

# PowerProtect Data Manager

Version 19.2

## Administration and User Guide

REV 03

October 2019

Copyright © 2016-2019 Dell Inc. or its subsidiaries. All rights reserved.

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

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

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

Dell EMC  
Hopkinton, Massachusetts 01748-9103  
1-508-435-1000 In North America 1-866-464-7381  
[www.DellEMC.com](http://www.DellEMC.com)

# CONTENTS

<b>Preface</b>		<b>9</b>
<b>Chapter 1</b>	<b>Getting Started</b>	<b>13</b>
	Introducing PowerProtect Data Manager software.....	14
	Accessing the PowerProtect Data Manager UI.....	14
	Replacing the default PowerProtect Data Manager certificate .....	15
	Getting Started.....	16
	UI tools and options .....	16
<b>Chapter 2</b>	<b>Managing Users</b>	<b>19</b>
	Managing user roles and privileges .....	20
	Managing users.....	20
	Default admin user.....	22
	Roles.....	22
	Privileges.....	25
	Resetting system-generated VM Direct credentials.....	30
	Managing LDAP or AD groups.....	30
	Managing keychains.....	31
	Add credentials.....	31
	LDAP or AD authentication.....	31
	Configuring LDAP or AD authorities and assigning roles.....	31
	Example: Configuring an AD authority .....	35
	Example: Configuring an LDAP authority.....	36
	Troubleshooting LDAP configuration issues.....	37
<b>Chapter 3</b>	<b>Managing Storage</b>	<b>39</b>
	Add protection storage .....	40
	Overview of PowerProtect Data Manager cloud tier.....	41
	Add Data Domain cloud protection storage.....	41
	Overview of PowerProtect Data Manager Cloud Disaster Recovery.....	41
<b>Chapter 4</b>	<b>Enabling the Microsoft Application Agent for SQL</b>	<b>43</b>
	About the Microsoft application agent for SQL.....	44
	Microsoft SQL Server data protection and replication requirements.....	44
	Protecting a stand-alone SQL Server.....	44
	Protecting SQL Server clustered environments.....	45
	Install and configure the Microsoft application agent for SQL Server.....	46
	Prerequisites .....	46
	Install the Microsoft application agent.....	46
	Upgrade the Microsoft application agent.....	48
	Uninstall the Microsoft application agent with the setup file.....	48
	Required privileges for backup and recovery of a stand-alone server...	49
	Required privileges for backup and recovery of an Always On availability group.....	49
	Required privileges for backup and recovery of a Failover Cluster Instance or Always On Failover Cluster Instance.....	50

	Stagger SQL discovery jobs in host scale-out environments.....	50
	Manage the Microsoft application agent for SQL.....	50
	Support for existing SQL agent backups with PowerProtect Data Manager.....	51
	Supporting existing SQL agent backups with PowerProtect.....	52
	Use the backup discovery tool for PowerProtect Data Manager management of existing backups.....	53
<b>Chapter 5</b>	<b>Enabling the Oracle RMAN Agent</b>	<b>55</b>
	About the Oracle RMAN agent.....	56
	Review Oracle data protection and replication requirements.....	56
	Prerequisites.....	56
	Protecting a stand-alone Oracle server.....	57
	Protecting Oracle RAC environments.....	57
	Install and configure the Oracle RMAN agent.....	58
	Install the Oracle RMAN agent.....	58
	Upgrade the Oracle RMAN agent.....	60
	Uninstall the Oracle RMAN agent.....	62
	Integration with PowerProtect Data Manager software.....	64
	Install the PowerProtect Data Manager agent.....	65
	Uninstall the PowerProtect Data Manager agent.....	67
	How the Oracle RMAN agent communicates with PowerProtect Data Manager.....	67
	Verify the connectivity from ddbmcon.....	71
	Discover the storage units.....	74
	Add or manage the Oracle application agent.....	74
	Supporting existing Oracle RMAN agent backups with PowerProtect Data Manager.....	75
	Support existing Oracle RMAN agent backups with PowerProtect Data Manager.....	76
<b>Chapter 6</b>	<b>Enabling the File System Agent</b>	<b>79</b>
	About the File System agent.....	80
	File System agent prerequisites.....	80
	Roadmap for protection with the File System agent.....	81
	Installing and configuring File System agent.....	82
	Install the File System agent on Linux.....	82
	Install the File System agent on Windows .....	82
	Silent installation of File System agent.....	83
	Uninstalling the File System agent .....	83
	Upgrade the File System agent.....	84
	Manage the File System agent.....	84
<b>Chapter 7</b>	<b>Enabling the Storage Direct Agent</b>	<b>87</b>
	About the Storage Direct agent.....	88
	Storage Direct agent prerequisites.....	88
	Additional setup and configuration file requirements for existing Storage Direct users.....	89
	Roadmap for protection with the Storage Direct agent (new users).....	91
	Roadmap for protection with the Storage Direct agent (existing Storage Direct users).....	93
	Installing or Upgrading Storage Direct.....	94
	Install the Storage Direct agent on Linux.....	94
	Upgrade the Storage Direct agent on Linux.....	95
	Install or Upgrade the Storage Direct agent on Windows .....	97

	Silent installation of the Storage Direct agent.....	98
	Uninstall the Storage Direct agent on Linux.....	98
	Uninstall the Storage Direct agent on Windows.....	98
	Manage the Storage Direct agent.....	98
<b>Chapter 8</b>	<b>Managing Assets</b>	<b>101</b>
	About asset sources, assets, and storage.....	102
	Prerequisites for discovering asset sources.....	102
	Adding a vCenter Server asset source.....	102
	Add a VMware vCenter Server.....	102
	Virtual asset discovery.....	104
	Creating a dedicated vCenter user account and assigning the role in vCenter.....	105
	Specify the required privileges for a dedicated vCenter user account ....	105
	VM Direct protection engine overview.....	108
	Add a VM Direct appliance.....	108
	Additional VM Direct actions.....	109
	Discovering an application or File System host .....	110
	Discover an Oracle or SQL application host.....	111
	Discover a File System Host.....	111
	Discover a Storage Direct agent host.....	112
	Add and discover the SMIS server for the Storage Direct agent.....	113
<b>Chapter 9</b>	<b>Managing Protection Policies</b>	<b>115</b>
	Protection policies.....	116
	Policy retention time considerations.....	116
	Data Domain protection considerations.....	116
	Before you a create protection policy.....	118
	Add a protection policy for virtual machine protection.....	118
	On-demand backups of virtual machines.....	121
	Additional options for managing virtual machine backups.....	122
	Add a protection policy for SQL database protection.....	122
	Add a protection policy for Oracle database protection.....	125
	Add a protection policy for File System protection.....	129
	Add a protection policy for Storage Direct protection.....	132
	Add a Cloud Tier protection policy.....	136
	Edit a protection policy.....	137
	Add or remove assets in a protection policy.....	137
	Removing expired backup copies.....	138
	Export protection .....	139
	Delete a protection policy.....	139
	Add a Service Level Agreement.....	140
	Export Asset Compliance.....	142
	Dynamic filters .....	143
	Creating virtual machine tags in the vSphere Client.....	143
	Add a dynamic filter.....	144
	Manually run a dynamic filter.....	145
	Edit or delete a dynamic filter .....	146
	Change the priority of the existing dynamic filter .....	146
<b>Chapter 10</b>	<b>Restoring Data and Assets</b>	<b>147</b>
	View copies.....	148
	Restore a virtual machine or VMDK.....	148
	Prerequisites to restore a virtual machine.....	149

	Restore to original virtual machine.....	149
	Restore individual virtual disks.....	151
	Restore to new.....	151
	Restore an instant access virtual machine.....	153
	File level restore.....	156
	Direct Restore to ESXi.....	158
	Restore an application-aware virtual machine backup.....	159
	Performing centralized restore of a File System host.....	159
	Centralized restore of File Systems in PowerProtect Data Manager..	159
	Restore of Storage Direct backups in PowerProtect Data Manager.....	161
	Restore the PowerProtect Data Manager server .....	162
	Restore operations for cloud tier.....	163
	Restore from cloud tier.....	163
<b>Chapter 11</b>	<b>Performing Self-service Backup and Restore of Application and File System Agents</b>	<b>165</b>
	Performing self-service backups of Microsoft SQL databases.....	166
	Performing self-service backups of Oracle databases.....	166
	Performing self-service backups of File Systems.....	167
	Performing self-service backups of Microsoft SQL databases.....	168
	Restore a SQL application host.....	168
	Restore an Oracle application host.....	168
	Performing self-service restore of a File System host.....	169
	Using the ddfsadmin utility for File Systems.....	169
	Self-service image-level restore of File Systems.....	170
	Self-service file-level restore of File Systems.....	171
<b>Chapter 12</b>	<b>Preparing for and Recovering from a Disaster</b>	<b>173</b>
	Managing system backups.....	174
	Manage PowerProtect Data Manager backups for disaster recovery.....	174
	Prepare the Data Domain recovery target.....	175
	Configure backups for disaster recovery.....	175
	Configure PowerProtect Data Manager server disaster recovery backups.....	176
	Record settings for disaster recovery.....	176
	Restore PowerProtect Data Manager from an external Data Domain system..	177
<b>Chapter 13</b>	<b>Managing Alerts, Jobs, and Tasks</b>	<b>179</b>
	Configure Alert Notifications.....	180
	View and manage System Alerts.....	180
	View and manage System Alerts.....	181
	Monitoring and viewing jobs.....	181
	Monitor and view tasks.....	182
	Restart a job or task.....	182
	Cancel a job or task.....	183
	Export logs for a job or task.....	184
<b>Chapter 14</b>	<b>Upgrading the PowerProtect Data Manager Software</b>	<b>185</b>
	Upgrade the software from PowerProtect Data Manager version 19.1.....	186
	Upgrade PowerProtect Data Manager from version 19.2 and later.....	187
	Managing certificates after upgrading from versions earlier than PowerProtect Data Manager version 19.1.....	188

<b>Chapter 15</b>	<b>Best Practices and Troubleshooting</b>	<b>191</b>
	Compatibility information.....	192
	Power off the PowerProtect Data Manager OVA.....	192
	Creating a dedicated vCenter user account and assigning the role in vCenter.192	
	Specify the required privileges for a dedicated vCenter user account ....	192
	Best practices with the VM Direct appliance.....	195
	Software and hardware requirements.....	196
	PowerProtect Data Manager resource requirements on VMware environment.....	197
	Configuration checklist for common issues.....	197
	VM Direct appliance performance and scalability.....	198
	Increasing the number of instant access sessions.....	199
	Enabling or disabling Changed Block Tracking.....	199
	Configure a backup to support vSAN datastores.....	200
	Disable SSL certification on the vCenter Server.....	200
	Troubleshooting backup configuration issues.....	200
	Troubleshooting virtual machine backup issues.....	201
	VM Direct limitations and unsupported features.....	201
	Managing command execution for VM Direct Agent operations on Linux .....	203
	SQL Server application-consistent backups fail with error "Unable to find VSS metadata files in directory".....	203
	Failed to lock Virtual Machine for backup: Another EMC VM Direct operation 'Backup' is active on VM .....	203
	vMotion operations are not allowed during active backup operations.203	
	Backups fail if certain characters are used in the virtual machine name, datastore, folder, or datacenter names.....	203
	Lock placed on virtual machine during backup and recovery operations continues for 24 hours if VM Direct appliance fails.....	204
	Trailing spaces not supported in SQL database names.....	204
	SQL databases skipped during virtual machine transaction log backup....	204
	Accessing Knowledge Base Articles.....	205
	Recover a failed PowerProtect Data Manager backup.....	205
	Troubleshooting virtual machine restore issues.....	205
	Troubleshooting instant access restore failures.....	207
	FLR Agent for virtual machine file-level restore.....	208
	Supported platform versions for file-level restore.....	209
	File-level restore and SQL restore limitations.....	210
	Troubleshoot recovery of PowerProtect Data Manager.....	212
	Application agent and File System agent co-existence.....	212
	Microsoft application agent for SQL Server application-aware protection.....	214
	Troubleshooting Microsoft Application Agent discoveries on Windows 2008 and Application Direct.....	216
	Supporting more than 50 database clients.....	216
	File System agent limitations.....	216
	Storage Direct agent limitations.....	218
	Time synchronization required between PowerProtect Data Manager and the systems it interfaces with.....	221
	PowerProtect Data Manager allows completion of protection policy when storage unit on the Data Domain cannot be created.....	221
	Viewing the DD Boost storage unit password.....	221
<b>Chapter 16</b>	<b>Modifying the System Settings</b>	<b>223</b>

	System settings.....	224
	Modify the network settings.....	224
	Modify the appliance time zone.....	224
	Change the system root user password.....	224
	Enable replication encryption.....	225
	License types.....	225
	PowerProtect Data Manager licenses.....	226
	System Support.....	227
	Register the Secure Remote Services gateway.....	227
	Callhome .....	228
	Set up the email server.....	230
	Add Auto Support.....	231
	Enable automatic upgrade package downloads.....	231
	Add a log bundle.....	231
	Monitor system state and system health.....	232
	Configure PowerProtect Central reporting.....	234
	Modifying the PowerProtect Data Manager virtual machine disk settings.....	235
	Modify the virtual machine memory configuration.....	235
	Modify the data disk size.....	235
	Modify the system disk size.....	237
	Configure the Data Domain system.....	237
<b>Chapter 17</b>	<b>PowerProtect plug-in within the vSphere Client</b>	<b>239</b>
	Overview of the PowerProtect plug-in within the vSphere Client.....	240
	Prerequisites to using the PowerProtect plug-in within the vSphere Client.....	241
	Monitor virtual machine protection copies.....	242
	Restore a virtual machine protection copy in the vSphere Client.....	242
<b>Chapter 18</b>	<b>VMware Cloud on Amazon Web Services (AWS) Support</b>	<b>245</b>
	PowerProtect Data Manager image backup and recovery for VMware Cloud on AWS.....	246
	Configure the VMware Cloud on AWS web portal console.....	246
	Amazon AWS web portal requirements.....	247
	Interoperability with VMware Cloud on AWS product features.....	247
	vCenter server inventory requirements.....	248
	VMware Cloud on AWS configuration best practices.....	248
	Add a VM Direct appliance.....	248
	Protection and recovery operations.....	249
	Interoperability with VMware Cloud on AWS product features.....	250
	Unsupported operations in VMware Cloud on AWS .....	250
	Troubleshooting VMware Cloud on AWS .....	250



# Preface

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

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

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

**Note:** References to Data Domain systems in this documentation, in the UI, and elsewhere in the product include Data Domain systems and the new PowerProtect DD systems.

## Purpose

This document describes how to install, configure, and administer PowerProtect Data Manager software.

## Audience

This document is intended for the host system administrator who is involved in managing, protecting, and reusing data across the enterprise by deploying PowerProtect Data Manager.

## Revision history

The following table presents the revision history of this document.

**Table 1** Revision history

Revision	Date	Description
03	October 29, 2019	This revision includes the following updates: <ul style="list-style-type: none"><li>File System agent limitations updates, including exclusions when performing block-based backups.</li><li>Add a protection policy for File System protection updates.</li></ul>
02	September 27, 2019	Post GA updates.
01	September 24, 2019	Initial release of this document for PowerProtect Data Manager 19.2.

## Related documentation

The following publications provide additional information:


- PowerProtect Data Manager Administration and User Guide*  
Describes how to configure the software.
- PowerProtect Data Manager Release Notes*  
Contains information on new features, known limitations, environment, and system requirements for the software.
- PowerProtect Data Manager Security Configuration Guide*  
Contains security information.


- *PowerProtect Data Manager Cloud Disaster Recovery Administration and User Guide*  
Describes how to deploy Cloud DR, protect VMs in the AWS cloud, and run recovery operations.
- *PowerProtect Data Manager for Cyber Recovery User Guide*  
Describes how to install, upgrade, patch, and uninstall the Dell EMC PowerProtect Cyber Recovery software.
- PowerProtect Data Manager API documentation: <https://developer.dellemc.com>  
Contains the PowerProtect Data Manager APIs and includes tutorials to guide to you in their use.

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

### Special notice conventions that are used in this document

The following conventions are used for special notices:

 **NOTICE** Identifies content that warns of potential business or data loss.

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

### Typographical conventions

The following type style conventions are used in this document:

**Table 2** Style conventions

<b>Bold</b>	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.
<i>Italic</i>	Used for full titles of publications that are referenced in text.
Monospace	Used for: <ul style="list-style-type: none"> <li>• System code</li> <li>• System output, such as an error message or script</li> <li>• Pathnames, file names, file name extensions, prompts, and syntax</li> <li>• Commands and options</li> </ul>
<i>Monospace italic</i>	Used for variables.
<b>Monospace bold</b>	Used for user input.
[ ]	Square brackets enclose optional values.
	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

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

### Where to find product documentation

- <https://www.dell.com/support>
- <https://community.emc.com>

### Where to get support

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

To access a product-specific page:

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

### Knowledgebase

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

To search the Knowledgebase:

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

### Live chat


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

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

### Service requests

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

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

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

To review an open service request:

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

### Online communities

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

### How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to [DPAD.Doc.Feedback@emc.com](mailto:DPAD.Doc.Feedback@emc.com).

# CHAPTER 1

## Getting Started

This section includes the following topics:

- [Introducing PowerProtect Data Manager software](#)..... 14
- [Accessing the PowerProtect Data Manager UI](#)..... 14

## Introducing PowerProtect Data Manager software

PowerProtect Data Manager software is an enterprise solution that provides software-defined data protection, deduplication, operational agility, self-service, and IT governance.

PowerProtect Data Manager enables the transformation from traditional centralized protection to an IT-as-a-service model, based on a self-service design. This design ensures that you can enforce compliance and other business rules, even when backup responsibilities are decentralized to individual database administrators and application administrators.

PowerProtect Data Manager key features include:

- Software-defined data protection with integrated deduplication, replication, and reuse
- Data backup and recovery self-service operations from native applications that are combined with central IT governance
- Multi-cloud optimization with integrated cloud tiering
- SaaS-based management, compliance, and predictive analytics
- Modern services-based architecture for ease of deployment, scaling, and upgrading

PowerProtect Data Manager integrates multiple data protection products within the Dell EMC Data Protection portfolio to enable data protection as a service, providing the following benefits:

- The data protection team can create data paths with provisioning, automation, and scheduling to embed protection engines into the infrastructure for high-performance backup and recovery.
- For large-scale environments, backup administrators can schedule Microsoft SQL and Oracle backups from a central location on the PowerProtect Data Manager server.
- PowerProtect Data Manager uses an agent-based approach to discover the protected and unprotected databases on an application server.
- PowerProtect Data Manager enables governed self-service and centralized protection by providing the ability to monitor and enforce Service Level Objectives (SLOs), identify violations of Recovery Point Objectives (RPO), and apply retention locks on backups created using the Microsoft application agent and the Oracle RMAN agent.
- PowerProtect Data Manager supports deploying an external VM Direct appliance for data movement with the VM Direct Engine. The PowerProtect Data Manager software comes pre-bundled with an embedded VM Direct appliance, which is automatically used as a fallback proxy for performing backup and restore operations when the added external proxies fail or are disabled. Dell EMC recommends that you always deploy external proxies because the embedded proxy has limited capacity for performing parallel backups.
- PowerProtect Data Manager supports integration of Cloud Disaster Recovery (Cloud DR), including workflows for Cloud DR deployment, protection, and recovery operations in the AWS cloud.

## Accessing the PowerProtect Data Manager UI

PowerProtect Data Manager provides a stand-alone UI that you can use to manage and monitor system behavior.

### Procedure

1. From a host that has network access to the virtual appliance, use Google Chrome to connect to the appliance:

```
https://appliance_hostname
```

**Note:** You can specify the hostname or the IP address of the appliance.

2. Log in with your user name and password.

If you receive an unsigned certificate warning, see [Replacing the default PowerProtect Data Manager certificate](#) on page 15 for instructions.

The **Getting Started** page appears.

- The left pane provides links to the available menu items. Expand a menu item for more options.
- The icons in the PowerProtect Data Manager banner provide additional options.

## Replacing the default PowerProtect Data Manager certificate

Use this procedure to replace the PowerProtect Data Manager UI and public API facing certificates with new self-signed or CA signed certificates.

### Before you begin

You must have the following keys and certificates in place:

- `/etc/ssl/certificates/customer/customerkey.pem`
- `/etc/ssl/certificates/customer/customer.pem`
- `/etc/ssl/certificates/customer/customer.keystore`
- `/etc/ssl/certificates/customca/customca.truststore`

### Procedure

1. Log in to the PowerProtect Data Manager system as the root user.

**Note:** PowerProtect Data Manager does not support using the `ssh` command with the root account. To use `ssh` to connect to the system and change the password for the root account, log in to `ssh` with the admin account, and then use the `su` command to change to the root account.

2. Run the following Unix commands:

```
cd /usr/local/brs/lib/ecdm-ui/app

ln -s /etc/ssl/certificates/customer/customer.pem cert.pem

ln -s /etc/ssl/certificates/customer/customerkey.pem private-key.pem

sudo systemctl restart nginx
```

3. Update the `/usr/local/brs/lib/zuul/conf/application.yml` file with following parameters:

**key-store:** Specify the file path where your key-store certificate is kept. For example: `/etc/ssl/certificates/customer/customer.keystore`

**key-store-password:** Specify a key-store password.

**key-password:** Specify a key password.

**key-alias:** Specify a key alias.

**trust-store:** Specify the file path where your trust-store certificate is kept. For example: `/etc/ssl/certificates/customca/customca.truststore`

**trust-store-password:** Specify a trust-store password.

4. Carry out the command: `zsu1 restart`
5. Log in to the <https://ecdm.customer.com> instance.
6. When prompted, accept the certificate.
7. Login to <https://ecdm.customer.com:8443>.

All external requests are now using your installed certificates.

## Getting Started

The **Getting Started** page provides configuration options that are required when the system is first deployed.

The **Getting Started** page appears upon first deployment of PowerProtect Data Manager and opens to this page by default until you click **Skip This**.

You can access the **Getting Started** page at any time by selecting **System Settings > Getting Started**.

**Table 3** PowerProtect Data Manager Getting Started menu items


Options	Description
<b>Support</b>	View and configure Secure Remote Services (SRS), Email Setup, Auto Support, Logs, System Health.
<b>Disaster Recovery Backup</b>	Configure and manage backups for disaster recovery.
<b>VMware vCenter</b>	Opens the <b>Infrastructure &gt; Asset Sources</b> page where you can add a vCenter instance as an asset source so that it can be added to a protection policy.
<b>Protect Assets</b>	Opens the Protection Policies page where you can manage Protection Life Cycle workflows for all asset types.

## UI tools and options

Learn about the available tools in the UI.







### PowerProtect Data Manager UI tools

**Table 4** PowerProtect Data Manager tools


Menu item	Description
 Dashboard	Provides a high-level view of the overall state the PowerProtect Data Manager system and includes the following information: <ul style="list-style-type: none"> <li>• Alerts—System alerts</li> <li>• Protection—Details about protection policies</li> <li>• Jobs—Status of all Jobs filtered by a selected time frame or status type. Select the status in the <b>Jobs</b> pane to open the <b>Jobs</b> window, where you can manage jobs, search, and view details.</li> <li>• Policy—Details include number of successes, failures, and excluded assets for each asset type</li> <li>• Protection Storage—Protection storage usage statistics</li> </ul>



**Table 4** PowerProtect Data Manager tools (continued)

Menu item	Description
	<ul style="list-style-type: none"> <li>• Recovery—Recovery statistics</li> <li>• Health—Details about the health of the system, including services, licenses, support, protection engines, server backups, and uptime.</li> </ul> <p>PowerProtect Data Manager refreshes the data hourly unless you run an ad-hoc discovery.</p>
 <p>Infrastructure</p>	<p>Click <b>Infrastructure</b> to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• View and manage Virtual Machine, SQL Database, Oracle Database, and File System assets</li> <li>• Add vCenter and Application and File System Host asset sources</li> <li>• View and manage Integrated Storage</li> <li>• Add a VM Direct appliance with the VM Direct protection engine for virtual machine data protection</li> <li>• Manage registration of RMAN Agent, Microsoft Application Agent, and File System Agent</li> <li>• View and manage Cloud disaster recovery</li> </ul>
 <p>Protection</p>	<p>Click <b>Protection</b> to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Add protection policy groups to SQL and Oracle databases, File Systems, and Virtual Machines</li> <li>• Manage SLA</li> <li>• Add, edit, and delete Dynamic Groups to SQL and Oracle databases, File Systems, and Virtual Machines</li> </ul>
 <p>Recovery</p>	<p>Click <b>Recovery</b> to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• View asset copy location details and initiate a Restore operation</li> <li>• Manage Instant Access Sessions</li> </ul>
 <p>Alerts</p>	<p>Click <b>Alerts</b> to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• View and acknowledge alerts and events.</li> <li>• View and drill down to Audit Logs.</li> <li>• Export audit logs to CSV files.</li> <li>• Set audit log boundaries.</li> </ul>
 <p>Administration</p>	<p>Click <b>Administration</b> to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Configure users and roles</li> <li>• Set password credentials and manage key chains</li> <li>• Configure alert notifications</li> <li>• Add LDAP Identity Sources</li> </ul>
	<p>Click <b>Jobs</b> to manage jobs, view by completed or running, filter, and view details.</p>







**Table 4** PowerProtect Data Manager tools (continued)

Menu item	Description
Jobs	
 Reporting	Click <b>Reporting</b> to log in to PowerProtect Central.

