the `rc.edt` file is not present in these directories, the registry variable (Windows) or environment variable (UNIX) `AGENT_TSM_RCEDT_FILENAME` can be set to the location of `rc.edt` if required.

ⓘ **NOTE:** Because a Spectrum Protect environment using EDT requires the agent to read from these files to collect configuration data, the agent must be on the same server as the Spectrum Protect server.

Monitoring Spectrum Protect remotely

When monitoring a Spectrum Protect instance remotely, you must install the Spectrum Protect client software on the host that will monitor the Spectrum Protect instance. The Spectrum Protect module uses the `dsmadmc` command included with the Spectrum Protect client software to connect to the Spectrum Protect instance and gather data.

In a default Spectrum Protect Client installation on a Windows computer, the administrative components required by Data Protection Advisor are not installed. To install the administrative components:

1. Click **Custom** when prompted during the TSM client installation.
2. Select **Administrative Client Command Line Files** and click **Next**.
   The Spectrum Protect client installation continues.
3. After the Spectrum Protect client installation is complete, initialize the client for the first time by starting the TSM Backup-Archive GUI from the **Start** menu. Use the wizard to configure the client.
4. To configure the client, accept the default **Help me configure the TSM Backup Archive Client** value and click **Next**. Either import an existing options file or create a new one when prompted.
5. Accept the default value **Create a new options file**. You must create a blank options file called`dsm.opt` in the `baclient` directory under the install directory for Spectrum Protect (default `C:\Program Files\Tivoli\TSM`).
6. Continue to progress through the wizard. Complete all of the windows in the wizard until a new options file is created.

About job data gathering after Spectrum Protect discovery

Read about Spectrum Protect job data gathering after you discover Spectrum Protect within Data Protection Advisor.

- When a new Spectrum Protect server is discovered, Data Protection Advisor gathers job data from 14 days before.
- The next time the Job Monitor request runs, the current poll time is set to the next day and data is collected for the next day.
- The current poll time is advanced one day at a time from 14 days back every time the Job Monitor request runs, collecting the data for that day until two weeks of data has been collected. Data collection resumes as normal from then on.
- The poll time default value is 1 day and is user-configurable under the Spectrum Protect Job Monitor request options section.

Data Collection Request Options by Module provides more information.

Monitoring of Veritas Backup Exec

Monitor Veritas Backup Exec servers from an agent running on the Backup Exec server or from an agent running on any other Windows computer in the environment. The Data Protection Advisor Agent service needs to run with a named account that can authenticate with the BackupExec server.

Monitoring of backup servers in a Veritas Cluster Server and Microsoft Cluster Server environment

This section provides configuration information for monitoring backup servers in Veritas Cluster Server and Microsoft Cluster Server (MSCS) environments.

Supported platforms

- Veritas Cluster Server is supported on Linux and Solaris
- MSCS is supported on Windows

The *Data Protection Advisor Software Compatibility Guide* provides more information on supported platform versions.

Monitoring backup applications configured as part of a cluster

You can monitor your backup applications that are configured as part of a cluster in a couple of ways.

To monitor to a backup application in a cluster environment:

1. Install a remote Agent on a system outside of the cluster. Ensure that:
   - the Agent can access the virtual server of the cluster using the required ports.
   - the Agent has any required backup application binaries installed.
2. Discover the virtual server of the cluster by using the Data Protection Advisor Discovery Wizard.
3. Collect data by using the remote Agent.

In this configuration if the server fails over, the cluster name always resolves and provides the backup data.

Alternative procedure for monitoring backup applications configured as part of a cluster

To monitor a backup application in a cluster environment as well as monitor the local host resources

1. Install a local agent on each host in the cluster for host monitoring only.
2. Select one of the agents on the physical servers to monitor the virtual server.

Before starting the Discovery Wizard for monitoring Veritas Backup Exec

To monitor a Veritas Backup Exec backup server remotely, the agent must run as a named user account rather than the Local System account. When installing the agent, you are prompted to specify whether the agent runs using the Local System account or as a named user.

The Backup Exec Credentials must use the username and password of a Windows administrator account on the Backup Exec server.

Select **Admin** > **System** > **Manage Credentials** to modify the Backup Exec Credentials that are created after you have used the Discovery Wizard to create a Backup Exec object.

Monitoring Backup Exec Remotely

To verify that the agent is running, launch the Windows Service Control Manager (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**). Right-click on the Data Protection Advisor agent service and select Properties:

1. Select the **Log On** tab of the Service Properties panel.
2. Select **This Account**.
3. Type the username and password of the local administrator account to run the service.

4. Modify the service account details and click **OK**.
5. Restart the service to activate the changes.

Monitoring Veritas NetBackup

Configure a Veritas NetBackup server that you want to monitor from an agent that runs on the NetBackup primary server or from an agent that runs on a different host such as, the Data Protection Advisor server.

When you monitor Veritas NetBackup from a proxy Agent, the proxy Agent can monitor NetBackup primary servers that are within the same NetBackup Media Manager (EMM) domain. Each EMM Domain requires an Agent.

Before starting the Discovery Wizard for monitoring Veritas NetBackup

Media Server Status data can only be collected if an agent is installed on the Media Server itself. It cannot be collected through proxy.

You must specify the `timeformat` option in the jobmonitor request for gathering openfiles, errors, and mount information. For example, "%m/%d/%Y %T"

If you would like Data Protection Advisor to collect job data from 14 days before, and for the reports show data straight away for NetBackup, enable the default historical data from the Job Monitor request. In the Data Protection Advisor web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Configuring NetBackup authentication for remote data collection

Ensure that you meet the following requirements to remotely gather data:

- Install the NetBackup Remote Administration Console, a component of the NetBackup server software on the agent's host.
- The agent’s host can successfully resolve the NetBackup primary server.
- The NetBackup primary server can successfully resolve the agent’s host.

The following sections describe how to resolve the agent host from the NetBackup primary server on UNIX and Windows.

Configuring NetBackup authentication for remote data collection on UNIX

If the NetBackup primary server is running on a UNIX host, add the name of the host, on which the agent is running to the `bp.conf` file on the NetBackup primary server.

To add the host:

1. Open the `/usr/openv/netbackup/bp.conf` file, and then add the following line:

   `SERVER = `*`Agenthost`*

   where, *Agenthost* is the agent’s hostname. The primary server can resolve the agent’s hostname.

2. Restart NetBackup on the primary server for the changes to take effect.

Configuring NetBackup authentication for remote data collection on Windows

If the NetBackup primary server is running on a Windows computer, add the name of the agent host through the NetBackup Administration Console:

1. On the NetBackup server, open the **NetBackup Administration Console**, and then open the **Master Server Properties** dialog box:

   Select **Netbackup Management** > **Host Properties** > **Master Servers**.

2. Double-click **Host** in the right-hand panel.
3. In the **Master Servers Properties, Servers** field, enter the name of the agent host to the list of additional servers that are allowed to access the primary server.
4. Click **OK**.
5. Restart the NetBackup services. Alternatively, restart the server to activate the changes.

Monitoring of VMware vSphere Data Protection

Monitor VMware vSphere Data Protection (VDP/A) servers using a Data Protection Advisor Agent installed on any remote computer in the environment, including the Data Protection Advisor Server.

Do not install a Data Protection Advisor Agent on the VMware vSphere Data Protection server.

Before starting the Discovery Wizard for monitoring VDP/A

No additional software is required to monitor a VMware vSphere Data Protection server remotely.

Ensure that you know the resolvable hostname or IP address of the VMware vSphere Data Protection server.

To gather data from a VMware vSphere Data Protection server, Data Protection Advisor connects directly to the VDP/A database. It connects to the database on the default port, which is 5555. The port is not configurable.

For monitoring of VDP 5.5, 5.8, and 6.0

1. Edit the `postgressql.conf` file. Uncomment line in the following and change `localhost` to `localhost, Agent_IP_Address`

   ```
   vi /data01/avamar/var/mc/server_data/postgres/data/postgresql.conf
   listen_addresses='localhost,Agent_IP_Address'
   ```

2. Edit the `pg_hba.conf` file. Add the second line:

   ```
   vi /data01/avamar/var/mc/server_data/postgres/data/pg_hba.conf
   host all all Agent_IP_Address/0 trust
   ```

3. Edit the firewall.base, `vi /etc/firewall.base`.
   a. Enable remote access to Postgres db service.
   b. Add the following lines to the bottom of the `firewall.base` file:

      ```
      iptables -I INPUT 1 -p tcp --dport 5555 -j ACCEPT
      iptables -I INPUT 1 -p tcp --dport 5558 -j ACCEPT
      ```

4. Reboot the VDP appliance.

Monitoring of DD Boost Enterprise Applications

Data Protection Advisor supports DD Boost Enterprise Applications (DDBEA) for backing up databases without the use of another backup application, such as backing up Oracle RMAN without the use of NetWorker. The Data Protection Advisor Software Compatibility Guide provides information on supported databases.

If monitoring the Enterprise App for backing up Oracle RMAN, follow the procedure provided in Monitoring of Oracle and Oracle RMAN.

If monitoring the Enterprise App for backing up Microsoft SQL Server, follow the procedure provided in Monitoring of Microsoft SQL Server.

If monitoring the Enterprise App for backing up PostgreSQL, follow the procedure provided in Monitoring of PostgreSQL.

If monitoring the Enterprise App for backing up SAP HANA, follow the procedure provided in Monitoring of SAP HANA.

Monitoring of Databases

This section describes how to monitor databases.

Monitoring of DB2

A DB2 database can be monitored from an agent running on the same host as the DB2 server, or from an agent running on a different host, such as the Data Protection Advisor server. The Data Protection Advisor Agent must be run on Windows or Linux.

Before starting the Discovery Wizard for monitoring DB2

For Data Protection Advisor Agent to collect data from DB2 database, you must copy the DB2 client .jar file to the Data Protection Advisor plugins directory.

1. Create a directory called *plugins* under`<DPA_install_dir>\agent\`.
2. Copy the DB2 client jar file *db2jcc4.jar* to the *plugins* folder under `..\EMC\dpa\agent\`.

   For the custom location or path add following tag: `<PLUGINSDIR>path </PLUGINSDIR> in dpaagent_config.xml` located under `<DPA_install_dir>\agent\etc`

   where *path* is the path of the directory created in step 1.

   For example `<PLUGINSDIR>c:\program files\emc\dpa\agent\plugins</PLUGINSDIR>`
3. If you Data Protection Advisor to collect job data from 14 days before, and for the reports show data straight away for DB2, enable the default historical data from the Job Monitor request. In the Data Protection Advisor web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Permissions

Ensure you have the correct permissions to gather data on DB2.

Ensure that you have Select operations privileges on:

- the `sysibmadm.db_history` view.
- the `<user_name>.UTILSTOP_DPABACKUP` and `sysibm.syscolumns` tables. This is required for version DB2 version 11.1.1.1 and later.

Configuring DB2 to show size field in Backup All Jobs report

You must create the DB2 EVENT MONITOR DPABACKUP on the DB2 database itself for the Data Protection Advisor Agent to send data to the Data Protection Advisor server with the DB2 backup size value.

- Data Protection Advisor supports calculating the backup size only for DB2 version 11.1.1 and later.
- The event monitor must be created by the same user whose credentials are assigned to the DB2 Jobmonitor request.

Carry out this procedure on the DB2 database itself. For information on how to carry out these steps on DB2, consult vendor documentation.

1. Create event: **`CREATE EVENT MONITOR DPABACKUP FOR CHANGE HISTORY WHERE EVENT IN (BACKUP) WRITE TO TABLE autostart`**
2. Turn on the event monitor.
3. Set the event monitor to `DPABACKUP state 1`.
4. Verify that the event has been created correctly. Carry out the backup database online. Type: **`backup database sample online`**

   The new record should be present in the table.
5. Select *__from UTILSTOP_DPABACKUP__.

About job data gathering after discovery

Read about job data gathering after you discover some applications within Data Protection Advisor.

The information in this section applies to the following applications:

- NetWorker
- Avamar
- Spectrum Protect (TSM)
- Data Protector
- Commvault
- NetBackup
- ArcServ
- DB2
- SAP HANA
- RMAN
- MSSQL

With regard to the applications above, note the following:

- When a new server is discovered, Data Protection Advisor gathers job data from 14 days before if you enable this feature.
- The next time the Job Monitor request runs, the current poll time is set to the next day and data is collected for the next day.
- The current poll time is advanced one day at a time from 14 days back every time the Job Monitor request runs, collecting the data for that day until two weeks of data has been collected. Data collection resumes as normal from then on.
- The poll time default value is 1 day and is user-configurable under the Job Monitor request options section.
- When setting data collection, the **Frequency** must always be a lower value than **max data time range each request will gather from**. Otherwise, request does not catch up to the current time and each time the request runs, it falls further behind and does not gather remaining data.

Data Collection Request Options by Module provides more information.

Monitoring of Microsoft SQL Server

Monitor Microsoft SQL Servers from an agent running on the SQL Server database, or from an agent running on any other Windows computer in the environment. The Data Protection Advisor Agent service needs to run with a named account that can authenticate with Microsoft SQL Servers.

NOTE: If the agent is installed with the named account, which is not a member of the local administrator's group, then the permissions for the named account must be modified to read, write, execute, and modify on the Data Protection Advisor Agent installation folder.

Ensure that you specify the firewall inbound rules to allow incoming connections to SQL Server Browser service SQLBrowser.exe. It uses UDP port 1434.

Before starting the Discovery Wizard for monitoring Microsoft SQL Server

To connect to SQL Server using Windows Authentication, the Data Protection Advisor Agent must run as a named user with MS-SQL access and not as the Local System Account. Verify that the service is running as the correct user before proceeding with the configuration of the database.

To monitor clustered SQL Server installations, set Data Protection Advisor to monitor it as a remote target even if the Data Protection Advisor Agent is installed locally on a physical node of the cluster. The target name should be set to the cluster alias name.

Ensure that the Data Protection Advisor Agent has read access to both the Data Protection Advisor Master and the MSDB databases during the Data Protection Advisor discovery test, even if you do not select database monitoring.

Agent requirements for monitoring Microsoft SQL Server

The agent needs to be able to connect to the SQL Server master database in order to gather the data required. The agent can either:

- Use SQL Server Authentication using the credentials of the request (if set).

- Use SQL Server Authentication using the credentials against an explicit master database in the list of databases to be monitored (if set)
- If these are not set, the agent uses Windows Authentication using the logon ID of the agent process.

If none of these are sufficient to connect to the master database, the request will not gather data.

User account requirements for monitoring Microsoft SQL Server

To gather data successfully, the user account used to connect to the SQL Server database must be granted specific privileges. The dbo (database owner) user account has the correct privileges by default.

If you do not want to connect with the dbo user account, configure a user with the following:

- Map the user to the database with the public role.
- Grant explicitly the VIEW SERVER STATE and VIEW DEFINITION privileges (SQL Server 2005 only).

  The VIEW SERVER STATE privilege is granted at the server level. The VIEW DEFINITION privilege might be granted at the server level (under the name VIEW ANY DEFINITION) or at the database, schema, or individual object level.
- Grant explicitly the EXECUTE permission of the system `stored procedure xp_readerrorlog`.

SQL Server 2005 and 2008

To grant server-wide privileges to the SQL Server login used by the agent, including VIEW DEFINITION privileges for all database tables, connect to the SQL Server as an administrator and run:

`GRANT VIEW SERVER STATE TO <login\domain> GRANT VIEW ANY DEFINITION TO <login\domain>`

However, to grant VIEW DEFINITION privileges for only the specific databases that you want to monitor, connect to the SQL Server as an administrator and run:

`GRANT VIEW SERVER STATE TO [login\domain] GRANT VIEW DEFINITION ON DATABASE :: <dbname> TO <username>`

To grant the EXECUTE permission of the system stored procedure xp_readerrorlog run:

`USE Master GO GRANT EXECUTE ON OBJECT::sys.xp_readerrorlog TO ddDBO GO`

Monitoring Microsoft SQL Server for replication analysis

The Data Protection Advisor server must connect as a database user with connect privileges for all of the databases and write privilege for the TEMPDB database. For Windows authentication, the user must be able to connect to all SQL Server databases and should have write privilege for the TEMPDB database.

Enable support of TLS 1.2 only

To enable TLS 1.2 only, the Data Protection Advisor Agent must use ODBC driver, which supports TLS version 1.2.

To use concrete ODBC driver, add the new string value `MSSQLSERVER_DRIVER` in registry:`HKEY_LOCAL_MACHINE\SOFTWARE\EMC\DPA\AGENT` . That value must contain the name of the installed ODBC Driver which supports version TLS 1.2. For example **`SQL Server Native Client 11.0`**

Monitoring of Oracle and Oracle RMAN

Data Protection Advisor can collect data from two parts of Oracle: from the Oracle database itself, where it collects metrics about the database instance; and from Oracle RMAN. In both cases, you must install Oracle client software.

Data Protection Advisor does not ship Oracle client (OCI) libraries with the Data Protection Advisor Agent. You can download the Oracle Instant Client software from oracle.com for the platform/OS you are installing on. Ensure that the architecture version matches your OS and Oracle versions. For example, to collect data from the Oracle 12c database, use the Oracle 12c instant client version. If you are collecting from mixed Oracle versions, use the latest version in your environment for the instant client. For the Data Protection Advisor Agent to collect data from an Oracle database or Oracle RMAN, Data Protection Advisor requires the following libraries for Oracle:

- `libociei.so`

- `libocci.so`
- `libclntsh.so`

  You must create a symbolic link for the `libclntsh.so` library to the current Oracle build directory. Creating symbolic link for current Oracle build directory on UNIX provides information.

Search for the line AGENT_ORACLE_CLIENT_PATH= in the `dpa.config` and the `dpa.custom` file, which is available in `<installdir>/agent/etc/dpa.config` and set the variable to the directory containing the Oracle client libraries - `libclntsh.so`.

You must manually copy it into `AGENT_ORACLE_CLIENT_PATH` in order to work with the Data Protection Advisor Agent.

On Windows this is `OCI.DLL` and on UNIX, it is `libclntsh.so`.

NOTE: The library must be for the same platform as the Data Protection Advisor Agent. Example, if a 64- bit Windows Data Protection Advisor agent is installed, then you must use the 64-bit Windows Oracle library.

You can download the Oracle Database Instant Client at Oracle Database Instant Client.

While installing the Data Protection Advisor Agent, you are prompted to specify if you want to use the Agent to monitor Oracle and if so, provide the location of the Oracle client libraries. On Windows, this action sets a registry setting and on UNIX modifies an environment variable in the `dpa.config` file. If you change the location of the libraries after the install process is completed, then you must perform these steps manually.

Refer the *Oracle Administrator's Guide* for other platforms-specific requirements such as Microsoft Visual Studio Redistributable on Windows.

Creating symbolic link for current Oracle build directory on UNIX

You must create a symbolic link for the `libclntsh.so` library to the current Oracle build directory. You must manually copy it into `AGENT_ORACLE_CLIENT_PATH` in order to work with the Data Protection Advisor Agent.

1. Install using `rpm` command. Run: **`rpm -i oracle.instantclient<version.build.architecture>.rpm`**.
   For example: **`rpm -i oracle.instantclient12.1-basic-12.1.0.2.0-1.x86.rpm`**
   The output of `/usr/lib/oracle/12.1/client64/lib` shows -shows the latest Oracle client. For example, `libclntsh.so.12.1`.
2. Create the symbolic link for libclntsh.so and add execution permission on the files. Run: **`ln -s libclntsh.so<version.build.architecture> libclntsh.so chmod 755 *`**
   For example: **`ln -s libclntsh.so.21.1 libclntsh.so chmod 755 *`**
3. Verify that the current Oracle build is created in `/usr/lib/oracle` (http://docs.oracle.com/cd/B19306_01/server.102/b14357/ape.htm)

Windows

Update the registry entry with the location of the Oracle instant client software:

a. Navigate to the folder where the Oracle client software is located.
b. Use regedit to manually edit the location of the Oracle instant client software.

Manually configuring Data Protection Advisor Agent to monitor Oracle database and Oracle RMAN

To manually configure the Data Protection Advisor Agent to monitor Oracle RMAN, perform one of the following steps:

- On Windows, set the `HKLM\SOFTWARE\EMC\DPA\AGENT` registry of value type REG_SZ as follows:

  Value name: *ORACLE_CLIENT_PATH*

  Value data: **`<directory containing the Oracle client libraries - oci.dll>`**

  NOTE: The registry key is created if you have selected the **Oracle database to be monitored** option while installing the Data Protection Advisor Agent. If the registry key is not created, manually create it.

- On UNIX, modify the `dpa.config` and `dpa.custom` files.

These files are available in the `<installdir>/agent/etc/` directory.

In the files, search for the line `AGENT_ORACLE_CLIENT_PATH=`, and set the variable to the directory that contains the Oracle client libraries - `libclntsh.so`.

Restart the Agent service if you have changed the `dpa.config` file to include the Oracle client path.

ⓘ **NOTE:** Ensure that you discuss RMAN licensing requirements with your Dell Technologies Account Representative.

Before starting the Discovery Wizard for monitoring Oracle

To monitor an Oracle database for data protection data, the agent must connect to the database as an Oracle user.

Data Protection Advisor does not require the operating system password to the Oracle server. Data Protection Advisor requires the Oracle username and password that is used for the RMAN catalog or system catalog queries only.

To connect to the Oracle database from the remote agent, perform the following:

1. Go to the https://www.oracle.com/in/database/technologies/instant-client/linux-x86-64-downloads.html site.
   a. Download the SQL Plus binaries of Oracle.
   b. Download the SDK binaries.
2. Copy the binaries to the folder where the basic installation package of Oracle Instant client is available.
3. Run the following command to connect to the database: `sqlplus.exe <username/Password of Oracle user>@<oracle server hostname:1521/database to connect>`

   ⓘ **NOTE:** If the command fails with the `vcruntime140.dll is missing` error, then download the "Microsoft Visual C++ 2015 redistributable package (x64) download" package and install it. After you install the Microsoft Visual C++ 2015 redistributable package, run the `sqlplus.exe <username/Password of Oracle user>@<oracle server hostname:1521/database to connect>` command to connect to the database.

To gather data successfully for Oracle databases, this user must be able to create and drop global temporary tables, and to perform selects on the following tables and views:

- V_$INSTANCE
- V_$PROCESS
- V_$DATABASE
- V_$PARAMETER
- DBA_DATA_FILES
- V_$SYSTEM_PARAMETER
- V_$DATAFILE
- V_$SESS_IO
- V_$SESSION
- DBA_FREE_SPACE
- V_$SESSMETRIC (Oracle 10 only)
- DBA_TABLESPACES
- DBA_TEMP_FILES
- DBA_EXTENTS
- USER_EXTENTS
- V$LOGFILE
- V$LOG
- AUDIT_ACTIONS
- V$CONTROLFILE

Any user with the SYSDBA role has these privileges by default, so Dell Technologies recommends that you specify a user that has the SYSDBA role when configuring the database for monitoring. If you do not want to use a user with the SYSDBA role to connect, then you can create a separate user and explicitly grant permissions on those tables or grant "create session" followed by SELECT_CATALOG_ROLE privilege and grant permissions to create and drop global temporary tables, as the following example shows:

ⓘ **NOTE:** The following information is required to get Oracle data from a cluster setup.

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT CREATE ANY TABLE TO limited_user;
GRANT SELECT ON V_$INSTANCE TO limited_user;
GRANT SELECT ON V_$PROCESS TO limited_user;
GRANT SELECT ON V_$DATABASE TO limited_user;
GRANT SELECT ON V_$PARAMETER TO limited_user;
GRANT SELECT ON DBA_DATA_FILES TO limited_user;
GRANT SELECT ON V_$SYSTEM_PARAMETER TO limited_user;
GRANT SELECT ON V_$DATAFILE TO limited_user;
GRANT SELECT ON V_$SESS_IO TO limited_user;
GRANT SELECT ON V_$SESSION TO limited_user;
GRANT SELECT ON DBA_FREE_SPACE TO limited_user;
GRANT SELECT ON DBA_TABLESPACES TO limited_user;
GRANT SELECT ON DBA_EXTENTS TO limited_user;
GRANT SELECT ON USER_EXTENTS TO limited_user;
GRANT SELECT ON DBA_TEMP_FILES TO limited_user;
GRANT SELECT ON V_$LOGFILE TO limited_user;
GRANT SELECT ON V_$LOG TO limited_user;
GRANT SELECT ON  AUDIT_ACTIONS TO limited_user;
GRANT SELECT ON V_$CONTROLFILE TO limited_user;
exit;
```

Or

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT CREATE ANY TABLE TO limited_user;
GRANT SELECT_CATALOG_ROLE TO limited_user;
GRANT RESOURCE,CONNECT TO limited_user;
exit
```

Starting with Oracle 12c and later (including RAC installation), Oracle has a multitenant architecture with two types of databases:

- Single multitenant container database (CDB)
- Multiple pluggable database (PDB)

The following users manage this architecture of Oracle:

- Common user — is a user that exists in the root database and all the PDB databases. This user has super privileges to manage the whole database (CDB) and can connect to the root and perform operations.
- Local user — exists only in one PDB and is local to that database only.

NOTE: In Oracle Database 12c Release 1 (12.1.0.1), the name of a common user must begin with C## or c## and the name of a local user must not begin with C## or c##. Starting with Oracle Database 12c Release 1 (12.1.0.2) the name of a common user must begin with characters that are a case-insensitive match to the prefix specified by the `COMMON_USER_PREFIX` initialization parameter. By default, the prefix is C##. The name of a local user must not begin with characters that are a case-insensitive match to the prefix specified by the `COMMON_USER_PREFIX` initialization parameter. Regardless of the value of `COMMON_USER_PREFIX`, the name of a local user can never begin with C## or c##. If the value of `COMMON_USER_PREFIX` is an empty string, then there are no requirements for common or local username with one exception: the name of a local user can never begin with C## or c##. Oracle recommends against using an empty string value because it might result in conflicts between the names of local and common users when a PDB is plugged into a different CDB, or when opening a PDB that was closed when a common user was created. If a database is a non-CDB (also in case if the current installation in not multitenant), a username cannot begin with C## or c##.

To connect to the container database (CDB), you can use a common user that has the SYSDBA role when configuring the database for monitoring. If you do not want to use a user with the SYSDBA role to connect, then you can create a separate common user (see Note above). This must be prefixed with "c##" or "C##" (or with a value that is specified in `COMMON_USER_PREFIX` initialization parameter, see Note above) and explicitly grant permissions on those tables or grant "create session" followed by `SELECT_CATALOG_ROLE` privilege, as in the above example.

To connect to a pluggable database (PDB), you can use a common user that has the SYSDBA role when configuring the database for monitoring. If you do not want to use a Common user with the SYSDBA role to connect, then you can create a PDB specific local user and explicitly grant permissions on those PDB tables or grant "create session" followed by `SELECT_CATALOG_ROLE` privilege of the PDB.

The `GRANT CREATE ANY TABLE` command allows this user to create and drop global temporary tables. Global temporary tables must be created and dropped during some Data Protection Advisor Agent requests. Data Protection Advisor does not create or drop any other tables. To prevent the limited_user from inserting records into any table, you can run the following SQL statement for increased security:

`ALTER USER limited_user QUOTA 0M ON <TABLESPACE>;` where the name of the tablespace for limited_user replaces *<TABLESPACE>*.

Before starting the Discovery Wizard for monitoring RMAN

To monitor an RMAN database for data protection data, the agent must connect to the database as an Oracle user.

Ensure that you have the following information connection parameters from the Oracle DBA or the RMAN catalog or system catalog queries:

- Oracle SID for RMAN Catalog
- Oracle TNS port being used for RMAN Catalog
- Oracle RMAN username and password with required privileges. These are `SELECT` only privileges or `SELECT_CATALOG_ROLE` privileges. For multiple RMAN catalogs on one Oracle Server, you must have the username and password into each schema. Best practice is to use the same username and password across all RMAN catalogs and schemas.
- RMAN schema owner name, and if there are multiple RMAN catalogs on one Oracle Server, every RMAN schema owner name.

To gather data successfully for Oracle RMAN Job Monitor Recovery Catalog, this user must be able to perform selects on the following tables and views:

- V_$RMAN_CONFIGURATION
- RC_BACKUP_SET
- V$PROXY_DATAFILE
- RC_RMAN_BACKUP_JOB_DETAILS
- RC_RMAN_CONFIGURATION
- RC_BACKUP_DATAFILE
- RC_BACKUP_PIECE
- RC_DATAFILE
- RC_DATABASE
- RC_BACKUP_CONTROLFILE
- RC_BACKUP_SPFILE
- RC_BACKUP_SPFILE_DETAILS
- RC_BACKUP_CONTROLFILE_DETAILS
- RC_BACKUP_DATAFILE_DETAILS
- RC_RMAN_STATUS
- RC_BACKUP_ARCHIVELOG_DETAILS
- RC_BACKUP_REDOLOG
- RCVER
- PRODUCT_COMPONENT_VERSION

To gather data successfully for Oracle Job Monitor Control File, this user must be able to perform selects on the following tables and views:

- V_$RMAN_CONFIGURATION
- V_$RMAN_STATUS
- V_$BACKUP_DATAFILE
- V_$BACKUP_PIECE
- V$BACKUP_SET
- V$PROXY_DATAFILE
- V$RMAN_BACKUP_JOB_DETAILS
- V$DATABASE
- V$DATAFILE
- V$BACKUP_DATAFILE_DETAILS
- V$BACKUP_ARCHIVELOG_DETAILS
- V$BACKUP_REDOLOG
- RCVER
- PRODUCT_COMPONENT_VERSION

Any user with the SYSDBA role has these privileges by default, so Dell Technologies recommends that you specify a user that has the SYSDBA role when configuring the database for monitoring. If you do not want to use a user with the SYSDBA role to connect, then you can create a separate user and explicitly grant permissions on those tables or grant "create session" followed by SELECT_CATALOG_ROLE privilege, as the following example shows:

NOTE: The following information is required to get Oracle data from a cluster setup.

For Oracle RMAN Job Monitor Recovery Catalog :

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT CREATE ANY TABLE TO limited_user;
GRANT SELECT ON V_$RMAN_CONFIGURATION TO limited_user;
GRANT SELECT ON RC_BACKUP_SET TO limited_user;
GRANT SELECT ON V$PROXY_DATAFILE TO limited_user;
GRANT SELECT ON RC_RMAN_BACKUP_JOB_DETAILS TO limited_user;
GRANT SELECT ON RC_RMAN_CONFIGURATION TO limited_user;
GRANT SELECT ON RC_BACKUP_DATAFILE TO limited_user;
GRANT SELECT ON RC_BACKUP_PIECE TO limited_user;
GRANT SELECT ON RC_DATAFILE TO limited_user;
GRANT SELECT ON RC_DATABASE TO limited_user;
GRANT SELECT ON RC_BACKUP_CONTROLFILE TO limited_user;
GRANT SELECT ON RC_BACKUP_SPFILE TO limited_user;
GRANT SELECT ON RC_BACKUP_SPFILE_DETAILS TO limited_user;
GRANT SELECT ON RC_BACKUP_CONTROLFILE_DETAILS TO limited_user;
GRANT SELECT ON RC_BACKUP_DATAFILE_DETAILS TO limited_user;
GRANT SELECT ON RC_RMAN_STATUS TO limited_user;
GRANT SELECT ON RC_BACKUP_ARCHIVELOG_DETAILS TO limited_user;
GRANT SELECT ON RC_BACKUP_REDOLOG TO limited_user;
exit;
```

Or

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT CREATE ANY TABLE TO limited_user;
GRANT SELECT_CATALOG_ROLE TO limited_user;
GRANT RESOURCE,CONNECT TO limited_user;
exit
```

By default, a virtual catalog user has no access to the base recovery catalog. The following privileges should be granted for him to get access to metadata:

```
GRANT RECOVERY_CATALOG_OWNER to limited_user;
 GRANT CATALOG for DATABASE db to limited_user;
```

For Oracle Job Monitor Control File:

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT CREATE ANY TABLE TO limited_user;
GRANT SELECT ON V_$RMAN_CONFIGURATION TO limited_user;
GRANT SELECT ON V_$BACKUP_DATAFILE TO limited_user;
GRANT SELECT ON V_$BACKUP_PIECE TO limited_user;
GRANT SELECT ON V_$RMAN_STATUS TO limited_user;
GRANT SELECT ON V_$BACKUP_SET TO limited_user;
GRANT SELECT ON V_$PROXY_DATAFILE TO limited_user;
GRANT SELECT ON V_$RMAN_BACKUP_JOB_DETAILS TO limited_user;
GRANT SELECT ON V_$DATABASE TO limited_user;
GRANT SELECT ON V_$BACKUP_DATAFILE_DETAILS TO limited_user;
GRANT SELECT ON V_$DATAFILE TO limited_user;
GRANT SELECT ON V_$BACKUP_ARCHIVELOG_DETAILS TO limited_user;
GRANT SELECT ON V_$BACKUP_REDOLOG TO limited_user;
GRANT SELECT ON V_$PROXY_DATAFILE TO limited_user;
GRANT SELECT ON V_$RMAN_BACKUP_JOB_DETAILS TO limited_user;
exit;
```

Or

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT CREATE ANY TABLE TO limited_user;
GRANT SELECT_CATALOG_ROLE TO limited_user;
GRANT RESOURCE, CONNECT TO limited_user;
exit
```

Starting with Oracle 12c and later (including RAC installation), Oracle has a multitenant architecture with two types of databases:

- Single multitenant container database (CDB)
- Multiple pluggable database (PDB)

To manage this architecture of Oracle, there are two types of users:

- Common user - is a user that exists in the root database and all the PDB databases. This user has super privileges to manage the whole database (CDB) and can connect to the root and perform operations.
- Local user - exists only in one PDB and is local to that database only.

NOTE: In Oracle Database 12c Release 1 (12.1.0.1), the name of a common user must begin with C## or c## and the name of a local user must not begin with C## or c##. Starting with Oracle Database 12c Release 1 (12.1.0.2) the name of a common user must begin with characters that are a case-insensitive match to the prefix specified by the `COMMON_USER_PREFIX` initialization parameter. By default, the prefix is C##. The name of a local user must not begin with characters that are a case-insensitive match to the prefix specified by the `COMMON_USER_PREFIX` initialization parameter. Regardless of the value of `COMMON_USER_PREFIX`, the name of a local user can never begin with C## or c##. If the value of `COMMON_USER_PREFIX` is an empty string, then there are no requirements for common or local username with one exception: the name of a local user can never begin with C## or c##. Oracle recommends against using an empty string value because it might result in conflicts between the names of local and common users when a PDB is plugged into a different CDB, or when opening a PDB that was closed when a common user was created. If a database is a non-CDB (also in case if the current installation in not multitenant), a username cannot begin with C## or c##.

To connect to the container database (CDB), you can use a common user that has the SYSDBA role when configuring the database for monitoring. If you do not want to use a user with the SYSDBA role to connect, then you can create a separate common user (see Note above). This must be prefixed with "c##" or "C##" (or with a value that is specified in `COMMON_USER_PREFIX` initialization parameter, see Note above) and explicitly grant permissions on those tables or grant "create session" followed by `SELECT_CATALOG_ROLE` privilege, as in the above example.

To connect to a pluggable database (PDB), you can use a common user that has the SYSDBA role when configuring the database for monitoring. If you do not want to use a Common user with the SYSDBA role to connect, then you can create a PDB specific local user and explicitly grant permissions on those PDB tables or grant "create session" followed by `SELECT_CATALOG_ROLE` privilege of the PDB.

If you would like Data Protection Advisor to collect job data from 14 days before, and for the reports show data straight away for Oracle RMAN, enable the default historical data from the Job Monitor request. In the Data Protection Advisor web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

The `GRANT CREATE ANY TABLE` command allows this user to create and drop global temporary tables. Global temporary tables must be created and dropped during some Data Protection Advisor Agent requests. Data Protection Advisor does not create or drop any other tables. To prevent the limited_user from inserting records into any table, you can run the following SQL statement for increased security:

`ALTER USER limited_user QUOTA 0M ON <TABLESPACE>;` where the name of the tablespace for limited_user replaces *<TABLESPACE>*.

Monitoring of PostgreSQL

A PostgreSQL database can be monitored from an agent running on the same host as the PostgreSQL database or from an agent running on a different host, such as the Data Protection Advisor server.

Before starting the Discovery Wizard for monitoring PostgreSQL

To monitor a PostgreSQL database, the agent must connect to the database as a PostgreSQL super user. A super user has the correct privileges by default. We recommend that you specify a super user when configuring the database for monitoring.

To create a super user, the PostgreSQL administrator must be a super user, and create the account as in the following example:

CREATE ROLE xxxxx WITH login superuser password yyyyyy ;

where *xxxxx* is the new username and *yyyyyy* the new user's password.

The following parameters will not be populated in the database server parameters table unless you are connecting to the database as a super user:

- config_file
- data_directory
- dynamic_library_path
- external_pid_file
- hba_file
- ident_file
- krb_server_keyfile
- log_directory
- log_filename
- preload_libraries
- unix_socket_directory

The following items are also unavailable unless you are connecting as a super user:

- In the datafile configuration table, the full path to the datafiles cannot be shown, as the path of the file is found in the data_directory parameter. The string (postgres data directory) is shown instead.
- In the connection status table, the f_command and f_status fields will not be populated with the right information. These fields will be set to <insufficient privileges>.

Connecting to the database as a super user populates all fields.

Monitoring of SAP HANA

A SAP HANA database can be monitored from an agent running on the same host as the SAP HANA server, or from an agent running on a different host, such as the Data Protection Advisor server. The Data Protection Advisor Agent must be run on Windows or Linux.

Before starting the Discovery Wizard for monitoring SAP HANA

For Data Protection Advisor Agent to collect data from SAP HANA database, you must copy the SAP HANA client .jar file to the Data Protection Advisor plugins directory.

1. Obtain the `SAP HANA client.jar` file either from the existing client install (`SAP\hdbclient`) directory, or download it from the SAP Development Tools page.
2. Create a directory called *plugins* under `<DPA_install_dir>\agent\`.
3. Copy the SAP HANA client jar file *ngdbc.jar* to the *plugins* folder under `..\EMC\dpa\agent\`.

   For the custom location or path, add following tag: `<PLUGINSDIR>path </PLUGINSDIR> in dpaagent_config.xml` located under `<DPA_install_dir>\agent\etc`

   Where *path* is the path of the directory that is created in step 1.

   For example, `<PLUGINSDIR>c:\program files\emc\dpa\agent\plugins</PLUGINSDIR>`

4. If you want Data Protection Advisor to collect job data from 14 days before, and for the reports show data straight away for SAP HANA, enable the default historical data from the Job Monitor request. In the Data Protection Advisor web console, go to **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

   > **NOTE:** By default, agent request is configured to connect to port 30115, which is a port, for instance, 01. To collect data from another instance or tenant, edit the **Database Port** option of the assigned request in the **Inventory** section of the Data Protection Advisor UI. Default port numbering convention for SAP HANA is 3NNYY, where NN is the instance ID. Therefore, the SQL port, for instance, 00 of the first tenant database is 30015. Discovery is successful, but data collection fails if the instance ID is incorrect. See the Ports and Connections section of the *SAP HANA Administration Guide* to determine the port number corresponding to your database system layout. For example:

Table 37. Port number for database

Instance ID	DB port
00	30015
01	30115
03	30315

Permissions for discovering data for SAP HANA

To gather data on SAP HANA, the database user must have certain privileges that allow the user to run SELECT queries.

The credentials are used by the Data Protection Advisor Agent to get access to the following tables:

- M_BACKUP_CATALOG view
- M_BACKUP_CATALOG_FILES view

Hdbuserstore is not supported with Data Protection Advisor. As per design, Data Protection Advisor requires the credentials of the SAP HANA database. On discovery, you must provide the same database credentials which exists in Hdbuserstore.

Usually, the privileges granted to the PUBLIC role are sufficient to read that data. For more information, refer to vendor information on privileges required for running SELECT queries.

Monitoring of applications using cloud-based solutions

This section describes how to monitor applications using Data Protection Advisor that is deployed on cloud-based solutions.

Monitoring applications on Amazon Web Services

Data Protection Advisor supports deployment of Data Protection Advisor within Amazon Web Services and on premises for discovery and monitoring of supported backup and monitoring applications on premises or within Amazon Web Services. The Dell Data Protection Advisor Software Compatibility Guide provides information about supported versions of backup and monitoring applications.