### Additional UI options

The following table describes the icons located in the PowerProtect Data Manager banner.

**Table 5** Additional options

Option	Description
	Click to enter search criteria to find assets, jobs, logs, and alerts.
	Click to see recent alerts.
	Click to configure and manage PowerProtect Data Manager system network, time zone, and NTP settings, DR backups, security, licenses, upgrades, authentication, agent downloads, and support, and to access the <b>Getting Started</b> page.
	Click to log out and log in as a different user.
	Click to see PowerProtect Data Manager version information.
	Click to obtain more information about PowerProtect Data Manager and how it can help you manage your backup copies.

# CHAPTER 2

## Managing Users

This section includes the following topics:

- [Managing user roles and privileges](#) ..... 20
- [Resetting system-generated VM Direct credentials](#)..... 30
- [Managing LDAP or AD groups](#)..... 30
- [Managing keychains](#)..... 31
- [LDAP or AD authentication](#)..... 31

## Managing user roles and privileges

Users can be defined as either local or LDAP/Active Directory. Users and LDAP groups can access all protection policies and assets within the PowerProtect Data Manager environment.

The role that is assigned to a user defines the privileges that are associated with the user and determines the tasks that the user can perform.


### Managing users

Only the Admin role can manage users.

The following roles can view users, roles, identity sources, and user groups:

- Admin
- User
- Export and Recovery Admin

Users can see only their own role within their own account.

 **Note:** User authorization grants or denies users access to PowerProtect Data Manager resources. Authorization is the same for locally authorized users and Microsoft Windows Active Directory/LDAP users.

You can create local users to perform management tasks. When you create a local user account, you must assign a role to the user.

### Add a user

You must have administrator credentials to add a user.

#### Procedure

1. Select **Administration > Users**.  
The **Users** window appears.
2. Click **Add**.
3. In the **New User** window, provide the following information:
  - **User first name**
  - **User last name**
  - **Username**
  - **Email Address**
  - **Password**
  - Retype to confirm password
  - **Force Password Change**—Enabled by default. Requires the user to update the password at first login.
  - **Role**
4. Click **Save**.

#### Results

The newly added user appears in the **Users** window.

## Edit or delete a user

You must have administrator credentials to edit or delete a user.

### Procedure

1. Select **Administration > Users**.  
The **Users** window displays the following information:
  - Username
  - User first name
  - User last name
  - User email address
  - User role
  - Date the user was created
2. Select the user you want to edit or delete.
3. Do one of the following:
  - To delete the user, click **Delete**.
  - To edit the user, click **Edit**, modify the user fields, and then click **Save**.

### Results

The changes appear in the **Users** window.

## Reset a password

Local users can reset a forgotten password using this procedure.

### Before you begin

- The user must be a local user.
- A reset password mail server must be configured.
- LDAP and Windows Active Directory users cannot reset their password using this procedure. Contact the system administrator to reset your password.

### About this task

Local users can receive an email with a link to reset their password. The reset password link in the email expires in 20 minutes, after which time they must request another link.

### Procedure

1. In the PowerProtect Data Manager login page, click **Forgot Password**.
2. In the **Forgot Password** dialog box, type your user name, click **Send Link**, and click **OK** to dismiss the informational dialog box.  
The system sends a message to the email address associated with your user name.
3. Open the email and click the link.
4. In the **Reset Password** dialog box, type a new password in the **New Password** and **Confirm New Password** fields, and click **Save**.  
The PowerProtect Data Manager login page appears.
5. Log in with your user name and new password.

## Default admin user

The default admin user is preassigned the Admin role during PowerProtect Data Manager installation.

The default admin user has super user control over PowerProtect Data Manager and cannot be deleted. However, you can modify the attributes of the default admin user.

## Roles

A role defines the privileges and permissions that a user has to perform a group of tasks. When a user is assigned a role, you grant the user all of the privileges that are defined by the role. Only one role can be associated to a user account.

### Admin role

#### Admin

The Admin role is responsible for setup, configuration, and all PowerProtect Data Manager management functions. The Admin role provides systemwide access to all functionality across all organizations. One default Admin role is assigned at PowerProtect Data Manager deployment and installation. You can add and assign additional Admin roles to users in your organization who require full access to the system.

This table outlines the privileges and tasks that are associated with the Admin role.

**Table 6** Admin role privileges and tasks

Privileges	Tasks
Activity Management	<ul style="list-style-type: none"> <li>• Manage Discovery Jobs</li> <li>• Manage Tasks</li> <li>• Workflow Execution</li> </ul>
Asset Management	<ul style="list-style-type: none"> <li>• View Data Source Assets</li> <li>• Manage Data Source Assets</li> <li>• View Protection Storage Targets</li> <li>• Manage Protection Storage Targets</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>• Monitor Events</li> <li>• Manage Events</li> <li>• View Historical Data</li> <li>• View Tasks and Activities</li> </ul>
Recovery and Reuse Management	<ul style="list-style-type: none"> <li>• View Host</li> <li>• Manage Host</li> <li>• Rollback to Production</li> <li>• Recovery to New Location</li> <li>• Export for Reuse</li> </ul>

**Table 6** Admin role privileges and tasks (continued)

Privileges	Tasks
Service Plan Management	<ul style="list-style-type: none"> <li>View Plans</li> <li>Manage Plans</li> <li>Assign Data Source to Plan</li> </ul>
Security and System Audit	<ul style="list-style-type: none"> <li>Monitor Security/System Audit</li> <li>Manage Security/System Audit</li> </ul>
Storage Management	<ul style="list-style-type: none"> <li>View Storage Array</li> <li>Manage Storage Array</li> <li>View Inventory Sources</li> <li>Manage Inventory Sources</li> </ul>
Support Assistance and Log Management	<ul style="list-style-type: none"> <li>View Diagnostic Logs</li> <li>Manage Diagnostic Logs</li> </ul>
System Management	<ul style="list-style-type: none"> <li>View System Settings</li> <li>Manage System Settings</li> </ul>
User/Security Management	<ul style="list-style-type: none"> <li>Manage User Security</li> <li>View User Security</li> </ul>

## User role

### User

The User role is responsible for monitoring the PowerProtect Data Manager Dashboard, Activity Monitor, and Notifications. The User role provides read-only access to monitor activities and operations. Assign the User role to users in your organization who monitor Dashboard activities, Activity Monitor, and Notifications but do not require the ability to configure the system.

This table outlines the privileges and tasks that are associated with the User role.

**Table 7** User role privileges and tasks

Privileges	Tasks
Activity Management	<ul style="list-style-type: none"> <li>Workflow Execution</li> </ul>
Asset Management	<ul style="list-style-type: none"> <li>View Data Source Assets</li> <li>View Protection Storage Targets</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>Monitor Events</li> <li>View Historical Data</li> <li>View Tasks and Activities</li> </ul>

**Table 7** User role privileges and tasks (continued)

Privileges	Tasks
Recovery and Reuse Management	<ul style="list-style-type: none"> <li>View Host</li> </ul>
Service Plan Management	<ul style="list-style-type: none"> <li>View Plans</li> </ul>
Security and System Audit	<ul style="list-style-type: none"> <li>Monitor Security/System Audit</li> </ul>
Storage Management	<ul style="list-style-type: none"> <li>View Storage Array</li> <li>View Inventory Sources</li> </ul>
Support Assistance and Log Management	<ul style="list-style-type: none"> <li>View Diagnostic Logs</li> </ul>
System Management	<ul style="list-style-type: none"> <li>View System Settings</li> </ul>
User/Security Management	<ul style="list-style-type: none"> <li>View User Security</li> </ul>

## Export and Recovery Admin role

### Export and Recovery Admin

The Export and Recovery Admin role is defined for a dedicated set of users who are solely responsible for PowerProtect Data Manager setup, configuration, and execution of data management tasks such as copy export and recovery operations. The Export and Recovery Admin role provides access only to those functions required for data export and recovery operations. This role and its operations are intended for a limited set of users whose actions are solely focused on data management, export, and recovery; and whose actions are audited routinely for security purposes. Assign the Export and Recovery Admin role to a user in your organization that requires access to data only to make it available to others in the organization to maintain a chain of custody record.

This table outlines the privileges and tasks that are associated with the Export and Recovery Admin role.

**Table 8** Export and Recovery Admin role privileges and tasks

Privileges	Tasks
Activity Management	None
Asset Management	<ul style="list-style-type: none"> <li>View Data Source Assets</li> <li>View Protection Storage Targets</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>Monitor Events</li> <li>View Historical Data</li> <li>View Tasks and Activities</li> </ul>
Recovery and Reuse Management	<ul style="list-style-type: none"> <li>View Host</li> <li>Manage Host</li> </ul>



**Table 8** Export and Recovery Admin role privileges and tasks (continued)

Privileges	Tasks
	<ul style="list-style-type: none"> <li>Rollback to Production</li> <li>Recovery to New Location</li> <li>Export for Reuse</li> </ul>
Service Plan Management	None
Security and System Audit	None
Storage Management	<ul style="list-style-type: none"> <li>View Storage Array</li> </ul>
Support Assistance and Log Management	<ul style="list-style-type: none"> <li>View Diagnostic Logs</li> </ul>
System Management	<ul style="list-style-type: none"> <li>View System Settings</li> </ul>
User/Security Management	<ul style="list-style-type: none"> <li>View User Security</li> </ul>

## Privileges

PowerProtect Data Manager privileges define the tasks that a user can perform and these privileges are assigned to roles.

### Activity Management Privileges

This table defines the Activity Management Privileges.

**Table 9** Activity Management Privileges

Privilege	Task
Manage Discovery Jobs	<ul style="list-style-type: none"> <li>Create discovery jobs.</li> <li>View discovery jobs.</li> <li>Edit discovery jobs.</li> <li>Delete discovery jobs.</li> </ul>
Manage Task	<ul style="list-style-type: none"> <li>Create task resources.</li> <li>View task resources.</li> <li>Edit task resources.</li> </ul>
Workflow Execution	<ul style="list-style-type: none"> <li>Start workflow execution.</li> <li>Cancel workflow execution.</li> <li>View the status of workflow execution.</li> </ul>

## Asset Management Privileges

This table defines the Asset Management Privileges.

**Table 10** Asset Management Privileges

Privilege	Task
Manage Data Source Assets	<ul style="list-style-type: none"> <li>• Create, read, edit, and delete a data source.</li> <li>• Create, view, edit, and delete the policy in the protection group resource.</li> <li>• Create, view, edit, and delete asset group resources.</li> <li>• Create, view, edit, patch, and delete tag category resources.</li> </ul>
Manage Protection Storage Targets	<ul style="list-style-type: none"> <li>• Create, view, edit, and delete a data target.</li> <li>• Create, view, edit, and delete asset group resources of protection storage targets.</li> </ul>
View Data Source Assets	<ul style="list-style-type: none"> <li>• View a data source.</li> <li>• View asset group resources.</li> <li>• View the policy of the protection group resource.</li> <li>• View tag category resources.</li> </ul>
View Protection Storage Targets	<ul style="list-style-type: none"> <li>• View a data target.</li> </ul>

## Monitoring Privileges

This table defines the Monitoring Privileges.

**Table 11** Monitoring Privileges

Privilege	Task
View Tasks or Activities	<ul style="list-style-type: none"> <li>• View task resources.</li> </ul>
View Historical Data	<ul style="list-style-type: none"> <li>• View historical data that relates to plans, arrays, data targets, data sources, and capacity data.</li> </ul>
Monitor Events	<ul style="list-style-type: none"> <li>• View alerts.</li> <li>• View external notifications.</li> </ul>
Manage Events	<ul style="list-style-type: none"> <li>• Acknowledge alerts and add notes.</li> <li>• Create, modify, and delete external notifications.</li> </ul>

## Service Policy Management Privileges

This table defines the Policy Management Privileges.

**Table 12** Policy Management Privileges

Privilege	Task
Assign Data Source to Policy	<ul style="list-style-type: none"> <li>Assign a data source to a protection policy resource.</li> </ul>
Manage Policies	<ul style="list-style-type: none"> <li>Create, view, edit, and delete the policy for a protection policy resource.</li> <li>Create, view, edit, and delete a policy definition resource.</li> <li>Create, view, edit, and delete schedule resources.</li> <li>Create, view, edit, and delete an objective definition resource.</li> <li>Create, read, edit, and delete an action definition.</li> </ul>
View Policies	<ul style="list-style-type: none"> <li>View the policy for a protection policy resource.</li> <li>View schedule.</li> <li>View a protection policy definition.</li> <li>View objective definition.</li> <li>View services.</li> <li>View service resources.</li> <li>View assets that are assigned to a protection policy.</li> <li>View action definitions.</li> <li>View asset group resources.</li> </ul>

## Recovery and Reuse Management Privileges

This table defines the Recovery and Reuse Management Privileges.

**Table 13** Recovery and Reuse Management Privileges

Privilege	Task
Export for Reuse	<ul style="list-style-type: none"> <li>Create, view, edit, and start export and reuse operations.</li> </ul>
Roll back to Production	<ul style="list-style-type: none"> <li>Create, view, edit, and start rollback to production operations.</li> </ul>
Recovery to Alternate Location	<ul style="list-style-type: none"> <li>Create, view, edit, and start recovery to alternate location operations.</li> </ul>
Manage Host	<ul style="list-style-type: none"> <li>Create, view, edit and delete a host.</li> </ul>
View Host	<ul style="list-style-type: none"> <li>View a host.</li> </ul>

## Storage Management Privileges

This table defines the Storage Management Privileges.

**Table 14** Storage Management Privileges

Privilege	Task
View Inventory Sources	<ul style="list-style-type: none"> <li>View a management interface.</li> <li>Read storage manager resources such as exported, deleted, and restored copies.</li> </ul>
View Storage Array	<ul style="list-style-type: none"> <li>View a storage array.</li> </ul>
Manage Storage Array	<ul style="list-style-type: none"> <li>Create, view, edit, and delete a storage array.</li> </ul>
Manage Inventory Sources	<ul style="list-style-type: none"> <li>Create storage manager resources and run creation-related storage array operations.</li> <li>Create exported and restored copies and run restore-related storage array operations.</li> <li>Create expunged copies and run deletion-related storage array operations.</li> <li>Create, view, edit, and delete a management interface.</li> </ul>

### Security Management Privileges

This table defines the Security Management Privileges.

**Table 15** Security Management Privileges

Privilege	Task
Manage User Security	<ul style="list-style-type: none"> <li>Create, view, edit, and delete users</li> <li>View roles</li> <li>Create, view, edit, and delete identity sources</li> <li>Create, view, edit, and delete user groups</li> <li>Create, view, edit, and delete whitelists</li> </ul>
View User Security	<ul style="list-style-type: none"> <li>View users and roles</li> <li>View identity sources and user groups</li> <li>View whitelists</li> </ul>

### System Management Privileges

This table defines the System Management Privileges.

**Table 16** System Management Privileges

Privilege	Task
View System Settings	<ul style="list-style-type: none"> <li>View SRS information.</li> </ul>

**Table 16** System Management Privileges (continued)

Privilege	Task
	<ul style="list-style-type: none"> <li>View Server Disaster Recovery artifacts.</li> <li>View Maintenance Mode.</li> <li>View License information.</li> <li>View Server Disaster Recovery Status.</li> <li>View node, Configuration EULA, OS User, Upgrade Package, Component, Configuration Status, Configuration Logs, Time Zone, and State resources</li> </ul>
Manage System Settings	<ul style="list-style-type: none"> <li>Manage Server Disaster Recovery activities.</li> <li>Manage SRS Gateway connection and other Telemetry communications.</li> <li>View and edit Node State resource.</li> <li>Update the license for the appliance.</li> <li>View Component, Configuration Status, Configuration Logs, Time Zone, and State resources</li> <li>View and edit node, Configuration EULA, OS User, and Lockbox resources.</li> <li>Create, view, edit, and delete the Upgrade Package resource</li> </ul>

### Support Assistance and Log Management Privileges

This table defines the Support Assistance and Log Management Privileges.

**Table 17** Support Assistance and Log Management Privileges

Privilege	Task
View Diagnostic Logs	<ul style="list-style-type: none"> <li>View Log bundle resources.</li> <li>View Log information resources.</li> <li>View the LogSource resource.</li> <li>View logs.</li> </ul>
Manage Diagnostic Logs	<ul style="list-style-type: none"> <li>Manage Log bundle resources.</li> <li>Retrieve Log information resources.</li> <li>Retrieve or edit the LogSource resource.</li> <li>Export logs.</li> </ul>

### Security and System Audit Privileges

This table defines the Security and System Audit Privileges.

**Table 18** Security and System Audit Privileges

Privilege	Task
Monitor Security/ System Audit	<ul style="list-style-type: none"> <li>View Security Audit–related events and activities.</li> </ul>
Manage Security/ System Audit	<ul style="list-style-type: none"> <li>Acknowledge Security Audit–related events and activities.</li> <li>Export Audit/Change Log of events and activities.</li> </ul>

## Resetting system-generated VM Direct credentials

PowerProtect Data Manager deploys the VM Direct Engine during installation with unique admin and root credentials.

### About this task

You must have PowerProtect Data Manager Admin role privileges to edit or delete a user.

### Procedure

1. Select **Administration > Credentials**.  
The **Credentials Management** window appears and displays the type, name, and username.
2. Select a VM Direct user and click **Edit**.
3. Modify the password in the **Edit Credentials** window and click **Save**.
4. Select **Infrastructure > Protection Engines > VM Direct Engines**.
5. Select a VM Direct Engine.
6. Select **redeploy** from the **ellipsis** list.

## Managing LDAP or AD groups

PowerProtect Data Manager requires you to configure an LDAP group, and the PowerProtect Data Manager users must be part of this group. Only the Admin role can create users or LDAP and AD groups.

### Users

You can create local users to perform management tasks. When you create a local user account, you must assign a role to the user.

### LDAP or AD groups

When you configure LDAP or AD authentication in the Authentication Service, use the User Group resources to assign roles to the LDAP groups. The User Group resource defines the role assignments for an LDAP or AD user group.

## Managing keychains

You can create, edit, delete, and view keychain credentials.

### Add credentials


#### Procedure

1. Select **Administration > Credentials > Add**.  
The **Add Credentials** window appears.
2. Enter the following information, and then click **Save**.
  - **Type**—The type of credential you would like to add
  - **Username**—The username associated with the credential you are adding
  - **Password**—The password associated with the username

## LDAP or AD authentication

When you authenticate users through an external authentication authority, users can log in with their authority username and password. The authority username and password are managed by Lightweight Directory Access Protocol (LDAP), Lightweight Directory Access Protocol over SSL (LDAPS), Microsoft Active Directory server (AD), or a Microsoft Active Directory server over SSL.

When the user's credentials are validated, the Authentication Service issues a token for the user. The PowerProtect Data Manager GUI uses the token information to authorize the user's activities.

 **Note:** You can configure only one authority.

### Configuring LDAP or AD authorities and assigning roles

Only the Admin role can configure an external LDAP, LDAPS, or AD authentication authority. You can configure LDAP or AD roles in **Administration > Identity Sources**.

#### Configure LDAP or Active Directory authentication

Only the Admin role can configure an external LDAP, LDAPS, or Active Directory authentication authority.

#### Procedure

1. Select **Administration > Identity Sources**.  
The **Identity Sources** window appears.
2. Click **New**.  
The **Identity Source Server** window appears.
3. In the **Required** tab, configure the following attributes:

Attribute	Description
Server Type	Select one: <ul style="list-style-type: none"> <li>• Active Directory</li> </ul>

Attribute	Description
	<ul style="list-style-type: none"> <li>LDAP</li> </ul>
Server Address	<p>Type the protocol and hostname or IP address of the LDAP or Active Directory server, in the following format:</p> <p><i>protocol://hostname_or_ip_address</i></p> <p>where:</p> <ul style="list-style-type: none"> <li><i>protocol</i> is <code>ldap</code> for LDAP or Active Directory authorities, and <code>ldaps</code> for LDAPS or Active Directory over SSL. For example, to configure an Active Directory server that is named <code>idd-ad.iddlab.com</code>, type <code>ldap://idd-ad.iddlab.com</code></li> <li><i>hostname_or_ip_address</i> is the FQDN or IP address of the external authentication authority. For example, <code>ldap://[2620:0:170:5a9::1:2]</code></li> </ul> <p><b>Note:</b> When you specify the LDAPS protocol, PowerProtect Data Manager automatically downloads the certificates required to connect to the authentication authority. Once downloaded, the <b>Certificate</b> field appears. Click <b>Verify</b> to compare the displayed certificate information with the expected authentication authority's certificate information. If the certificates match, click <b>Accept</b> to continue with the setup. Otherwise, click <b>Cancel</b> to cancel the setup.</p>
Domain	<p>Type the base distinguished name (DN) of the LDAP or Active Directory authority.</p> <p>For example, <code>dc=pp_lab, dc=ldap.example.com</code></p>
Port	<p>Type the port number that the external authentication authority uses.</p> <ul style="list-style-type: none"> <li>For LDAP and Active Directory, the default port number is 389.</li> <li>For LDAPS and Active Directory over SSL, the default port number is 636.</li> </ul>
User Search	<ol style="list-style-type: none"> <li>Type the <i>objectClass</i> that the authentication service uses when searching for users in the LDAP or AD hierarchy.</li> <li>Ensure that you specify a search path that is relative to the base DN that you specified in the Domain option.</li> </ol> <p>For example:</p> <ul style="list-style-type: none"> <li>For an Active Directory configuration, specify the value in the <i>objectClass</i> property for an AD user. For example, type <code>user</code>.</li> <li>For an LDAP configuration, specify the value in the <i>objectClass</i> property. For example, type <code>account</code>.</li> </ul>
Group Search	<ol style="list-style-type: none"> <li>Type the <i>objectClass</i> of the search path that you want the authentication service to use when searching for groups in the LDAP or AD hierarchy.</li> <li>Ensure that you specify a search path that is relative to the base DN that you specified in the Domain attribute.</li> </ol>



Attribute	Description
	<p>For example:</p> <ul style="list-style-type: none"> <li>For an Active Directory configuration, specify the value in the <i>objectClass</i> property for an AD group. For example, type <code>group</code>.</li> <li>For an LDAP configuration, specify the value in the <i>objectClass</i> property for an LDAP group. This value should be a structural objectClass. For example, type <code>group</code>.</li> </ul>
Query User	<p>Type a user account that has full read access to the LDAP or AD directory, in the following formats:</p> <ul style="list-style-type: none"> <li>For Active Directory, the format is <code>user@domain</code>, or the DN of the query user. For example, <code>administrator@ldap.example.com</code> or <code>cn=administrator,dc=example,dc=com</code>.</li> <li>For LDAP, the format is <code>user@domain</code>. For example, <code>administrator@ldap.example.com</code>.</li> </ul>
Query Password	Type the password of the user account that you specified in the <b>Query User</b> attribute.

4. (Optional) In the **Advanced** tab, configure the following attributes:

Attribute	Description
User Search Path	<p>Type the DN of the search path that the authentication service uses when searching for users in the LDAP or AD hierarchy. Ensure that you specify a search path that is relative to the base DN that you specified in the Domain option. For example:</p> <ul style="list-style-type: none"> <li>For an AD configuration, specify the value in the <i>objectClass</i> property for an AD user.</li> <li>For an LDAP configuration, specify the value in the <i>account</i> object class.</li> </ul>
User Group Search Path	<p>Type the DN of the search path that the authentication service should use when searching for groups in the LDAP or AD hierarchy. Ensure that you specify a search path that is relative to the base DN that you specified in the Domain attribute. For example:</p> <ul style="list-style-type: none"> <li>For an AD configuration, specify the value in the <i>objectClass</i> property for an AD group.</li> <li>For an LDAP configuration, specify the value in the <i>posixGroup</i> object class.</li> </ul>
Group Attribute Name	<p>Type the attribute that the authentication service should use to validate the group name in the LDAP or AD hierarchy. For example:</p> <ul style="list-style-type: none"> <li>For an AD configuration, specify <code>sAMAccountName</code>.</li> <li>For an LDAP configuration, specify <code>cn</code>.</li> </ul>
Group Member Attribute	Type the attribute that the authentication service should use to validate the group member in the LDAP or AD hierarchy.

Attribute	Description
	For example: <ul style="list-style-type: none"> <li>• For an AD configuration, specify <i>member</i>.</li> <li>• For an LDAP configuration, specify <i>memberUid</i>.</li> </ul>
User Attribute ID	Type the attribute that the authentication service should use to validate the username in the LDAP or AD hierarchy. For example: <ul style="list-style-type: none"> <li>• For an AD configuration, specify <i>sAMAccountName</i>.</li> <li>• For an LDAP configuration, specify <i>cn</i>.</li> </ul>

5. Click **Save**.
6. Assign LDAP or AD groups to a role. The section [Add LDAP group-to-role mapping](#) on page 34 provides instructions.

This step is required before you can log in to the UI with an LDAP or AD account.

### Edit an LDAP or AD authority configuration

Only the Admin role can edit an LDAP or AD authority.

#### Procedure

1. Select **Administration > Identity Sources**.
2. Select the Identity Source you would like to edit, and then click **Edit**.
3. Edit the LDAP attributes as required.
4. Click **Save**.