- Ensure that you configure the Data Protection Advisor Data Collection Agent in the same Amazon Web Services space as the objects that you plan to monitor by using Amazon Web Services.
- If you are configuring Data Protection Advisor to monitor applications that are deployed on cloud-based solutions using a VPN, ensure that ports and protocols are available across the VPN. If you are using nonstandard ports, work with your Cloud services provider or with Amazon Web Services to open nonstandard ports. Data Protection Advisor port settings provides information about standard Data Protection Advisor ports.

1. Deploy Data Protection Advisor in your Amazon Web Services environment.

   Installing Data Protection Advisor provides information about Data Protection Advisor installation. See Amazon Web Services documentation for specific product requirements.

2. Discover the supported application on the Data Protection Advisor instance within Amazon Web Services.

   The sections in this chapter provide information. For example, to discover and monitor NetWorker, Monitoring of NetWorker provides information.

Monitoring applications on Microsoft Azure

Data Protection Advisor supports deployment of Data Protection Advisor within Azure for discovery and monitoring of supported backup and monitoring applications. The *Data Protection Advisor Software Compatibility Guide* provides information on supported versions of backup and monitoring applications.

1. Deploy Data Protection Advisor in your Azure environment.

   Installing Data Protection Advisor provides information on Data Protection Advisor installation. Refer to Azure documentation for specific product requirements.

2. Discover the supported application on the Data Protection Advisor instance within Azure.

   The sections in this chapter provide information. For example, to discover and monitor NetWorker, Monitoring of NetWorker provides information.

Monitoring applications on Google Cloud Platform

Data Protection Advisor supports deployment of Data Protection Advisor within Google Cloud Platform for discovery and monitoring of supported backup and monitoring applications. The Dell Data Protection Advisor Software Compatibility Guide provides information on supported versions of backup and monitoring applications.

1. Deploy Data Protection Advisor in your Google Cloud Platform environment.

   Installing Data Protection Advisor provides information on Data Protection Advisor installation. Refer to Google Cloud Platform documentation for specific product requirements.

2. Discover the supported application on the Data Protection Advisor instance within Google Cloud Platform.

   The sections in this chapter provide information. For example, to discover and monitor NetWorker, Monitoring of NetWorker provides information.

Monitoring of hosts

This section describes monitoring of hosts.

Data Protection Advisor provides the Host System monitoring option to monitor configuration, performance, and status of the operating system during host discovery.

Monitoring operating systems

Use the Discovery Wizard Host System to monitor configuration, performance, and status of the operating system. There are several Data Protection Advisor modules that gather different types of information, as described in the following table.

Table 38. System monitoring modules

Module	Description
Host	Gathers basic information about the operating system type.
Disk	Gathers configuration, status, and performance information on the disks attached to the host.
Fibre Channel HBA	Gathers configuration, status, and performance information on Fibre Channel HBAs configured on the computer.
File system	Gathers configuration, status, and performance information on the file systems mounted to the host.
Memory	Gathers configuration, status, and performance information on memory in the host.
NetInt	Gathers configuration, status, and performance information on network interface cards in the host.
Process	Gathers information on any processes running on the host.
Processor	Gathers configuration, status, and performance information on all CPUs on the host.

Gathering of data from UNIX operating systems

To perform system monitoring on UNIX computers, install an agent on the host that is to be monitored. It is not possible to gather system information remotely from UNIX computers.

Discovering agent hosts for UNIX for gathering data

UNIX hosts are discovered using SSH or telnet/ftp with root access.

If security requirements do not allow for root credentials to be supplied to Data Protection Advisor, sudo is a workaround that can temporarily elevate a user's credentials to root for specific commands configured in the sudoers file.

Modifying sudoers file for Data Protection Advisor storage discovery

A user can log in to a UNIX host as a non-root user, and use sudo to run SCSI commands successfully to discover storage related information for the host. The following is an example of what needs to be added to the sudoers file

```
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers file.
#
# Host alias specification
# User alias specification
# Cmnd alias specification
# Defaults specification
# User privilege specification
root    ALL=(ALL) ALL
# Uncomment to allow people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL
# Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL
# Samples
# %users  ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users  localhost=/sbin/shutdown -h now
user_alias ALL = (ALL) PASSWD: /var/tmp/IllumAgent/apolloreagent
# Defaults specification
# User privilege specification
root ALL=(ALL) ALL
CMGU ALL=NOPASSWD:CMGEMC
# Uncomment to allow people in group wheel to run all commands
# %wheel ALL=(ALL) ALL
# Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL
# Samples
# %users ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users localhost=/sbin/shutdown -h now
```

#cmguser ALL=(ALL) NOPASSWD: ALL

Gathering of data from Windows operating systems

To gather performance data from a Windows host, you must install Windows Management Infrastructure (WMI) on the Windows host you are monitoring.

It is possible to gather all system monitoring information remotely from Windows computers, with the exception of Fibre Channel HBA information. To gather Fibre Channel HBA information, the agent must be installed on the computer. Monitoring a Windows host remotely provides more details on the steps required to monitor a Windows host remotely.

To set up system monitoring for a system on which an agent is installed, assign the system monitoring requests to the host or group to monitor.

Discovering agent hosts for Windows for gathering data

If application discovery is being performed without an agent, Windows host discovery uses Remote Procedure Calls (RPC) for replication analysis and WWI for System information.

Checking RPC Communication

1. Open the Run dialog box from the Windows **Start** menu.
2. Type:

   ```
   net use \\<servername>\admin$ /user:<username>
   ```

3. Click **Enter**. Type the password.
4. A successful connection should return the following message: `The command completed successfully.`
5. Delete the network map. Type:

   ```
   net use \\servername\admin$ /delete
   ```

Checking WMI Communication

1. Open the Run dialog box from the Windows **Start** menu.
2. Type WBEMtest and click **Connect** in the Windows Management Instrumentation Tester dialog box.
3. In the **Connect** field, type **`\\<servername\root\cimv2`**.
4. In the **Credentials** fields, type the username and password used to connect to the application host you are monitoring.
5. Click **Connect** to return to the Windows Management Instrumentation Tester dialog box. Click **Query**.
6. In the **Enter Query** field, type:

   ```
   select * from win32_processor
   ```

7. Click **Apply**.
   If WMI can connect, data from the application host is displayed.

Monitoring a Windows host remotely

All system information can be gathered remotely from a Windows computer with the exception of Fibre Channel HBA information. To monitor a Windows computer remotely, you must install an agent on another Windows computer. You cannot remotely monitor a Windows computer from an agent running on a UNIX computer.

To monitor a Windows host from another Windows computer, the Data Protection Advisor agent service must run as administrator on the computer performing the monitoring. Modifying the login parameters of the agent service provides more information.

Modifying the login parameters of the agent service

Checking if this is required. To modify the login parameters of the agent service:

1. Launch the Windows Services control manager: **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**).
2. Select the Data Protection Advisor Agent service.
3. Right-click and select **Properties** from the menu.
4. Select the **Log On** tab in the **Properties** dialog box.
5. Select **This Account**.
6. Type the username and password of the administrator that the service to run as.
7. Click **OK** and restart the service.

Monitoring activity on a remote computer

1. Create a host object for the computer to monitor in the web console. The name of the object is the hostname of the remote host. The hostname must be resolvable from the computer on which the agent that will be monitoring the object is running.
2. Assign requests to that object to specify the data to gather.
3. Mark each request as a proxy request and complete the details.
4. To complete the proxy details, type the name of the host for the agent in the **Proxy Host** field.

5. Create a Windows credential for the Administrator account on the computer being monitored. This account can be the name of a Local Administrator or that of a Domain Administrator.
6. Notify the agent that will monitor the server of the changes by reloading the agent.

Monitoring of a host for system data

Monitor an application host for system data from an agent running on the host or another host in the environment.

Before starting the Discovery Wizard for monitoring a host for system data

System data can only be gathered from UNIX systems by an agent local to the UNIX host.

Configuring for Replication Analysis

Use the Discovery Wizard to perform Storage Replication Analysis.

- For ProtectPoint backup and recovery configuration, ensure that you have application discovery ability.
- For ProtectPoint backup and configuration, ensure that you synchronize the time, within a maximum of 1-minute difference, of the host that is protected by ProtectPoint with the Solutions Enabler host that manages the storage array that the application is mapped to.
- Ensure that communication between the monitored host and the recoverability process is enabled:
  - For monitoring Windows servers remotely, you must enable RPC services and ensure that they are accessible to the recoverability agent.
  - For UNIX/Linux remote application monitoring, you must enable SSHD and ensure that it is accessible to the recoverability agent.
  - For UNIX/Linux remote application monitoring, you must enable FTP/Telnet services and ensure that they are accessible to the recoverability agent.

Monitoring of Microsoft Exchange Server

To discover Microsoft Exchange Server, you must discover the host that Microsoft Exchange Server runs on. An Exchange Server can be monitored for recoverability from an agent installed on the same host as the Exchange Server or an agent installed remotely.

NOTE: Microsoft Exchange can only be monitored for replication analysis, and for system information from the Exchange server host.

Before starting the Discovery Wizard for monitoring Microsoft Exchange Server

The account used to connect Data Protection Advisor to the Exchange server must be a domain user with Exchange read-only administrator rights and local administrator rights. Data Protection Advisor does not support replication analysis for two Exchange information stores on a cluster. To connect to the exchange application you must have Exchange read-only administrator rights. To retrieve the disks information from Windows you must be an operating system user with local administrator rights.

Monitoring Oracle for Replication analysis

To monitor an Oracle database for replication analysis, the agent must connect to the database as an Oracle user able to perform selects on the following tables and views:

- DBA_DATA_FILES
- DBA_TEMP_FILES
- DBA_TABLESPACES
- V_$DATAFILE
- V_$LOGFILE
- V_$CONTROLFILE
- V_$LOG_HISTORY
- V_$ARCHIVED_LOG
- V_$INSTANCE

- V_$DATABASE
- V_$PARAMETER
- DICT
- DBA_TAB_COLUMNS

When monitoring Oracle on a Windows platform, the operating system user specified in the Credential must belong to the group ORA_DBA. On UNIX, if you use UNIX authentication, you need not define the credentials in the database.

Updating Oracle statistics

To gather accurate figures on the number of rows and size of tables and indexes, it is important that Oracle statistics are updated on a regular basis. The Oracle documentation contains more details on how to set up a job to update Oracle statistics.

One method to update Oracle statistics on a Schema is to run the following command:

```
exec dbms_stats.gather_schema_stats(ownname => '***SCHEMANAME***', estimate_percent => 5,
cascade => true, options => 'GATHER');
```

Monitoring of RecoverPoint

You must monitor RecoverPoint from an agent installed remotely, the Data Protection Advisor server, for example.

When discovering RecoverPoint, Data Protection Advisor supports discovering only one management IP. Additionally, Data Protection Advisor supports monitoring only the management IP and not the RPA IP. Ensure that you monitor the Management IP and not the RPA IP.

Monitoring of primary storage

This section describes how to monitor primary storage.

Data Protection Advisor breaks primary storage out to the following categories:

- File Servers
- Storage Arrays for Replication Analysis
- Disk Management Servers

Monitoring of file servers

This section describes how to monitor file servers.

Monitoring of EMC File Storage

EMC File Storage must be monitored from an agent running on a remote computer, for example, the Data Protection Advisor server.

ⓘ **NOTE:** EMC File Storage is interchangeably referred to as Celerra File Storage.

Before starting the Discovery Wizard for Monitoring EMC File Storage

The EMC File Storage module gathers information from EMC File Storage through an XML API and directly from the EMC File Storage Control Station. You must create an administrator with specific privileges on the EMC File Storage:

1. Log in to the EMC File Storage Manager web browser interface as an administrator.

   You can also use the command line interface to create a Data Protection Advisor administrator.
2. Navigate to **Security** > **Administrators**.
3. Create a new administrator, with a username of Data Protection Advisor, for example.
4. Select **Local Only Account** and type and confirm a password for the administrator.
5. Select a **Primary Group** of at least opadmin level of privilege. Data Protection Advisor does not need greater privileges than those assigned by opadmin.
6. Enable the following client access options:

- XML API v2 allowed
- Control Station shell allowed

7. Click **OK**.

The Data Protection Advisor Credential used to connect to the EMC File Storage must contain the username and password of the EMC File Storage administrator you created.

Monitoring of disk management servers

This section describes how to monitor disk management servers.

Monitoring of HP Command View

Monitor a HP EVA Disk Array through HP Command View from an agent running on the Command View host, or remotely from an agent running on a different host, such as the Data Protection Advisor server.

The username and password used to gather data must match a valid username and password defined in the CommandView CIM server. You can configure this from the CommandView management interface.

Data Protection Advisor gathers data from HP Command View using SMI-S on the default secure port of 5989.

Monitoring of protection storage

This section describes how to monitor protection storage.

Monitoring of PowerProtect DD

Data Protection Advisor monitors PowerProtect DD backup appliances. For DDOS 4.8, only Tape Drive and Tape Library Status and Configuration information is returned. You must enable the PowerProtect DD analysis request on the PowerProtect DD systems on which you want to gather the data.

Limitations

Data Protection Advisor has a limitation for data collection and reporting of case-sensitive MTree names of a PowerProtect DD System. It is recommended to not have case-sensitive MTree names.

Before starting the Discovery Wizard for monitoring PowerProtect DD

You must enable SNMP on port 161 and SSH on port 22 on the PowerProtect DD backup appliance. You also must set the SNMP community string. You can do this from the command line.

- Ensure that you have user role rights to run SSH requests on the PowerProtect DD system.
- Ensure that you have user admin privileges to run PCR (Physical Capacity Reporting) for monitoring DDOS 5.7 or higher.

1. Log in to the PowerProtect DD appliance console using the sysadmin account.
2. Type the following command to check the existing configuration:

   `snmp show ro-communities`

   `snmp add ro-community <string> hosts <host IP address>`

   Where *<string>* is the selected community string (for example, public) and *<host IP address>* is the IP address of the Data Protection Advisor Agent that you are using to monitor the PowerProtect DD. You have to disable and reenable SNMP for the new string to take effect.

   ```
   snmp disable
   snmp enable
   ```

   To run any PowerProtect DD SNMP data collection request, it requires an `SNMP` type credentials otherwise it returns an error message.

If you are not using a community string of public, you must change the community string that is used in the PowerProtect DD Credential.

You can also set SNMP settings through the **System Settings** tab of the PowerProtect DD Enterprise Manager interface.

3. Edit the Data Protection Advisor PowerProtect DD SSH Credential to specify an SSH username and password configured on the PowerProtect DD device. Go to **System Settings** > **Credentials** > **Manage Credentials** in the Data Protection Advisor web console.

   To run any PowerProtect DD SSH data collection request, it requires a `STANDARD` type credentials otherwise it returns an error message.

   This is required for the following.

   - To ensure configuration of SSH PCR data collection when monitoring DDOS 5.7 or higher.
     - When the request runs, it gathers statistics for the command polling period time, and then it creates the physical capacity measurement schedule on the PowerProtect DD. The PowerProtect DD then gathers the statistics. The statistics are gathered, collected, and sent to the Data Protection Advisor server when the subsequent request runs. As a result, the first time the request runs no data is collected on the reports; data is collected and reported only at the second run of the request. Data Protection Advisor post installation steps for secure communication provides more information.
     - The command polling period is rounded up to a full day time. The command polling period value is set to twice the polling period value with the proviso that the command polling period is at least 2 days time. For example, if the polling period is set to 24 hours or less, Data Protection Advisor gathers statistics for 2 days. If the polling period is set to 3 days, the Data Protection Advisor gather statistics for 6 days.
   - To get LUN information from PowerProtect DD such as devices, device-groups, pools, static-images, and access groups for ProtectPoint SnapVX Backup and Recovery.

Monitoring of StorageTek ACSLS Manager

StorageTek ACSLS Manager cannot be monitored remotely. A Data Protection Advisor agent must be installed on the ACSLS AIX or ACSLS Solaris host.

Before starting the Discovery Wizard for Monitoring StorageTek ACSLS Manager

The agent must be installed and running on the StorageTek ACSLS Manager server that you want to monitor.

- After installing the agent, verify that the *ACS_HOME* value in the *DPA.config* file matches the location in which ACSLS is installed.
- Verify that the *ACSDBDIR* value in the *DPA.config* file matches the path to the *ACSLS DB* folder. The default is `export/home/ACSDB 1.0`.

Monitoring of tape libraries

Data Protection Advisor can gather information about tape libraries and the drives within those tape libraries. When you specify a hostname, ensure that the name of the tape library is resolvable from the host that is monitoring the tape library.

Before starting the Discovery Wizard for monitoring tape libraries

The tape library credentials must contain the read-only community string for the tape library in the **Password** field of the **Credential Properties** dialog box. Unless the community string was modified on the tape library, set the community string to **Public**.

Select **System Settings** > **Credentials** > **Manage Credentials** to modify the tape library credentials that are created after using the Discovery Wizard to create a tape library object.

Monitoring the IBM System Storage TS 3500 tape library

Use the Tape Library Specialist web interface to enable Simple Network Management Protocol (SNMP) requests for the IBM System Storage TS 3500 Tape Library. To enable SNMP requests:

1. Type the Ethernet IP address on the URL line of the browser.
2. Select **Manage Access** > **SNMP Settings**. In the **SNMP Trap Setting** field, view the current setting then click to enable SNMP requests.
3. Ensure that the **SNMP Requests Setting** field is set to **Enabled**.

Monitoring the IBM TotalStorage 3583 tape library

Configure the Remote Management Unit (RMU) to enable SNMP for the IBM TotalStorage 3583 Tape Library. To enable SNMP:

1. In the RMU, click **Configuration**.
2. In the SNMP Configuration region, perform the following:
   - To enable the feature, select **ON** in the **SNMP Enabled** field.
   - To enable or disable SNMP alerts, select **ON** or **OFF** in the **Alerts Enabled** field.
   - In the **Manager** field, type the SNMP server address.
   - In the **Public Name** field, type the name of the read-only SNMP community.
   - In the **Private Name** field, type the name of the read/write SNMP community.
3. Click **Submit** and review the changes.
4. Type the password and click **Confirm**. Redirect the browser if required.
5. Click **Done** to reboot.

Monitoring the IBM TotalStorage 3584 tape library

To enable SNMP from the web interface of the IBM TotalStorage 3584 tape library:

1. From the Welcome screen of the Tape Library Specialist Web Interface, select **Manage Access** > **SMNP Settings**.
2. In the **SNMP Trap Setting** field, view the current setting, and select the button to enable or disable SNMP requests.

Alternately, to enable SNMP requests from the operator panel:

3. From the Activity screen of the tape library operator panel, select **MENU** > **Settings** > **Network** > **SNMP** > **Enable/Disable SNMP Requests** > **ENTER**.
   The screen displays the current status of SNMP requests.
4. Press **UP** or **DOWN** to specify ENABLED or DISABLED for SNMP messaging, and click **ENTER**.

   To accept the new setting and return to the previous screen, click **BACK**.

   The Enable/Disable SNMP Requests screen redisplays the new setting.

Monitoring the Oracle SL24 Tape Autoloader and SL48 tape library

Configure the Remote Management Interface (RMI) to enable SNMP for the Oracle StorageTek SL24 Tape Autoloader or SL48 Tape Library. To enable SNMP:

1. In the RMI, navigate to **Configuration** > **Network**.
2. Ensure the **SNMP Enabled** checkbox is enabled.
3. The **Community Name** string must be contained in the credentials used to connect to this Tape Library in Data Protection Advisor.
4. Click **Submit** and review the changes.

Monitoring the HP StorageWorks tape library

Configure the NeoCenter utility to enable SNMP for the tape library. To enable SNMP:

1. Launch the NeoCenter utility from the host.
2. Select **Configure** from the Main screen menu. The **Configure** dialog box appears.
3. Select the **SNMP Traps** tab.
4. In one of the available **Trap Address** fields, type the IP address of the Data Protection Advisor server.

Monitoring of switches and I/O devices

This section describes how to monitor switches and I/O devices.

Monitoring of Fibre Channel switches

Data Protection Advisor gathers information about ports on Fibre Channel switches, including configuration, connectivity status, and throughput.

When you specify a hostname, ensure that the name of the switch is resolvable on the agent’s host.

Before starting the Discovery Wizard for monitoring Fibre Channel switches

To ensure that Brocade switches return all data, verify that the Fibre Channel Alliance MIB is loaded and enabled on the switch. This MIB might not be installed on the switch by default. To enable FA-MIB support on Brocade switches, log in as an administrator and run the snmpmibcapset command. Change the FA-MIB parameter to Yes. Click Enter to accept the default for the other settings.

For example:

```
telnet <switch>
> snmpmibcapset
The SNMP Mib/Trap Capability has been set to support
 FE-MIB SW-MIB FA-MIB SW-TRAP FA-TRAP
 FA-MIB (yes, y, no, n): [yes]
 SW-TRAP (yes, y, no, n): [enter]
 FA-TRAP (yes, y, no, n): [enter]
 SW-EXTTRAP (yes, y, no, n): [enter]
>
```

Monitoring of IP switches

When you are specifying a hostname, ensure the name of the switch is resolvable on the agent’s host.

Before starting the Discovery Wizard for monitoring IP switches

The IP Switch Credentials must contain the SNMP community string for the IP switch in the **Password** field of the **Credential Properties** dialog box. Unless the community string was modified on the IP switch, set the community string to public.

Select **System Settings** > **Credentials** > **Manage Credentials** to modify the IP Switch Credentials that are created after you have used the Discovery wizard to create an IP switch object.

Monitoring of Xsigo I/O Director

When you are specifying a hostname for the Xsigo I/O Director, ensure the hostname or IP address of the Director is resolvable on the agent’s host.

Before starting the Discovery Wizard for monitoring Xsigo I/O Director

The Xsigo Director SNMP credentials must contain the SNMP community string for the Director in the **Password** field of the Credential. Unless the community string was modified on the Director, set the community string to public.

Select **System Settings** > **Credentials** > **Manage Credentials** to modify the default Xsigo Director SNMP Credentials if required, or to create a new credential.

Virtualization management

This section describes how to monitor a virtualized environment.

Monitoring of VMware environment

Monitor your VMware environment from an agent running on the VirtualCenter Server or remotely from an agent running on a different host, such as the Data Protection Advisor server.

- The Discovery Wizard can be used to add a vCenter server to Data Protection Advisor. Go to **Inventory** > **Discovery Wizard** > **Virtualization Management** .
- To add a vCenter server, you must provide the vCenter hostname and credentials for a vCenter user.
- You can select whether to monitor the vCenter host only or to also monitor the virtual machines that are connected to the vCenter host.
  - If you select to monitor virtual machines, Data Protection Advisor queries the vCenter Server and displays a list of virtual machines. The discovery process can take a while if there are many virtual machines configured on the vCenter server.
  - For each virtual machine, you can select whether you want to discover the host in Data Protection Advisor. Discovering the host adds the host to the Data Protection Advisor inventory.
  - For each virtual machine selected for discovery, you can enable Host System Monitoring, which gathers configuration, performance and analysis data. For each virtual machine selected for Host System Monitoring, you can specify which Data Protection Advisor Agent should be used to monitor the virtual machine. You can change the Data Protection Advisor Agent for multiple machines simultaneously by using CTRL-Click or SHIFT-Click to select multiple systems.
    - Windows virtual machines can have Host System Monitoring performed using a remote Data Protection Advisor Agent such as the Data Protection Advisor Agent installed on the Data Protection Advisor Server; or a local agent, such as Data Protection Advisor Agent installed on each Windows virtual machine.
    - UNIX/ Linux virtual machines must have a Data Protection Advisor Agent installed on the virtual machine for Host System Monitoring, on a local agent.
  - If you choose to do host monitoring for each VM, you must provide Windows credentials for each Windows Virtual Machine being monitored with a remote agent. The credentials can either be a local administrator or a domain administrator. You can change the credential for multiple machines simultaneously by using CNTRL-Click or SHIFT-Click to select multiple systems. You need not provide these credentials if you are monitoring the vCenter.
  - Discovered virtual machines are displayed under the vCenter object in Data Protection Advisor and by default is added to Configuration / Servers / Application Servers group. You can change and add groups for the virtual machines to appear. Go to **Inventory** > **Discovery Wizard** > **Destination Group.**.
- The final screen of the vCenter Discovery Wizard displays a summary of options selected. If you click **Finish**, it adds the objects to Data Protection Advisor and enables monitoring options that are selected.

NOTE:

- For vCenter 6.7 U3, the Data Protection Advisor user must be a member of the SystemConfiguration.Administartors group in vCenter.
- For vCenter 7.0 and later, the Data Protection Advisor user must be a member of the SystemConfiguration.ReadOnly group in vCenter.

Monitoring of RecoverPoint for VMs

You must monitor RecoverPoint for VMs from an agent installed remotely; the Data Protection Advisor server, for example. The Data Protection Advisor Agent must be run on Windows or Linux.

When discovering RecoverPoint for VMs, Data Protection Advisor supports discovering only one management IP. Additionally, Data Protection Advisor supports monitoring only the management IP and not the RPA IP. Ensure that you monitor the Management IP and not the RPA IP.

Before starting the Discovery Wizard for monitoring RecoverPoint

Data Protection Advisor needs to be able to connect to the RecoverPoint environment Command Line Interface (CLI) through a secure SSH connection on port 22. Data Protection Advisor connects to the RecoverPoint appliance using the default CLI user admin, but any defined user with sufficient privileges to run a CLI command remotely using SSH is possible; the monitor account is sufficient.

However, Data Protection Advisor must not connect with the RecoverPoint user boxmgmt because user boxmgmt is reserved for starting the RecoverPoint installation manager automatically.

If you are running RecoverPoint 4.1 where the default user is "monitor," then you must create a new user because the default user specified in Data Protection Advisor no longer exists. If you do not create a new user after installing RecoverPoint 4.1, the request with RecoverPoint Credentials from Data Protection Advisor fails.

Monitoring of clusters

This section describes how to monitor clusters.

Monitoring of Microsoft Server Failover Cluster

To discover Microsoft Server Failover Cluster, you must install the agent on each machine which is in the cluster. The *Data Protection Advisor Software Compatibility Guide* provides information on supported versions.

You must discover Microsoft Server Failover Cluster by a remote agent within the Data Protection Advisor Discovery Wizard. This agent should be installed on one of machine from the cluster. Data Protection Advisor provides two discovery options:

- **Monitor Cluster and hosts which are included in cluster**—If you select this, Data Protection Advisor automatically selects Clustered Server the Cluster with Cluster Configuration and Cluster Status requests.

  Data Protection Advisor assigns the Host Monitoring, Host Configuration, and Host status requests to all hosts which are included in cluster.

- **Monitor only Cluster**—If you select this, Data Protection Advisor automatically selects the Cluster with Cluster Configuration and Cluster status requests.

NOTE: Hosts that are included in cluster will not have the assigned requests.

Monitoring of Veritas Cluster Server and Veritas Infoscale Availability

To discover Veritas Cluster Server and Veritas Infoscale Availability, you must install the agent on each machine which is in the cluster. The *Data Protection Advisor Software Compatibility Guide* provides information on supported versions.

You must discover Veritas Cluster Server and Veritas Infoscale Availability by a remote agent within the Data Protection Advisor Discovery Wizard. This agent should be installed on one of machine from the cluster. Data Protection Advisor provides two discovery options:

- **Monitor Cluster and hosts which are included in cluster**—If you select this, Data Protection Advisor automatically selects Clustered Server the Cluster with Cluster Configuration and Cluster Status requests.

  Data Protection Advisor assigns the Host Monitoring, Host Configuration, and Host status requests to all hosts which are included in cluster.

- **Monitor only Cluster**—If you select this, Data Protection Advisor automatically selects the Cluster with Cluster Configuration and Cluster status requests.

NOTE: Hosts that are included in cluster will not have the assigned requests.

Monitoring of protection servers

This section describes how to monitor protection servers.

Monitoring of PowerProtect Data Manager

The Data Protection Advisor agent running on any host, including the hosts that are installed on the Data Protection Advisor server can monitor both the software and the appliance instances of PowerProtect Data Manager. During PowerProtect Data Manager discovery, Data Protection Advisor uses the remote agent only as the data collection agent and the local agent option is disabled. Agent uses REST API to gather data from PowerProtect Data Manager using the HTTPS protocol. The default port is 8443. PowerProtect Data Manager uses SQLite JDBC to connect to databases. SQLite extracts the appropriate native library file into the temporary folder of the operating system. Hence in Windows and Linux, a nonroot user needs access to the temp folder of the operating system to install the agent.

Manually discovering a host or object

ⓘ **NOTE:** The steps that display vary based on the object that you are discovering.

1. Select **Inventory** > **Discovery Wizard**.
2. In **Objects to Discover**, select one of the following:
   - **Host** and then select Host.
   - **Primary Storage** and then select File Storage.
   - **Protection Storage** and then select PowerProtect DD, Disk Library, NetApp NearStore, or Tape Library.
   - **Switch** and then select Fibre Channel switch, IP switch, or Xsigo switch.
3. Select the option to manually discover the host or object.
4. Identify the application host by hostname or IP address, alias, operating system, credential, security role credential, remote data collection agent, or ports. If you are discovering Primary Storage, Protection Storage, or Switches, then go to step 8.
5. Select **Host System Monitoring** for each host that you want to discover. If you do not select the option during discovery, you can later Add Requests and its options.
6. Select whether a Local or Remote data collection agent that gathers data for this application. If you selected **Host System Monitoring** and your host is running Linux, UNIX, or other non-Windows platforms, select local data collection agent. For Remote data collection agents, select the host with an agent installed.

   ⓘ **NOTE:** If you had specified a Data Collection Agent for RecoverPoint or RecoverPoint for VMs, in the **Viewing and editing Data Collection defaults** area, the agent is displayed here by default.

   To add or edit an agent, specify the fields that are described in the following table:

   Table 39. Fields for Agent configuration

Field	Description
Hostname	Name of the host with the data collection agent installed.
Display Name	Name of the host with the data collection agent installed that displays.
Operating System	Operating system of the host with the data collection agent installed.
Host System Monitoring	Select to monitor configuration, performance, and status for this host.

7. If you selected Host System Monitoring and Remote data collection agent or agentless, select or set the application host credential.

   ⓘ **NOTE:** If you had specified a credential for RecoverPoint or RecoverPoint for VMs in the **Viewing and editing Data Collection defaults** area, the credential is displayed here by default.

8. (optional) Test the connection to the object. If the test fails for host or credential errors, click **BACK** to resolve and then retest.
9. (optional) Add the object to a group or to multiple groups. Press **Ctrl** or **Shift** and click to select multiple objects.
10. (optional) If you have defined custom attributes, select the attributes that you want to apply to the discovered objects. Create attributes in **System Settings** > **Custom Attributes**.
11. Click **FINISH** to start the Discovery Job, which adds the objects to the Object Library and selected destination groups.

About job data gathering after discovery

Read about job data gathering after you discover some applications within Data Protection Advisor.

The information in this section applies to the following applications:

- NetWorker
- Avamar
- Spectrum Protect (TSM)
- Data Protector
- Commvault
- NetBackup

- ArcServ
- DB2
- SAP HANA
- RMAN
- MSSQL

With regard to the applications above, note the following:

- When a new server is discovered, Data Protection Advisor gathers job data from 14 days before if you enable this feature.
- The next time the Job Monitor request runs, the current poll time is set to the next day and data is collected for the next day.
- The current poll time is advanced one day at a time from 14 days back every time the Job Monitor request runs, collecting the data for that day until two weeks of data has been collected. Data collection resumes as normal from then on.
- The poll time default value is 1 day and is user-configurable under the Job Monitor request options section.
- When setting data collection, the **Frequency** must always be a lower value than **max data time range each request will gather from**. Otherwise, request does not catch up to the current time and each time the request runs, it falls further behind and does not gather remaining data.

Data Collection Request Options by Module provides more information.

Monitored objects and groups

Objects overview

Data Protection Advisor discovers the applications and devices in your data protection environment and stores these logical and physical entities as objects in the object library. Discovered objects are grouped into the following categories in the object library:

- Applications
- Hosts
- Storage
- Switches

The following rules apply to objects:

- No two objects can share the same name
- No object can share its name with an alias of another object

The object library enables you to view objects and their attributes.

Searching for objects

You might search for objects to change Data Collection Requests for multiple objects at once.

1. **Select Inventory** > **Object search** .
2. Type the search criteria:
   - In the **Name** field, type the object name. For example, hostname, application name, switch name.
   - In the **Types** field, select the object type. You can choose top-level object types, like Host and Switch; Backup Server, Backup Client, Backup Pool under Backup Application; and all Application object types.
   - In the **Groups** field, select the object group or Smart Group.
   - In the **Groups** field, select **Not In** if you would like to search for objects that are not included in a group, including Smart Groups. **In** is selected by default.
   - In the **Requests** field, filter by request. If you want to search by requests not assigned, select **Not Assigned**. **Assigned** is selected by default.
   - In the **Agent** field, select the Agent from the Data Collection Agent.
   - In the **Attributes** field, select the attribute. In the **Select Attributes** dialog, if you want to search by attributes not assigned, select **Not Assigned**. **Assigned** is selected by default. If you select Not Assigned, the Value and Clear columns are disabled.

   Note the following regarding search for Backup Client, Backup Pool under Backup Application:

   - The **Requests** and **Agent** search options are not available with the search for backup clients and pools.

- Data Collection requests and assignments are not available on results of backup clients and pools searches.

   The **Types** and **Groups** fields are organized the same as within the Report Scope Configuration tree. If you enter multiple search criteria, use AND to join them.

3. Click **Search**.

   The search displays up to 500 items. To limit the number of items below 500, restrict your search criteria.

   NOTE: Data Protection Advisor returns an object in the search bar only if the object is active and is successfully collecting data.

Viewing objects

Select **Inventory** > **Object Library** .

Viewing and editing attributes for multiple objects

Use this procedure to select multiple objects returned from an object search and view and edit the attributes assigned to multiple objects in one action.

1. Search for the objects that you would like to view or edit the attributes.

   Searching for objects provides information.

2. Select the objects that are returned in the search, and right-click to select **Set Attributes**.
   The **Attributes – Multiple Objects** window appears.
3. To edit the attributes for the selected objects, select the check boxes next to the **Name** column and then click **OK**.

Editing data collection for objects

As part of the discovery process, the Data Protection Advisor Discovery Wizard assigns data collection requests directly to an object during object creation. To edit the default data collection requests for a specific object:

Searching for objects provides additional information on editing data collection requests.

1. Select **Inventory** > **Object Library.**
2. **Select a host and then click the** > **Data collection** > **tab.**
3. Click **Properties**.
4. Select a request and then click **Edit**.

Manage Data Collection Defaults provides information on default data collection requests. The *Data Protection Advisor Online Help* set provides procedures to add, edit and view data collection requests.

Groups

A group is a collection of objects. For example, you can create a group of objects that are used by an application. This way, when you apply a policy to the group, the policy is applied to all of the objects within the group.

NOTE: An object can exist in more than one group.

Configuration group

The Configuration group is created by default. The Configuration group is created with an initial structure that groups the data protection environment into Servers, Switches, and Storage. All data protection hosts, devices, and applications discovered by the Discovery Wizard are first added to the Configuration group. Objects that are removed from the Configuration group are not deleted. Objects removed from Configuration group appear under Objects Not In Groups..

Creating groups

1. Go to **Inventory** > **Group Management**.
2. In the object inventory, select **Groups** and click **Create Group**.

3. Type a name for the new group.
4. From the object inventory, select the host or group of hosts that you would like to be in the group.
5. Copy and paste the hosts into the new group you have created.
   Ensure that you do not cut or delete the hosts from their original object inventory location.

Object attributes

Object attributes extend the information that Data Protection Advisor holds about an object. After a custom attribute is created, the attribute can be enabled for any valid objects as per custom attribute settings and a value can be assigned.

When creating or editing an object, attributes are filtered to be associated with one or more specific types of objects, and only to objects with an existing attribute that matches a given value.

For example, an Asset Tag attribute might be created to represent an asset identifier for the physical components of an operating environment (such as hosts, storage arrays, and switches). The Asset Tag attribute need not be assignable to logical components like database instances or processes.

In the attribute definition, the Asset Tag is configured to be associated with a subset of physical object types. You can further configure this attribute to only be associated with physical object types that have an attribute of Business Unit, for example.

Smart Groups

Smart Groups allow users with administrative privileges to create groups that are populated dynamically with information from the results of Data Protection Advisor reports. A Smart Group runs a custom report and then creates objects based on the results of the report.

The main benefit of Smart Groups is that they provide high levels of flexibility. Administrators can set up Smart Groups to dynamically create lists of objects that match specific business and technical criteria.

Creating Smart Groups

The *Data Protection Advisor Online Help* provides more information on creating Smart Groups. Multilevel Smart Group and Single-level Smart Group provide more information on these options.

1. Select **Inventory** > **Group Management.**
2. Click **Create Group** and then **Create Smart Group**.
3. Specify a name for the Smart Group in the **Smart Group Name** field.
4. Specify the Time Zone for the Smart Group.
5. Select an option: **Single-level Smart Group** or **Multilevel Smart Group** and click **Configure Smart Group Level**.
6. Specify the **Generation Frequency**:
   - If you would like Data Protection Advisor to generate the Smart Group at a scheduled time, select frequency type **Once a day at** or **Schedule**.
   - If you would like to generate the Smart Group when you create or edit it, select frequency type **On demand**.
7. Specify the fields for each report object chosen and click **OK**.
8. If you would like to configure the Smart Group to store and report on the content nodes historically, set **Enable History** to **On**.

   By default **Enable History** is configured to **Off**.
9. Click one of the following:
   - **Save and Run** if the Generation Frequency type is set to **Once a day at** or **Schedule**.
   - **OK** if the Generation Frequency type is set to **On demand**.

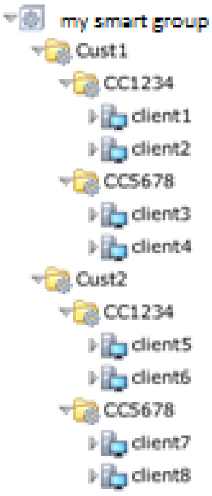
Multilevel Smart Group

Unlike Single-level Smart Group, which returns only one level of child objects that are based on the Smart Group, the Multilevel Smart Group can create multiple levels of child objects from a single Smart Group. It also allows you to configure which fields you want to be used in which level, and what type of object you want to be created. There is no limit to the number of levels that you can configure. If required, you could have a complete mapping of your Data Protection Advisor environment using multilevel Smart Groups.

For example, a report that is used in the Smart Group that returns the data in the following table could be configured to return the object configuration that is shown in the figure below when run.

Table 40. Multilevel Smart Group example

Customer	Cost Center	Client
Cust1	CC1234	Client1
Cust1	CC1234	Client2
Cust1	CC5678	Client3
Cust1	CC5678	Client4
Cust2	CC1234	Client5
Cust2	CC1234	Client6
Cust2	CC5678	Client7
Cust2	CC5678	Client8



- my smart group
  - Cust1
    - CC1234
      - client1
      - client2
    - CC5678
      - client3
      - client4
  - Cust2
    - CC1234
      - client5
      - client6
    - CC5678
      - client7
      - client8

Figure 4. Object library Multilevel Smart Group configuration example

You can assign chargeback and data protection policies to either the Smart Group or to the child objects returned, and see when the structure was last refreshed or generated. By default, the Smart Group generates daily. Also, because hierarchical groups can integrate with external data sources, you can create a single hierarchy Smart Group to create the object structure that may exist in an external system or database.

Only users with permissions to see the Smart Group can see it, expand it, and run reports on it.

Single-level Smart Group

Single-level Smart Group a single set of objects from a report contained in one level of hierarchy. You can assign the same items that you can assign to typical objects, including analyses and scheduled reports. Data Protection Advisor can then generate alerts and reports for a Smart Group outputting objects.

For example, a financial firm might have a convention where the first two characters of each backup client indicate the business unit to which the client is assigned. If the first two characters are a and m, then the backup client belongs to the asset management group. Due to the nature of the business, a large number of clients are created, renamed, or removed daily. Rather than spend a lot of time updating the group configuration each day, the Data Protection Advisor administrator can create a Smart Group that uses the existing Backup Client Configuration report to list each backup client. In the Smart Group, the administrator can filter the results to only contain clients that start with a and m.