### Delete an LDAP or AD authority configuration

Only the Admin role can delete an existing LDAP or AD authority configuration.

#### Procedure

1. Select **Administration > Identity Sources**.
2. Select the Identity Source you would like to delete, and then click **Delete**.

### Add LDAP group-to-role mapping

Only the Admin role can add LDAP group-to-role mapping.

#### Procedure

1. Select **Administration > Identity Sources**.
2. Select the identity source for which you would like to add group-to-role mapping, and then click **New Group Map**.
3. Assign the LDAP or AD groups to a role.
4. Click **Add**.

### Modify LDAP group-to-role mapping

Only the Admin role can modify LDAP group-to-role mapping.

#### Procedure


1. Select **Administration > Identity Sources**.

2. Select the identity source for which you would like to edit group-to-role mapping, and then click **New Group Map**.
3. Assign the same LDAP or AD groups to a different role.
4. Click **Add**.

### Delete LDAP group-to-role mapping

Only the Admin role can delete LDAP group-to-role mapping.

#### Procedure

1. Select **Administration > Identity Sources**.
2. Select the group or group roles you would like to delete, and then click .

### Example: Configuring an AD authority

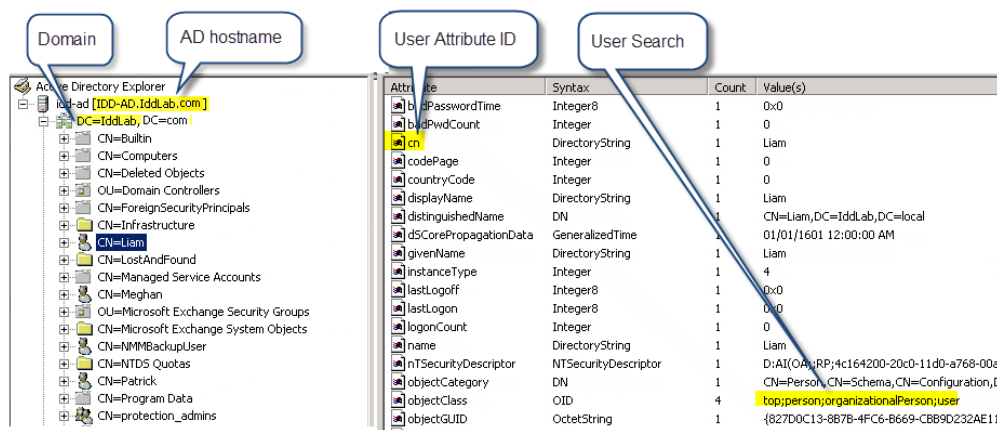
In this example, an AD server that is named *idd-ad.iddlab.com* has an AD group called *Protection\_admins*. *Protection\_admins* contains three users: Meghan, Patrick, and Liam. These users require access to the PowerProtect Data Manager UI with the privileges that are assigned to the User role.

#### View the properties of the AD configuration

To view the properties of the AD configuration, use a third-party tool such as the AD Explorer program.

The following figure provides an example of the key user attributes on the AD server, which are required to configure *idd-ad.iddlab.com*.

**Figure 1** AD and user properties in AD Explorer



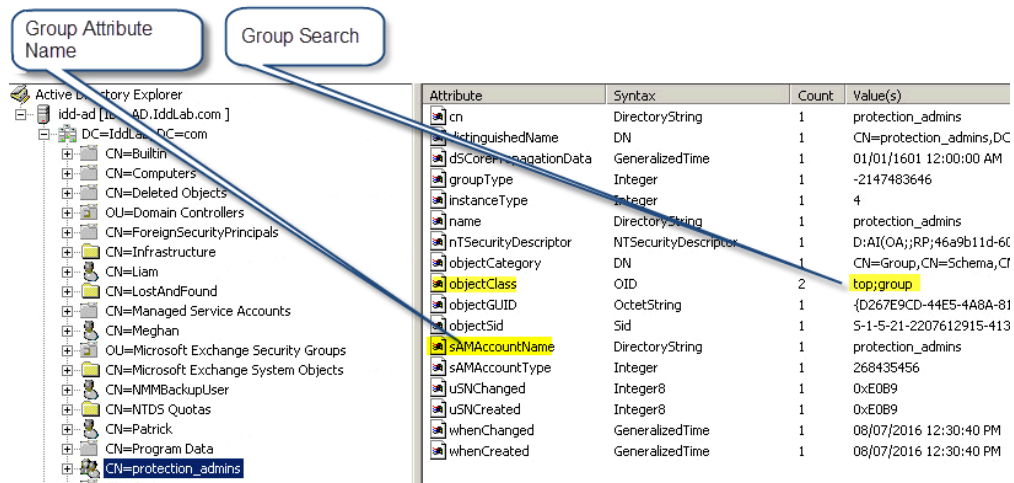
Based on this AD configuration, specify the following values for PowerProtect Data Manager LDAP configuration options:

- Domain: `dc=iddlab, dc=com`
- Hostname: `idd-ad-iddlab.com`
- User Search: One of the following values: `top`, `inetOrgPerson`, or `user`
- User Attribute ID: `cn`

#### Configure the *idd-ad.iddlab.com* authority

The following figure provides an example of the group attributes that are required to configure the *idd-ad.iddlab.com* authority.

**Figure 2** AD group properties in AD Explorer



Based on the properties of *Protection\_admins*, specify the following values for the LDAP configuration options:

- Group Search: `top` or `group`
- Group Attribute Name: `sAMAccountName`

### Example: Configuring an LDAP authority

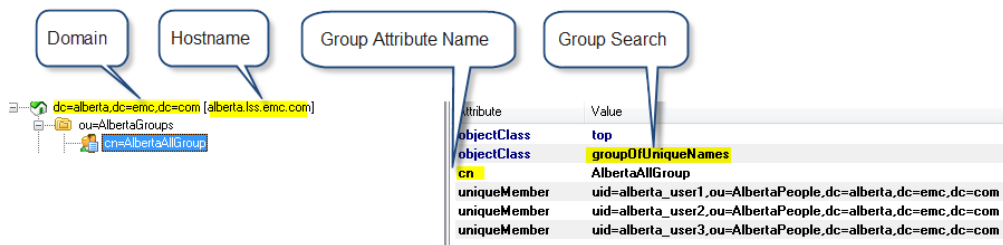
In this example, an LDAP server that is named *alberta.lss.emc.com* has a group that is named *AlbertaAllGroups*. *AlbertaAllGroups* contains three LDAP users: *alberta\_user1*, *alberta\_user2*, and *alberta\_user3*. These users require access to the PowerProtect Data Manager UI with the privileges that are assigned to the User role.

#### View the LDAP configuration properties

To view the properties of the LDAP configuration, use a third party tool such as the LDAP Admin program.

The following figure provides an example of the key user attributes to use when configuring an LDAP authority.

**Figure 3** LDAP Admin server and group attributes



Based on this configuration, specify the following values for the LDAP configuration options:

- Domain: `dc=alberta,dc=emc,dc=com`
- Hostname: `alberta.lss.emc.com`
- Group Search: `groupOfUniqueNames`.

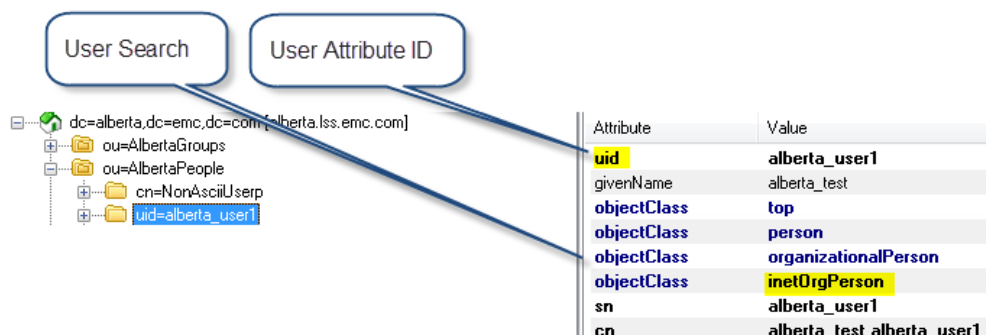
**Note:** Only structural object classes may be values for the group search. So, in the example, although `top` is an object class, only `groupOfUniqueNames` can be used as a group search value.

- Group Attribute Name: `cn`

### Specify values in the user search attribute

The following figure provides an example of the value to specify in the user search attribute.

**Figure 4** LDAP Admin user search attribute



Based on this configuration, specify the following values for the LDAP configuration options:

- User Search: One of the following objectClass values: `top`, `person`, `organizationalPerson`, or `inetOrgPerson`
- User Attribute ID: `cn`

## Troubleshooting LDAP configuration issues

This section provides information about error messages that might appear when you configure an external authority for authentication.

For more information about LDAP configuration errors, refer to [http://wiki.servicenow.com/index.php?title=LDAP\\_Error\\_Codes#gsc.tab=0](http://wiki.servicenow.com/index.php?title=LDAP_Error_Codes#gsc.tab=0).

### User credentials are incorrect

The following message appears when the user credentials that you specified are not correct:

```
org.springframework.ldaps.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903A9, commentL AcceptSecurityContext error, data 52e, vldb1]
```

To resolve this issue, ensure that the values in the **Query User** and **Query Password** fields are correct.

### Base DN is not correct

The following message appears when Base DN is not correct:

```
org.springframework.ldap.InvalidNameException: Invalid name: domain_name
```

To resolve this issue, ensure that the value in the **Domain** field is correct.

## Format of the Server Address field is not correct

The following message appears when the format of the **Server Address** field is not correct:

```
org.springframework.ldap.UncategorizedLdapException: Uncategorized Exception  
occurred during LDAP processing; nested exception is  
javax.naming.NamingException: Cannot parse url: url
```

To resolve this issue, ensure that you specify the **Server Address** field in the following format:

- For an LDAP or Active Directory authority: `ldap://hostname_ip_address`
- For an LDAPS or Active Directory over SSL authority: `ldaps://hostname_ip_address`

# CHAPTER 3

## Managing Storage

This section includes the following topics:

- [Add protection storage](#) .....40
- [Overview of PowerProtect Data Manager cloud tier](#).....41
- [Overview of PowerProtect Data Manager Cloud Disaster Recovery](#).....41

## Add protection storage

### About this task

The PowerProtect Data Manager UI enables users with administrator credentials to add the following storage types:

- Data Domain Management Center
- External Data Domain system

**Note:** References to Data Domain systems in this documentation, in the UI, and elsewhere in the product include Data Domain systems and the new PowerProtect DD systems.

### Procedure

1. Select **Infrastructure > Storage**.

The **Storage** window appears.

2. In the **Protection Storage** tab, click **Add**.
3. In the **Add Storage** dialog box, select a storage system (Data Domain System, Data Domain Management Center).

**Note:** If using the Storage Direct agent to move snapshot backups from a VMAX storage array to a Data Domain system, you do not need to add a Data Domain Management Center.

4. Specify the storage system attributes:
  - a. In the **Name** field, specify a storage name.
  - b. In the **Address** field, specify the hostname, fully qualified domain name (FQDN), or the IP address.  
  
If you specify a virtual machine for the storage name, use the FQDN.
  - c. In the **Port** field, specify the port for SSL communication.
5. Under **Add Credentials**, if you have already configured Data Domain credentials that are common across Data Domain systems, select an existing keychain from the **Select Keychain** list. Alternatively, you can add new credentials, and then click **Save**.
6. If a trusted certificate does not exist on the storage system, a dialog box appears requesting certificate approval. Review the certificate and then click **Verify**.
7. Click **Save** to exit the **Add Storage** dialog and initiate the discovery of the storage system.

A dialog box appears to indicate that the request to add storage has been initiated.

**Note:** Discovery time is based on networking bandwidth. The resources that are discovered and those that are doing the discovery take a performance hit each time that you go through a discovery process. It might appear that PowerProtect Data Manager is not updating the storage data while the discovery is in progress.

PowerProtect Data Manager can add up to three assets of the same type simultaneously and up to 10 assets simultaneously.

8. In the **Storage** window, click **Discover** to refresh the window with any newly discovered storage systems.

When a discovery completes successfully, the **Status** column updates to **OK**.



9. To modify a storage system location:
  - a. In the **Storage** window, select the storage system from the table.
  - b. Click **Set Location**.  
The **Set Location** window appears.
  - c. Click **Location > Add**.  
The **Add Location** window appears.
  - d. In the **Name** field, type a location name for the asset, and click **Save**.
10. To manage MTrees in the **Storage** window, select the storage system from the table and click **Manage MTrees**.

### Results

PowerProtect Data Manager displays External Data Domain systems only in the **Storage Name** column. PowerProtect Data Manager displays Data Domain Management Center storage types in the **Managed By** column.

## Overview of PowerProtect Data Manager cloud tier

The PowerProtect Data Manager cloud tier feature works in tandem with the Data Domain Cloud Tier feature to move PowerProtect Data Manager backups from Data Domain systems to the cloud. This provides long-term storage of PowerProtect Data Manager backups by seamlessly and securely tiering data to the cloud.

From the PowerProtect Data Manager UI, you configure cloud tier to move PowerProtect Data Manager backups from Data Domain to the cloud, and you can perform seamless recovery of these backups.

Data Domain cloud storage units must be pre-configured on the Data Domain system before they are configured for cloud tier in the PowerProtect Data Manager UI. The *Data Domain Operating System Administration Guide* provides further information.

### Add Data Domain cloud protection storage

You can add cloud tier storage by accessing either the physical or virtual Data Domain system.

#### Procedure

- The "DD cloud tier" chapter of the *DD OS Administration Guide*, available on [Dell EMC Online Support](#), provides instructions.

**Note:** If a protection policy has both replication and tiering objectives defined, ensure that replication from any system occurs before tiering. For example, create backups to DD A, replicate from DD A to DD B, and then tier from DD A to Cloud.

## Overview of PowerProtect Data Manager Cloud Disaster Recovery

The Cloud DR feature enables you to deploy a Cloud DR Server in the public cloud and provide DR protection to the cloud as part of the PowerProtect Data Manager protection life cycle. From the PowerProtect Data Manager, you can run DR work flows in the cloud and monitor the progress of these jobs.

For example, to validate that you can fail over a VM copy to the cloud before a disaster occurs, from PowerProtect Data Manager, you select a network in the cloud, start a DR test, and monitor

its progress. If you want to fail over a production VM, from PowerProtect Data Manager, you select a network in the cloud, start the DR failover operation, and then bring up the restored VM within AWS.

To learn about Cloud DR work flows within PowerProtect Data Manager, see the *PowerProtect Data Manager Cloud Disaster Recovery Administration and User Guide*.

# CHAPTER 4

## Enabling the Microsoft Application Agent for SQL

This section includes the following topics:

- [About the Microsoft application agent for SQL](#)..... 44
- [Microsoft SQL Server data protection and replication requirements](#)..... 44
- [Protecting a stand-alone SQL Server](#)..... 44
- [Protecting SQL Server clustered environments](#)..... 45
- [Install and configure the Microsoft application agent for SQL Server](#).....46
- [Manage the Microsoft application agent for SQL](#)..... 50
- [Support for existing SQL agent backups with PowerProtect Data Manager](#)..... 51

## About the Microsoft application agent for SQL

The Microsoft application agent enables an application administrator to protect and recover the SQL application data on the application host. PowerProtect Data Manager integrates with the Microsoft application agent to check and monitor backup compliance against protection policies. PowerProtect Data Manager also enables central scheduling for backups.

You can install the Microsoft application agent on a Windows SQL Server host by using the install wizard. [Install and configure the Microsoft application agent for SQL Server](#) on page 46 provides instructions.



### Note:

PowerProtect Data Manager supports the co-existence of the Microsoft SQL agent and the File System agent on Windows.

To enable the discovery and scheduling of backups with PowerProtect Data Manager, you must approve the client in the PowerProtect Data Manager UI.

Software compatibility information for the PowerProtect Data Manager software and application agents is provided in the eLab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.

## Microsoft SQL Server data protection and replication requirements

PowerProtect Data Manager can manage and monitor data protection and replication for Microsoft SQL Server assets through integration with the Microsoft application agent.

After installing the Microsoft application agent, review the following information for additional requirements before adding the Microsoft application agent as an asset source in PowerProtect Data Manager and discovering the SQL Server assets.

Verify that the environment meets the following requirements:

- Ensure that you do not mix 32-bit and 64-bit instances on the same SQL Server host. PowerProtect Data Manager operations do not support hosts with a mix of 32-bit and 64-bit SQL Server instances.
- Ensure that all clocks on the SQL Server host, domain controller, and PowerProtect Data Manager are time-synced to the local NTP server to ensure discovery of the backups.
- Ensure that the SQL Server and the PowerProtect Data Manager system network can see and resolve each other.
- Ensure that port 7000 is open on the SQL Server host.
- Ensure that DNS is configured correctly on the Application Agent Host for SQL Server.

## Protecting a stand-alone SQL Server

Learn how to configure protection of a stand-alone SQL Server.

### Procedure

1. Add storage for Data Domain Management Console or the External Data Domain.  
[Add protection storage](#) on page 40 provides information.
2. Install the Microsoft application agent on the SQL Server host.  
[Install the Microsoft application agent](#) on page 46 provides information.

3. Add or approve the Microsoft application agent in PowerProtect Data Manager.  
[Manage the Microsoft application agent for SQL](#) on page 50 provides information.
  4. Discover and add the credentials for the SQL application host.  
[Discover an Oracle or SQL application host](#) on page 111 provides information.
  5. Create a protection policy to protect the SQL host.  
[Add a protection policy for SQL database protection](#) on page 122 provides information.
- Note:** You cannot perform a backup to a secondary Data Domain device. You can only restore from a secondary Data Domain device

## Protecting SQL Server clustered environments

Learn how to configure protection of SQL Server clustered environments, including Always On availability groups and Failover Cluster Instances.

### About this task

On each node in the cluster, repeat the steps to install the Microsoft application agent, and then add and discover the application host in PowerProtect Data Manager.

- NOTICE** Protection of Failover Cluster Instances (FCI) requires that all nodes in the cluster be registered to the PowerProtect Data Manager server. Prior to registration, the node must be the active node and own all the disks in the cluster. The recommended method is to failover all nodes to the registering node. Repeat this step for all nodes in the cluster and any nodes added to the cluster. Failure to perform this step results in unpredictable results during protection policy.

### Procedure

1. Add a storage system.  
[Add protection storage](#) on page 40 provides information.
  2. Install the Microsoft application agent on each node in the cluster.  
[Install the Microsoft application agent](#) on page 46 provides information.
  3. Configure the required user privileges on each node in the cluster.  
[Required privileges for backup and recovery of a Failover Cluster Instance or Always On Failover Cluster Instance](#) on page 50 provides information.
  4. Add or approve the Microsoft application agent on each node in the cluster.  
[Manage the Microsoft application agent for SQL](#) on page 50 provides information.
  5. Discover and add the credentials for each SQL application host.  
[Discover an Oracle or SQL application host](#) on page 111 provides information.
  6. Create a protection policy to protect the cluster.  
[Add a protection policy for SQL database protection](#) on page 122 provides information.
- Note:** You cannot perform a backup to a secondary Data Domain device. You can only restore from a secondary Data Domain device

# Install and configure the Microsoft application agent for SQL Server

Learn how to install and configure the Microsoft application agent for SQL Server.

## Prerequisites


Ensure that a SQL Server environment meets the following prerequisites before you install the Microsoft application agent:

- Install the following applications on the Windows host:
  - Microsoft SQL Server
  - The SQL Server Management Studio (SSMS)
  - .NET Framework 4.0  
If you are installing ItemPoint for table-level recovery, install .NET Framework 4.5.
- In the PowerProtect Data Manager UI, select **Agent Downloads** from the **System Settings** menu, select the Microsoft application agent download package, `msappagent192_win_x64.zip`, and then download the package to the Windows SQL Server host.
- Log in to the SQL Server host as an Administrator to install the Microsoft application agent.
- To deploy the Common Language Runtime (CLR) assembly, ensure that you have Administrator access to the SQL Server host and the master database. If the SQL Server host is running in a domain, ensure that you have access as a Domain administrator.

## Install the Microsoft application agent

Learn how to install the Microsoft application agent.

### About this task

 **Note:** In Always On availability group or cluster environments, you must install the Microsoft application agent on each node in the cluster.

### Procedure

1. In the PowerProtect Data Manager UI:
  - a. Select **Agent Downloads** from the **System Settings** menu.
  - b. Select the Microsoft application agent download package, `msappagent192_win_x64.zip`.
  - c. Download the package to the host where you want to install the Microsoft application agent.
2. Open `msappagent192_win_x64.zip` with WinZip.

When you are prompted for a password, type the password that you received with the software license.
3. Use WinZip to unzip the `msappagent192_win_x64.zip` file.
4. In the unzipped folder, launch `emcmsappagent-19.2.0.0.exe`.

The installation wizard appears.
5. On the **Welcome Wizard** page, select **I agree to the license term and agreements**, and then click **Next**.

6. On the **Change Install Location** page, perform one of the following tasks:
  - To install the Microsoft application agent in the default folder, leave the installation location as-is.  
The default installation folder is `C:\Program Files\DPSAPPS\MSAPPAGENT`.
  - To specify a different installation location, perform the following steps:
    - a. Click **Change**.
    - b. In the dialog box that appears, specify the installation location.
    - c. Click **OK**.
7. Click **Next**.
8. On the **Configure Installation Options** page, specify any of the following installation options, as required:
  - To integrate the Microsoft application agent with PowerProtect for centralized or self-service protection of SQL Server data, select the following options, as required:
    - To install the Microsoft application agent software, select **Application Direct**.
    - To install the SQL Server Management Studio plug-in user interface, select **SSMS Plug-in**.  
You can use the SSMS plug-in to perform self-service SQL Server backup and restore operations.
    - To enable table-level restores, select **ItemPoint**.  
This option installs ItemPoint for Microsoft SQL Server, which you can use to perform table-level restores.
    - You must specify the PowerProtect appliance details by performing the following steps:
      - a. Select **PowerProtect Data Manager Integration**.
      - b. In the **Appliance Hostname or IP address** field, type the hostname or IP address of the PowerProtect server.
  - To install the VM Direct Engine to recover application-aware SQL virtual machine backups, select the following options, as required:
    - ⓘ **Note:** Installation of the Microsoft application agent requires port 7000 on SQL Server and port 8443 on PowerProtect to be open bidirectionally. These ports enable communication between the Microsoft application agent and PowerProtect.
    - Select **VM Direct Engine**.  
ⓘ **Note:** The PowerProtect appliance details are disabled when you select the **VM Direct Engine** option.
    - To install the SQL Server Management Studio plug-in user interface, select **SSMS Plug-in**.
    - To enable table-level restores, select **ItemPoint**.  
This option installs ItemPoint for Microsoft SQL Server, which you can use to perform table-level restores.

9. Click **Install >**.
10. On the **CLR assembly deployment wizard** page, perform the following steps:
  - a. Select or clear the SQL Server instances on which you want to deploy the CLR Assembly. By default, all the SQL Server instances are selected.
  - b. To deploy CLR Assembly, select one of the following authentication options:
    - **Current Windows User**
    - **Use Windows Authentication**
    - **Use Database Authentication**
  - c. In the **User name** and **Password** fields respectively, type the username and the password of the user who has the privileges to deploy the CLR Assembly.
  - d. Click **Deploy**.
  - e. Click **Install**.
  - f. After the deployment completes, click **Next**.
11. On the **Complete the Setup** page, click **Finish**.

## Upgrade the Microsoft application agent

The Microsoft application agent 19.2 does not support a direct upgrade from an earlier version if you are using an earlier version of PowerProtect Data Manager.

To upgrade to version 19.2, you must uninstall and then reinstall the Microsoft application agent.

The following sections provide instructions:

- [Uninstall the Microsoft application agent with the setup file](#) on page 48
- [Install the Microsoft application agent](#) on page 46

## Uninstall the Microsoft application agent with the setup file

### About this task

To uninstall the Microsoft application agent for SQL Server with the setup file, perform the following steps.

### Procedure

1. Launch **emcmsappagent-19.2.0.0.exe**.
2. On the **Install Modification** page, select **Remove**, and then click **Next**.
3. On the **Configure Uninstallation Options** page, click **Remove**.
4. On the **Removing the CLR assembly** page:
  - a. Select the required SQL Server instances to remove the CLR Assembly.  
By default, all the SQL Server instances are selected.
  - b. Select one of the following options to remove the CLR assembly:
    - **Use Windows Authentication**
    - **Use Database Authentication**
  - c. In the **User name** and **Password** fields, type the credentials for the user who has the privileges to remove CLR assembly.



- d. Click **Remove**.
- e. After the removal completes, click **Next**.
5. On the **Complete the Setup** page, click **Finish**.

### Results

The Microsoft application agent is uninstalled.

## Required privileges for backup and recovery of a stand-alone server

Learn about the user requirements for stand-alone backup and recovery.

### Required SQL Server roles

Assign the user the following SQL Server roles:

- sysadmin
- public

### Required Windows user permissions

Create a local or domain Windows user account and assign the following roles:

- For table-level backup and recovery, assign administrative privileges.
- For database-level backup and recovery, assign the following permissions:
  - Add the user to the "Create global objects" Windows policy
  - Assign the following permissions to the data and log folder of the database:
    - Read
    - Write
    - List folder contents

The default data and log folder is the SQL Server installation path. For example, for SQL Server 2012 the default path is `C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\`

## Required privileges for backup and recovery of an Always On availability group

Learn about the user requirements for stand-alone backup and recovery.