As Data Protection Advisor automatically updates the client configuration list every time it obtains data from the backup server, this list is kept up-to-date with whatever changes are made within the backup environment.

Other examples include:

- All backup clients containing exch.
- All hosts with an E: drive.
- All objects with severity 1 alerts in the last day.

Smart Group History

Smart Group History enables you to store and report on the content nodes historically.

The Smart Group History setting allows you to report on changes within Smart Groups, so service providers can provide accurate historical billing.

If the Enable History setting is turned on, then every time the Smart Group is generated subsequently, the history is stored. If the setting is turned off, then all history is deleted and only the current state is stored when the Smart Group is regenerated. By default, the Enable History setting is set to **Off**.

Gathering historical backup data using Data Protection Advisor web console

You can gather historical backup data on Avamar, BackupExec, DB2, Data Protector, NetWorker, NetBackup, Oracle RMAN, SAP HANA, and Spectrum Protect.

Consider the following when you gather historical backup data using Data Protection Advisor web console:

- You cannot gather historical backup data at the host level. You must go one level down in the configuration tree, to the application object. For example, to collect historical data from NetWorker, choose the Networker application object below the host level object.
- You can only gather historical backup from the JobMonitor requests.

1. In the web console, select **Inventory** > **Group Management**.
2. In the configuration tree, select the application object for which you'd like to gather historical backup data.

   The application object **Details** window opens.
3. In the host details window, select the **Data Collection** tab.
4. In **Data Collection**, select the JobMonitor request.
5. Right-click **Run** and select **Gather historical data**.
6. In the **Gather historical data** window, click **OK**.

   The same credentials and data options are available as for the request itself.
7. Click **Close** to the a dialog box that appears confirming that Data Protection Advisor is gathering the historical backup data.
8. Click **History** to view collected tests. The rows highlighted in orange indicate results from a historical backup gather.

Configuring policies, rules, and alerts

Policies and alerts overview

Data Protection Advisor contains customizable policies and rules that control how Data Protection Advisor generates alerts, measures backup and replication performance and determines values for chargeback reporting.

Policies

Data Protection Advisor policies are a collection of user data about how backup and replication should operate in the environment (recoverability and data protection policies) or about the cost of storage and data protection operations (chargeback policies).

Recoverability, backup, and service level management reports then show how the operations in the environment compare to the policy settings, for example, gaps in the recoverability chain for a storage array, or if a backup server is not meeting a Recovery Point Objective.

Data Protection Advisor provides the following policy types:

- Analysis policies - are a collection of one or more rules that are used primarily for generating alerts. Alerts are displayed by default in the **Alerts** section. You can edit the policy to send events to emails, scripts, SNMP traps, or Windows Event Logs. Policies and generating events provides more information.
- Protection policies - are a collection of user data about how backup and replication should operate in the environment. These policies consist of recoverability and protection rules. These are used primarily for generating alerts. Alerts are displayed by default in the **Alerts** section.
- Chargeback policies - are used to determine the cost of storage and data protection operations for chargeback reports.

By default, analysis, protection, and chargeback policies are off for all objects and groups.

Analysis policies

An analysis policy is a collection of one or more rules that is assigned to an object or group. Rules contain the logic for when to issue an alert. The analysis engine compares monitored data to the conditions in a rule, and triggers alerts when a rule is matched. Event-based rules trigger an alert in response to data that is streaming into the Data Protection Advisor server. Schedule-based rules periodically compare data in the Data Protection Advisor Datastore against rules to detect a match. Alerts can contain dynamic textual information and might include populated links to reports. Only analysis policies can generate alerts.

Analysis rule template

An analysis rule template is a set of instructions that defines the rules logic. When a rule template is added to an analysis policy, the Analysis Engine carries out certain operations and then displays the resulting events in the **Alerts** section of the web console.

A rule template consists of the name of the rule along with details that specify how that rule is run.

For example, a rule template can be created to monitor whether a file system is likely to exceed 90% utilization in the next hour.

An Analysis Policy contains multiple rules that apply to different object types. The Analysis Engine only runs the rules that are applicable to a given object. For example, if the object is a switch, then the Analysis Engine will only run the rules in the policy that apply to switches.

Event-based rules versus schedule-based rules

Event-based rules work in response to data that is streaming into the Data Protection Advisor server in real time and triggers alerts. There are five types of conditions for event-based rules:

- Condition filter—Alert on a set condition; for example, backup failed. Condition filter is the most common condition for event-based rules.
- Lack of event—Alert if an event does not occur for defined period of time; for example, Agent is down.
- Prediction—Alert if an event occurs in a defined period of time; for example, Filesystem is filling up.
- Configuration change—Alert if there is any type of change in your configuration; for example, active or inactive, version, OS type, specific fields, increase or decrease by a certain percentage.
- Inventory change—Alert if there is new type of node is auto-created; for example, new RMAN instances.

Schedule-based rules run periodically to check whether to issue an alert. Depending on the type of schedule you have set to collect the data, the alerts could be sent hours after issue was detected in the Data Protection Advisor server.

For both schedule-based rules and event-based rules, you must create a policy that contains a rule, apply the policy to a group of applicable nodes, and ensure that new data that is received for the nodes with the applied policy contains entities that fulfil rules conditions. Data Protection Advisor web console provides a rich rule editor that allows you to create, edit, and customize both event- and schedule-based rules according to your needs. Creating an analysis rule provides more information.

Guidelines for analysis rules components

Consider the following main components when you are creating analysis rules: the category of the rule that you are setting the alert for, object type that you want to monitor and create the alert for, and the object attributes that you are alerting on.

Data Protection Advisor contains a robust repository of analysis rules system rule templates. Before you create a custom analysis rule, check that one does not exist that fits your needs. Go to **Policies** > **Analysis Policies** > **System Rule Templates**. If you select a System Rule Template and edit it, Data Protection Advisor clears out the customizations used to build the policy, which means you do not see how Data Protection Advisor builds the policy.

Analysis rule category

Categories are a way for Data Protection Advisor to store the analysis rules. They are also a way for you to filter and locate analysis rules that you have created. There is no hard and fast rule about choosing a category for analysis rules that you create. If you create a custom analysis rule, select a category from the dropdown that best fits a way that you will remember or find the rule that you are setting. The *Data Protection Advisor Online Help* provides information about the analysis policy categories.

Object type and attributes

The object type and attributes you select depend on the scenario on which you want to trigger the alert; for example, the objects you are monitoring and data being gathered about them. If you need assistance with the data being gathered on the objects that Data Protection Advisor monitors, the *Data Protection Advisor Data Collection Reference Guide* provides information on objects and attributes, where the table names within each module function map to an object, and the field name within each table map to an attribute. Within the object type and alert trigger you can configure and further filter this information for the rule.

Creating an analysis rule

Use the Data Protection Advisor rule editor to create an analysis rule template. The following is a high-level overview of the process. The *Data Protection Advisor Online Help* provides detailed instructions on how to create, edit, or copy an Analysis Rule template.

This is a general procedure for creating an analysis rule. Specific examples for event-based and schedule-based analysis rules follow.

1. In the Data Protection Advisor web console, navigate to **Policies** > **Analysis Policies** > **Custom Rule Templates**.
2. Click **CREATE CUSTOM RULE TEMPLATE**.
   The **Create Rule Template** screen is displayed.
3. Provide a name and description for the alert that is triggered by this rule.
4. Select a category associated with the rule.

   The *Data Protection Advisor Online Help* provides information on rule categories and descriptions.
5. Specify whether the rule is event based or a scheduled rule.

   An event-based rule triggers an alert in response to data that is streaming into the Data Protection Advisor server. A Schedule-based rule runs periodically to check whether to issue an alert.

   If the rule is a Schedule-based rule, set the **Report Parameters Default Values**.
6. Select the appropriate object types:
   - by hierarchy
   - by function
7. Define when and how the alert must be triggered.

   Note that Data Protection Advisor does not support the option to test the `Lack of event` trigger for `Number of samples`, even though the option still appears as valid in the Data Protection Advisor web console. Data Protection Advisor supports the `Number of samples` option for `Time window`.

Creating event-based rules for condition filter

Event-based rules work in response to data that is streaming into the Data Protection Advisor server in real time and triggers alerts on a set condition; for example, backup failed. The condition filter is the most common condition for event-based rules.

The procedure below focuses on creating a rule to alert for a failed backup.

1. Go to **Policies** > **Analysis Policies** > **Custom Rule Templates**, and then click **Create Custom Rule Template**.
2. Populate the **Name/Alert Message** field with a rule name relevant to the condition that you are setting for the rule.
   For example, **`backup failed`**

   If required, you can enter a condition description.

   There is an existing system template rule that is called Backup Failed, which you can edit if you like. This example shows you how to create it from scratch.
3. In the **Category** field, select the relevant category from the list that best fits the rule you are setting.
   For example, **Data Protection**.

In this case, Data Protection is the most appropriate category because you want to alert on data that is not protected.

4. Configure the object type. For this example, to alert on backups that have failed on each backup client, select the Backupjob object.
   a. In **Object Type**, click **Select**.
      The **Select Object Types** dialog box appears.
   b. Expand Backup Applications, expand the BackupClient object, and then select **Backupjob** from the **Select Object Type** list and click **SELECT OBJECT TYPE**.

      You can use the filter function to find the object you would like to monitor on.

      The object type that you select depends on the scenario on which you want to trigger the alert.
5. Configure the alert trigger. For this example, to look only at failed jobs, select the trigger, and then set conditions filters to find only the failed jobs:
   a. In the **Alert Trigger** section, click **SELECT**.
   b. In the **Select Alert Trigger** dialog box, select **Conditions Filter**, and then click **SELECT & EDIT ALERT TRIGGER**.
   c. In the **Edit Filter** dialog box, click **+ ADD CONDITION** to add the condition for the filter, and then click the left **SELECT VALUE**.
   d. In the **Select Value** dialog box:
      - From the **Value Type** list, select **Attribute**, and then click **Browse**.

        In the **Browse Attributes** dialog box, select the required attribute by using filters on the column headers, and then click **SELECT ATTRIBUTE**.

        Click **OK**.
      - From the **Value Type** list, select **Calculated Value**, and add function, parameter, and attribute to specify a mathematical expression.

        To add a function, select the function, select the attribute, select the interval, and then select the condition.

        NOTE: Configure the function according to the attributes of the function. For example, the **Average** function has the `Select Attribute`, `Select Interval`, and `Select Condition` attributes.

        Click **OK**.

        Creating event-based rules for condition filter using calculated value provides more information about the calculated value.
   e. In the **Edit Filter** dialog box, from the **SELECT OPERATOR** list, select **Is**.
   f. Click the right **SELECT VALUE**.
   g. In the **Select Value** dialog box:
      i. From the **Value Type** list, select **Static Value**.

         The other value types are:

         - **Attribute**: Enables you to select an attribute as the value.
         - **Parameter**: Enables you to create a parameter, and use it as the value.
         - **Calculated Value**: Enables you to create a mathematical expression by using functions and use the expression as the value. Creating event-based rules for condition filter using calculated value provides more information about the calculated value.
      ii. From the **Value** list, select **Failed**.
      iii. Click **OK**.
   h. In the **Edit Filter** dialog box, click **OK**.

   According to the requirement, configure and filter the rule alert trigger.

   NOTE: To edit an **Alert Trigger**, click **Edit** in the **Alert Trigger** section, and perform steps 5c through 5h.
6. Configure the alert:
   a. In the **Alert** section, click **Select**.
      The **Edit Alert** dialog box appears.
   b. On the **Alert Fields** tab, select the severity from the list.
   c. On the **Description & Resolution** tab, specify the description and resolution information that you want to include in the alert.

d. On the **Associated Reports** tab, either select a system template report or create a custom report to be generated after the alert appears.

7. Click one of the save options.

Creating event-based rules for condition filter using calculated value

Create a rule for condition filter using the **Calculated Value** option. The **Calculated Value** option allows the user to build mathematical expression that can be used to create a rule.

The following procedure provides information about how to use **Calculated Value** option to create a rules filter. Perform the following steps in the **Select Value** screen.

1. When you select **Calculated Value** in the `Value Type` drop-down list, a text box for entering a mathematical expression is enabled.
2. Click one of the following options to create a mathematical expression:
   - **Add Function** - The available functions are *Average*, *Sum*, *Count*, *Max*, and *Min*.
   - **Add Parameter** - This option allows you to create a parameter, or select an existing parameter.
   - **Add Attribute** - This option allows you to choose an attribute that is available in the system.
3. Click **Add Function**, and select the appropriate function.

   The syntax for all the functions is same.

   ```
   Average(Select Attribute, Select Interval, Select Condition (Optional))
   ```

   a. Click *Select Attribute* variable to browse the available attributes.
   The **Browse Attributes** page is displayed.

   b. Select the appropriate attribute, and then click **Select Attribute** in the **Select Attribute** window.
   The *Select Attribute* variable is updated in the function.

   c. Click *Select Interval* variable to configure the interval.
   The **Select Interval** page is displayed.

   d. Configure the `Interval Type`, and the click **Select** in the **Select Interval** page.

   Two options are available:
   - Time Period - This option allows you to configure a static value or a parameter.
   - Number of Samples - Only static values are allowed.

   e. Click *Select Condition (Optional)* variable to add a condition using attribute, operator, and values.

   This step is similar to adding a conditional filter.
4. Click **Add Parameter** to open the drop-down list.

   The syntax for the parameter is:

   ```
   Parameter:Default Value
   ```
5. Click **Create New Parameter** to create a parameter:

   a. Select **Create New Parameter** to go to the **Add Parameter** page.

   b. Configure the following in the **Add Parameter** page.
   - **`Parameter Name`**
   - **`Default Valuer`**

   c. Click **Add** to add the parameter to the filter.
6. Click **Select Existing Parameter** to add an existing parameter in the **Select Parameter** page.
7. Click **Add Attribute** to browse the attributes.
   The **Browse Attribute** page is displayed.
8. Select the appropriate attribute, and then click **Select Attribute**.
9. Once the mathematical expression is built, click **OK** to save the filter.

Creating event-based rules for configuration change

Event-based rules work in response to data that is streaming into the Data Protection Advisor server in real-time and triggers alerts for any type of configuration changes. For example, changes for active or inactive, version, OS type, specific fields, increase or decrease by a certain percentage of any metric that Data Protection Advisor monitors.

This procedure focuses on a change from client active to inactive.

1. Go to **Policies** > **Analysis Policies** > **Custom Rule Templates**, and then click **Create Custom Rule Template**.
2. Populate the **Name/Alert Message** field with a rule name relevant to configuration change you are triggering the alert for. For example, **`client active status changed`**

   You can enter a condition description as well, if you like. This is optional.
3. In the **Category** field, select **Change Management** from the dropdown.
4. Configure the object type:
   a. In **Object Type**, click **Select**.
   The **Select Object Types** window opens.
   b. Expand Backup Applications, and select **Backup Client** from the **Select Object Type** list and click **Select Object Type**.
5. Configure the alert trigger. For this example, we want to look any client that changed from active to inactive, so we select the appropriate trigger.
   a. In **Alert Trigger**, click **Select**.
   The **Select Alert Trigger** window opens.
   b. Select **Change Control** radio button and then click **Select and Edit Filter**.
   The **Edit Alert Trigger - Change Control** window opens.
   c. Select **ClientConfig** from the dropdown.
   d. Select the box next to **Active** and click **OK**.

   Note that this rule configuration alerts on any changes in this field, not just active to inactive.

   No conditions filters are needed because we want to see the configuration change on all clients.
6. Configure the alert:
   a. In **Alert**, click **Select**.
   The **Edit Alert** window opens.
   b. In the **Alert Fields** tab, select the severity from the dropdown.
   c. In the **Description & Resolution** tab, configure any description and resolution information you want to be sent with the alert.
   d. In the Associated Reports tab, select a system template report or create a custom report that you would like to be generated upon the alert.
7. Click one of the save options.

Creating event-based rules for lack of event

Event-based rules work in response to data that is streaming into the Data Protection Advisor server in real-time and triggers an alert if an event does not occur for defined period of time; for example, Agent is down.

The procedure focuses on creating a rule to alert for production Agent is down, and to keep generating the alert every hour that the production Agent is down.

1. Go to **Policies** > **Analysis Policies** > **Custom Rule Templates**, and then click **Create Custom Rule Template**.
2. Populate the **Name/Alert Message** field with a rule name relevant to the lack of event for which you are setting for the rule.
   For example, **`Data Protection Advisor Agent down`**

   You can enter a condition description as well, if you like. This is optional.
3. In the **Category** field, select the relevant category from the dropdown that best fits the rule you are setting.
   For example, **Administrative**.
4. Configure the object type. For this example, we want to alert on Agents that have gone down, so we select the AgentStatus.
   a. In **Object Type**, click **Select**.
   The **Select Object Types** window opens.
   b. Expand the Host object, and then select **AgentStatus** from the **Select Object Type** list and click **Select Object Type**.

   You can use the filter function to easily find the object you would like to monitor on.

   The object type you select depends on the scenario on which you want to trigger the alert.
5. Configure the alert trigger. For this example, we want to look only at production Agents that have gone down, so we select the trigger and set conditions filters to find only Agents that are down:
   a. In **Alert Trigger**, click **Select**.
   The **Select Alert Trigger** window opens.
   b. Select **Event/Data Collection Did Not Occurr** radio button and then click **Select and Edit Alert Trigger**.

The **Edit Alert Trigger** window opens.

c. For option 1, Select what you want to monitor, select the radio buttons for **Event did not occur** and **AgentStatus**.
d. For option 2, select the radio button next to **Keep Generating**.
e. For option 3, if you want to specify a type of hostname with a naming convention, for example, *prod* for production, select **Edit Conditions Filter** radio button and then click **Select Attribute**.
f. Ensure that **Attribute** radio button is selected for **Value Type** field and click **Browse** for the **Attribute** field.
g. In **Browse Attributes**, select the **name** attribute and then click **OK**.
h. Click **Select Operator** and set a value of **Contains** and click **OK**.
i. Click **Select Value**, select the **Static Value** radio button, in the **Value** field type `prod` and click **OK**.
j. Click **OK** in the **Edit Filter** window.
k. For option 4, select the radio button next to **Time Period** and select **Static Value**from the drop down and select **1** from the number dropdown and **hours** from the time period dropdown, and then click **OK**.

The scenario for which you are configuring the alert affects how you configure and how, if at all, you further filter rule alert trigger.

6. Configure the alert:
   a. In **Alert**, click **Select**.
   The **Edit Alert** window opens.
   b. In the **Alert Fields** tab, select the severity from the dropdown.
   c. In the **Description & Resolution** tab, configure any description and resolution information you want to be sent with the alert.
   d. In the Associated Reports tab, select a system template report or create a custom report that you would like to be generated upon the alert.
7. Click one of the save options.

Creating event-based rules for inventory change

Event-based rules work in response to data that is streaming into the Data Protection Advisor server in real-time and triggers alerts if there is new type of node is auto-created.

The procedure focuses on creating a rule to alert when an RMAN backup client instance is auto-created.

1. Go to **Policies** > **Analysis Policies** > **Custom Rule Templates**, and then click **Create Custom Rule Template**.
2. Populate the **Name/Alert Message** field with a rule name relevant to the condition you are setting for the rule.
   For example, `new RMAN database backed up to central recovery catalog`

   You can enter a condition description as well, if you like. This is optional.
3. In the **Category** field, select the relevant category from the dropdown that best fits the rule you are setting.
   For example, **Configuration**.
4. Configure the object type. For this example, we want to alert on new RMAN backup client instances, so we select the OracleRMANBackupclient object.
   a. In **Object Type**, click **Select**.
   The **Select Object Types** window opens.
   b. Expand Host, expand the Applications and Databases, expand the Oracle Application, and then select **OracleRMANBackupclient** from the **Select Object Type** list and click **Select Object Type**.

   You can use the filter function to easily find the object you would like to monitor on.

   The object type you select depends on the scenario on which you want to trigger the alert.
5. Configure the alert trigger. For this example, we want to look only at newly created objects, so we select the trigger and set conditions filters to find only inventory changes:
   a. In **Alert Trigger**, click **Select**.
   The **Select Alert Trigger** window opens.
   b. Select **Inventory changes** radio button and then click **Select and Edit Filter**.
   The **Edit Alert Trigger - inventory Change** window opens.
   c. In option 1 **Select operations to monitor**, ensure that **Created** is selected, and then click **OK**.