### Required SQL Server roles

Assign the user the following SQL Server roles:

- sysadmin
- public

### Required Windows user permissions

Create a Windows user account with one of the following configurations:

- The built-in Windows Administrator
- A domain user added to the Administrators user group
- A local user account added to the Administrators user group on each node in the cluster. The username and password must be the same on each node.

**Note:** If you are using an account that you created (an account that is not the built-in Windows Administrator), you must launch the tool where you will perform the backup or recovery with elevated permissions (run as administrator).

## Required privileges for backup and recovery of a Failover Cluster Instance or Always On Failover Cluster Instance

Learn about the user requirements for Failover Cluster Instance or Always On Failover Cluster Instance backup and recovery.

### Required SQL Server roles

Assign the user the following SQL Server roles:

- sysadmin
- public

### Required Windows user permissions

Create a Windows user account with one of the following configurations:

- The built-in Windows Administrator
- A domain user added to the Administrators user group

**i** **Note:** If you are using an account that you created (an account that is not the built-in Windows Administrator), you must launch the tool where you will perform the backup or recovery with elevated permissions (run as administrator).

## Stagger SQL discovery jobs in host scale-out environments

In the host scale-out environment, where there are large number of SQL hosts to register to PowerProtect Data Manager, consider the following methods for staggering the SQL discovery jobs.

### Kick off the installer in smaller group of hosts

If you are installing MS appAgent by script, kick off the installer in smaller groups of hosts. The discovery jobs will kick off after the agent installation; therefore, distributing the installer in smaller groups will help stagger the incoming discovery results to PowerProtect Data Manager.

### Stagger the Schedule Discovery in Inventory Sources

When you create an Inventory Sources custom group for SQL, PowerProtect Data Manager sets the default schedule to be disabled. If you choose to enable daily discovery, consider staggering this schedule at different times among different Inventory Sources.

## Manage the Microsoft application agent for SQL

You can add a new Microsoft application agent for SQL data protection, approve and reject pending agent requests, and edit and delete existing agents.

### Procedure

1. Go to **Infrastructure > Application Agents**.  
The **Application Agents** window appears.
2. Click **Add**.  
The **Add Application/FS Agent** window appears.
3. Select one of the following options:
  - **Add IP Address or CSV Filename**.  
This process is also called *Whitelisting*.

- If you select **Add IP Address**, perform the following steps:
  - a. Type the IP Address for the application agent.
  - b. Specify the date until which the application agent is pre-approved.
  - c. Click **Save**.
- If you select **CSV Filename**, perform the following steps:
  - a. Click the **Choose File** icon.
    - ⓘ **Note:** The contents of the .CSV file must be in the following format, for example:
 

```
"10.25.115.113"
"10.25.115.112"
"10.25.115.145"
```
  - b. The **Explorer** window appears.
    - a. Select the `.csv` file, and then click **Open**.  
The file displays in the **Application/FS Agents** window.
    - c. Select the date until which the application or File System agent is preapproved.
    - d. Click **Save**.
- If you have disabled `Auto whitelist`, perform the following steps:
 

The `Auto whitelist` option enabled by default. When `Auto whitelist` is enabled, all pre-approved Application Agents are automatically approved.

  - a. Select the wanted application agent.
  - b. Click one of the following options:
    - **Approve**
    - **Reject**
    - **Edit**, then make the wanted changes.
    - **Remove**
  - c. Click **Save**.

#### After you finish

For application agents, the section [Discover an application host](#) describes how to set the host credentials before you schedule a backup.

## Support for existing SQL agent backups with PowerProtect Data Manager

The Microsoft application agent provides the capability to onboard existing stand-alone deployments, including their existing backups, to PowerProtect Data Manager. Existing backups are Microsoft application agent backups that you performed before integrating the Microsoft application agent with the PowerProtect Data Manager software and before adding an asset to a PowerProtect Data Manager protection policy.

- ⓘ **Note:** You can onboard up to three previous months of existing backups.

Retention lock is not supported for discovered existing backups in PowerProtect Data Manager.

Onboarding of DD Boost-over-FC backups is not supported.

With the onboarding capability, PowerProtect provides the following centralized features:

- Visibility of both existing backups and any new self-service or PowerProtect Data Manager policy-driven backups of onboarded assets.
- Automatic configuration of target protection storage based on the PowerProtect Data Manager protection policies that are used for your database.
- All the other functionality that is provided for PowerProtect Data Manager protection policies.


When you create a protection policy, the PowerProtect Data Manager software creates a storage unit on the specified Data Domain backup host that is managed by PowerProtect Data Manager. All subsequent backups will go to this new storage unit. This implementation overrides the backup host and storage unit information that is provided in the script with the backup host and storage unit information that is provided by PowerProtect Data Manager.

## Supporting existing SQL agent backups with PowerProtect

Learn how to support existing SQL agent backups.

### Procedure

1. Upgrade the Microsoft application agent on the SQL Server host.  
[Upgrade the Microsoft application agent](#) on page 48 provides information.
2. Run the backup discovery tool, `AgentBackupDiscovery.exe`, to enable management of existing SQL agent backups with PowerProtect.  
[Use the backup discovery tool for PowerProtect Data Manager management of existing backups](#) on page 53 provides information.

 **Note:** Step 2 enables the discovery of old backup copies that the Microsoft application agent created during self-service backups with stand-alone deployments.

3. Register and approve the Microsoft application agent in PowerProtect Data Manager.  
[Manage the File System agent](#) on page 84 provides information.  
After a few minutes of approving the SQL host, all the old backup copies start to be discovered. Depending on the number of backups, the discovery and subsequent visibility of the backups in PowerProtect Data Manager can take some time. The retention time of the discovered existing backup copies will be equal to the retention time set in the protection policy plus 14 days rounded off to the next day.
4. Discover and add the credentials for the SQL application host.  
[Discover an Oracle or SQL application host](#) on page 111 provides information.
5. Create a protection policy to protect the SQL host. For onboarding assets, only a subset of databases can be onboarded. It is not mandatory for all the databases on the host to be onboarded.  
[Add a protection policy for SQL database protection](#) on page 122 provides information.

The first backup after onboarding must be a full backup:

- The first centralized backup is automatically promoted to a full backup.
- The first self-service backup is automatically performed as a full backup.

**Note:** You cannot perform a backup to a secondary Data Domain device. You can only restore from a secondary Data Domain device.

6. Perform a self-service backup of the Microsoft SQL databases. Onboarded assets can be part of either a centralized or self-service protection policy.

[Performing self-service backups of Microsoft SQL databases](#) on page 166 provides information.

## Use the backup discovery tool for PowerProtect Data Manager management of existing backups

To enable the PowerProtect Data Manager management of existing backups after you have upgraded from a previous version of Microsoft application agent, you must run the backup discovery tool, `AgentBackupDiscovery.exe`. Existing backups are Microsoft application agent backups that you performed before integrating the Microsoft application agent with the PowerProtect Data Manager software.

**NOTICE** After you run the backup discovery tool, you can continue to use the existing backup scripts to perform the Microsoft application agent backups. Ensure that all the databases backed up with a particular script are added to a single protection policy. By default, the PowerProtect Data Manager overrides the Data Domain details by using the storage unit from the protection policy. If you do not want the Data Domain details to be overridden, use the `-a "SKIP_DD_OVERRIDE=TRUE"` option in the backup scripts.

To discover the existing backups by using the backup discovery tool, perform the following steps.

1. In the Microsoft application agent installation directory, `C:\Program Files\DPSAPPS\MSAPPAGENT\bin`, run `AgentBackupDiscovery.exe` as the administrator.

The **Discovery of existing backups** dialog box appears.

**Note:** If the program does not start but displays the following message, an ongoing backup discovery process is running, as invoked by the PowerProtect Data Manager:

```
Backup discovery is in progress. Please wait for it to complete.
```

When the discovery process is complete, you can run the backup discovery tool.

2. In the Data Domain system list in the dialog box, select the appropriate Data Domain IP address or hostname, storage unit, and username for the existing backups that you want the PowerProtect Data Manager software to discover.

**Note:** Select only one storage unit at a time. After discovery is complete for the storage unit, you can run the backup discovery tool again to discover the backups of another storage unit.

3. In the **Client hostname** field, you can change the client hostname from the default local hostname as needed.

To enable the backup discovery for an AAG or FCI, you must specify the appropriate client hostname:

- If the host is part of an AAG, specify the Windows cluster name.
- If the host is part of a SQL virtual server or FCI, specify the virtual server name.

4. In the **Backup discovery time period** field, select the number of months for the time period, as the time in the past when the backups were performed. You can select 1 month, 2 months, or 3 months for the time period.

5. After you have specified the required field values, click **Generate**.

When the PowerProtect Data Manager software completes the generation of the backup metadata or breadcrumbs, the following message appears in the dialog box. Depending on the number of old backups, the generation of breadcrumbs can take some time:

```
Breadcrumbs generated successfully.
```

The retention time for the discovered backup is calculated as follows:

(Retention time set for the previously performed backup) + (PowerProtect Data Manager retention value) + (padding to midnight), where the PowerProtect Data Manager retention value for older backups is 14 days by default.

# CHAPTER 5

## Enabling the Oracle RMAN Agent

This section includes the following topics:

- [About the Oracle RMAN agent](#)..... 56
- [Review Oracle data protection and replication requirements](#)..... 56
- [Protecting a stand-alone Oracle server](#)..... 57
- [Protecting Oracle RAC environments](#)..... 57
- [Install and configure the Oracle RMAN agent](#)..... 58
- [Add or manage the Oracle application agent](#).....74
- [Supporting existing Oracle RMAN agent backups with PowerProtect Data Manager](#).....75

## About the Oracle RMAN agent

The Oracle RMAN agent enables an application administrator to protect and recover the Oracle data on the application host. PowerProtect Data Manager integrates with the Oracle RMAN agent to check and monitor backup compliance against protection policies. PowerProtect Data Manager also enables central scheduling for backups.

The Oracle RMAN agent installation is a command-line process whereby the user installs the required Oracle RMAN agent and PowerProtect Data Manager software. PowerProtect Data Manager then sets the Data Domain host, storage unit, user, and password. [Install and configure the Oracle RMAN agent](#) on page 58 provides instructions.

**Note:** PowerProtect Data Manager supports the coexistence of the Oracle RMAN agent and the File System agent on Linux.

Software compatibility information for the PowerProtect Data Manager software and application agents is provided in the eLab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.

## Review Oracle data protection and replication requirements

PowerProtect Data Manager can manage and monitor data protection and replication for Oracle assets through integration with the Oracle RMAN agent.

After installing the Oracle RMAN agent, review the following information for additional requirements before adding the Oracle RMAN agent as an asset source in PowerProtect Data Manager and discovering the agent assets.

### Prerequisites

Ensure that you meet the required prerequisites before you add an Oracle asset.

Verify that the environment meets the following requirements:

- Ensure that all clocks on both the Oracle host and PowerProtect Data Manager are time-synced to the local NTP server to ensure discovery of the backups.
- Ensure that the Oracle host and the PowerProtect Data Manager network can see and resolve each other.
- Ensure that port 7000 is open on the Oracle host.
- If you are going to register Oracle RAC nodes to PowerProtect Data Manager, set the `db_domain` parameter on every RAC node in the RAC database instance:

1. Use `sqlplus` to log in to your database.
2. Run the command: `sqlplus / as sysdba`
3. Run the command: `show parameters db_domain`

The following output is displayed:

```

NAME TYPE VALUE -----
-----
db_domain string SQL> alter system set db_domain='admdb'
scope=spfile sid='*';
System altered.
```



1. shutdown immediate;
2. startup;

## Protecting a stand-alone Oracle server

Learn how to configure protection of a stand-alone Oracle server.

### Procedure

1. Add a storage system.  
[Add protection storage](#) on page 40 provides information.
2. Install the Oracle RMAN agent on the Oracle server host.  
[Install the Oracle RMAN agent](#) on page 58 provides information.
3. Add or approve the Oracle RMAN agent in PowerProtect Data Manager.  
[Add or manage the Oracle application agent](#) on page 74 provides information.
4. Discover and add the credentials for the Oracle application host.  
[Discover an Oracle or SQL application host](#) on page 111 provides information.
5. Create a protection policy to protect the Oracle server host.  
[Add a protection policy for Oracle database protection](#) on page 125 provides information.

## Protecting Oracle RAC environments

Learn how to configure protection of Oracle RAC environments.

### About this task

You must repeat the steps to install the Oracle RMAN agent, and then add and discover the application host in PowerProtect Data Manager on each node in the Oracle RAC environment.

### Procedure

1. Add a storage system.  
[Add protection storage](#) on page 40 provides information.
2. Install the Oracle RMAN agent on each Oracle RAC node.  
[Install the Oracle RMAN agent](#) on page 58 provides information.
3. Add or approve the Oracle RMAN agent on each Oracle RAC node.  
[Add or manage the Oracle application agent](#) on page 74 provides information.
4. Discover and add the credentials for each Oracle application host.  
[Discover an Application Host](#) provides information.
5. Create a protection policy group to protect the Oracle RAC nodes.  
[Add a protection policy for Oracle database protection](#) on page 125 provides information.

# Install and configure the Oracle RMAN agent

Learn how to install and configure the Oracle RMAN agent.

## Install the Oracle RMAN agent

Learn how to install the Oracle RMAN agent on all the Linux database servers that must access the Data Domain system.

### About this task

**NOTICE** You must use the Oracle RMAN agent version 19.2 with PowerProtect Data Manager version 19.2. If a previous version of Oracle RMAN agent is installed, you must upgrade to version 19.2.

Run the `install.sh` script to install the Oracle RMAN agent 19.2 or to upgrade from an earlier version of the Oracle RMAN agent. The script installs the Oracle RMAN agent in a user-specified directory or in the default installation directory, `$HOME/opt/dpsapps/rmanagent`.

Run the `install.sh -h` or `install.sh --help` command to obtain more information about the script operation.

Complete the following steps to download the Oracle RMAN agent and perform a new installation of the software on Linux.

**Note:** In a RAC system, you must install the Oracle RMAN agent and PowerProtect Data Manager agent on each node.

### Procedure

1. In the PowerProtect Data Manager UI:
  - a. Select **Agent Downloads** from **Dashboard > System Settings**.
  - b. Select the Oracle RMAN agent download package, `ddrman192_linux_x86_64.tar`.
  - c. Download the package to the Oracle server host on Linux.
 

**Note:** As an alternative, you can download the Oracle RMAN agent package from the Support website at <https://support.emc.com>.
2. Change the ownership of the tar file to the oracle user by running the following command:

```
# chown -R oracle:oinstall ddrman192_linux_x86_64.tar
```

Uncompress the downloaded tar file using the oracle user by running the following command:

```
# tar -vxf ddrman192_linux_x86_64.tar
```

3. Ensure that no backups are running. Stop the RMAN processes before you install the Oracle RMAN agent.
4. As one of the system's Oracle users (recommended), run the `install.sh` script:

```
$ install.sh
```

5. The `install.sh` script displays the following prompt:

```
Do you want to install under the default installation directory /home/oracle/opt/dpsapps/rmanagent? (y or n)
```

Type the appropriate value:

- To install in the default directory, type `y`.
- To install in a non-default directory that already exists, type `n`.

The script then prompts you to enter the installation directory pathname:

```
Enter the full pathname of the installation destination:
```

Type the pathname of an already created installation directory.

**i** **Note:** The user-specified installation directory must be a directory that is created specifically for the Oracle RMAN agent 19.2 installation, and must not be the `ORACLE_HOME` directory. The complete directory pathname must be specified, without a slash (`/`) at the end.

The `install.sh` script displays the following output:

```
The lib directory /home/oracle/opt/dpsapps/rmanagent/lib is created.
The config directory /home/oracle/opt/dpsapps/rmanagent/config is created.
The bin directory /home/oracle/opt/dpsapps/rmanagent/bin is created.
The breadcrumbs directory /home/oracle/opt/dpsapps/rmanagent/breadcrumbs
is created.
Installing the Oracle RMAN agent.
Copying the lockbox libraries to /home/oracle/opt/dpsapps/rmanagent/lib/.
Copying libddobk.so to /home/oracle/opt/dpsapps/rmanagent/lib/.
Copying libDDBoost.so to /home/oracle/opt/dpsapps/rmanagent/lib/.
Copying ddutil to /home/oracle/opt/dpsapps/rmanagent/bin/.
Copying the dependency libraries to /home/oracle/opt/dpsapps/rmanagent/
lib/.
Copying the configuration file to /home/oracle/opt/dpsapps/rmanagent/
config/.
Copying the ddbmcon program to /home/oracle/opt/dpsapps/rmanagent/bin/.
Creating the lockbox.
Successfully installed the Oracle RMAN agent.
```

6. If `ORACLE_HOME` is set in the environment, the `install.sh` script displays the following type of prompt. Type `n`, as required for a new installation:

```
The Oracle RMAN agent library, libddobk.so, does not exist in /space/oracle/app/oracle/product/12.1.0/dbhome_1/lib.
Do you want to update settings in /space/oracle/app/oracle/product/12.1.0/dbhome_1 directory so that RMAN scripts from previous
installation can be reused? (y or n) n
```

The installation script exits.

7. To verify the installed version of Oracle RMAN agent, run the following command:

```
$ /home/oracle/opt/dpsapps/rmanagent/bin/ddutil -i
```

## Upgrade the Oracle RMAN agent

An upgrade of the Oracle RMAN agent to version 19.2 requires additional steps when the pre-19.2 Oracle RMAN agent is integrated with Enterprise Copy Data Management (eCDM). In that case, you must also upgrade the eCDM integration to a PowerProtect Data Manager integration.

### About this task

**Note:** If Oracle RMAN agent versions earlier than version 4.0 are installed, refer to the latest *PowerProtect Oracle RMAN Agent Administration Guide* for information about how to upgrade the pre-4.0 versions.

### Procedure

1. To obtain details about the Data Domain hosts and storage units that eCDM or PowerProtect has registered with the Oracle RMAN agent, run the `ddutil -s` command on the Oracle RMAN agent client host. For example:

```
ddutil -s
```

```
Data Domain Hostname: 10.36.52.98

FC Service Name: None
FC Service Enabled: false

Storage Unit: PLC-PROTECTION-1557475568457

User: PLC-PROTECTION-1557475568457
Type: PRIMARY
```

2. If the pre-19.2 Oracle RMAN agent is integrated with eCDM, perform the following steps to upgrade the eCDM software to PowerProtect Data Manager software:

- a. In the eCDM UI menu, select **Upgrade** under **System Settings**.

- b. To upload the upgrade package, click **Upload Package**.

The following message appears when the package has been uploaded:

```
Package uploaded successfully.
```

- c. To run the upgrade process, click **Perform Upgrade**.

- d. When prompted to verify the certificate details and confirm the upgrade, click **Yes**.

The following message appears when each package component has been upgraded:

```
State: UPGRADED
```

3. To stop the eCDM agent on the Oracle RMAN agent client host, run the following command:

```
/usr/local/ecdm/ecdm-agent/bin/ecdm-agent.bin stop
```

The following message appears when the eCDM agent is stopped:

```
eCDM Agent daemon control 'stop' is successful
```

4. Upgrade the Oracle RMAN agent according to the instructions in [Install the Oracle RMAN agent](#) on page 58.

For example, when you run the `install.sh` script to perform the upgrade, the following type of output appears:

```
install.sh
Do you want to install under the default installation directory /home/
oracle/opt/dpsapps/rmanagent? (y or n) y
An Oracle RMAN agent already exists. Do you want to continue the
installation? (y or n) y
Installing the Oracle RMAN agent.
Copying the lockbox libraries to /home/oracle/opt/dpsapps/rmanagent/
lib/.
Copying libddobk.so to /home/oracle/opt/dpsapps/rmanagent/lib/.
Copying libDDBoost.so to /home/oracle/opt/dpsapps/rmanagent/lib/.
Copying ddutil to /home/oracle/opt/dpsapps/rmanagent/bin/.
Copying the dependency libraries to /home/oracle/opt/dpsapps/rmanagent/
lib/.
Copying the ddbmcon program to /home/oracle/opt/dpsapps/rmanagent/bin/.
Upgrading the lockbox.
Import operation is not needed because the lockbox version is already
updated.
As a PowerProtect Data Manager user, update the existing Data Domain
details? (y or n) y
Data Domain server name: 10.36.52.98
Data Domain Storage Unit name: PLC-PROTECTION-1557475568457
Successfully updated the DD Boost credentials in the lockbox.
As a PowerProtect Data Manager user, update the existing Data Domain
details? (y or n) n
Updated the lockbox.
Successfully installed the Oracle RMAN agent.
Do you want to uninstall the previous Oracle RMAN agent in /u01/app/
oracle/product/12.1.0/dbhome_1 directory? (y or n) y
The Oracle RMAN agent is uninstalled.
Do you want to update settings in /u01/app/oracle/product/12.1.0/
dbhome_1 directory so that RMAN scripts from previous installation can
be reused? (y or n) y
Updating settings in the /u01/app/oracle/product/12.1.0/dbhome_1
directory.
Settings are updated.
Installation is completed.
```

5. If you upgraded the eCDM software to PowerProtect Data Manager software in step 2, perform the following steps to uninstall the eCDM agent and install the PowerProtect agent:

- a. To uninstall the eCDM agent, run the `rpm -e ecdm-agent-3.0.0-15_1.x86_64` command. For example:

```
rpm -e ecdm-agent-3.0.0-15_1.x86_64
Uninstalling ecdm-agent...
ecdmagent.service - eCDM Agent Service
Loaded: loaded (/etc/systemd/system/ecdmagent.service; enabled)
:
```

- b. To install the PowerProtect agent, run the `rpm -ivh adm-agent-19.x.x.rpm` command, where `x.x` is the current version. For example:

```
rpm -ivh adm-agent-19.1.0.rpm
warning: adm-agent-19.1.0.rpm: Header V3 RSA/SHA1 Signature, key ID
5301dfb7: NOKEY
Preparing... ##### [100%]
```

```

Updating / installing...
1:adm-agent-19.1.0-1_SNAPSHOT201904#####
[100%]
Installing adm-agent...
2019/05/10 14:48:56 Adding current path for configurations: /usr/
local/ecdm/ecdm-agent/bin
2019/05/10 14:48:56 nameLogfile logfile
2019/05/10 14:48:56 Flags &{ControlAction:install Unregister:false
Upgrade:false LogFile:/usr/local/ecdm/ecdm-agent/logs/admagent.log
Port:7000 AgentID: ECDMHost: ECDMPort:8443 ECDMScheme:https
AppAgentPaths:[]}
2019/05/10 14:48:57 ADM Agent daemon control 'install' is successful

Please run /usr/local/ecdm/ecdm-agent/bin/register.sh to register
this system to a Dell EMC PPDM Server.
If OS authentication is disabled for one or more Oracle databases on
the client, refer to Oracle RMAN agent Administration Guide to use
another authentication option for discovery.
    
```

6. To register the Oracle RMAN agent to the PowerProtect server, run the `register.sh` script. For example:

```

/usr/local/ecdm/ecdm-agent/bin/register.sh
2019/05/10 14:49:25 Adding current path for configurations: /usr/local/
ecdm/ecdm-agent/bin
2019/05/10 14:49:25 nameLogfile logfile
2019/05/10 14:49:25 Flags &{ControlAction:stop Unregister:false
Upgrade:false LogFile:/usr/local/ecdm/ecdm-agent/logs/admagent.log
Port:7000 AgentID: ECDMHost: ECDMPort:8443 ECDMScheme:https
AppAgentPaths:[]}
2019/05/10 14:49:25 ADM Agent daemon control 'stop' is successful
Enter PowerProtect Data Manager IP/Hostname: blrv136h018.lss.emc.com
Enter App Agent Home (press enter for default home /home/oracle/opt/
dpsapps/rmanagent):
unregister host
2019/05/10 14:49:35 Adding current path for configurations: /usr/local/
ecdm/ecdm-agent/bin
:
Do you want to set the default retention time for automatic retention
management by PowerProtect of existing backups? (y or n) y
Provide default retention time in number of days: 2
Allow SYSDBA access for RMAN agent? (y or n) y
2019/05/10 14:49:45 Adding current path for configurations: /usr/local/
ecdm/ecdm-agent/bin
2019/05/10 14:49:45 nameLogfile logfile
2019/05/10 14:49:45 Flags &{ControlAction:start Unregister:false
Upgrade:false LogFile:/usr/local/ecdm/ecdm-agent/logs/admagent.log
Port:7000 AgentID: ECDMHost:blrv136h018.lss.emc.com ECDMPort:8443
ECDMScheme:https AppAgentPaths:[/home/oracle/opt/dpsapps/rmanagent]}
2019/05/10 14:49:45 ADM Agent daemon control 'start' is successful
    
```

7. To complete the upgrade, manually approve the Oracle RMAN agent from the PowerProtect Data Manager server. [Manage the File System agent](#) on page 84 provides information.

## Uninstall the Oracle RMAN agent

Run the `uninstall.sh` script to uninstall the Oracle RMAN agent 19.2. You can also run the script to uninstall a previous version of the Oracle RMAN agent.