   The scenario for which you are configuring the alert affects how you configure and how, if at all, you further filter rule alert trigger.
6. Configure the alert:
   a. In **Alert**, click **Select**.
   The **Edit Alert** window opens.

b. In the **Alert Fields** tab, select the severity from the dropdown.
c. In the **Description & Resolution** tab, configure any description and resolution information you would like to be sent with the alert.
d. In the Associated Reports tab, select a system template report or create a custom report that you want to be generated upon the alert.

7. Click one of the save options.

Creating event-based rules for prediction

Event-based rules work in response to data that is streaming into the Data Protection Advisor server in real-time and triggers alerts of an event occurs in a defined period of time.

The procedure focuses on creating a rule to alert when an Avamar server is predicted to reach 90% utilized within the next 24 hours.

1. Go to **Policies** > **Analysis Policies** > **Custom Rule Templates**, and then click **Create Custom Rule Template**.
2. Populate the **Name/Alert Message** field with a rule name relevant to the condition you are setting for the rule.
   For example, `Avamar server predicted to reach 90% in next 24 hours`

   You can enter a condition description as well, if you like. This is optional.

   There is an existing system template rule called Backup Failed, which you can edit if you like. This example shows you how to create it from scratch.
3. In the **Category** field, select the relevant category from the dropdown that best fits the rule you are setting.
   For example, **Resource Utilization**.
4. Configure the object type. For this example, we want to alert Avamar backup servers, so we select the Backup Application object.
   a. In **Object Type**, click **Select**.
   The **Select Object Types** window opens.
   b. Expand Backup Applications, expand the Backup Server, and then select **Backup Application** from the **Select Object Type** list and click **Select Object Type**.

   You can use the filter function to easily find the object you would like to monitor on.

   The object type you select depends on the scenario on which you want to trigger the alert.
5. Configure the alert trigger. For this example, we want to look only at particular backup servers reaching a target utilization within a certain period, so we select the trigger and set conditions filters to find only predictive behaviour:
   a. In **Alert Trigger**, click **Select**.
   The **Select Alert Trigger** window opens.
   b. Select **Predictive Time** radio button and then click **Select and Edit Filter**.
   The **Edit Filter** window opens.
   c. For option 1, Select attribute to predict, click **Browse**.
   The **Select Attribute** window opens.
   d. From the BackupApplication Object Type select the row with the AttributeName **Utilisation**, click **Select Attribute** and click **OK**.

   You can use the filter function to easily find the category and Attributename you would like.

   e. For option 2, Set threshold, select **Static Value** and type or scroll up to `90` .
   f. For option 3, Specify when to send alert, select **Static Value** and select **1** and **Days** from the dropdowns.
   g. Skip option 4; there are no conditions filters for this example.
   h. For option 5, Select prediction method, leave the default selection.
   i. Click **OK** .

   The scenario for which you are configuring the alert affects how you configure and how, if at all, you further filter rule alert trigger.
6. Configure the alert:
   a. In **Alert**, click **Select**.
   The **Edit Alert** window opens.
   b. In the **Alert Fields** tab, select the severity from the dropdown.
   c. In the **Description & Resolution** tab, configure any description and resolution information you want to be sent with the alert.
   d. In the Associated Reports tab, select a system template report or create a custom report that you would like to be generated upon the alert.
7. Click one of the save options.

Creating schedule-based rules

Schedule-based rules periodically compare data in the Data Protection Advisor Datastore against rules to detect a match against a specific problem that you want to track. It uses a report to do this. You can use a System Template report or a custom report.

The procedure focuses on creating a rule to alert for three strikes failed backup clients.

1. Go to **Policies** > **Analysis Policies** > **Custom Rule Templates**, and then click **Create Custom Rule Template**.
2. Populate the **Name/Alert Message** field with a rule name relevant to the condition you are setting for the rule.
   For example, **`schedule based three strikes failed backup`**

   You can enter a condition description as well, if you like. This is optional.

   There is an existing system template rule called Backup Failed, which you can edit if you like. This example shows you how to create it from scratch.
3. In the **Type** field, select **Scheduled** from the dropdown.
4. In the **Category** field, select the relevant category from the dropdown that best fits the rule you are setting.
   For example, **Data Protection**.
5. Select the report. For this example, we want to alert on three strikes failed backup clients, so we select the Three Strike Failed Client report.
   a. In **Select Report Template**, click **System Report Templates**.
   b. Select **Three Strike Failed Client** from the **System Template Name** list and click **Select Template and Edit Options**.

      You can use the filter function to easily find the object you would like to monitor on.

      The object type you select depends on the scenario on which you want to trigger the alert.
6. Configure the options.
   a. In Number of Alerts, select the options that best suits your needs.

      If you select **Generate a separate alert for each row**, Data Protection Advisor sends a different alert for each client. This information is useful because it is granular. However, if you are alerting on a lot of clients you may receive a lot of alerts.

      If you select **Generate one alert for all rows**, Data Protection Advisor sends an alert for top-level nodes. This is useful if you want fewer alerts because you have a lot of clients; however, the information is less granular.
   b. In Default settings, click **Select Schedule** and select one of the Manage Schedule options or click **Create Schedule** to create your own schedule that defines when the rule will run.

      We do not recommend selecting **Always** from among the Manage Schedule options because this option overloads the server.
   c. Ensure that you review the time period selection and either leave the default selection or change the selection.
   d. Click **OK**.
7. Configure the alert:
   a. In **Alert**, click **Select**.
      The **Edit Alert** window opens.
   b. In the **Alert Fields** tab, select the severity from the dropdown.
   c. In the **Description & Resolution** tab, configure any description and resolution information you want to be sent with the alert.
   d. In the **Associated Reports** tab, select a system template report or create a custom report that you want to be generated upon the alert.
   e. In the **Rule Objects** tab, ensure that you select the **Object Type** and select **Name Field** and **Sub Name Field** from the dropdowns.
8. Click one of the save options.

Adding an analysis rule to an Analysis Policy

After a rule template is added to an Analysis Policy, the Analysis Engine carries out certain operations and then displays the resulting events in the **Alerts** section of the web console.

The Analysis Policies can contain multiple analysis rules that apply to different types of objects. Data Protection Advisor automatically applies the appropriate rules from the applied Analysis Policy to an object. For example, Data Protection Advisor applies rules for switches to switches only, not to backup servers.

Analysis Engine actions log file

The `actions.log` contains one record for each successful Analysis Engine action notification.

The Analysis Engine actions can be:

- email
- SNMP
- scrpt
- Windows event log

The `actions.log` contains only the information about successful actions. It does not contain failure information or warnings of failing actions. The default location for the `actions.log` is `$instalationDir\services\logs`. This location is not user-configurable.

Analysis policy rule categories

Capacity planning

Capacity planning analysis policies create alerts about events that indicate that resources might soon run out. The following table describes these jobs.

Assigning alerts for pools and storage array analysis policies

When you assign the following analysis policies to objects, consider the following recommended severity levels:

- Storage pool is filling Up - Severity 3
- Storage pool is filled Up - Severity 2
- Storage Array is filling Up - Severity 1

Table 41. Capacity planning

Rule	Description	Parameters
File system filling up	Generates alerts if a file system utilization will exceed 90% in the next 2 weeks.	Max Predicted Utilization - 100% Number of hours to forecast - 336
Running out of backup client licenses	Generates alerts if the license only permits you to monitor less than an additional 25 computers.	Maximum client licenses - 25
Storage pool is filling Up	Alerts when according to the growing trend there will not be space left on the pool for the selected time period.	Minimum Free Space Allowed - 0 Days to Forecast - 90
Storage pool is filled up	Alerts when there is no space on the pool to physically allocate a new LUN.	Initial Consumed Capacity - 3
Storage Array is Filling Up	Alerts when there is no space left to allocate a new LUN on the pool and there are no free disks available on the storage array.	Initial Consumed Capacity - 2
Empty tapes running low	Generates alerts if there will be no empty tapes available in a tape pool within 6 weeks.	Maximum Predicted Count - 0 Number of hours to forecast - 1008
TSM Database filling up	Generates an alert if the TSM Database is predicted to reach 100% usage within 2 weeks.	Number of Hours to Forecast - 336 Maximum Predicted Utilization - 100
TSM Database utilization high	Generates an alert if the TSM Recovery log is predicted to reach 100% usage within 2 weeks.	Number of Hours to Forecast - 336 Maximum Predicted Utilization - 100

Change management

Change management analysis policies alert about changes in the environment. The following table describes these jobs.

Table 42. Change management

Rule	Description	Parameters
Backup client configuration changed	Generates alerts if the configuration of a backup client has been modified.	N/A
Backup device configuration changed	Generates alerts if the configuration of a backup device has been modified.	N/A
Backup group configuration changed	Generates alerts if the configuration of a backup group has been modified.	N/A
Disk firmware level changed	Generates alerts if the firmware level of a disk has changed.	N/A
Disk serial number changed	Generates alerts if a disk serial number has changed.	N/A
Object operating system changed	Generates alerts if the operating system of a object has changed.	N/A
RecoverPoint Active RPA changed	Generates an alert if the active RPA has changed since the last analysis run.	N/A
RecoverPoint for VMs Consistency Group Copy is disabled	Alert if a RecoverPoint for VMs Consistency Group Copy is disabled	N/A
RecoverPoint RPA Link Status Changed	Generates an alert if the status of the RPA link has changed since the last analysis run.	N/A
Tape drive firmware level changed	Generates alerts if the firmware level on a tape drive has changed.	N/A
Tape drive serial number changed	Generates alerts if the serial number of a tape drive has changed.	N/A

Configuration

The configuration analysis policies monitor the environment for device or application configuration issues. The following table describes these jobs.

Table 43. Configuration

Rule	Description	Parameters
Backup client inactive	Generates alerts if a backup client is not scheduled to run.	N/A
Fileserver export and LUN on same volume	Generates alerts if a fileserver export is on the same volume as a LUN.	N/A
LUN on given volume	Generates alerts if a LUN has been configured on vol0.	Volume - vol0
IP autonegotiation mismatch	Generates alerts if there is an autonegotiation mismatch between a host and its switch port.	N/A
IP duplex mismatch	Generates alerts if there is a duplex mismatch between object and switch.	N/A
Not enough virtual memory	Generates alerts if the amount of virtual memory on a computer is less than 1.5 times the amount of physical memory.	N/A

Table 43. Configuration (continued)

Rule	Description	Parameters
Volume priority not normal	Generates alerts when volume priority is set to something other than normal.	N/A

Data protection

The data protection analysis policies monitor the environment for exceptions related to backup and recovery issues. The following table describes the monitored jobs.

Table 44. Data protection

Rule	Description	Parameters
Application restore time estimate too high	Generates alerts if it is estimated that it will take more than 12 hours to restore an application.	Recovery time objective - 12 hours
Application recovery point objective missed	Alert if an application has not had a successful backup in more than 72 hours.	Recovery point objective - 72 hours
Backup failed	Alert generated if a backup fails.	N/A
No Successful backups in one minute	Alert generated if a backup fails two consecutive times.	Maximum failures - 2
Backup larger than average	Generates an Alert if a backup Job is double its size of its average size over the last 14 days.	Days of history - 14 days Deviation - 100%
Backup not occurred for many days	Alert is generated if a host has not had a backup in the last 3 days.	Maximum days not backed up - 3
Backup Running at Same Time as Server Operation	Generates an alert if there were any backups completed over a period that overlapped with any of the following operations on the backup server: ● Delete volumes ● Expirations ● Storage pool copies ● Moves ● Database backup ● Migrations ● Reclamations	None.
Backup spans multiple tapes	Alert is generated if a backup spans more than 3 tapes.	Maximum number of tapes - 3
Full backup smaller than average	Generates alerts if a Full backup is less than 50% of its usual size.	Days of History - 14 days Deviation - 50%
Full backup not occurred for many days	Generates alerts if a host has not had a successful full backup in the last 14 days.	Maximum Days Not Backed Up - 14
Mirror not updated for a number of hours	Generates alerts if a Remote Disk Mirror has not been updated in at least 2 days.	Maximum Exposure - 48 hours
Too many backups without a full	Generates alerts if there have been more than seven runs of a backup Job since the last Full backup.	Maximum Non Fulls - 7
No NetWorker bootstrap generated	Generates an alert if there has not been a NetWorker bootstrap ran in the last 48 hours.	Maximum hours without bootstrap - defaults to 48 hours

Table 44. Data protection (continued)

Rule	Description	Parameters
TSM Database Backup Running at Same Time as Server Operation	Generates an alert if a database backup process completed while there was other activity on the backup server, including other backups	None.
TSM Database Backup Occurred	Alerts if there was a TSM database backup in the last 24 hours, or returns the last TSM backup time if there was no backup.	Time - 24 Hours

Licensing

The licensing analysis policies monitor the environment and generate alerts about licensing issues. The following table describes these policies in more detail.

Table 45. Licensing

Rule	Description	Parameters
License expired	Generates an alert if a license in Data Protection Advisor has expired.	N/A
License nearing expiration	Generates an alert if a license will expire in the next week.	Minimum days before expiry - defaults to 7 days

Performance

The performance analysis policies monitor the environment and generate performance problem alerts. The following table describes these jobs in detail.

Table 46. Performance

Rule	Description	Parameters
Backup slower than average	Generates an alert if the performance of a backup job is 50% less than its average over the last 2 weeks.	Days of history - 14 Deviation - 50%
Backup Job overrunning	Generates an alert if a backup has been running for more than 18 hours.	Max Runtime - 18 hours
Fileserver cache hit rate low	Generates alerts if the cache hit rate of a fileserver drops below 80%.	Minimum cache hit rate - 80%
Full backup succeeded but slow	Generates an alert if a full backup ran at less than 300 KB/sec.	Minimum expected speed - 300 KB/sec

Provisioning

The provisioning analysis policies generate alerts about events that might require provisioning operations. The following table describes the jobs.

Table 47. Provisioning

Rule	Description	Parameters
File system snapshot space under utilized	Generates alerts if the peak snapshot usage over the last 14 days is less than 80%.	Days to examine usage - 14 Minimum peak snapshot usage - 80%

Recoverability

Recoverability analysis policies alert about Recoverability. The following table describes these jobs.

Table 48. Recoverability

Rule	Description	Parameters
DR Host Visibility Check for RecoverPoint/A	that the devices of the recovery-point are mapped, masked and visible by the DR-host	N/A
DR Host Visibility Check for RecoverPoint/S	that the devices of the recovery-point are mapped, masked and visible by the DR-host	N/A
Recoverability Exposure	Recoverability Exposure	N/A
Consistent Device Replication Check for Point in Time RecoverPoint/A	Best practice check. An alert will be generated in case the consistency operation was not issued; but it is recommended by the vendor.	N/A
Consistent Device Replication Check for Point in Time RecoverPoint/S	Best practice check. An alert will be generated in case the consistency operation was not issued; but it is recommended by the vendor.	N/A
Consistent Device Replication Check for Point in Time SNAPVX	Best practice check. An alert will be generated in case the consistency operation was not issued; but it is recommended by the vendor.	N/A
Application Consistency Violation	Inconsistent Replication: Application was not in backup mode during replication process	N/A
Application Not in Backup mode	Application Not in Backup mode during replication creation	N/A
Consistency Group is disabled	Consistency Group is disabled.	N/A
Invalid Replication	Images for object have failed or missed schedule	N/A
Logs not on Disk	Application log file is not found on disk	N/A
Not all the devices are part of a replication group	The device is not part of a Replication group	N/A
Not Protected Logs	Inconsistent Replication: The file is required for recovery but was not protected	N/A
Partially Replicated	Object is partially replicated	N/A
The continuous replication is halted	The continuous replication is halted	N/A
Storage Object Not Protected	Application Storage Object not protected	N/A
The link status for a continuous replication is down	The link status for a continuous application is down	N/A

Resource utilization

Resource utilization analysis policies generate alerts about events that have occurred because of resource utilization problems within the environment. The following table describes these jobs in detail.

Table 49. Resource utilization

Rule	Description	Parameters
Aggregate snapshot utilization high	Generates an alert if an aggregate snapshot utilization is higher than a specified threshold.	Maximum aggregate snapshot utilization - default is 90%
CPU pegged	Generates an alert if the CPU Utilization on a host is greater than 90% for last 30 minutes.	Maximum CPU utilization - defaults to 90% Number of minutes - 30 minutes
Disk pegged	Generates an alert if a disk on a host is greater than 90% busy for over 30 minutes.	Maximum Disk Busy Percentage - 90% Number of minutes - defaults to 30 minutes
Fibre Channel port utilization high	Generates an alert if a Fibre Channel port exceeds 70% of its max throughput.	Maximum utilization - 70%
Fibre Channel port no BB credits	Generates an alert if a Fibre Channel port has ran out of buffer to buffer credits.	N/A
File system file utilization high	Generates an alert if the number of files on a file system is greater than 90% of the max number allowed.	Maximum file system file utilization - 90%
File system snapshot utilization high	Generates an alert if a file systems snapshot utilization is above 90%.	Maximum file system snapshot utilization - defaults to 90%
File system utilization high and increasing	Generates alerts if a file system utilization is above 90% and is increasing.	Maximum file system utilization - defaults to 90%
Memory utilization high	Generates an alert if memory utilization on a host is greater than 90%.	Maximum memory utilization - defaults to 90%
Network utilization high	Generates an alert if a network interface exceeds 70% of its rated throughput.	Maximum utilization - defaults to 70%
RecoverPoint Journal Utilization High	Generates an alert if the journal utilization for an RPA is above a specified warning or critical threshold.	Warning threshold Critical Threshold
RecoverPoint Journal Utilization High	Generates an alert if the SAN utilization for an RPA is above a specified warning or critical threshold.	Warning threshold Critical Threshold
RecoverPoint RPA WAN Usage High	Generates an alert if the WAN utilization for an RPA is above a specified warning or critical threshold.	Warning threshold Critical Threshold
RecoverPoint Replication Lag High	Generates an alert if the replication time or data lag is above a specified warning or critical level.	Time Lag Warning threshold Time Lag Critical Threshold Data Lag Warning threshold Data Lag Critical Threshold
TSM Database Utilization High	Generates an alert if the TSM Database utilization exceeds 90%.	Maximum Database Utilization - 90%
Expiration Process Duration Exceeds Expectation	Generates an alert if the TSM Expiration process take longer than an hour to run, or more than 25% longer that the	% Increase - 25% Period - 7

Table 49. Resource utilization (continued)

Rule	Description	Parameters
	average expiration process time over the last seven days.	Max Duration - 1
TSM Recovery Log Utilization High	Generates an alert if the TSM Database utilization exceeds 90%	Maximum Recovery Log Utilization - 90%

Service Level Agreements

Service Level Agreement (SLA) analysis policies generate alerts about SLA violations. The following table describes the SLA jobs.

Table 50. Service Level Agreement

Rule	Description	Parameters
Backup succeed but failed SLA requirements	Generates an alert if a backup was successful but outside of its backup window.	N/A

Status

Status category analysis policies generate alerts when there is concern of the current status of a monitored device or application match. The following table describes status jobs.