### About this task

Run the `uninstall.sh -h` or `uninstall.sh --help` command to obtain more information about the script operation.

You can run the `uninstall.sh` script manually or automatically. To enable the automatic operation, you must set the appropriate environment variables as listed in [Table 19](#) on page 63:

- When the variables are not set, the script runs manually and prompts for the required values.
- When the variables are set, the script runs automatically and performs the uninstallation according to the environment variable settings.

**Table 19** Environment variables for uninstallation of Oracle RMAN agent

Environment variable	Description	Default and valid values
<code>RMAN_AGENT_HOME</code>	Specifies the installation directory for the Oracle RMAN agent.	<ul style="list-style-type: none"> <li>• <code>/home/oracle1/opt/dpsapps/rmanagent</code> (default).</li> <li>• Valid complete pathname of the directory for installation of Oracle RMAN agent.</li> </ul> <p><b>Note:</b> The directory pathname must not end with a slash (<code>/</code>).</p>
<code>RMAN_AGENT_UNINSTALL_OPTIONS</code>	Specifies the software components to uninstall.	<ul style="list-style-type: none"> <li>• Undefined (default).</li> <li>• <code>NONE</code> or <code>none</code>—Specifies to keep the Oracle RMAN agent software, and not perform the uninstallation.</li> <li>• <code>BINARY</code> or <code>binary</code>—Specifies to uninstall the software, but not the lockbox or the configuration file.</li> <li>• <code>FULL</code> or <code>full</code>—Specifies to uninstall the software, lockbox, and configuration file.</li> </ul>

**Note:** It is not necessary to uninstall the Oracle RMAN agent for an upgrade. An existing Oracle RMAN agent is overwritten during an upgrade.

Perform the following steps to uninstall the Oracle RMAN agent.

#### Procedure

1. Ensure that backup and restore operations are not in progress when you uninstall the Oracle RMAN agent.
2. If you want the uninstallation script to run automatically, ensure that `RMAN_AGENT_HOME` and `RMAN_AGENT_UNINSTALL_OPTIONS` are set as described in [Table 19](#) on page 63.

To verify the value of an environment variable, run the `echo` command. For example:

```
# echo $RMAN_AGENT_HOME
```

```
/home/oracle/opt/dpsapps/rmanagent
```

To set an environment variable, run the `export` command. For example:

```
# export RMAN_AGENT_HOME=/opt/dpsapps/rmanagent
```

3. As an Oracle user, run the `uninstall.sh` script:

**Note:** It is recommended that you set the `RMAN_AGENT_HOME` environment variable before you run the `uninstall.sh` script.

```
# ./uninstall.sh
```

4. If the script does not run automatically, type the appropriate values at the prompts:
  - a. When prompted, specify whether you want to enter the directory pathname of the Oracle RMAN agent installation:

```
An installation directory pathname is not specified. Do you want to
enter the installation pathname? (y or n)
```

If you type `y`, then the script prompts for the installation location. Type the complete pathname of the installation location, without a slash (`/`) at the end.

- b. When prompted, specify whether you want the lockbox and configuration file to be removed:

```
Do you want to remove the lockbox and the configuration file? (y or n)
```

- c. If the script detects an additional installation of Oracle RMAN agent, the script prompts whether to uninstall that version. You can specify to keep or uninstall the software.

The script removes the Oracle RMAN agent software and prints the following message:

```
The Oracle RMAN agent is uninstalled from the /home/oracle/opt/dpsapps/
rmanagent directory.
Uninstallation is completed.
```

## Integration with PowerProtect Data Manager software

This procedure enables the integration of Oracle RMAN agent with PowerProtect Data Manager, which enables PowerProtect Data Manager to monitor, manage, and analyze the Oracle RMAN agent backups on Linux.

### **NOTICE**

PowerProtect Data Manager can create and manage replication copies based on the protection policies.

PowerProtect Data Manager performs these operations whether the backup is created by the DBA or by the PowerProtect Data Manager centralized backup scheduler.

Because PowerProtect Data Manager controls the replication, when the Oracle RMAN agent is deployed with PowerProtect Data Manager, the following self-service replication operations are disabled:

- Creation of multiple backup copies with the `RMAN BACKUP COPIES` command.
- MTree replication to create backup copies on a secondary Data Domain system.

You can restore from replicated copies of backups that were performed with a previous version of Oracle RMAN agent.



When you perform a self-service backup managed by PowerProtect Data Manager, the PowerProtect Data Manager protection policy settings for the given database will override the target protection storage settings specified in the RMAN backup script, including the Data Domain server hostname and storage unit name.

1. Install and register the required PowerProtect Data Manager application data management (ADM) agent on the Oracle RMAN agent host as described in [Install the PowerProtect Data Manager agent](#) on page 65.
2. Enable the `ddbmcon` program to connect to the local Oracle databases during PowerProtect Data Manager operations. [How the Oracle RMAN agent communicates with PowerProtect Data Manager](#) on page 67 provides details.
3. Verify the connectivity from the `ddbmcon` program to the Oracle database by using the `ddutil` program with the required options. [Verify the connectivity from ddbmcon](#) on page 71 provides details.
4. Ensure that the `/etc/oratab` file contains a complete list of all the Oracle SIDs on the host. The Oracle RMAN agent uses the information in the file to discover the database resources on the system, which enables the PowerProtect Data Manager operations.

In an Oracle RAC environment, ensure that the `/etc/oratab` file contains an entry for each database instance. Manually add any database instance entries that do not yet exist in the file. Each entry must have the following format:

```
<ORACLE_SID>:<ORACLE_HOME>:<N|Y>
```

**Note:** Only with Oracle RAC 12.2 or later, each entry can have the following format:

```
<DATABASE_UNIQUE_NAME>:<ORACLE_HOME>:<N|Y>
```

As recommended by Oracle, ensure that all the archived redo logs in the Oracle RAC environment reside on shared storage or a shared cluster file system that is accessible from all the RAC nodes. Select one node to be the backup node and set the `IS_RAC_BACKUP_NODE` parameter accordingly, as described in [Configuration file requirements for connection to local databases](#) on page 68.

## Install the PowerProtect Data Manager agent

You must install the PowerProtect Data Manager agent as the root user on the Oracle RMAN host so that the Oracle RMAN agent can communicate with the PowerProtect Data Manager server.

### About this task

**Note:** In a RAC system, you must install the Oracle RMAN agent and PowerProtect Data Manager agent on each node.

### Procedure

1. Log in as the root user on the Oracle RMAN host.
2. To install the PowerProtect Data Manager agent, run the following command:

```
rpm -ivh adm-agent-19.2.0.rpm
```

```
warning: adm-agent-19.2.0.rpm: Header V3 RSA/SHA1 Signature, key ID
5301dfb7: NOKEY
Preparing... ##### [100%]
```

```

Updating / installing...
1:admagent-19.2.0-1_SNAPSHOT201904##### [100%]
Installing adm-agent...
2019/05/10 14:48:56 Adding current path for configurations: /usr/local/
ecdm/ecdm-agent/bin
2019/05/10 14:48:56 nameLogfile logfile
2019/05/10 14:48:56 Flags &{ControlAction:install Unregister:false
Upgrade:false LogFile:/usr/local/ecdm/ecdmagent/logs/admagent.log
Port:7000 AgentID: ECDMHost:ECDMPort:8443 ECDMScheme:https AppAgentPaths:
[]}
2019/05/10 14:48:57 ADM Agent daemon control 'install' is successful
Please run /usr/local/ecdm/ecdm-agent/bin/register.sh to register this
system to a Dell EMC PPDM Server.
If OS authentication is disabled for one or more Oracle databases on the
client, refer to Oracle RMAN Agent Administration Guide to use another
authentication option for discovery.
    
```

The adm-agent-19.2.0.rpm file is installed in the /usr/local/ecdm/ecdm-agent directory.

3. To register the Oracle RMAN agent with the PowerProtect Data Manager server, run the register.sh script:

```
/usr/local/ecdm/ecdm-agent/bin/register.sh
```

```

2019/05/10 14:49:25 Adding current path for configurations: /usr/local/
ecdm/ecdm-agent/bin
2019/05/10 14:49:25 nameLogfile logfile
2019/05/10 14:49:25 Flags &{ControlAction:stop
Unregister:false Upgrade:false LogFile:/usr/local/ecdm/ecdmagent/
logs/admagent.log Port:7000 AgentID: ECDMHost:
ECDMPort:8443 ECDMScheme:https AppAgentPaths:[]}
2019/05/10 14:49:25 ADM Agent daemon control 'stop' is successful
    
```

- a. When prompted by the register.sh script, type the hostname or IP address of the PowerProtect Data Manager home:

```
Enter PowerProtect Data Manager IP/Hostname:
```

```
Enabling the Oracle RMAN application agent blrv136h018.lss.emc.com
```

- b. When prompted, type the location of the Oracle RMAN agent installation:

```
Enter App Agent Home (press enter for default home /home/oracle/opt/
dpsapps/rmanagent):
```

- c. When prompted, you can set the retention time as the number of days that the PowerProtect Data Manager will retain any backups that already exist on the system:

```
Do you want to set the default retention time for automatic retention
management by PowerProtect of existing backups? (y or n) y
Provide default retention time in number of days: 1
```

- d. When prompted, specify whether Oracle OS authentication will use the SYDBDA role when connecting to Oracle. If you type n, then OS authentication will use the SYSBACKUP role:

```
Allow SYSDBA access for RMAN agent? (y or n) y
```

The script completes by starting the daemon that connects to PowerProtect Data Manager:

```
2019/05/10 14:49:45 ADM Agent daemon control 'start' is successful
```

## Uninstall the PowerProtect Data Manager agent

You must uninstall the PowerProtect Data Manager agent as the root user on the Oracle RMAN host.

### Procedure

1. Log in as the root user on the Oracle RMAN host.
2. Query the Oracle client for an installed adm agent by running the following command:

```
# rpm -qa | grep adm*
```

```
adm-agent-19.2.0-1_SNAPSHOT20190530071531.x86_64
```

3. If the adm agent exists on the Oracle client, uninstall the adm agent by running the following command:

```
# rpm -e adm-agent-19.2.0-1_SNAPSHOT20190530071531.x86_64
```

## How the Oracle RMAN agent communicates with PowerProtect Data Manager

The Oracle RMAN agent program `ddbmcon` handles all communication between the Oracle RMAN agent and PowerProtect Data Manager.

**Note:** You cannot run the `ddbmcon` program manually. The program is only run by the PowerProtect Data Manager agent.

When the `ddbmcon` program performs discovery, backup, or deletion operations, it connects to the Oracle database. The following authentication methods are supported:

1. Database authentication—The `ddbmcon` program first tries to connect to the Oracle database instance by using database authentication. The program tries to use the database administrator username and password to connect to the database instance.
2. Oracle wallet authentication—If database authentication fails or is not enabled, the `ddbmcon` program tries to connect by using Oracle wallet authentication. The program tries to use the parameter settings from the configuration file to connect to the database instance.
3. Operating system authentication—If Oracle wallet authentication also fails or is not enabled, the `ddbmcon` program tries to connect by using operating system authentication. The program tries to change the real process user ID to the Oracle installation user ID, to connect to the database instance.

The `ddbmcon` program tries all these authentication methods for each Oracle database instance. The program reports a connection error if it cannot connect to the database instance by using any of these methods. If one of these methods succeeds, the `ddbmcon` program ignores the other authentication methods and proceeds to retrieve the information as used by the PowerProtect Data Manager.

Ensure that you enable one of these three authentication methods for the `ddbmcon` program. For maximum ease of use, it is recommended that you enable the operating system authentication

method. Both the database and Oracle wallet authentication methods require additional configuration steps on the Oracle host and parameter settings in the configuration file `rman_agent.cfg`.

### Configuration file requirements for connection to local databases

As required for certain `ddbmcon` program operations, you must complete the required configuration settings to enable the authentication method that you want the program to use. Each authentication method has its own requirements for parameter settings in the configuration file.

During the Oracle RMAN agent installation, the configuration file template, `rman_agent.cfg`, is installed in the `$RMAN_AGENT_HOME/config` directory. To enable a particular authentication method, you must set the required parameters in the `rman_agent.cfg` configuration file.

The configuration file template includes the following information.

```


#####
#
# rman_agent.cfg
#
# All rights reserved.
#
# Oracle RMAN agent 19.2
#
# This template is designed to help users to configure the authentication of
# RMAN agent. Check the product administration guide for a complete list of
# all the supported parameters and rules for editing the configuration file.
#
# Make a copy of this file before making any modifications.
# To enable a parameter, uncomment or add the parameter in the file and
# specify its value.
#
#####
#
#####
# Oracle parameters.
# There can be repetitive sections of Oracle parameters. The Oracle database
# the parameters belong to is described in the section name: SID_name. The
# name here must be replaced by the SID of the database.
# #####
[SID_name]
# ORACLE_SERVICE =
# ORACLE_USER =
# ORACLE_OS_USER =
# TNS_ADMIN =
# RMAN_CATALOG_SERVICE =
# RMAN_CATALOG_USER =
# IS_RAC_BACKUP_NODE =

```

To set a particular parameter in the configuration file, such as `ORACLE_SERVICE`, remove the `#` symbol at the start of the parameter line and add the parameter value after the equal sign (=).

You can complete the following settings in the configuration file:

- `SID_name` is mandatory for each authentication method when you set any parameters in the file for a particular system ID (SID). `[SID_name]` (for example, `[SID_orcl]`) must appear on a separate line before all the parameter settings for the SID:
  - For Oracle 10g, 11g, and non-RAC systems, `SID_name` must match the SID in the `/etc/oratab` file.
  - For Oracle 12c RAC systems, `SID_name` must match the SID that runs on the local host.

 **Note:** Each Oracle SID on the same system requires its own entries in the configuration file. You must use the same configuration file for all the Oracle SIDs.

- `ORACLE_SERVICE` is mandatory for database authentication and Oracle wallet authentication. Specifies the TNS or Net service name of the Oracle database.
- `ORACLE_USER` is mandatory for database authentication only. Specifies the database username as saved in the lockbox.
- `ORACLE_OS_USER` is mandatory for operating system authentication when the username for connection is different than the `ORACLE_OSDBA_USER` username. Specifies the operating system user that will connect to the Oracle database for operating system authentication. When this parameter is set, `ORACLE_OSDBA_USER` is ignored.
- `TNS_ADMIN` is mandatory for database authentication and Oracle wallet authentication when the Oracle Net configuration files including `tnsnames.ora` reside in a non-default directory. Specifies the pathname of the non-default directory. When this parameter is not set, the system default directory `$ORACLE_HOME/network` is used.
- `RMAN_CATALOG_SERVICE` is mandatory when an RMAN catalog is used for backup or recovery of the database. Specifies the TNS name of the RMAN catalog.
- `RMAN_CATALOG_USER` is mandatory for each authentication method when an RMAN catalog is used. Specifies the catalog database username as saved in the lockbox.
- `IS_RAC_BACKUP_NODE` is highly recommended in an Oracle RAC environment only. In the Oracle RAC environment, select a single node to be the backup node and set this parameter to `TRUE` to specify that the `SID_name` node is the backup node. Set this parameter to `FALSE` when the `SID_name` node is not the backup node.

The following topics provide more details about the configuration requirements of each particular authentication method.

## Authentication requirements

The following subtopics provide details about the three authentication methods that the `ddbmcon` program supports.

### Database authentication requirements

Before the `ddbmcon` program can use database authentication to connect to an Oracle database, you must complete the required configuration to enable the database authentication method. Database authentication can be used to connect to a target database or catalog database.

To enable the database authentication method, run the `ddutil` command with the appropriate options to store the database administrator credentials in the lockbox:

```
ddutil -C -a USER_TYPE=DATABASE_ADMIN [-a DATABASE_SIDS=<database_SIDs>] [-a
USERNAME=<administrator_username>]
```

**Note:** If the lockbox does not exist when you run the `ddutil` command, the command creates the lockbox in the default directory.

The options `-C` and `-a USER_TYPE=DATABASE_ADMIN` are mandatory. If you do not specify the other `-a` options, `-a DATABASE_SIDS=<database_SIDs>` and `-a USERNAME=<administrator_username>`, the command prompts for the database SIDs and administrator username. The command always prompts for the administrator password.

If multiple databases exist on the system and all use the same administrator username and password, you can add the credentials for all the databases to the lockbox with the same `ddutil` command. You must specify the database SIDs as a comma-separated list. For example:

```
ddutil -C -a USER_TYPE=DATABASE_ADMIN
```

```
'RMAN_AGENT_HOME' is retrieved from ddutil runtime location as '/home/oracle/opt/dpsapps/rmanagent'
Database SIDs (to a maximum of 19 SIDs):
orcl1,orcl2,orcl3,orcl4,orcl5,db1,db2
Database administrator name: SYS
Password: xxxxxx
Re-enter password: xxxxxx
Successfully set the Oracle database administrator credentials in the lockbox.
Enabling the Oracle RMAN application agent.
```

The following example command includes all the supported `-a` options:

```
ddutil -C -a USER_TYPE=DATABASE_ADMIN -a
DATABASE_SIDS=orcl1,orcl2,orcl3,orcl4,orcl5,db1,db2 -a USERNAME=SYS
```

```
'RMAN_AGENT_HOME' is retrieved from ddutil runtime location as '/home/oracle/opt/dpsapps/rmanagent'
Password: xxxxxx
Re-enter password: xxxxxx
Successfully set the Oracle database administrator credentials in the lockbox.
```

To enable the database authentication method, you must also set the following parameters for each required SID in the `rman_agent.cfg` configuration file:

- Set `ORACLE_SERVICE` and `ORACLE_USER`. `ORACLE_USER` must match the username that is saved in the lockbox.
- If the Oracle Net configuration files reside in a non-default directory, set `TNS_ADMIN` to the directory pathname.
- If an RMAN catalog is used, set `RMAN_CATALOG_SERVICE` and `RMAN_CATALOG_USER`.

For example, the `rman_agent.cfg` configuration file includes the following settings to enable the database authentication for the database SID `orcl`:

```
[SID_orcl]
ORACLE_SERVICE = DBFS
ORACLE_USER = ORACLE1
TNS_ADMIN = /home/oracle/wallet
```

To confirm that database authentication is enabled, you can log in as the root user and run the `ddutil` commands as described in [Verify the connectivity from ddbmcon](#) on page 71.

## Oracle wallet authentication requirements

Before the `ddbmcon` program can use Oracle wallet authentication to connect to an Oracle database, you must complete the required configuration to enable the Oracle wallet authentication method. Oracle wallet authentication can be used to connect to a target database or catalog database.

To enable the Oracle wallet authentication method, you must set the following parameters for each required SID in the `rman_agent.cfg` configuration file:

- Set `ORACLE_SERVICE` to the TNS or Net service name. For example, set the parameter to the value `DBFS`.
- If the Oracle Net configuration files reside in a non-default directory, set `TNS_ADMIN` to the directory pathname.
- If an RMAN catalog is used, set `RMAN_CATALOG_SERVICE` and `RMAN_CATALOG_USER`.

For example, the `rman_agent.cfg` configuration file includes the following settings to enable the Oracle wallet authentication for the database SID `orcl`:

```
[SID_orcl]
ORACLE_SERVICE = DBFS
TNS_ADMIN = /home/oracle/<alternate_TNS_location>
```

To confirm that Oracle wallet authentication is enabled, you can log in as the root user and run the `ddutil` commands as described in [Verify the connectivity from ddbmcon](#) on page 71.

## Operating system authentication requirements

The operating system authentication method can only be used on systems with a single Oracle home or with multiple Oracle homes that were all installed by the same user. During authentication, the `ddbmcon` program either obtains the Oracle installation user ID or reads the operating system username from the `rman_agent.cfg` configuration file. Then the program changes the real user of the process to the Oracle installation user or the operating system user, to connect to the database instance.

**Note:** The operating system user specified in the configuration file takes precedence over the Oracle installation user.

When the `ddbmcon` program uses the authentication method on a system with multiple Oracle homes that were installed by different users, the program returns information for only one Oracle home. The program returns a connection error for the other Oracle homes.

During the backup discovery, the `ddbmcon` program tries to use the operating system authentication method only after the database authentication and Oracle wallet authentication methods have both failed to connect to the Oracle database.

To enable the operating system authentication method, you must set the following parameters for each required SID in the `rman_agent.cfg` configuration file:

- If the username to be used for the connection is different than `ORACLE_OSDBA_USER`, set `ORACLE_OS_USER`.
- If an RMAN catalog is used, set `RMAN_CATALOG_SERVICE` and `RMAN_CATALOG_USER`.

For example, the `rman_agent.cfg` configuration file includes the following settings to enable the operating system authentication for the database SID `orcl`:

```
[SID_orcl]
ORACLE_OS_USER = ORACLE1
```

To confirm that operating system authentication is enabled, you can log in as the root user and run the `ddutil` commands as described in [Verify the connectivity from ddbmcon](#) on page 71.

## Verify the connectivity from ddbmcon

You can run the `ddutil` command as the root user with the appropriate `-v` option to verify the connectivity from the `ddbmcon` program to the Oracle database.

The following subtopics describe the three supported levels of verification with the `ddutil -v` command:

- Host verification
- Instance verification
- RMAN verification

### Host verification

To perform the host verification, run the `ddutil -v host` command as the root user.

The `ddutil -v host` command output includes the Oracle instances found on the system and basic information about each Oracle instance.

For example, the following `ddutil -v host` command lists one Oracle instance and the authentication method as database authentication:

```
ddutil -v host
```

```
'RMAN_AGENT_HOME' is retrieved from ddutil runtime location as '/opt/dpsapps/
rmanagent'.
The ORACLE_HOME environment variable could not be retrieved.
Reported application instance:
  Version: 11.2.0.1.0
  Install location: /home/oracer/app/oracer/oracle/product/11.2.0/db_1
  Database identifier: 1040017416
  Oracle SID: CER
  Authentication type: Oracle database user
```

### Instance verification

To perform the instance verification, run the `ddutil -v inst` command as the root user. The command tests the OCI connection to the database, and provides similar output to the host verification command. In addition, the output lists the database objects that are discovered. You can use the command to determine if the `ddbmcon` program has the required read access for the database objects.

For example, the following `ddutil -v inst` command lists one Oracle instance and the database objects. The authentication method is listed as database authentication:

```
ddutil -v inst
```

```
'RMAN_AGENT_HOME' is retrieved from ddutil runtime location as '/opt/dpsapps/
rmanagent'.
The ORACLE_HOME environment variable could not be retrieved.
Reported application instance:
  Version: 11.2.0.1.0
  Install location: /home/oracer/app/oracer/oracle/product/11.2.0/db_1
  Database identifier: 1040017416
  Oracle SID: CER
  Authentication type authentication: Oracle database user

Application instance detailed information:
  Database name : CER
    Database object : SYSTEM
    Database object : SYSAUX
    Database object : PSAPUNDO
    Database object : PSAPCER
    Database object : CATBS
```



## RMAN verification

To perform the RMAN verification, run the `ddutil -v rman` command as the root user. This verification is required only if you use an RMAN catalog. Database authentication or Oracle wallet authentication can be used to connect to an RMAN catalog. (Operating system authentication cannot be used with the RMAN catalog.)

The `ddutil -v rman` command tests whether the `ddbmcon` program can connect to the target database and catalog database through an RMAN script, as required to perform an active deletion of Oracle backups.

**Note:** To enable an active deletion through RMAN, the Data Domain credential must be stored in the lockbox.

The `ddutil -v rman` command displays the following three sections of output for the RMAN verification:

### 1. Target database connection information:

- Authentication type, listed as operating system user, Oracle database user, or Oracle wallet user.
- For operating system authentication, only the operating system user is listed.
- For database authentication, the operating system user, Oracle service, and database user are listed.
- For Oracle wallet authentication, the Oracle service and `TNS_ADMIN` value are listed.

### 2. Catalog database connection information:

- Authentication method, listed as Oracle database user or Oracle wallet user.
- For database authentication, the database service and database user are listed.
- For Oracle wallet authentication, the Oracle service and `TNS_ADMIN` value are listed.

### 3. Output of the RMAN script, which shows the connection information and any error messages.

For example, the following `ddutil -v rman` command displays the three sections of output, showing that the database authentication method is used for both the target database and catalog database:

```
ddutil -v rman
```

```
'RMAN_AGENT_HOME' is retrieved from ddutil runtime location as '/opt/dpsapps/
rmanagent'.
The ORACLE_HOME environment variable could not be retrieved.
Reported RMAN instance connection:
  Oracle SID: CER

  Target database authentication: Oracle database user
  Oracle OS dba user: oracer
  Oracle service: CER
  Oracle database user: system

  RMAN catalog authentication: Oracle database user
  Catalog database service: SAP.world
  Catalog database user: catowner

  RMAN output:

Recovery Manager: Release 11.2.0.1.0 - Production on Fri Dec 15 14:30:15 2017
Copyright (c) 1982, 2009, Oracle and/or its affiliates. All rights reserved.
RMAN> connect *****
2>
3> connect *****
```

```

4>
5>
connected to target database: CER (DBID=1040017416)
connected to recovery catalog database
Recovery Manager complete

```

## Discover the storage units

When a PowerProtect Data Manager protection policy is created, the PowerProtect Data Manager server assigns its storage unit to the Oracle databases that are protected by the protection policy. Both the manual backups and scheduled backups of these Oracle databases are sent to this storage unit.