Table 51. Status

Name	Description	Rule	Parameters
Backup Server Errors	Generates an alert if a backup server error is logged (TSM only).	Backup server errors	N/A
CG Copy for VMs link down	CG Copy of RecoverPoint for VMs is enabled and the link is down.	CG Copy for VMs link down	Entity; CgCopyStatus Condition "enabled is false (or 0- please check)" fields: data transfers not "Active"
CPU Offline	Generates an alert if a CPU is offline.	CPU offline	N/A
Agent Heartbeat Failed	Generates an alert if an agent fails to send in its heartbeat.	Agent heartbeat failed	N/A
Agent Log File Message	Alerts on any message that appears in the agent log files.	Agent Log Messages	N/A
Disk Failed	Generates an alert if a disk has failed.	Disk failed	N/A
EDL Failover occurred	Generates an alert if one EDL appliance fails over to another.	EDL Failover Occurred	N/A
Fan Inactive	Generates an alert if a fan on a device is inactive.	Fan inactive	N/A
Fibre Channel Port Changed State	Generates an alert if a Fibre Channel port has changed state.	Fibre Channel port changed state	N/A
Less than 75% of Backup Devices Available	Generates an alert if less than 75% of the backup devices on a backup server are Up.	Less than x% of backup devices available	Lowest backup device availability - defaults to 75%

Table 51. Status (continued)

Name	Description	Rule	Parameters
More Than 3 Backup Devices Unavailable	Generates an alert if there are more than 3 backup devices on a backup server Down.	Many backup devices unavailable	Maximum number of downed devices - 3
Network Interface Changed State	Generates an alert if network interface gets a link up or link down event.	Network interface changed state	N/A
Object Restarted	Generates an alert if a host has been rebooted.	Object restarted	N/A
Object Status not Up	Generates an alert if a object's status changes to anything except active.	Object Status not Up	N/A
PSU Inactive	Generate an alert if a Power Supply Unit is not active.	PSU inactive	N/A
Publisher Hung	Generates an alert if the Publisher queue hasn't changed since the last poll.	Publisher Queue Hung	N/A
Server Log File Message	Alerts on any messages appearing in server log files.	Server Log Messages	N/A
Tape Drive Needs Cleaning	Generates an alert if a tape drive needs cleaning.	Tape drive needs cleaning	N/A
Tape Drive Not Okay	Generates an alert if a tape drive is reporting a status other than OK.	Tape drive not okay	N/A
Tape Library Not Okay	Generates an alert if a tape library is reporting a status other than OK.	Tape library not okay	N/A
Thermometer Inactive	Generates an alert if a thermometer becomes inactive.	Thermometer Inactive	N/A
Thermometer Overheating	Generates an alert if a thermometer on a device indicates that it is overheating.	Thermometer overheating	N/A
Waiting For Writable Tapes For More Than 30 Minutes	Generates an alert if a backup server has been waiting more than 30 minutes for a writable tape.	Waiting for writable devices	Maximum outstanding devices - defaults to 0 Minutes before alerting - defaults to 30 minutes
Xsigo Fan Less Than 90% of Normal Speed	Generates an alert if the speed of a fan on a Xsigo Director falls below 90% of the normal speed.	Xsigo Fan Speed Less than Expected	Percentage to Check - defaults to 90%.

Troubleshooting

The troubleshooting analysis policies provide help for troubleshooting problems with the environment. The following table describes these jobs.

Table 52. Troubleshooting

Rule	Description	Parameters
Backup failed due to client network errors	Generate an alert if a backup failed on a client while it experienced an increase in network errors.	N/A
Backup job failed due to high client CPU utilization	Generate an alert if a backup failed on a client, while the CPU utilization on the computer was greater than 90%.	Maximum processor utilization - defaults to 90%
Backup job failed due to high client memory utilization	Generates an alert if a backup failed on a client whilst the memory utilization on that client was greater than 90%.	Maximum memory utilization - defaults to 90
Backup failed due to high server CPU utilization	Generates an alert if a backup failed on a client whilst the CPU utilization on the backup server was greater than 90%.	Maximum processor utilization - defaults to 90%
Backup failed due to high server memory utilization	Generates an alert if a backup fails whilst the memory utilization on the backup server is greater than 90%.	Maximum memory utilization - defaults to 90%
Backup failed due to server network errors	Generates an alert if a backup failed while there was an increase in the number of network errors on the backup server.	N/A
Disk failed for a number of hours	Generates an alert if a disk is in a failed state for more than 48 hours. Applicable to Linux and Solaris.	Maximum failure time - defaults to 48 hours
Fibre Channel port reporting errors	Generates an alert if a Fibre Channel port is reporting errors.	N/A
Fibre Channel port reporting more than x% errors	Generates an alert if more than 1% of all frames going through a Fibre Channel port have errors.	Maximum percentage errors - defaults to 1%
Network interface reporting errors	Generates an alert if errors are being seen on a network interface.	N/A
Network interface reporting more than x% errors	Generates an alert if more than 1% of the packets travelling through a network interface have errors.	Maximum percentage errors - defaults to 1%
Tape drive reporting errors.	Generates an alert if there is an increase in the number of errors seen on a tape drive.	Include Recoverable Errors - defaults to False

Protection policies

Protection policies are used to define service level agreements and exposure reporting to calculate whether a backup ran in its backup window and to calculate whether an application or host is meeting its recovery time objective (RTO) and recovery point objective (RPO). Protection policies also determine how an application, host, or device should be replicated or backed up. Policies are assigned to objects and consist of a set of rules that dictate:

- For replication: the type of copy, the replication level, and the schedule.
- For backups: the level of backup and the schedule.

Data Protection Advisor reports then compare the protection policy for an object to the actual replication or backup taking place to display the level of compliance with policy.

Chargeback policies

Chargeback reports provide the ability to perform a financial cost analysis for backups, restores, and data protection replication operations in a customer's environment. Data Protection Advisor calculates a cost for each backup client and can charged back to the business unit that is responsible for that client or set of clients.

Data Protection Advisor calculates chargeback using two models: one for data backup and restore, and one for the protection and replication of storage data by RecoverPoint. Data Protection Advisor calculates chargeback for clients based on the inputs for each type.

Backup chargeback

Data Protection Advisor breaks out backup chargeback by cost per GB backed up and other backup costs.

Cost Per GB Backed Up uses the following inputs:

- Base Size - Baseline backup size in GB for base costing.
- Base Cost - Total cost for backup up to the base size specified.
- Cost of Each Additional GB - Additional cost per GB for backups greater than the base size.

Data Protection Advisor derives other Backup Costs from the Chargeback Policy and uses the following inputs:

- Cost Per Backup - the cost per backup (derived from the chargeback policy).
- Cost per GB Retained - the cost per gigabyte stored (derived from the chargeback policy).
- Cost Per Restores - the cost per restore (derived from the chargeback policy).
- Cost per GB Restored - the cost per gigabyte restored (derived from the chargeback policy).
- Cost Per Tape - the cost per tape used for backup (derived from the chargeback policy).

Storage chargeback

Data Protection Advisor breaks out storage chargeback by cost per GB stored, cost per GB replicated, and snaps.

Cost Per GB Stored uses the following inputs:

- Cost Based On - chargeback calculated on either storage used or storage allocated.
- Base Size - Amount of base storage space allocated in GB.
- Base Cost - A one-off price for the base size.
- Cost of Each Additional GB - the price per GB after base size is exceeded.

Cost Per GB Replicated uses the following inputs:

- Base Size - Amount of base storage space allocated in GB.
- Base Cost - A one-off price for the base size.
- Cost of Each Additional GB - the price per GB after base size is exceeded.

Snaps uses the following inputs:

- Cost Per GB - the price per GB.

A Chargeback Policy allows you to specify a value for each of these parameters. Data Protection Advisor calculates the total cost for a client by adding each of the different cost elements. For example, if you want to implement a chargeback model where you charge $5 for each backup that took place and $0.20 for each GB that was backed up, then you can specify values for these fields in the chargeback policy but not specify values for the other parameters.

You assign a backup client objects a cost center, which allows Data Protection Advisor to calculate Chargeback costs by cost center. A default cost center exists for objects that have not been assigned a cost center.

You can create multiple chargeback policies, and different clients or groups of clients can have different policies assigned to them. For example, if you wanted to calculate the chargeback cost for one group of backup clients based on the number of backups performed and another group based on the number of tapes used during the backup process, you can create two chargeback policies and associate them with each group of clients.

Policies and generating events

When an analysis policy finds a matching condition, Data Protection Advisor generates an event. All events are automatically logged in to the Data Protection Advisor Datastore. You can view all events in the **Alerts** section of the web console.

You can edit policies to:

- generate an email
- run a script
- send an SNMP trap
- write an event to a Windows Event Log

Editing rules in policies

To edit all the rules in the policy, go to **Policies** > **Analysis Policies** > **Edit** > **Edit Policy-based actions**.

Alternatively, edit actions on a per-rule basis. To edit actions on a per-rule basis:

1. Go to **Policies** > **Analysis Policies** > **[select a policy] and click Edit**.
2. Under Analysis Rules, highlight the rule name to edit, and click **Edit Actions**.
3. In the **Edit Actions** window, ensure that the Rule-based actions radio button is selected.

Alternatively, edit or overrule all the rules in a policy or on a per-rule basis from the Inventory area. This is applicable only to the roles that have permissions to edit the policy.

4. Go to **Inventory** and select the object.
5. Select **Properties**.
6. Within the object **Details** window, click the **Policies** tab.
7. Click **Edit Override Settings**. .

   Edit Override Settings is available only if the role has privileges to do so. Otherwise, the option is **View Settings**
8. Within the object **Override Policy Settings** window, make applicable changes, either on a per-rule level or at a policy level; and click **OK** when finished making changes.

The *Data Protection Advisor Online Help* provides additional information on create, edit, or copy an Analysis Rule template.

Parameters for generating alerts from scripts

You must place scripts in the `<install-dir>/services/shared/commands` directory on the Data Protection Advisor Application server.

The following table describes the parameters to the script to use to perform actions.

Table 53. Script field parameters

Parameter	Description
Node	Name of the node to which the alert applies.
Text	Textual error message as defined in the ruleset.
Severity	Severity of the alert (Critical, Error, Warning, Informational).
Name	Name of the analysis that triggered this alert.
Alert ID/Event ID	ID that uniquely describes this alert.
First occurrence	Timestamp that details the time that this alert first occurred.
Last occurrence	Timestamp that details the time that this alert last occurred.
Count	Number of times this alert has been issued.
View	Name of the view to which the analysis is assigned.
Node	Name of the node to which the analysis is assigned.

Table 53. Script field parameters (continued)

Parameter	Description
Category	Category of the rule (possible values: Administrative, AssetManagement, CapacityPlanning, ChangeManagement, Compliance, Configuration, DataProtection, Execution, Performance, Provisioning, Recoverability, ResourceUtilization, SLA, Status, System, Troubleshooting).

The following table describes the arguments that are passed to a script in an alert action.

Table 54. Script alert arguments

Argument	Description
$1	Event node.
$2	Event message.
$3	Event severity (as set in the analysis properties).
$4	Name of analysis that caused the event.
$5	Alert ID (unique for this run of the script).
$6	Event ID (unique for this alert).
$7	First occurrence (timestamp).
$8	Last occurrence.
$9	Count.
$10	Category.
$11	Description of the alert.

NOTE: If you are running a script in a UNIX environment, you must enclose parameters with 2 digits in curly brackets: {xx}. For example, `$ {11}`.

Rule Template

A rule is the set of instructions that the Data Protection Advisor Analysis Engine uses to determine whether a condition has been met and if an alert is generated. For example, the file system filling up rule contains the set of rules to determine if any file systems will exceed the threshold at a certain point in the future.

An Analysis job uses a rule to perform analysis and alerting based on information within the Data Protection Advisor database. When Data Protection Advisor is installed, a number of pre-defined rules are installed that can monitor for common problems that might occur in the environment. You can use these rules as the basis for implementing an analysis policy. Data Protection Advisor provides a rules editor that you can use to create entirely new rules.

The term *rule template* is used to differentiate the rule definition from the rule instance. The rule template defines the rule's logic. When a rule template is added to an analysis policy, it becomes a rule instance (or a rule) that the Analysis Engine will run. Also, when rule templates are added to a policy, users can specify the values for any parameters. This allows rules to be reused by different policies.

For example

A Tier 1 policy might generate an alert when disk space is 80% utilized. A Tier 2 policy can generate an alert when disk space is 90% utilized. This can be handled with the same rule template that uses a parameter for utilization.

Policy application

You can apply policies directly to a group or an object. Policies that are applied directly to an object always take precedence. When you set a policy at the group level, objects in the group that do not have their own policies, they inherit the group's policy. The best practice is to apply the policy at the highest group level. Policies cannot be applied to Smart Groups.

If an object is moved from one group to another group, the most recently applied policy is implemented. For example, if you move an object from Group A to Group B, the object inherits the policy of Group B.

An administrator or any user with the Edit Node privileges can apply a policy to a group or object.

Creating, editing, or copying a credential

Credentials are used by the data collection agent to connect to hosts, applications, and devices for data collection. Once a credential is created, it can be assigned when configuring data collection for an object using the Discovery Wizard or from Inventory.

1. Go to **System Settings** > **Credentials** > **Manage Credentials**.
2. Perform one of the following:
   - To create a credential, click **CREATE CREDENTIAL**.
   - To edit a credential, select the credential and then click **EDIT**.
   - To copy a credential, select the credential and then click **SAVE AS**.
   - To delete a credential, select the credential and then click **DELETE**.
3. Type a name for the credential.
4. Select the type of credential.
5. Perform one of the following based on the type of credential:
   - If you select **SNMP**, specify the SNMP version, and do the following:

     If the SNMP version is 2:

     a. Specify the community string (the string with which to connect to the device).
     b. Confirm the community string, and click **OK**.

     If the SNMP version is 3:

     a. Specify the **Username**.
     b. (Optional) Specify the Authentication Protocol. The protocol can be MD5 or SHA1.
     c. Specify the Authentication Password, then confirm it.
     d. (Optional) Specify the Privacy Protocol. The protocol can be AES or DES.
     e. Specify the Privacy Password, then confirm it.
     f. Click **OK**.
   - If you select **Standard**, type the username and password.
   - If you select **UNIX**, type the username and password. Click **Advanced Options** to switch to root (su) after connecting or use sudo to become root after connecting.
   - If you select **Windows**, type the domain, username, and password.
6. Click **OK**.

5

Upgrade Data Protection Advisor JRE patches

Topics:

Upgrading Data Protection Advisor JRE overview

Data Protection Advisor JRE upgrade patch allows you to upgrade the JRE version in Data Protection Advisor without upgrading the Data Protection Advisor version.

A separate Data Protection Advisor JRE patch is published on the Dell support site. Ensure that the Data Protection Advisor JRE Patch is required only when the current Data Protection Advisor JRE version is lower than Data Protection Advisor JRE Patch available on the Dell support site. See the README.txt document available in the Data Protection Advisor JRE patch for more information.

Data Protection Advisor JRE upgrade prerequisites

Perform the following steps before you upgrade Data Protection Advisor JRE.

1. Data Protection Advisor JRE upgrade patch takes a backup of the old JRE and removes it upon successful upgrade of the new JRE. However, it is recommended to take a backup of the old JRE folder.

   For Data Protection Advisor App Server and DataStore, the path is: `<DPA Installation path>/dpa/services/_jre`;

   For Data Protection Advisor Agent, the path is: `<DPA Installation path>/dpa/_jre`

   Delete the backup of the JRE folder after Data Protection Advisor services are started successfully.
2. Ensure that you have admin and root privileges which do not retain the `RUN_AS_USER` configuration.
3. Back up the Data Protection Advisor Datastore by using the `dpa ds export` command.
4. Stop the Data Protection Advisor Application server and agent. It is recommended to perform a complete backup of the host running Data Protection Advisor Application server.
5. Stop the Data Protection Advisor Datastore. It is recommended to complete backup of the host running Data Protection Advisor Datastore server. If your infrastructure is running on VM, stop the Data Protection Advisor Application and Datastore servers and take a snapshot of the Data Protection Advisor Application and Datastore servers to facilitate restoring them if there are upgrade problems.
6. This utility contains customized JRE package compatible with Data Protection Advisor. Do not use any JRE packages from other external sources.
7. When upgrading Data Protection Advisor JRE patch in clustered environments, stop the Data Protection Advisor Application service on all servers. Upgrade the Datastore first, and then upgrade the Application servers. You must stop the Application service because when the services are on separate machines, the installer cannot stop the services.
8. In the replication environment, upgrade the primary data store and then upgrade the secondary data store.
9. Ensure that the system has 500 MB of free space for the Data Protection Advisor JRE upgrade.
10. This utility is only applicable for JAVA 8.
11. If upgrading on Unix or Linux, ensure that the `unzip` command is present on your system.

    ⓘ **NOTE:**

- This package is available in .zip format. For example, `dpa_jre_upgrade_<releasev_month>_<releasev_version>_<os>.zip`.
- You must extract the .zip file. For example, `Linux/Unix: unzip -x dpa_jre_upgrade_<releasev_month>_<releasev_version>_<os>.zip .`

Upgrading Data Protection Advisor JRE

Perform the following steps to upgrade Data Protection Advisor JRE.

1. To extract the Data Protection Advisor JRE upgrade package and run the appropriate commands.
   - On Windows, use the command prompt and run the following command from the directory where Data Protection Advisor JRE upgrade utility is extracted:

     ```
     dpa_jre_upgrade_<releasev_month>_<releasev_version>_<os>.exe --
     install_path="<dpa_path>"
     ```

     ```
     default dpa path: "C:\Program Files\EMC\"
     ```

   - On Linux or Solaris, run the following commands:
     - Open the terminal from the directory where Data Protection Advisor JRE upgrade utility is extracted and added to the executable permission.

       ```
       chmod +x dpa_jre_upgrade_<releasev_month>_<releasev_version>_<os>
       ```

     - Run the Data Protection Advisor JRE upgrade command.

       ```
       ./dpa_jre_upgrade_<releasev_month>_<releasev_version>_<os> --
       install_path="<dpa_path>"
       ```

       ```
       default dpa path: “/opt/emc/”
       ```

2. When prompted for Data Protection Advisor services to stop the option, select either **Y** or **N**.
   - If you want to stop the Data Protection Advisor services, select **Y**. The system proceeds with the JRE upgrade process.
   - If you do not want to stop Data Protection Advisor services, select **N**. The system stops the JRE upgrade and terminates without upgrading the JRE version.
3. When prompted for Data Protection Advisor services to start option, select either **Y** or **N**.
   - If you want to start Data Protection Advisor services, select **Y**. The system starts the Data Protection Advisor services.
   - If you do not want to start the Data Protection Advisor services, select **N**.

Data Protection Advisor JRE upgrade command options

Following are the command options:

- --help — Displays the help screen.
- --quiet — Suppresses all output except warning and error messages.
- --no-restart — This option does not restart Data Protection Advisor services after the upgrade.
- --install_path — Data Protection Advisor installation path. This must be the last argument of the command.

6

Uninstalling Data Protection Advisor

This chapter includes the following sections:

Topics:

Uninstalling the software

This section describes how to uninstall Data Protection Advisor in both UNIX/Linux and Windows environments.

Run the following command:

```
<DPA_install_directory>/_uninstall/ Uninstall_Data_Protection_Advisor
```

Add `-i silent` to the command if you want silent uninstallation. The uninstaller will not ask you for input.

When uninstalling the Data Protection Advisor Datastore, a warning indicating that the uninstaller will remove the features that were installed during product installation appears indicating that the database will be removed.

Uninstalling by using silent command line

- On UNIX/Linux machines, start a command shell, navigate to the _uninstall directory and type the following command: **`./Uninstall_Data_Protection_Advisor -i silent`**
- On Windows machines, type the following command through the command line: **`Uninstall_Data_Protection_Advisor.exe -i silent`**

Uninstalling through user interface on Windows

1. Select **Start** > **Control Panel** > **Programs and Features.**
2. Uninstall **Data Protection Advisor** from the list of installed applications.

Agent-only uninstallation

You cannot uninstall only the Agent from the Data Protection Advisor Application server or Datastore server installation.

If you would like to upgrade the Data Protection Advisor Agent, upgrade the Agent only on the existing Data Protection Advisor Application server or Datastore server installation. Upgrades provides information on carrying out upgrades.

7

Troubleshooting

This chapter includes the following sections:

Topics:

Installation troubleshooting

Alternate Data Protection Advisor Datastore upgrade

Use this method to upgrade the Datastore to without using the `pg_upgrade` command.

Not that the in carrying out this procedure, the Data Protection Advisor Datastore Agents will be erased.

1. Stop the Data Protection Advisor Datastore application
2. Create a Data Protection Advisor Datastore export.
3. Delete the existing Data Protection Advisor Datastore installation.
4. Install a fresh Data Protection Advisor Datastore of the latest version of Data Protection Advisor.
5. import export in new ds
6. Carry out a Data Protection Advisor Datastore application upgrade.
7. Provide Data Protection Advisor Datastore password to the upgraded Datastore application with the `dpa ds dspwd` command.

Data Protection Advisor Agent does not restart or register after Data Protection Advisor Server password change

If the Data Protection Advisor Agent does not restart or register after the Data Protection Advisor Server password was changed during installation, it could be because the Agent password on the Data Protection Advisor Server has been changed and the password on the Data Protection Advisor Agent has not been changed to match it.

To get the Data Protection Advisor Agent to restart or register, set the password on the Agent to the same value as is set on the Data Protection Advisor Server. Installing the Data Protection Advisor Agent provides information.

Data Protection Advisor Datastore on Linux failure to start after installation

In certain circumstances the Kernel settings of the system running the Data Protection Advisor Datastore may need to be tuned for the Datastore to start up correctly.

If the Datastore fails to start and errors in the Data Protection Advisor log file reference shared memory segments, then the values specified in the following file may need to be tuned according to your system specifications.

- Linux: Investigate tuning values for SHMMAX and SHMMIN in the /etc/sysctl.conf

Data Protection Advisor secondary Datastore upgrade after running the `dpa ds rep` command fails with a Java exception

In certain circumstances after Data Protection Advisor split and a secondary Datastore upgrade, the **`dpa ds rep`** command fails with a Java exception. If you try to upgrade the Datastore to the latest version after encountering the error, the Data Protection Advisor secondary Datastore status appears as `datatastore is not configured for replication.`

To resolve this issue, perform the following steps:

On Linux:

1. Type the **`./dpa ds rep --debug`** command to verify the configured replication.

   You can ignore exceptions, if any. Note down information about the primary Datastore IP address and Role (secondary).
2. Type the **`./dpa.sh ds save <file_name>`** command to save the Datastore configuration before you attempt to upgrade to the latest patch. For example, **`./dpa.sh ds save ds.conf`**.
3. Save the file (`ds.conf`) and proceed with the upgrade.
4. Type **`./dpa.sh ds rep --debug`** to check the replication status after the upgrade.
5. If there are issues, type the **`./dpa.sh ds load <file_name>`** command to load the saved configuration file. For example, **`./dpa.sh ds load ds.conf`**.

On Windows:

1. Type the **`dpa ds rep --debug`** command to verify the configured replication.

   You can ignore exceptions, if any. Note down information about the primary Datastore IP address and Role (secondary).
2. Type the **`dpa ds save <file_name>`** command to save the Datastore configuration before you attempt to upgrade to the latest patch. For example, **`dpa ds save ds.conf`**.
3. Save the file (`ds.conf`) and proceed with the upgrade.
4. Type **`dpa ds rep --debug`** to check the replication status after the upgrade.
5. If there are issues, type the **`dpa ds load <file_name>`** command to load the saved configuration file. For example, **`dpa ds load ds.conf`**.

NOTE: Ensure that you run the `./dpa.sh ds save <file_name>` or the `dap ds save <file_name>` command before upgrading to save the current working state of the Data Protection Advisor Datastore.

Data Protection Advisor web console launch failure on Windows Server 2012

If the Data Protection Advisor web console fails to launch on Windows Server 2012, check if:

The Internet Explorer Enhanced Security Configuration (IE ESC) stops the Data Protection Advisor web console from launching. Do not stop the notification of the block by clearing the Continue to prompt when website content is blocked option because Data Protection Advisor never comes past Starting services. Please wait.

The workaround for this is to disable the IE ESC.

Postinstallation memory adjustment

When the Data Protection Advisor Application and Datastore services are originally installed, they automatically tune memory parameters based on your system RAM. If at a later stage you either increase or decrease the amount of RAM installed on the host you must run the `tune` command so that the Data Protection Advisor memory parameters are adjusted correctly.

When you run the `tune` command, you must specify the amount of RAM installed on the host. For example, if the Application server memory is changed to 64GB and the Datastore memory is changed to 32GB, you would run the following commands:

- On the application server: **`dpa app tune 64GB`**
- On the datastore server: **`dpa ds tune 32GB`**

Data Protection Advisor automatically configures itself to use a portion of the memory amount specified in the command.

Error messages during upgrades

If there is an error during the upgrade process, the Data Protection Advisor server stops. This could occur under the following circumstances:

- Errors in SQL upgrade scripts
    - Result: The server stops and does not continue.
    - Suggested action: Contact EMC Technical Support.
- Errors in system metadata upgrade; for example, system reports, rule templates
    - Result: The server stops, but you have the option to continue the upgrade.
    - Suggested action: You can disregard this message and continue with the Data Protection Advisor server upgrade. However, the Data Protection Advisor system might be unstable. If you do stop the server upgrade, Contact EMC Technical Support
- Errors in the custom data upgrade; for example, custom analysis rules
    - Result: An error message is thrown indicating the problem.

      ```
      Suggested action: You can disregard this message and continue with the Data
      Protection Advisor server upgrade. However, you should expect the custom rule that
      failed to upgrade not to work. An error is recorded in the log file.
      ```

Permissions required for the agent to work under a non default user

- On Linux, add the agent user to the group **Disk**.
- On Windows:
    1. Add the user agent to the following groups:
        - Performance Log Users
        - Performance Monitor Users
        - Distributed DCOM Users
    2. In the **WMI Control Properties Security** tab, add user for Root/CIMV2, Root/WMI, and root and then enable the following options:
        - **Enable Account**
        - **Remote Enable**

Data Protection Advisor installer fails with an error

The Data Protection Advisor installer fails shortly after launch, generating an error on the command line.

```
Preparing to install
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Launching installer...
JRE libraries are missing or not compatible....
Exiting....
```

There can be different causes for this error. Typically the installer error indicates that there is a lack of space in the temporary directory or file system where it is extracting the installer archive to.

The resolution is to ensure that there is sufficient space in the operating system temporary directory or file system.

The temporary directory or the file system is available in the following locations:

- On UNIX and Linux platforms: `/tmp` folder.
- On Windows: `c:\Windows\Temp` folder.

Ensure that a minimum of 5 GB of free space is available in the temporary directory or file system.

Data Protection Advisor installer failure during installation or upgrade

Data Protection Advisor installer fails after proceeding partially during installation or upgrade, generating an error on the command line.

```
Invocation of this Java Application has caused an InvocationTargetException. This
application will now exit. (LAX)

Stack Trace:
java.lang.NoClassDefFoundError: Could not initialize class java.awt.Toolkit
at java.awt.Component.<clinit>(Component.java:593)
at com.zerog.ia.installer.actions.InstallUninstaller.bv(Unknown Source)
at com.zerog.ia.installer.actions.InstallUninstaller.installSelf(Unknown Source)
at com.zerog.ia.installer.InstallablePiece.install(Unknown Source)
at com.zerog.ia.installer.InstallablePiece.install(Unknown Source)
at com.zerog.ia.installer.GhostDirectory.install(Unknown Source)
at com.zerog.ia.installer.InstallablePiece.install(Unknown Source)
at com.zerog.ia.installer.Installer.install(Unknown Source)
at com.zerog.ia.installer.LifeCycleManager.consoleInstallMain(Unknown Source)
at com.zerog.ia.installer.LifeCycleManager.executeApplication(Unknown Source)
at com.zerog.ia.installer.Main.main(Unknown Source)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
at com.zerog.lax.LAX.launch(Unknown Source)
at com.zerog.lax.LAX.main(Unknown Source)
This Application has Unexpectedly Quit: Invocation of this Java Application has caused
an InvocationTargetException. This application will now exit. (LAX)
```

There can be different causes for this error. Typically the installer error indicates that there are missing operating system libraries that are required to complete the installation or upgrade process.

To resolve the issue, do the following:

1. Run the `ldd` command to identify the missing library files on the operating system.

   ```
   [root@hostname lib64]# ldd /opt/emc/dpa/services/_jre/lib/amd64/libawt_xawt.so
   linux-vdso.so.1 => (0x00007ffea7fc8000)
   libpthread.so.0 => /lib64/libpthread.so.0 (0x00007f90393b1000)
   libm.so.6 => /lib64/libm.so.6 (0x00007f90390ae000)
   libawt.so => /opt/emc/dpa/services/_jre/lib/amd64/libawt.so (0x00007f9038ddc000)
   libXext.so.6 => not found
   libX11.so.6 => not found
   libXrender.so.1 => not found
   libdl.so.2 => /lib64/libdl.so.2 (0x00007f9038bd7000)
   libXtst.so.6 => not found
   libXi.so.6 => not found
   libjava.so => /opt/emc/dpa/services/_jre/lib/amd64/libjava.so (0x00007f90389aa000)
   libjvm.so => not found
   libc.so.6 => /lib64/libc.so.6 (0x00007f90385e8000)
   /lib64/ld-linux-x86-64.so.2 (0x00007f903982c000)
   libjvm.so => not found
   libjvm.so => not found
   libverify.so => /opt/emc/dpa/services/_jre/lib/amd64/libverify.so (0x00007f90383d8000)
   libjvm.so => not found
   ```

2. Obtain and install the missing libraries on the operating system using the normal methods such as `yum` or `rpm`.

   NOTE: Ensure that you install the appropriate binaries for the operating system (64-bit).

3. Verify if the missing libraries are installed using the `ldd` command and ensure that there are no further libraries that are listed as `not found`.

   NOTE: Sometimes, the library that is listed as "not found" can be resolved after the previous libraries in the list are installed, for example, `libjvm.so`.

Log files

Log files provide important information when troubleshooting problems.

ⓘ **NOTE:** The following section describes the log file locations for a standard Data Protection Advisor installation. If the default installation directory was changed during installation, the location of the log directory will be different.

By default, logs contain warnings and error and informational messages. These may not provide enough information when troubleshooting complex problems.

Changing default log detail level

Go to **System Settings** > **Logging**.

Viewing install log file

The `Data_Protection_Advisor_Install_[two-digit date]_[two-digit month]__[year]_[two-digit hour]_[two-digit minute]_[two-digit seconds].log` file is generated during installation and contains all log messages. For successful installations, you can find this file in the install directory (for example,`/opt/emc/dpa/_install`). For unsuccessful installations on UNIX platforms, you can find the file in the root of the system drive. On Windows platforms, you can find the file on the desktop.

Viewing server log files

Data Protection Advisor generates the server log files in the following default locations:

- UNIX:`/opt/emc/dpa/services/logs`
- Windows: `C:\Program Files\EMC\Data Protection Advisor\services\logs`

If you have provided a non-default location, check the log files in the respective folders.

Server log files

The default location for following log files is `<install_dir>\services\logs\` .

- `Server.log`—Contains all log comments generated from the Data Protection Advisor Application Server
- `actions.log`—Contains successful Analysis Engine actions
- `reportengine.log`—Contains all log comments generated from the Data Protection Advisor Report Engine
- `listener.log`— Contains all log comments generated from the Data Protection Advisor Listener related to the server receiving agent data and processing it

Viewing agent log files

The agent log files are generated in the following default locations:

- UNIX:`/opt/emc/dpa/agent/logs`
- Windows: `C:\Program Files\EMC\Data Protection Advisor\agent\log\agent.log`

If you have provided a non-default location, check the log files in the respective folders.

Managing log files

When a log file reaches its maximum size, and the maximum number of log files exist in the log file directory, Data Protection Advisor deletes the oldest log file for that process and creates a new log file. You can modify the maximum log file size and maximum number of log files. You can also change the location of log files, if required.

Enabling alternative log rotation on VMs running Windows

There is a known issue (DPA-24288) on VMs running Windows that causes the logs not to rotate because of the file being locked. To resolve the issue, enable the alternative log rotation method, which changes the way the logs are being used. The highest numbered log is the latest, and not the `agent.log` file.

1. Create the following string registry:

   `HKLM\SOFTWARE\EMC\DPA\AGENT\ALTLOGROTATE`
2. Set the value to **`true`**.
3. Restart the agent.

Erroneous memory data in installer log file

The Free Memory and Total Memory data indicated at the top of the installation log files is erroneous. The correct Free Memory and Total Memory data is located further down in the log file, under `STDERR ENTRIES`.

The Corrected Total Memory data indicated under `Executing IAUpdatePostgesconfFile: [INFO]` refers to data being used for the Data Protection Advisor Datastore service.

Running a Data Protection Advisor Agent request in debug mode using Data Protection Advisor web console

The Data Protection Advisor Agent request in debug mode, also sometimes called a *modtest*, is a support tool. If you are encountering problems with a Data Collection Defaults, an EMC Technical Support Engineer may ask you to run the Agent request debug mode from the Data Protection Advisor web console. You can run Data Protection Advisor Agent request in debug mode, download the zip file directly from the Data Protection Advisor web console with no need of going to Data Protection AdvisorServer to retrieve the zip file, and send the zip file for analysis. The Agent request debug mode runs the selected request and retrieves the output and the log messages, in debug log level, and by default stores that report xml as a zip file to the following location: `<DPA_HOME>\services\shared\modtests`, where `<DPA_HOME>` is the location of the Data Protection Advisor installation.

Consider the following when running Data Protection Advisor Agent request in debug mode using Data Protection Advisor web console:

- The test cannot be run if the Collection Request is disabled.
- The test cannot be run if the Collection Request isn't applicable on the object.
- If you are running Google Chrome: you should change the default security setting for the URL to low:

  Go to **Trusted Sites**, add the URL to Trusted Sites list, and set security to **low**.

1. In the web console, select **Inventory** > **Object Library**.
2. In the Object Library, select the Data Protection Advisor server under **All hosts**.
3. In the host details window, select the **Data Collection** > **tab**.
4. In **Data Collection**, select the Request.
5. Right-click **Run** and select **Run in Debug**.
6. In the **Run in Debug - host/status** window, select credentials and data options.
7. Click **Close** to the a dialog box that appears confirming that the test is running.
8. Click **History** to view collected tests. The rows highlighted in orange indicate results from a Data Protection Advisor Agent request in debug mode.
9. Click the test result. If a Windows Security Login appears, enter your Data Protection Advisor server credentials and click **OK**.
10. To access the successfully collected tests, go to `<DPA_HOME>\services\shared\modtests`.

    If you are on a remote web browser, you can download a link which allows you to transfer the zip to your machine (where the browser is) if you look at the history for the request and click on the orange modtest line.

Default modtest deletion schedule

Data Protection Advisor deletes modtest files from the Data Protection Advisor server weekly on Sunday at 4:00 a.m. Data Protection Advisor removes all test results files older than seven days. This schedule is not configurable.

Generate Support Bundle

The Generate Support Bundle option is a support tool. Generate Support Bundle provides information.

Viewing Data Protection Advisor JRE upgrade log files

The JRE upgrade log files are generated in the following default locations:

- UNIX: `/opt/emc/dpa/services/logs/`dpa_security_rollup_patch_upgrade_<*time_stamp*>.log
- Windows: `C:\Program Files\EMC\DPA\services\logs\`dpa_security_rollup_patch_upgrade_<*time_stamp*>.log

If only Data Protection Advisor agent is installed:

- UNIX: `/opt/emc/dpa/agent/logs/`dpa_security_rollup_patch_upgrade_<*time_stamp*>.log
- Windows: `C:\Program Files\EMC\DPA\agent\logs\`dpa_security_rollup_patch_upgrade_<*time_stamp*>.log

If you have provided a nondefault location, check the log files in the respective folders.

Data collection troubleshooting

This section describes the steps that you can take to diagnose problems when trying to gather data. We assume the following scenario:

- Data Protection Advisor was successfully installed.
- The Discovery Wizard was successfully run to create the object to monitor.
- Requests have been assigned to the object and the agent has been reloaded.
- Sufficient time (fifteen minutes) has passed to allow the agent to gather data.
- An appropriate report has been run that returns no data when data should exist for the object.

Troubleshooting data collection: first actions

Review any errors returned by the Agent Errors report and take corrective action if possible; for example, resolve an authentication problem.

1. Verify that the time period selected for the report is correct.
2. Check that the correct requests have been assigned to the object.

   Select **Inventory** > **Object Library** > **[select node]** > **Data Collection**. Verify that the requests are configured correctly.

3. Rerun the request.

Troubleshooting data collection: second actions

1. If no resolvable agent errors are reported, select **Admin** > **System**, click **Configure System Settings**, and verify the data collection agent settings.
2. If the status shows that the agent is active, verify that the process is active on the operating system on which the agent is installed.
3. Run the Agent log reports in the web console followed by the Agent Status, and then the Data Collection History report.
4. Rerun the report. If the report continues to show no data, open the agent log and look for any problems. For example, was an incorrect value entered during agent installation. Log files describes how to view the log files.

Preparing a log file for submission to Dell Support

1. Set the Log Level of the process to **Debug** in System Settings, as described in Log files.
2. Stop the agent process.
3. Go to the directory in which the log file is stored. Rename or remove all existing log files for the process.
4. Restart the process.

   Restarting an agent reloads all the requests that are assigned to that agent and starts the data gathering routine. This ensures that all requests have been attempted. Starting a new log file removes the need to search through long log files for a problem.
5. Select **Inventory** > **Object Library** > **[select node]** > **Data Collection** and then select **History**.

   Alternatively, run an Agent History report.
6. Rerun the request to confirm that data is not being gathered.
7. Select **System Settings** > **Logging** and set to **Info**.
8. Make a copy of the log for submission to Dell Support.

Troubleshooting report output failure

If reports are hanging after you save them with the message `Please wait while generating report`, and you are using Internet Explorer, it could be because you do not have the XMLHTTP option enabled. To enable the XMLHTTP option:

This is in relation to DCE-1546.

1. Go to **Internet Options** > **Advanced**
2. Scroll to **Security** and select **Enable Native XMLHTTP Support**, then click **OK.**

Troubleshooting report generation or publishing problems

If scheduled reports fail to generate, or if they generate properly but fail to publish, perform the following actions:

- If a custom report, check that report template has been designed correctly in **Run Reports** area.
- Check that report template runs properly in **Run Reports** area.
- Check that report template properly saved (exported) in desired format.
- Check errors/warnings in `server.log` regarding scheduled reports.

If these actions do not resolve the issue, contact EMC Technical Support.

System clock synchronization

As part of the User Authentication process, Data Protection Advisor relies on the system clock times on the client machine and the server differing by less than one minute. In the event that clock times are unsynchronized, the following error message is displayed:

```
User Authentication failed due to the times on the client and server not matching. Ensure
that the times are synchronized.
```

To resolve this issue, ensure that the system clock times on the client and server are synchronized.

You should use NTP to synchronize the Data Protection Advisor Server and all the Data Protection Advisor Agent hosts as well. This is imperative for accurate data collection.

Troubleshooting MFA issues

This section describes common MFA issues that you might encounter.

Unable to save details on the RSA Authentication page

If you are unable to save details on the RSA Authentication page, do the following:

- Verify if you have correctly specified all the mandatory details (RSA Client ID, RSA Base URL, and RSA Access ID).
- Check the logs for exceptions, if any.
- Check if the port is open and enabled.
- Check if the RSA server is up and running.
- Check the firewall settings on the server.

Unable to log in to the application when MFA is enabled

If you are unable to log in to Data Protection Advisor when MFA is enabled, do the following.

- Check if the user is present on the RSA Server and the Data Protection Advisor application.
- Ensure that the username is the same on the RSA server and Data Protection Advisor.

Unable to log in to the application when MFA is enabled (RSA token issue)

If a token issue or any other issue prevents you from logging into Data Protection Advisor when MFA is enabled, do the following:

1. Disable MFA using the CLI. Navigate to the Data Protection Advisor install location: `EMC\DPA\services\bin`.
2. Type the `dpa app mfa disable` command.

MFA is disabled and you can log in without the RSA token.

Telemetry data collection in Data Protection Advisor

Telemetry data collection helps Dell Technologies to gain powerful insights into how users navigate through the applications. It enables precise pinpointing of areas for improvement by analyzing the usage patterns. This data-driven approach empowers Dell Technologies to streamline user interfaces, prioritize features, and optimize system performance.

Enable telemetry data collection

By default, the telemetry data collection is disabled. You can opt in or opt out of the telemetry data collection by using one of the following ways:

- After you log in to the Data Protection Advisor UI, a notification banner allows you to **ACCEPT** or **DECLINE** the telemetry data collection. Click the **For more details click here** link to read the **Telemetry Notice** and get more information about the data collection process. The notification appears every time you log in to the Data Protection Advisor UI until you accept or decline it.
- Another way to opt in or opt out of the telemetry data collection is to click the user icon and then click **User Preferences**.
  - In the **Preference** tab, click the **Enable Telemetry** toggle to the on position.
  - If you want to disable the telemetry data collection, click the **Enable Telemetry** toggle to the off position.