To display the storage units and their assigned databases on the Oracle RMAN agent host, run the `ddutil -s` command.

**Note:** The `ddutil -s` command might display a storage unit type of "secondary." However, you cannot perform a backup to a secondary device. You can only restore from a secondary device.

For example:

```
ddutil -s
```

```

Data Domain Hostname: 10.36.52.98

FC Service Name: None
FC Service Enabled: false

Storage Unit: RMAN87-SS-CT-blrv35a029-a7bc3
User: RMAN87-SS-CT-blrv35a029-a7bc3
Type: PRIMARY

Storage Unit: RMAN87-SS-CT-blrv35b179-c9de5
User: RMAN87-SS-CT-blrv35b179-c9de5
Type: PRIMARY

```

## Add or manage the Oracle application agent

You can add a new Oracle application agent, approve and reject pending agent requests, and edit and delete existing agents.

### Procedure

1. Go to **Infrastructure > Application Agents**.  
The **Application Agents** window appears.
2. Click **Add**.  
The **Add Application/FS Agent** window appears.
3. Select one of the following options:
  - **Add IP Address or CSV Filename**.  
This process is also called *Whitelisting*.
    - If you select **Add IP Address**, perform the following steps:
      - a. Type the IP Address for the application agent.

- b. Specify the date until which the application agent is pre-approved.
  - c. Click **Save**.
- If you select **CSV Filename**, perform the following steps:
    - a. Click the **Choose File** icon.
 

**Note:** The contents of the .CSV file must be in the following format, for example:

```
"10.25.115.113"
"10.25.115.112"
"10.25.115.145"
```
    - The **Explorer** window appears.
    - b. Select the `.csv` file, and then click **Open**.  
The file displays in the **Application/FS Agents** window.
    - c. Select the date until which the application or File System agent is preapproved.
    - d. Click **Save**.
  - If you have disabled `Auto whitelist`, perform the following steps:  
The `Auto whitelist` option enabled by default. When `Auto whitelist` is enabled, all pre-approved Application Agents are automatically approved.
    - a. Select the wanted application agent.
    - b. Click one of the following options:
      - **Approve**
      - **Reject**
      - **Edit**, then make the wanted changes.
      - **Remove**
    - c. Click **Save**.

#### After you finish

For application agents, the section [Discover an application host](#) describes how to set the host credentials before you schedule a backup.

## Supporting existing Oracle RMAN agent backups with PowerProtect Data Manager

The Oracle RMAN agent 19.1 introduced the capability to onboard existing stand-alone deployments, including their existing backups, to PowerProtect Data Manager. Existing backups are Oracle RMAN agent backups that you performed before you have integrated the Oracle RMAN agent with the PowerProtect Data Manager software and added an asset to a PowerProtect Data Manager protection policy.

- Note:** Retention lock is not supported for discovered existing backups in PowerProtect Data Manager.
- Onboarding of DD Boost-over-FC backups is not supported.

With the onboarding capability, PowerProtect Data Manager provides the following centralized features:

- Visibility of both existing backups and any new self-service or PowerProtect Data Manager policy-driven backups of onboarded assets.
- Retention management of all backups. The retention time of existing backups can be set during the PowerProtect Data Manager registration.
- Automatic configuration of target protection storage based on the PowerProtect Data Manager protection policies that are used for your database.
- All the other functionality that is provided for PowerProtect Data Manager protection policies.


### Self-service operations use the Data Domain backup host and storage unit managed by PowerProtect Data Manager

With Oracle RMAN agent 19.1 or later, you can provide the Data Domain backup host and storage unit in the RMAN scripts. After you use PowerProtect Data Manager to add an asset to the protection policy, you might want to keep using the existing RMAN scripts instead of or along with scheduling backups through PowerProtect Data Manager.

When you create a protection policy, the PowerProtect Data Manager software creates a storage unit on the specified Data Domain backup host that is managed by PowerProtect Data Manager. All subsequent backups will go to this new storage unit. This implementation overrides the backup host and storage unit information that is provided in the script with the backup host and storage unit information that is provided by PowerProtect Data Manager.

### Setting and reporting the retention time for existing backups

With Oracle RMAN Agent 19.1 or later, any backups that are performed before you add an asset to a PowerProtect Data Manager protection policy are considered existing backups. You can set the retention time for existing backups during registration with the PowerProtect Data Manager server by using the `register.sh` script. This retention time is reported to PowerProtect Data Manager during backup discovery.

 **Note:** If a retention time is not specified for existing backups, the backup copies in PowerProtect Data Manager will never expire.

## Support existing Oracle RMAN agent backups with PowerProtect Data Manager

Learn how to support existing Oracle RMAN agent backups.

### Procedure


1. Upgrade the Oracle RMAN agent on the Oracle server host.  
[Upgrade the Oracle RMAN agent](#) on page 60 provides information.
2. Register and approve the Oracle RMAN agent in PowerProtect Data Manager.  
[Manage the File System agent](#) on page 84 provides information.

After a few minutes of approving the Oracle agent, all the old backup copies start to be discovered. Depending on the number of backups, the discovery and subsequent visibility of the backups in PowerProtect Data Manager can take some time. The retention time of the discovered existing backup copies will be equal to the retention time set in the protection policy plus 14 days and 1 day.

3. Discover and add the credentials for the Oracle RMAN agent host.  
[Discover an Oracle or SQL application host](#) on page 111 provides information.
4. Create a protection policy to protect the Oracle RMAN agent host.  
[Add a protection policy for Oracle database protection](#) on page 125 provides information.

The first backup after onboarding must be a full backup:

- The first centralized backup is automatically promoted to a full backup.
- For the first self-service backup after onboarding, the Oracle DBA must run a full backup script.

 **Note:** You cannot perform a backup to a secondary Data Domain device. You can only restore from a secondary Data Domain device.

5. Perform a self-service Application Direct backup of Oracle databases. Onboarded assets can be part of either a centralized or self-service protection policy.

[Performing self-service backups of Oracle databases](#) on page 166 provides information.



# CHAPTER 6

## Enabling the File System Agent

This section includes the following topics:

- [About the File System agent](#)..... 80
- [File System agent prerequisites](#)..... 80
- [Roadmap for protection with the File System agent](#)..... 81
- [Installing and configuring File System agent](#)..... 82
- [Manage the File System agent](#)..... 84

## About the File System agent

The File System agent enables an application administrator to protect and recover data on the file system host. PowerProtect Data Manager integrates with the File System agent to check and monitor backup compliance against protection policies. PowerProtect Data Manager also enables central scheduling for backups.

You can install the File System agent on the host that you plan to protect by using the installation wizard. [Installing and configuring File System agent](#) on page 82 provides instructions.

**Note:** PowerProtect Data Manager supports the co-existence of agents on the same Windows or Linux host for the following:

- Microsoft SQL agent and the File System agent on Windows.
- Oracle/RMAN agent and the File System agent on Linux.

Software compatibility information for the PowerProtect Data Manager software and the File System agent is provided in the eLab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.

## File System agent prerequisites

Review the following prerequisites before installing and enabling the File System agent in PowerProtect Data Manager and discovering the File System assets.

### Windows and Linux prerequisites

- Both the PowerProtect Data Manager server software and the File System agent have to be the same version. For example, using a 19.1 version File System agent with PowerProtect Data Manager version 19.2 is not supported.
- Ensure that your host is a 64-bit system. PowerProtect Data Manager supports only 64-bit hosts.
- Ensure that your host is a supported operating system version. Software compatibility information for the PowerProtect Data Manager software is provided in the eLab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.
- Ensure that all clocks on both the host and PowerProtect Data Manager are time-synced to the local NTP server to ensure discovery of the backups.
- Ensure that the host and the PowerProtect Data Manager network can see and resolve each other.
- Note that LVM/VxVM partitions/volumes are supported, but not physical partitions.
- Each volume group on LVM2 or VxVM must have at least 10% free space for a block based backup to succeed.
- Review the limitations in the section [File System agent limitations](#) on page 216.

### Linux File System prerequisites

- Ensure that the File System has the `/etc/fstab` entry. Without the `/etc/fstab` entry, discovery fails.
- If you plan to perform file level restores on SuSE Linux (SLES) versions 11 SP1, SP2, or SP3, complete the following:
  1. Log in to the system you are restoring from as `root`.



2. In a command prompt, type `yast2 iscsi-client .`
  3. For **Service Start**, choose **Manually**, and then click **OK**.
- Install the `lsb_release` package:

1. Mount the ISO:

```
[root@RHEL73-224-16 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 30G 0 disk
├─sda1 8:1 0 1G 0 part /boot
├─sda2 8:2 0 14G 0 part
├─rhel-root 253:0 0 12.5G 0 lvm /
├─rhel-swap 253:1 0 1.5G 0 lvm [SWAP]
sdb 8:16 0 30G 0 disk
├─VG1-LV1 253:2 0 2G 0 lvm /volume1_ext3
sr0 11:0 1 3.5G 0 rom /run/media/root/RHEL-7.3 Server.x86_64
[root@RHEL73-224-16 ~]#
```

2. Add the Local REPO:

```
[root@RHEL75-224-18 ~]# cat /etc/yum.repos.d/local.repo
[local]
name=local
baseurl=file:///run/media/root/RHEL-7.3\ Server.x86_64
enabled=1
gpgcheck=1
gpgkey=file:///run/media/root/RHEL-7.3\ Server.x86_64/RPM-GPG-KEY-
redhat-release
*
```

3. Execute the YUM command:

```
yum install redhat-lsb
```

As a result, all the dependency packages are installed.

## Roadmap for protection with the File System agent

The following roadmap provides the steps required to configure the File System agent in PowerProtect Data Manager in order to run protection policies.

### Procedure

1. Add a storage system.  
[Add protection storage](#) on page 40 provides information.
2. Install the File System agent on the File System host.  
[Installing and configuring File System agent](#) on page 82 provides information.
3. Add or approve the File System agent on each File System host.  
[Manage the File System agent](#) on page 84 provides information.
4. Discover the File system asset.  
[Discover a File System Host](#) provides information.
5. Create a protection policy to protect the File System.  
[Add a protection policy for File System protection](#) on page 129 provides information.

**Note:** You cannot perform a backup to a secondary Data Domain device. You can only restore from a secondary Data Domain device

## Installing and configuring File System agent

Learn how to install and configure the File System agent for Linux and Windows.

### Install the File System agent on Linux

Learn how to install the File System agent on supported Linux systems.

#### Before you begin

- Ensure that you review the prerequisites provided in [File System agent prerequisites](#) on page 80.
- Download the File System agent software package to the Linux host.

#### Procedure

1. In the PowerProtect Data Manager UI:
  - a. Select **Agent Downloads** from the **System Settings** menu.
  - b. Select the File System agent download package for Linux, `fsagent192_linux_x86_64.tar.gz`.
  - c. Download the package in the location that you want to install the File System agent.
2. Untar the installer by running `gunzip *` followed by `tar -xvf`.
3. Run the installation script `install.sh`.
4. Enter the PowerProtect Data Manager server IP address.

**Note:** If the File System agent will co-exist with another application agent, ensure that you register the agent with the existing PowerProtect Data Manager server IP. When you register the agent with a PowerProtect Data Manager server that is different from the currently registered server, no warning message displays, and requests are routed to the newer server instance.

#### After you finish

If the host is not already whitelisted or approved, add the File System host to the PowerProtect Data Manager server. [Add or manage Application/File System Agents](#) provides more information.

Discover File System assets. [Discover a File System Host](#) provides more information.

### Install the File System agent on Windows

Learn how to install the File System agent on supported Windows systems.

#### Before you begin

- Ensure that you carry out the prerequisites provided in [File System agent prerequisites](#) on page 80.
- Download the File System agent software package.

#### Procedure

1. In the PowerProtect Data Manager UI:

- a. Select **Agent Downloads** from the **System Settings** menu.
  - b. Select the File System agent download package for Windows, `fsagent192_win_x64.zip`.
  - c. Download the package in the location that you want to install the File System agent.
2. Open the `fsagent-19.2.0.0.exe` installation file.
  3. Follow the wizard installation steps to provide the installation location and the PowerProtect Data Manager server IP address.
  4. Click **Install**.
  5. Click **Finish**.

#### After you finish

If the host is not already whitelisted or approved, add the File System host to the PowerProtect Data Manager server. [Add or manage Application/File System Agents](#) provides more information.

Discover File System assets. [Discover a File System Host](#) provides more information.

## Silent installation of File System agent

You can perform a silent installation or uninstallation of the File System agent.

#### Silent installation commands

To perform the silent installation to the default path, run:

```
fsagent-19.2.0.0.exe /s PPDMHostName=<<PPDM-server-IP>>
```

To perform the silent installation to a different path, run:

```
fsagent-19.2.0.0.exe /s PPDMHostName=<<PPDM-server-IP>>  
ProductInstallPath="D:\alternate-path"
```

**Note:** *PPDMHostName* is a mandatory option in the command line. If a value is not provided, the product is installed without PowerProtect registration, and no backups can be initiated from the UI. Specifying *ProductInstallPath* is optional, but if used, the value cannot be empty.

#### Silent uninstallation commands

To perform a silent uninstall without uninstalling common components (such as ADM or BBB), run:

```
fsagent-19.2.0.0.exe /s /uninstall
```

To perform a silent uninstall while also uninstalling common components, run:

```
fsagent-19.2.0.0.exe /s /uninstall UnInstallPPDMAgent="1" UnInstallBBBWT="1"
```

## Uninstalling the File System agent

You can uninstall the File System agent for SQL Server with the setup file.

#### Procedure

1. Launch `DPSFSAgent-19.2.0.0.exe`.
2. On the **Install Modification** page, select **Remove**, and then click **Next**.

3. On the **Complete the Setup** page, click **Finish**.
4. After the uninstall completes you must remove the working directory from `C:\Program Files\DPSFSSGENT`.

## Upgrade the File System agent

There is no direct upgrade option for the File System agent. If you have the File System agent for PowerProtect Data Manager 19.1 and you want to upgrade to release 19.2, perform the following steps.

### Procedure

1. Uninstall the PowerProtect Data Manager 19.1 File System agent, but keep the existing folders. [Uninstalling the File System agent](#) on page 83 provides instructions.
2. Install and register the PowerProtect Data Manager 19.2 File System agent for Linux or Windows with the same PowerProtect Data Manager server in the same location. [Install the File System agent on Linux](#) on page 82 and [Install the File System agent on Windows](#) on page 82 provide instructions.
3. Approve the new instance of the File System agent on the PowerProtect Data Manager server. [Manage the File System agent](#) on page 84 provides instructions.

## Manage the File System agent

You can add a File System agent, approve and reject pending agent requests, and edit and delete existing agents.

### About this task

**Note:** PowerProtect Data Manager supports the coexistence of the following agents on the same Windows or Linux host:

- SQL agent and File System agent on Windows.
- Oracle/RMAN agent and File System agent on Linux.

### Procedure

1. Select **Infrastructure > Application Agents**.
2. In the **Application Agents** window, click **Add**.
3. In the **Add Application/FS Agent** window, select one of the following options:

**Note:** The Auto Whitelist option is enabled by default. When `Auto whitelist` is enabled, all pre-approved Application Agents are automatically approved.

- **Add IP Address**

Perform the following steps:

- a. Type the IP Address for the application agent.
- b. Specify the date until which the application agent is pre-approved.
- c. Click **Save**.

- **CSV Filename**

Perform the following steps:

- a. Click the **Choose File** icon.

**Note:** The contents of the .CSV file must be in the following format, for example:

```
"10.25.115.113"  
"10.25.115.112"  
"10.25.115.145"
```

The **Explorer** window appears.

- b. Select the `.csv` file, and then click **Open**.  
The file displays in the **Application/FS Agents** window.
  - c. Select the date until which the application or File System agent is preapproved.
  - d. Click **Save**.
4. If you have disabled `Auto whitelist`, select an application agent, and then select one of the following options:
- **Approve**
  - **Reject**
  - **Edit** Make the required changes.
  - **Remove**



# CHAPTER 7

## Enabling the Storage Direct Agent

This section includes the following topics:

- [About the Storage Direct agent](#).....88
- [Storage Direct agent prerequisites](#)..... 88
- [Additional setup and configuration file requirements for existing Storage Direct users](#)..... 89
- [Roadmap for protection with the Storage Direct agent \(new users\)](#).....91
- [Roadmap for protection with the Storage Direct agent \(existing Storage Direct users\)](#).....93
- [Installing or Upgrading Storage Direct](#).....94
- [Manage the Storage Direct agent](#)..... 98

## About the Storage Direct agent

Storage Direct uses snapshot backup technology to protect data on VMAX storage arrays, moving storage group data from the VMAX to a Data Domain system. Starting in release 19.2, the PowerProtect Data Manager software enables an application administrator to configure the Storage Direct agent and create self-service protection policies within the PowerProtect Data Manager UI to facilitate the setup of backups for new users and the importing of the setup for existing users into PowerProtect Data Manager. PowerProtect Data Manager also enables you to roll back the snapshot backup data to the original location or a different location.

You can install the Storage Direct agent on the host that you plan to protect by using the installation wizard. [Installing or Upgrading Storage Direct](#) on page 94 provides instructions.

When you install and configure the agent, Storage Direct takes the data from VMAX storage groups, creates a snapshot backup, and transfers the data to a Data Domain system. Using FTS technology, the host running your applications accesses the source LUNs from the VMAX where the storage group data resides. A link is then established between FTS devices on the VMAX and the destination Data Domain system, enabling the creation of a virtual drive (vDisk), vDisk pool, and mTree on the Data Domain.

Upon the approval/registration of the Storage Direct agent in the PowerProtect Data Manager UI, and the addition and discovery of Data Domain systems and the SMIS server, the Storage Direct agent is enabled for use. The storage groups in the VMAX can then be discovered by PowerProtect Data Manager for the purposes of assigning unprotected storage groups to a protection policy.

Software compatibility information for the PowerProtect Data Manager software and the Storage Direct agent is provided in the eLab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.

## Storage Direct agent prerequisites

If you are a new user of Storage Direct, or an existing user updating to the Storage Direct agent for PowerProtect Data Manager 19.2, review the following prerequisites before enabling the Storage Direct agent in PowerProtect Data Manager and discovering the VMAX storage groups:

- Ensure that the vDisk user is an administrator.
- Ensure that the LUNs of the storage groups to be protected are masked to the host.
- Ensure that your host is a 64-bit system. PowerProtect Data Manager supports only 64-bit hosts.
- Only Windows and Linux platforms are supported through the PowerProtect Data Manager server.
- Ensure that your host is a supported operating system version.  
Software compatibility information for the PowerProtect Data Manager software is provided in the eLab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.
- After the Data Domain discovery, ensure that the vDisk Pool and DD Boost storage units are available in PowerProtect Data Manager by navigating to **Infrastructure > Storage**, selecting the Data Domain and then selecting **Manage Storage Units**.
- Ensure that all clocks on both the host and PowerProtect Data Manager are time-synced to the local NTP server to ensure discovery of the backups.



- Ensure that the host and the PowerProtect Data Manager network can see and resolve each other.
- If using replication, ensure that you add a secondary Data Domain system.

## Additional setup and configuration file requirements for existing Storage Direct users

Existing Storage Direct users who want to enable the Storage Direct agent in PowerProtect Data Manager 19.2 must satisfy the following additional requirements.

### Upgrade requirements

Review the following setup requirements specific to existing Storage Direct users who are upgrading to the latest Storage Direct agent release for PowerProtect Data Manager 19.2:

- During the upgrade, on the **Configure Installation Options** page, click **PowerProtect Data Manager registration**, and then provide the PowerProtect Data Manager server IP so that the Storage Direct agent can register with the PowerProtect Data Manager server.
- Also during the upgrade, on the **Configuration File Input** page, click **Select the Configuration Files**, browse to the location of your configuration file(s), and for each configuration file, click **Add**.

### Configuration file requirements

For new users who are installing and configuring the Storage Direct agent for the first time, a configuration file is created automatically in the `C:\Program Files\DPSAPPS\ppfsagent\config` directory upon the addition of storage groups to a **VMAX Storage Group** protection policy. This configuration contains information about the VMAX and Data Domain system attributes and the storage groups being protected by this policy, and is required to perform self-service backup and restore.

Existing Storage Direct users, however, already have one or more configuration files that contain this information. In order to ensure that PowerProtect Data Manager can use your existing configuration file(s), review the file contents and, where required, modify those contents or your environment to satisfy the following requirements:

- If importing one configuration file, ensure that all backup vDisks on the Data Domain belong to the same pool. Device groups, however, can be different. For example, if you have two source storage groups (SG1 and SG2), you can create one device group for the backup vDisks of SG1, and another device group for the backup vDisks of SG2.  
Note that if importing multiple configuration files per host, vDisks can belong to different pools.
- Only storage groups can be added to the file, and not IDs of the source LUNs or details about the secondary Data Domain system.
- The file must contain the `Ddboost` and `DdvdiskUser`, with their corresponding passwords in the lockbox.
- The `Devicepath` cannot start with a `/`.

Additionally, the file must be in one of the following formats:

**Example 1** Format 1: One restore device group and one restore storage group

This format is optimal when you have one restore device group and one restore storage group. In this format:

**Example 1** Format 1: One restore device group and one restore storage group (continued)

- There is one entry for `RESTORE_DEVICE_GROUP` and `VMAX_FASTX_RESTORE_SG` for all Source Storage Groups.
- All Storage Groups map to a single `RESTORE_DEVICE_GROUP` and `VMAX_FASTX_RESTORE_SG`
- Since only one of the `RESTORE_DEVICE_GROUP` or `VMAX_FASTX_RESTORE_SG` attributes is used, comment the one not in use.
- If using `RESTORE_DEVICE_GROUP`, then the corresponding pool information for `RESTORE_DEVICE_POOL` must be provided, and the attribute uncommented.
- If using `VMAX_FASTX_RESTORE_SG`, then comment the `RESTORE_DEVICE_GROUP` and `RESTORE_DEVICE_POOL` attributes.

The following output shows an example layout of this format.

```
[PRIMARY_SYSTEM]
DDBOOST_USER = <boost_user>
DEVICE_HOST = <dd_host>
DEVICE_PATH = <ddbboost_devPath>
DDVDISK_USER = <vdisk_user>
# RESTORE_DEVICE_POOL = <device_pool>
# RESTORE_DEVICE_GROUP = <device_group>
# DD_BOOST_FC =
# DD_PORT =
VMAX_FASTX_RESTORE_SG = <restore_sg>
# SELECT_VISIBLE_RESTORE_DEVICES =
|
|
|
[BACKUP_SOURCE_DEVICES]
# SRC_DEVICE1 = 000196700638:00F1A
# SRC_DEVICE_n =
SRC_GROUP1 = <symmId:SourceGrp1>
SRC_GROUP2 = <symmId:SourceGrp2>
SRC_GROUP3 = <symmId:SourceGrp3>
# SRC_GROUP_n =
```

**Example 2** Format 2: Multiple restore device groups and restore storage groups

This format is optimal when you have multiple restore device groups and restore storage groups. In this format:

- For each source storage group, there should be a corresponding restore storage group and restore device group.
- The same number of entries must exist for `RESTORE_DEVICE_GROUP` and `VMAX_FASTX_RESTORE_SG` as the number of source storage groups in a 1:1 mapping, and the order should be maintained, as in the first `RESTORE_DEVICE_GROUP` and `VMAX_FASTX_RESTORE_SG` entry should correspond to `SRC_GROUP1`, the second `RESTORE_DEVICE_GROUP` and `VMAX_FASTX_RESTORE_SG` entry should correspond to `SRC_GROUP2`, and so on.
- Since there should only be one entry of `RESTORE_DEVICE_GROUP` and `VMAX_FASTX_RESTORE_SG`, other entries should be commented.

The following output shows an example layout of this format.

**Example 2** Format 2: Multiple restore device groups and restore storage groups (continued)

```
[PRIMARY_SYSTEM]
DDBOOST_USER = <boost_user>
DEVICE_HOST = <dd_host>
DEVICE_PATH = <ddbboost_devPath>
DDVDISK_USER = <vdisk_user>
# RESTORE_DEVICE_POOL = <device_pool_sg1>
# RESTORE_DEVICE_GROUP = <device_group_sg1>
# RESTORE_DEVICE_GROUP = <device_group_sg2>
# RESTORE_DEVICE_GROUP = <device_group_sg_3>
# DD_BOOST_FC =
# DD_PORT =
VMAX_FASTX_RESTORE_SG = <restore_sg1>
# VMAX_FASTX_RESTORE_SG = <restore_sg2>
# VMAX_FASTX_RESTORE_SG = <restore_sg3>
# SELECT_VISIBLE_RESTORE_DEVICES =
|
|
|
[BACKUP_SOURCE_DEVICES]
# SRC_DEVICE1 = 000196700638:00F1A
# SRC_DEVICE n =
SRC_GROUP1 = <symmId:SourceGrp1>
SRC_GROUP2 = <symmId:SourceGrp2>
SRC_GROUP3 = <symmId:SourceGrp3>
# SRC_GROUP n =
```

## Roadmap for protection with the Storage Direct agent (new users)

For users new to Storage Direct (ProtectPoint) and PowerProtect Data Manager, the following roadmap provides the steps required to configure protection of the Storage Direct agent in PowerProtect Data Manager for movement of snapshot backups from the VMAX storage area to the DD system.

### Before you begin

Review any prerequisites in the section [Storage Direct agent prerequisites](#) on page 88, and make note of any limitations in the section [Storage Direct agent limitations](#) on page 218.

### Procedure

1. Set up the SMIS server in the PowerProtect Data Manager UI:
  - a. Add the SMIS server.
  - b. Initiate a discovery of the SMIS server.
  - c. Verify that the discovery completed successfully.

[Add and discover the SMIS server for the Storage Direct agent](#) on page 113 provides information.

2. Set up the Data Domain system in the PowerProtect Data Manager UI:
  - a. Add a primary Data Domain system.
  - b. (Optional) If using replication, add a secondary Data Domain system.
  - c. Initiate a discovery of the Data Domain system(s).
  - d. Verify that the discovery completed successfully.

[Add protection storage](#) on page 40 provides information.

**Note:** If using the Storage Direct agent to move snapshot backups from a VMAX storage array to a Data Domain system, you do not need to add a Data Domain Management Center.

3. Install the Storage Direct agent on the Storage Direct/ProtectPoint host system.

[Installing or Upgrading Storage Direct](#) on page 94 provides information.

4. Approve the Storage Direct agent in the PowerProtect Data Manager UI on each Storage Direct/ProtectPoint host system.

[Manage the Storage Direct agent](#) on page 98 provides information.

5. Ensure that the Storage Direct agent has been discovered.

[Discover a Storage Direct agent host](#) on page 112 provides information.

6. In the PowerProtect Data Manager UI, verify that the VMAX assets (storage groups) have been discovered, and that the host name appears next to these assets.

[Add and discover the SMIS server for the Storage Direct agent](#) on page 113 provides information about how to verify that these assets have been discovered, and [Add a protection policy for Storage Direct protection](#) on page 132 provides information about adding assets to a protection policy.

7. Create a protection policy in the PowerProtect Data Manager UI by selecting the **Storage Group** policy type and choosing the **I want PPDM to automatically provision and manage all storage needed to achieve this objective** option.

[Add a protection policy for Storage Direct protection](#) on page 132 provides information.

8. Review the configuration file that is automatically generated upon the successful configuration of the Storage Direct agent in PowerProtect Data Manager to ensure that the file contains the information identified in [Additional setup and configuration file requirements for existing Storage Direct users](#) on page 89. This file is required to perform self-service backup and restore.

[Add a protection policy for Storage Direct protection](#) on page 132 provides information about the type of information that the configuration file contains, and how this file is used when executing the backup command.

**Note:** Do not make any changes to this configuration file.

9. Run the `protectpoint snapbackup create` command with the configuration file name specified in order to perform the self-service backup.

The *Storage Direct Agent Installation and Administration Guide*, and the **After you finish** section of [Add a protection policy for Storage Direct protection](#) on page 132, provide information about running this command with the configuration file.

## Roadmap for protection with the Storage Direct agent (existing Storage Direct users)

For existing users of Storage Direct (ProtectPoint), the following roadmap provides the steps required to configure protection of the Storage Direct agent in PowerProtect Data Manager for movement of snapshot backups from the VMAX storage area to the DD system.

### Before you begin

Review any prerequisites in the section [Storage Direct agent prerequisites](#) on page 88 and [Additional setup and configuration file requirements for existing Storage Direct users](#) on page 89, and make note of any limitations in the section [Storage Direct agent limitations](#) on page 218.

### Procedure

1. Set up the SMIS server in the PowerProtect Data Manager UI:
  - a. Add the SMIS server.
  - b. Initiate a discovery of the SMIS server.
  - c. Verify that the discovery completed successfully.

[Add and discover the SMIS server for the Storage Direct agent](#) on page 113 provides information.

2. Set up the Data Domain system in the PowerProtect Data Manager UI:
  - a. Add a primary Data Domain system.
  - b. (Optional) If using replication, add a secondary Data Domain system.
  - c. Initiate a discovery of the Data Domain system(s).
  - d. Verify that the discovery completed successfully.

[Add protection storage](#) on page 40 provides information.

**Note:** If using the Storage Direct agent to move snapshot backups from a VMAX storage array to a Data Domain system, you do not need to add a Data Domain Management Center.

3. Modify your existing configuration file(s) to ensure that the file contains the information required by PowerProtect Data Manager to run the **VMAX Storage Group** policy, and to ensure the file is in an acceptable format, as described in the section [Additional setup and configuration file requirements for existing Storage Direct users](#) on page 89.
4. Upgrade the Storage Direct agent on the Storage Direct/ProtectPoint host system.
 

[Installing or Upgrading Storage Direct](#) on page 94 provides information.
5. Approve the Storage Direct agent in the PowerProtect Data Manager UI on each Storage Direct/ProtectPoint host system.
 

[Manage the Storage Direct agent](#) on page 98 provides information.
6. Ensure that the Storage Direct agent has been discovered.
 


[Discover a Storage Direct agent host](#) on page 112 provides information.
7. In the PowerProtect Data Manager UI, verify that the VMAX assets (storage groups) have been discovered, and that the host name appears next to these assets.

[Add and discover the SMIS server for the Storage Direct agent](#) on page 113 provides information about how to verify that these assets have been discovered, and [Add a](#)

[protection policy for Storage Direct protection](#) on page 132 provides information about adding assets to a protection policy.

8. Create a protection policy in the PowerProtect Data Manager UI by selecting the **Storage Group** policy type and choosing the **I will provision and manage my own storage** option. [Add a protection policy for Storage Direct protection](#) on page 132 provides information.
9. Review the configuration file that is automatically generated upon the successful configuration of the Storage Direct agent in PowerProtect Data Manager to ensure that the file contains the information identified in [Additional setup and configuration file requirements for existing Storage Direct users](#) on page 89. This configuration file will be used going forward instead of your previous configuration file(s) to perform self-service backup and restore.

[Add a protection policy for Storage Direct protection](#) on page 132 provides information about the type of information that the configuration file contains, and how this file is used when executing the backup command for the initial snapshot.

 **Note:** Do not make any changes to this configuration file.

10. Run the `protectpoint snapbackup create` command with the configuration file name specified in order to perform the self-service backup.

The *Storage Direct Agent Installation and Administration Guide*, and the **After you finish** section of [Add a protection policy for Storage Direct protection](#) on page 132, provide information about running this command with the configuration file.

## Installing or Upgrading Storage Direct

Learn how to install or upgrade Storage Direct to the Storage Direct agent for PowerProtect Data Manager 19.2.

### Install the Storage Direct agent on Linux

Learn how to install the standalone ProtectPoint agent for PowerProtect Data Manager, also known as the Storage Direct agent, on supported Linux systems.

#### Before you begin

- Ensure that you review the prerequisites provided in [Storage Direct agent prerequisites](#) on page 88.
- Download the Storage Direct agent software package to the Linux host.

#### Procedure

1. In the PowerProtect Data Manager UI:
  - a. Select **Agent Downloads** from the **System Settings** menu.
  - b. Select the Storage Direct agent download package for Linux, `storagedirectagent192_linux_x86_64.tar.gz`.
  - c. Download the package to the location where you want to install the Storage Direct agent.
2. Unpack the Storage Direct software package:
  - a. Run the following command:

```
gunzip storagedirectagent192_<platform>.tar.gz
```

b. Run the following command:

```
tar -xvf storedirectagent192_<platform>.tar
```

c. Run the following command:

```
rpm --import RPM_KEY
```

3. Provide "Execute" +x permissions on the `install.sh` file.
4. Install the Storage Direct software as the `root` user by running the installation script:

```
install.sh
```

**Note:** During the installation, you are prompted for the hostname or IP address of the PowerProtect Data Manager. As an alternative, you can include the `--server` option when you run the `install.sh` installation script, as in the following:

```
install.sh --server=<PowerProtect_Data_Manager_server_hostname_or_IP>
```

To obtain a list of all the available command options for the `install.sh` command, run the command `install.sh --help` or `install.sh -h`. The command also supports the `--debug` or `-d` option for debugging purposes.

The product is installed in the `/opt/dpsapps/ppfsagent` directory. Two rpms are installed as part of the installation script:

- `adm-agent-rpm-19.2.0.rpm`
- `storedirectagent-19.2.0.0-0.x86_64.rpm`

#### After you finish

Complete the host registration with the PowerProtect Data Manager server. [Add and discover the SMIS server for the Storage Direct agent](#) on page 113 provides more information.

Approve the pending Storage Direct agent request so that you can discover the VMAX assets, also known as storage groups. [Manage the Storage Direct agent](#) on page 98 provides more information.

## Upgrade the Storage Direct agent on Linux

Learn how to upgrade to the standalone ProtectPoint agent for PowerProtect Data Manager, also known as the Storage Direct agent, on supported Linux systems.

#### Before you begin

- Ensure that you review the prerequisites provided in [Storage Direct agent prerequisites](#) on page 88, and the **Upgrade requirements** section in [Additional setup and configuration file requirements for existing Storage Direct users](#) on page 89.
- Download the Storage Direct agent software package to the Linux host.

#### Procedure

1. In the PowerProtect Data Manager UI:

- a. Select **Agent Downloads** from the **System Settings** menu.
  - b. Select the Storage Direct agent download package for Linux, `storagedirectagent192_linux_x86_64.tar.gz`.
  - c. Download the package to the location where you want to install the Storage Direct agent.
2. Unpack the Storage Direct software package:
    - a. Run the following command:

```
gunzip storagedirectagent192_<platform>.tar.gz
```

- b. Run the following command:

```
tar -xvf storagedirectagent192_<platform>.tar
```

- c. Run the following command:

```
rpm --import RPM_KEY
```

3. Provide "Execute" `+x` permissions on the `install.sh` file.
4. Upgrade the Storage Direct software as the `root` user by running the installation script with the `-u` option, as in the following:

```
install.sh -u
```

**i Note:** Later in the upgrade, you are prompted for the hostname or IP address of the PowerProtect Data Manager. As an alternative, you can include the `--server` option when you run the `install.sh -u` command, as in the following:

```
install.sh -u --
server=<PowerProtect_Data_Manager_server_hostname_or_IP>
```

The product is upgraded in the `/opt/dpsapps/ppfsagent` directory. Two rpms are installed as part of the installation script:

- `adm-agent-rpm-19.2.0.rpm`
- `storagedirectagent-19.2.0.0-0.x86_64.rpm`

5. For `Do you wish to give existing config file path?, type y`, and then provide the path to the configuration files.

A prompt appears requesting if you have additional configuration files. If you have more than one existing configuration file, type `y`, and provide the additional path.

6. For `Do you wish to upgrade adm-agent?, type y`.
7. If you did not specify the PowerProtect Data Manager server name when running the `install.sh -u` command, a prompt appears requesting if you want to register Storage Direct with the PowerProtect Data Manager server. Type `y`, and then type the PowerProtect Data Manager server FQDN or IP address.



**After you finish**

Complete the host registration with the PowerProtect Data Manager server. [Add and discover the SMIS server for the Storage Direct agent](#) on page 113 provides more information.

Approve the pending Storage Direct agent request so that you can discover the VMAX assets, also known as storage groups. [Manage the Storage Direct agent](#) on page 98 provides more information.

## Install or Upgrade the Storage Direct agent on Windows

Learn how to install or upgrade to the standalone ProtectPoint agent for PowerProtect Data Manager, also known as the Storage Direct agent, on supported Windows systems.

**Before you begin**

- Ensure that you review the prerequisites provided in [Storage Direct agent prerequisites](#) on page 88, and the **Upgrade requirements** section in [Additional setup and configuration file requirements for existing Storage Direct users](#) on page 89.
- Download the Storage Direct agent software package to the Windows host.

**Procedure**

1. In the PowerProtect Data Manager UI:
  - a. Select **Agent Downloads** from the **System Settings** menu.
  - b. Select the Storage Direct agent download package for Windows, for example, `storagedirectagent_192_win_x64.zip`.
  - c. Download the package in the location that you want to install the Storage Direct agent.
2. To launch the installer, unzip the `storagedirectagent192_win_x64.zip` file and then run the `storagedirectagent192_win_x64.exe` program.

The installation wizard opens.

3. Click **Next**.
4. Select **I accept the terms in the License Agreement**, and then click **Next**.
5. On the **Configure Installation Options** page, click **PowerProtect Data Manager registration**, and then type the PowerProtect Data Manager server hostname or IP address in the **Appliance hostname or IP address** text box so that the Storage Direct agent can register with the PowerProtect Data Manager server.
6. If upgrading, on the **Configuration File Input** page, click **Select the Configuration Files**, browse to the location of your configuration file(s), and for each configuration file, click **Add**.
7. When completed, click **Install**.
8. Click **Finish** to exit the installation wizard.

**After you finish**

Complete the host registration with the PowerProtect Data Manager server. [Add and discover the SMIS server for the Storage Direct agent](#) on page 113 provides more information.

Approve the pending Storage Direct agent request so that you can discover the VMAX assets, also known as storage groups. [Manage the Storage Direct agent](#) on page 98 provides more information.

## Silent installation of the Storage Direct agent

You can perform a silent installation of the Storage Direct agent on Linux or Windows.

### Silent installation commands

To perform the silent installation to the default path:

- On Linux, run `install.sh -- server PPDM server name`
- On Windows, run `storagedirectagent-19.2.0.0.exe /s PPDMHostName=<PPDM-server-IP>`

**Note:** *PPDMHostName* is a mandatory option in the command line. If a value is not provided, the product is installed without PowerProtect registration, and no backups can be initiated from the application host. Specifying *ProductInstallPath* is optional, but if used, the value cannot be empty.

## Uninstall the Storage Direct agent on Linux

You can uninstall the Storage Direct agent by using the `uninstall.sh` script, which is included when you untar the installer.

### Procedure

1. Run `uninstall.sh`.
2. Type **y** to confirm that you want to uninstall the agent.

If you have the ADM agent installed as well, a message appears indicating Other application agents might be using adm agent... Do you wish to uninstall adm agent[y/n]:

3. Type **y** or **n** for the ADM uninstall.

The Storage Direct agent uninstall starts.

4. After the uninstall completes, remove the working directories located at `/opt/dpsapps/` and `/usr/local/ecdm/`.

## Uninstall the Storage Direct agent on Windows

You can uninstall the Storage Direct agent by using the setup file.

### Procedure

1. Launch `storagedirectagent-19.2.0.0.exe`.
2. On the **Install Modification** page, select **Remove**, and then click **Next**.
3. On the **Complete the Setup** page, click **Finish**.
4. After the uninstall completes, remove the working directory located at `C:\Program Files\DPSAPPS\ppfsagent`.

## Manage the Storage Direct agent


After the Storage Direct installation completes, an entry with the agent host name appears in the **Infrastructure > Application Agents** window of the PowerProtect Data Manager UI. From this window, you can approve or reject a pending Storage Direct agent request, and edit and delete existing agents.

### About this task

## Procedure

1. Select **Infrastructure > Application Agents**.
2. In the **Application Agents** window, select the entry that contains the host name, and click **Approve**.

The status changes from **Awaiting Approval** to **Registered**.

 **Note:** The `Auto whitelist` option, which enables you to pre-approve application agents automatically, is disabled by default. When you enable this option, the Storage Direct agent registration is approved automatically.



# CHAPTER 8

## Managing Assets

This section includes the following topics:

- [About asset sources, assets, and storage](#)..... 102
- [Prerequisites for discovering asset sources](#)..... 102
- [Adding a vCenter Server asset source](#)..... 102
- [Creating a dedicated vCenter user account and assigning the role in vCenter](#)..... 105
- [VM Direct protection engine overview](#)..... 108
- [Discovering an application or File System host](#) ..... 110
- [Add and discover the SMIS server for the Storage Direct agent](#)..... 113

## About asset sources, assets, and storage

In PowerProtect Data Manager, assets are the basic unit that PowerProtect Data Manager protects. Asset sources are the mechanism that PowerProtect Data Manager uses to communicate with and manage the storage and assets. Storage is where PowerProtect Data Manager adds and stores copies and protection.

PowerProtect Data Manager supports Data Domain Management Center (DDMC) as the storage and programmatic interface for controlling the Data Domain systems, as well as external Data Domains.

Assets can be virtual machines, SQL databases, Oracle databases, File systems or VMAX storage groups.

PowerProtect Data Manager supports backing up assets and adding the asset sources either through a PowerProtect Application Agent for DD Boost backups, or by connecting to vCenter and performing virtual machine backups.

## Prerequisites for discovering asset sources

Perform these tasks before you discover the asset sources.

- Ensure that the PowerProtect Data Manager is deployed and configured in the environment. The *PowerProtect Data Manager Deployment Guide* provides information.
- Log in with administrative rights.
- Configure all asset sources with an NTP server.
- Before you register an SQL application, ensure that the Data Domain has been discovered successfully.
- For discovery of App/File System asset sources:
  - Ensure that all clocks on both the App/File System host and PowerProtect Data Manager are time-synced to the local NTP server to ensure discovery of the backups.
  - Ensure that the App/File System host and the PowerProtect Data Manager network can see/resolve each other.
  - Ensure that port 7000 is open on the App/File System host.

## Adding a vCenter Server asset source

After you register a vCenter Server with PowerProtect Data Manager, you can use the **Asset Sources** window in the PowerProtect Data Manager UI to add a vCenter Server asset source to the PowerProtect Data Manager environment.

### About this task

Adding a vCenter Server asset source is required if you want to schedule a backup through PowerProtect Data Manager.

## Add a VMware vCenter Server

Perform the following steps to add a vCenter Server as an asset source in the PowerProtect Data Manager UI.

### Before you begin

- You must have Administrator privileges.

- By default, PowerProtect Data Manager enforces SSL certificates during communication with vCenter Server. If a certificate appears, click **Verify** to accept the certificate.
  - ① **Note:** It is highly recommended that you do not disable certificate enforcement. If disabling the certificate is required, carefully review the instructions in the section [Disable SSL certification on the vCenter Server](#) on page 200

### Procedure

1. Select **Infrastructure > Asset Sources**.

The **Asset Sources** window appears.

2. Select the **vCenter** tab.
3. Click **Add**.

The **Add vCenter** dialog displays.

4. Specify the source's attributes:

- a. In the **Name** field, specify the vCenter Server name.

- b. In the **Address** field, specify the fully qualified domain name (FQDN) or the IP address.

- ① **Note:** For a vCenter Server, we recommend that you use the FQDN instead of the IP address.

- c. In the **Port** field, specify the port for communication if you are not using the default port, 443.

5. Under **Host Credentials**, choose an existing entry from the list to use for the vCenter user credentials. Alternatively, you can click **Add** from this list to add new credentials, and then click **Save**.

- ① **Note:** Ensure that you specify the credentials for a user whose role is defined at the vCenter level, as opposed to being restricted to a lower level container object in the vSphere object hierarchy.

6. If you want to make a subset of the PowerProtect Data Manager UI's functionality available within the **vSphere Client**, move the **vSphere Plugin** slider to the right.

Available functionality includes the monitoring of active virtual machine/VMDK protection policies, and restore options such as **Restore to Original**, **Restore to New**, and **Instant Access**.

- ① **Note:** You can unregister the vSphere plug-in at any time by moving the slider to the left.

7. If the vCenter's SSL certificate cannot be trusted automatically, a dialog box appears requesting certificate approval. Review the certificate and click **Verify**.
8. Click **Save**.

The vCenter Server information that you entered now appears as an entry in a table on the **Asset Sources** window.

- ① **Note:** Although PowerProtect Data Manager automatically synchronizes with the vCenter server under most circumstances, certain conditions might require you to initiate a manual discovery.

After a successful discovery, PowerProtect Data Manager starts an incremental discovery in the background periodically to keep updating PowerProtect Data Manager with new changes in vCenter. You can always do an ad-hoc discovery.

9. Select **Infrastructure > Assets**.

The **Assets** window appears.

10. If not already selected, click the **Virtual Machines** tab.

When discovery has completed successfully, the virtual machine assets discovered in the vCenter display. Note that discovery time is based on networking bandwidth. The resources that are discovered and those that are doing the discovery take a performance hit each time that you go through a discovery process. It might appear that PowerProtect Data Manager is not updating the Asset Sources data while the discovery is in progress.

**After you finish**

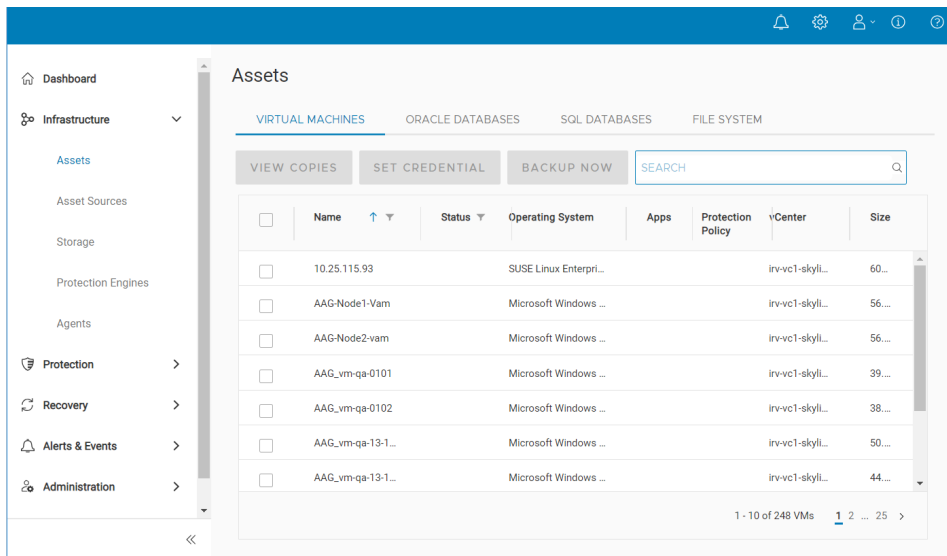
Upon successful discovery of the vCenter's virtual machine assets, you can add a VM Direct appliance to facilitate data movement, and then create virtual machine protection policies to back up these assets. Note that the PowerProtect Data Manager software comes pre-bundled with an embedded VM Direct Engine, which is automatically used as a fallback proxy for performing backups and restores when the added external proxies fail or are disabled. It is recommended that external proxies should always be deployed since the embedded proxy has very limited capacity for performing parallel backups. To add a VM Direct Engine, go to **Infrastructure > Protection Engines**.

## Virtual asset discovery

After you add a vCenter Server as an asset source, an automatic discovery of VMware entity information from the vCenter Server is initiated.

After automatic discovery, the virtual assets for the vCenter Server appear in the **Assets** window of the PowerProtect Data Manager UI under the **Virtual Machines** tab, as shown in the following figure.

**Figure 5** Assets window after vCenter Server discovery



The initial vCenter Server discovery identifies all ESX clusters, hosts, and virtual machines within the vCenter Server. Subsequent discoveries are performed automatically, according to a fixed interval, to identify any additional or changed VMware entities since the last discovery operation. You can also manually initiate a discovery of VMware entities at any time from the **vCenter** tab of the **Asset Sources** window by selecting a vCenter Server and clicking **Discover**.

Upon vCenter Server and virtual asset discovery, the PowerProtect Data Manager VM Direct protection engine facilitates the management of virtual assets as PowerProtect Data Manager



resources for the purposes of backup and recovery. We recommend that you also add an external VM Direct Engine in the **Protection Engines** window. You can protect virtual machine assets by manually adding the assets to a virtual machine protection policy, or by using dynamic filters to determine which assets will be included in a protection policy according to pre-defined rules.

## Creating a dedicated vCenter user account and assigning the role in vCenter

Dell EMC strongly recommends that you set up a separate vCenter user account at the root level of the vCenter that is strictly dedicated for use with PowerProtect Data Manager and the VM Direct protection engine.

Use of a generic user account such as “Administrator” might make future troubleshooting efforts difficult as it might not be clear which “Administrator” actions are actually interfacing, or communicating, with PowerProtect Data Manager. Using a separate vCenter user account ensures maximum clarity if it becomes necessary to examine vCenter logs.

You can specify the credentials for this vCenter user account when you add the vCenter as an asset source in the UI. Note that when adding the vCenter, ensure that you specify a user whose role is defined at the vCenter level, as opposed to being restricted to a lower level container object in the vSphere object hierarchy.

## Specify the required privileges for a dedicated vCenter user account

You can use the **vSphere Client** to specify the required privileges for the dedicated vCenter user account, or you can use the **PowerCLI**, which is an interface for managing vSphere. The following table includes the privileges required for this user.

### About this task

**Table 20** Minimum required vCenter user account privileges

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
Alarms	<ul style="list-style-type: none"> <li>Create alarm</li> <li>Modify alarm</li> </ul>	<pre>\$privileges = @( 'System.Anonymous', 'System.View', 'System.Read', 'Global.ManageCustomFields', 'Global.SetCustomField', 'Global.LogEvent', 'Global.CancelTask', 'Global.Licenses', 'Global.Settings', 'Global.DisableMethods', 'Global.EnableMethods', 'Folder.Create', 'Datastore.Rename', 'Datastore.Move', 'Datastore.Delete', 'Datastore.Browse', 'Datastore.DeleteFile', 'Datastore.FileManagement', 'Datastore.AllocateSpace', 'Datastore.Config', 'Network.Config', 'Network.Assign', 'Host.Config.Storage', 'VirtualMachine.Inventory.Create', 'VirtualMachine.Inventory.Register', 'VirtualMachine.Inventory.Delete', 'VirtualMachine.Inventory.Unregister', 'VirtualMachine.Interact.PowerOn',</pre>
Datastore	<ul style="list-style-type: none"> <li>Allocate space</li> <li>Browse datastore</li> <li>Configure datastore</li> <li>Low-level file operations</li> <li>Move datastore</li> <li>Remove datastore</li> <li>Remove file</li> <li>Rename datastore</li> </ul>	
Extension	<ul style="list-style-type: none"> <li>Register extension</li> <li>Unregister extension</li> <li>Update extension</li> </ul>	
Folder	<ul style="list-style-type: none"> <li>Create folder</li> </ul>	

**Table 20** Minimum required vCenter user account privileges (continued)

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
Global	<ul style="list-style-type: none"> <li>Cancel task</li> <li>Disable methods</li> <li>Enable methods</li> <li>Licenses</li> <li>Log event</li> <li>Manage custom attributes</li> <li>Settings</li> <li>Set custom attribute</li> </ul>	<pre>'VirtualMachine.Interact.PowerOff', 'VirtualMachine.Interact.Reset', 'VirtualMachine.Interact.ConsoleInteract', 'VirtualMachine.Interact.DeviceConnection', 'VirtualMachine.Interact.SetCDMedia', 'VirtualMachine.Interact.ToolsInstall', 'VirtualMachine.Interact.GuestControl', 'VirtualMachine.GuestOperations.Query', 'VirtualMachine.GuestOperations.Modify', 'VirtualMachine.GuestOperations.Execute', 'VirtualMachine.Config.Rename', 'VirtualMachine.Config.Annotation', 'VirtualMachine.Config.AddExistingDisk', 'VirtualMachine.Config.AddNewDisk', 'VirtualMachine.Config.RemoveDisk', 'VirtualMachine.Config.RawDevice', 'VirtualMachine.Config.HostUSBDevice', 'VirtualMachine.Config.CPUCount', 'VirtualMachine.Config.Memory', 'VirtualMachine.Config.AddRemoveDevice', 'VirtualMachine.Config.EditDevice', 'VirtualMachine.Config.Settings', 'VirtualMachine.Config.Resource', 'VirtualMachine.Config.UpgradeVirtualHardware', 'VirtualMachine.Config.ResetGuestInfo', 'VirtualMachine.Config.AdvancedConfig', 'VirtualMachine.Config.DiskLease', 'VirtualMachine.Config.SwapPlacement', 'VirtualMachine.Config.DiskExtend', 'VirtualMachine.Config.ChangeTracking', 'VirtualMachine.Config.ReloadFromPath', 'VirtualMachine.Config.ManagedBy', 'VirtualMachine.State.CreateSnapshot', 'VirtualMachine.State.RevertToSnapshot', 'VirtualMachine.State.RemoveSnapshot', 'VirtualMachine.Provisioning.MarkAsTemplate', 'VirtualMachine.Provisioning.DiskRandomAccess', 'VirtualMachine.Provisioning.DiskRandomRead', 'VirtualMachine.Provisioning.PutVmFiles', 'Resource.AssignVMToPool', 'Resource.HotMigrate', 'Resource.ColdMigrate', 'Alarm.Create', 'Alarm.Edit', 'Task.Create', 'Task.Update', 'Sessions.ValidateSession', 'Extension.Register', 'Extension.Update', 'Extension.Unregister', 'VApp.ApplicationConfig', 'VApp.Export', 'VApp.Import' )</pre>
Host	<ul style="list-style-type: none"> <li>Configuration &gt; Storage partition configuration</li> </ul>	
Network	<ul style="list-style-type: none"> <li>Assign network</li> <li>Configure</li> </ul>	
Resource	<ul style="list-style-type: none"> <li>Assign virtual machine to resource pool</li> <li>Migrate powered off virtual machine</li> <li>Migrate powered on virtual machine</li> </ul>	
Sessions	<ul style="list-style-type: none"> <li>Validate session</li> </ul>	
Tasks	<ul style="list-style-type: none"> <li>Create task</li> <li>Update task</li> </ul>	
vApp	<ul style="list-style-type: none"> <li>Export</li> <li>Import</li> <li>vApp application configuration</li> </ul>	
<b>Virtual Machine</b>		
Configuration	<ul style="list-style-type: none"> <li>Add existing disk</li> <li>Add new disk</li> <li>Add or remove device</li> <li>Advanced</li> <li>Change CPU count</li> <li>Change resource</li> <li>Configure managed by</li> <li>Disk change tracking</li> <li>Disk Lease</li> <li>Extend virtual disk</li> <li>Host USB device</li> <li>Memory</li> </ul>	<pre>New-VIRole -Name 'PowerProtect' -Privilege (Get-VIPrivilege -Id \$privileges)</pre>

**Table 20** Minimum required vCenter user account privileges (continued)

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
	<ul style="list-style-type: none"> <li>• Modify device settings</li> <li>• Raw device</li> <li>• Reload from path</li> <li>• Remove disk</li> <li>• Rename</li> <li>• Reset guest information</li> <li>• Set annotation</li> <li>• Settings</li> <li>• Swapfile placement</li> <li>• Upgrade virtual machine compatibility</li> </ul>	
Guest Operations	<ul style="list-style-type: none"> <li>• Guest operation modifications</li> <li>• Guest operation program execution</li> <li>• Guest operation queries</li> </ul>	
Interactions	<ul style="list-style-type: none"> <li>• Configure CD media</li> <li>• Console interaction</li> <li>• Device Connection</li> <li>• Guest operating system management by VIX API</li> <li>• Power off</li> <li>• Power on</li> <li>• Reset</li> <li>• VMware Tools install</li> </ul>	
Inventory	<ul style="list-style-type: none"> <li>• Create new</li> <li>• Register</li> <li>• Remove</li> <li>• Unregister</li> </ul>	
Provisioning	<ul style="list-style-type: none"> <li>• Allow disk access</li> <li>• Allow read-only disk access</li> <li>• Allow virtual machine download</li> <li>• Mark as Template</li> </ul>	
Snapshot Management	<ul style="list-style-type: none"> <li>• Create snapshot</li> <li>• Remove Snapshot</li> <li>• Revert to snapshot</li> </ul>	

## VM Direct protection engine overview

The VM Direct protection engine is the virtual machine data protection solution within PowerProtect Data Manager. This solution enables you to deploy a VM Direct Engine in the vSphere environment to perform virtual machine snapshot backups, moving the data to a Data Domain system.

The VM Direct protection engine is enabled after you add a vCenter Server in the **Asset Sources** window, which enables you to collect VMware entity information from the vCenter server and save the virtual machines as PowerProtect Data Manager resources for the purposes of backup and recovery.

To view statistics for the VM Direct engine, manage and monitor VM Direct engines, and add an external VM Direct engine to facilitate data movement, go to **Infrastructure > Protection Engines**. [Add a VM Direct appliance](#) on page 108 provides more information.

**i** **Note:** In the **VM Direct Engines** pane, **VMs Protected** refers to the number of assets protected by PowerProtect Data Manager. This count does not indicate that all of the virtual machines have been protected successfully. To determine the success or failure of asset protection, use the **Jobs** window.

When you add an external VM Direct Engine, the **VM Direct Engines** pane provides the following information:

- The VM Direct Engine IP address and name, which can be useful for troubleshooting network issues.
- The vCenter and ESXi hostname.
- The VM Direct Engine status (green check mark if the VM Direct Engine is ready, red x if the VM Direct Engine is not fully operational). The status includes a short explanation to help you determine why a VM Direct Engine is not in a fully operational state.
- The transport mode that you selected when adding the VM Direct Engine (Hot Add, Network Block Device, or the default setting Hot Add, Failback to Network Block Device).

## Add a VM Direct appliance

In the **Protection Engines** window, perform the following steps to deploy a VM Direct appliance to facilitate data movement with the VM Direct protection engine.

### About this task


The PowerProtect Data Manager software comes bundled with an embedded VM Direct appliance, which is automatically used as a fallback proxy for performing backups and restores when the added external proxies fail or are disabled. Dell EMC recommends that you deploy external proxies because the embedded proxy has limited capacity for performing parallel backups.

### Procedure


1. In the **VM Direct Engines** pane of the **Protection Engines** window, click **Add**.
2. In the **Add VM Direct Engines** dialog box, fill out the required fields (marked with an asterisk).

Consider the following:

- Only IPv4 addresses are supported for the **Gateway**, **IP Address**, **Netmask**, and **Primary DNS**.
- If you have added multiple vCenter Server instances, the **vCenter to Deploy** list enables you to choose the vCenter where you want to deploy the VM Direct Engine.

 **NOTICE** Do NOT select the internal vCenter in this step.

- The **ESX Host/Cluster** list enables you to choose on which cluster or ESX host you want to deploy the additional VM Direct Engine.
- The **Network** list shows all the networks that are available under the selected ESX Host/Cluster.
- The **Data Store** list shows all datastores that are accessible to the selected ESX Host/Cluster based on ranking (whether the datastores are shared, local, or NFS), and available capacity (the datastore with the most capacity appearing at the top of the list).
- You can choose the specific datastore on which the VM Direct appliance will reside or leave the default selection of **<automatic>** to enable PowerProtect Data Manager to determine the best location to host the VM Direct appliance.
- The **Transport Mode** list enables you to force using only Hot Add or only Network Block Device (NBD) transport modes or to default to Hot Add mode and fallback to NBD only if Hot Add cannot be used.

 **Note:** When configuring the VM Direct appliance in a VMware Cloud on AWS environment, ensure that you select the transport mode as Hot Add only. VMware Cloud on AWS does not support the NBD transport mode.

### 3. Click **Save**.

The VM Direct appliance is added to the **VM Direct Engines** pane. Note that it may take several minutes before the additional VM Direct appliance is registered in PowerProtect Data Manager. The VM Direct appliance appears in the vSphere Client window.

## Results

When an extra VM Direct appliance is deployed and registered, this appliance is used by PowerProtect Data Manager instead of the embedded VM Direct appliance for any data protection operations involving virtual machine protection policies, unless all added VM Direct appliances are unavailable. If no added VM Direct appliance is available, the embedded VM Direct appliance is used as a fallback to perform limited scale backups and restores. If you do not want to use an added VM Direct appliance, you can disable that proxy. [Additional VM Direct actions](#) on page 109 provides more information.

### After you finish

If the VM Direct appliance deployment fails, review the network configuration of PowerProtect Data Manager in the **System Settings** window to correct any inconsistencies in network properties. After successfully completing the network reconfiguration, you must delete the failed VM Direct appliance and then add the VM Direct appliance in the **Protection Engines** window.

When configuring the VM Direct appliance in a VMware Cloud on AWS environment, if the VM Direct appliance is deployed to the root of the cluster instead of inside the Compute-ResourcePool, you must move the VM Direct appliance inside the Compute-ResourcePool.

## Additional VM Direct actions

For additional VM Direct actions, such as enabling, disabling, redeploying or deleting the VM Direct Engine, use the **Protection Engines** window.

### Disable a VM Direct Engine

You can disable an added VM Direct Engine that you do not currently require for virtual machine backup and recovery. To disable a VM Direct Engine:

1. On the **Protection Engines** window, select the VM Direct Engine that you want to disable from the table in the **VM Direct Engines** pane.

2. In the far right of the **VM Direct Engines** pane, click the three vertical dots.
3. From the menu, select **Disable**.

**Note:** A disabled VM Direct Engine is not used for any new protection activities, and is not automatically upgraded during an PowerProtect Data Manager upgrade.

### Delete a VM Direct Engine

When you disable a VM Direct Engine, the **Delete** button is enabled. If you no longer require the VM Direct Engine, perform the following steps to delete the engine:

1. Select the VM Direct Engine that you want to remove from the table in the **VM Direct Engines** pane.
2. In the far right of the **VM Direct Engines** pane, click the three vertical dots.
3. From the menu, select **Disable**.
4. Click **Delete**.

### Enable a disabled VM Direct Engine

When you want to make a disabled VM Direct Engine available again for running new protection activities, perform the following steps to re-enable the VM Direct Engine.

1. Select the VM Direct Engine that you want to re-enable from the table in the **VM Direct Engines** pane.
2. In the far right of the **VM Direct Engines** pane, click the three vertical dots.
3. From the menu, select **Enable**.

**Note:** If a PowerProtect Data Manager version upgrade occurred while the VM Direct Engine was disabled, a manual redeployment of the VM Direct Engine is also required.

### Redeploy a VM Direct Engine

If a PowerProtect Data Manager software update occurred while a VM Direct Engine was disabled, or an automatic upgrade of the VM Direct Engine did not occur due to network inaccessibility or an environment error, the **Redploy** option enables you to manually update the VM Direct Engine to the current version in use with the PowerProtect Data Manager software. Perform the following steps to manually redeploy the VM Direct Engine.

1. Select the VM Direct Engine that you want to redeploy from the table in the **VM Direct Engines** pane.
2. In the far right of the **VM Direct Engines** pane, click the three vertical dots.
3. If the VM Direct Engine is not yet enabled, select **Enable** from the menu.
4. When the VM Direct Engine is enabled, select **Redploy** from the menu.

The VM Direct Engine is redeployed with its previous configuration details.

## Discovering an application or File System host

After you register an application host with PowerProtect Data Manager, you can use the **Asset Sources** window to discover an application or file system host, and modify the application host credentials.

### About this task

For application hosts, discovery is required if you want to schedule a backup. You must add credentials to the SQL or Oracle database so that PowerProtect Data Manager can access the database to create backups.

## Discover an Oracle or SQL application host

Perform the following steps to discover an Oracle or SQL application host as an asset source in the PowerProtect Data Manager UI.

### Procedure

1. Select **Infrastructure > Asset Sources**.

The **Asset Sources** window appears.

2. Select the **App/File System Host** tab.
3. If you are adding an Oracle or SQL database, select the host entry and click **Edit Credentials**.


The **Edit Credentials** dialog appears.

4. If you are adding credentials for:

- An Oracle database:

Ensure that you specify CredentialType: **tnsName** or **FileName** for DBUSER, RMAN, and WALLET users. If you do not specify **tnsName** or **FileName** Credential Type for DBUSER, RMAN, and WALLET, backups fail. OS user does not require **tnsName** or **FileName** CredentialType.

[Authentication requirements](#) on page 69 provides details about the authentication requirements for an Oracle database.

 **Note:** Credentials that you set at the host level supersede the credentials that you set at the protection policy level.


- A SQL database:

Ensure that you specify the OS credentials for the SQL host. Ensure that these credentials have the rights to perform the Microsoft SQL Server backup and restore operations.

5. Click **Save**.

An entry for the Application Host with the specified information displays as an entry in a table on the **Asset Sources** window.

Discovery time is based on networking bandwidth. The resources that are discovered and those that are doing the discovery take a performance hit each time that you go through a discovery process. It might appear that PowerProtect Data Manager is not updating the Asset Sources data.

 **Note:** Click **Discover** at any time if any additions or other changes to your Asset Sources have taken place outside of the PowerProtect Data Manager environment.

### Results

If the database is properly configured, these application hosts can now be added to a PowerProtect Data Manager protection policy.

## Discover a File System Host

Perform the following steps to discover a File System Host as an asset source in the PowerProtect Data Manager UI.

### Procedure

1. Select **Infrastructure > Asset Sources**.

The **Asset Sources** window appears.

2. Select the **App/File System Host** tab.
3. Select the file system host and click **Discover**.

The **Discover** dialog appears with an option to set the discovery schedule.

4. From the **Discovery Schedule** list, select the time of day to initiate the discovery, or select **Manual** to disable scheduled discovery. You can also select the **Discover Now** checkbox to perform the discovery upon completion of this procedure.

**Note:** From the **App/File System Host** tab, you can click **Discover** at any time if any additions or other changes to your Asset Sources have taken place outside of the PowerProtect Data Manager environment. Asset discovery is also initiated by default after registration of the host to PowerProtect Data Manager and at hourly intervals. Discovery time is based on networking bandwidth. Note that each time you initiate a discovery process, the resources that are discovered and those that are handling the discovery impact system performance.

5. Click **Save**.

### Results

When the File System is configured correctly, it can be added to a PowerProtect Data Manager protection policy.

## Discover a Storage Direct agent host

By default, discovery of the Storage Direct agent host occurs automatically upon approval of the agent in the PowerProtect Data Manager UI. If the Storage Direct agent storage group assets have not yet been discovered, or if you added a storage group after approving the Storage Direct agent, perform the following steps to initiate a manual discovery of the Storage Direct agent host.

### Procedure

1. Select **Infrastructure > Asset Sources**.

The **Asset Sources** window appears.

2. Select the **App/File System Host** tab.

Available agents display in the table with their host name. If an agent has not yet been successfully discovered, the **Discovery Status** displays as **Failed** or **Unknown**.

3. Select the Storage Direct agent host and click **Discover**.

The **Discover** dialog appears with an option to set the discovery schedule.

4. From the **Discovery Schedule** list, select the time of day to initiate the discovery, or select **Manual** to disable scheduled discovery. You can also select the **Discover Now** checkbox to perform the discovery upon completion of this procedure.

**Note:** From the **App/File System Host** tab, you can click **Discover** at any time if any additions or other changes to your Asset Sources have taken place outside of the PowerProtect Data Manager environment. Asset discovery is also initiated by default after registration of the host to PowerProtect Data Manager and at hourly intervals. Discovery time is based on networking bandwidth. Note that each time that you initiate a discovery process, the resources that are discovered and those that are handling the discovery impact system performance.

5. Click **Save**.



## Results

If the Storage Direct agent is properly configured, the storage group assets can now be added to a PowerProtect Data Manager **Storage Group** protection policy.

# Add and discover the SMIS server for the Storage Direct agent

In order to enable protection of data with the Storage Direct agent in PowerProtect Data Manager, the addition of an SMIS server is required. The SMIS server facilitates the discovery of LUNs for the storage groups configured in the VMAX. Perform the following steps to discover the SMIS server as an asset source in the PowerProtect Data Manager UI.

## Procedure

1. Select **Infrastructure > Asset Sources**.

The **Asset Sources** window appears.

2. Select the **SMIS server** tab.

3. Click **Add**.

The **Add SMIS Server** dialog box appears.

4. Provide the name, IP address, and port number of the SMIS server.
5. Under **Host Credentials**, choose an existing entry from the list to use for the SMIS server user credentials, or click **Add** from this list to add new credentials.
6. Click **Verify** to check that the trusted certificate is valid for the specified host.
7. Click **Save**.

An entry appears for SMIS in the table on the **Asset Sources** window.

**Note:** A message does not appear if credential verification for this host was unsuccessful. If the credentials are invalid, the status of the SMIS server entry in the **SMIS Server** tab of the **Infrastructure > Asset Sources** window will indicate **Failed**.

8. Select the checkbox next to the entry and click **Discover** to initiate discovery of the assets, or storage groups, in the VMAX.

**Note:** Asset discovery is also initiated by default after registration of the host to PowerProtect Data Manager, and at daily intervals. Discovery time is based on networking bandwidth. Note that each time that you initiate a discovery process, the resources that are discovered and those that are handling the discovery impact system performance.

When the discovery completes successfully, the **Discovery Status** column updates to **OK**.

## After you finish

PowerProtect Data Manager initiates the automatic discovery of the assets (storage groups) within the VMAX. To verify the discovery of storage groups, go to the **Infrastructure > Assets** window and select the **VMAX Storage Groups** tab. Upon host registration with the PowerProtect Data Manager server, all of the assets for the host (both those currently protected and unprotected) display in the **Assets** window along with the host name.

**Note:** Ensure that you run a **Discover** of the SMIS server each time that you add a LUN to a storage group.



# CHAPTER 9

## Managing Protection Policies

This section includes the following topics:

- [Protection policies](#)..... 116
- [Before you create protection policy](#)..... 118
- [Add a protection policy for virtual machine protection](#)..... 118
- [Add a protection policy for SQL database protection](#)..... 122
- [Add a protection policy for Oracle database protection](#)..... 125
- [Add a protection policy for File System protection](#)..... 129
- [Add a protection policy for Storage Direct protection](#)..... 132
- [Add a Cloud Tier protection policy](#)..... 136
- [Edit a protection policy](#)..... 137
- [Add or remove assets in a protection policy](#)..... 137
- [Removing expired backup copies](#)..... 138
- [Export protection](#) ..... 139
- [Delete a protection policy](#)..... 139
- [Add a Service Level Agreement](#)..... 140
- [Export Asset Compliance](#)..... 142
- [Dynamic filters](#) ..... 143

## Protection policies

Protection policies define sets of objectives that apply to specific periods of time. These objectives drive configuration, active protection, and copy-data-management operations that satisfy the business requirements for the specified data. Each plan type has its own set of user objectives.

Users with the System Admin role can create protection policies.

You can create the following types of protection policies:

- VMware Virtual Machines
- SQL Databases
- Oracle Databases
- File Systems

## Policy retention time considerations

The retention time of the protection copy set is different from the time that was configured in PowerProtect Data Manager.

PowerProtect Data Manager applies an algorithm to determine the duration for which regular and self-service copies must be retained. The retention time for backups is calculated as follows:

- Centralized backups: (start time of current FULL backup) + (schedule period configured in PowerProtect Data Manager) + (retention value from PowerProtect Data Manager configuration) + (padding to midnight)
- Self-service backups: (start time of current FULL backup) + (retention value from PowerProtect Data Manager configuration) + (PowerProtect Data Manager self-service schedule period value) + (padding to midnight), where PowerProtect Data Manager self-service schedule period value = 14 days (default).

### Maximum retention period for protection policy backups

According to the schedule type specified for a protection policy, the following maximum retention periods apply:

- Hourly backups — 31 days
- Daily backups — 31 days
- Weekly backups — 52 weeks
- Monthly backups — 12 months

## Data Domain protection considerations

Read about the following considerations around Data Domain protection policies and PowerProtect Data Manager.

- PowerProtect Data Manager – created Storage Units must not be changed by the Data Domain administrator to set up Storage Units replication.
- PowerProtect Data Manager-created Storage Units must not be configured for cloud tiering.
- When you create a protection policy, PowerProtect Data Manager creates a Data Domain Boost storage unit and assigns a DD Boost user to it. The following limitations apply to the number of supported PowerProtect Data Manager protection policies on the supported Data Domain model to the number of active Data Domain Storage Units.

**Table 21** Supported PowerProtect Data Manager protection policies and Storage Units by Data Domain version

Data Domain System	DD OS Version	Storage Units Supported	Supported configurable concurrently active Storage Units /supported number of PowerProtect Data Manager protection policies
DD9800	6.0 and later	256	256
DD9500	5.7 and later	256	256
DD6800, DD9300	6.0 and later	128	128
DD6300	6.0 and later	100	32
DD990, DD4200, DD4500, DD7200	5.7 and later	128	128
All other DD systems	5.7 and later	100	Up to 32 based on the model
DD9500	5.6	100	64
DD990, DD890	5.3 and later	100	Up to 32 based on the model
DD7200, DD4500, DD4200	5.4 and later	100	Up to 32 based on the model
All other DD systems	5.2 and later	100	Up to 14 based on the model

**Table 22** Supported Storage Units in DDVE by TB

Number TBs in DDVE	Maximum Number of Storage Units	Supported configurable concurrently active Storage Units / supported number of PowerProtect Data Manager protection policies
4 6 8	100	6
32 48	100	14
64 96	100	32

## Before you create a protection policy

Consider the following points before creating a protection policy.

- An asset can only be protected by one policy at a time. If you move assets between different protection policies at some point, ensure that you unconfigure the assets from the current policy before moving them to the new policy.
  - ① **Note:** If an SQL server is also a virtual machine, you can still protect the SQL database with an application-consistent backup without interfering with the SQL agent-based backup.
- Before adding replication to a protection policy, ensure that you add a remote Data Domain system as the replication location. [Add Protection Storage](#) provides detailed instructions about adding a remote Data Domain system.

### Managing backup frequency

To avoid high CPU usage that can lead to failure issues, do not schedule backups more often than recommended in the following table:

Backup type	Minimum frequency recommendation
Archive Log	30 minutes
Differential	6 hours
Incremental Cumulative	12 hours
Full	Daily

## Add a protection policy for virtual machine protection

A protection policy enables you to select a specific group of assets that you want to back up. Use the PowerProtect Data Manager UI to create a virtual machine protection policy.

### Before you begin

Dell EMC recommends to distribute the virtual machine asset protection workload over multiple ESXi hosts so that you do not exceed the ESXi NBD session limit. Note that if the limit is reached, you can manage the workload by deploying an external VM Direct appliance on the host/cluster using Hot Add transport mode.

To create Application Aware protection policies for virtual machines, ensure that:

- You manually update the vmx configuration parameter `disk.EnableUUID` to `True` by using the **vSphere Web Client**.
- The vSphere version that you are running uses a supported version of VMware Tools. Software compatibility information for the PowerProtect Data Manager software is provided in the eLab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.
- The virtual machine has direct access to the Data Domain client.
- The virtual machine uses SCSI disks only, and the number of available SCSI slots matches at least the number of disks.
- The Windows account that is used for the protection policy has both Microsoft Windows administrative rights and Microsoft SQL Server login and sysadmin rights.
- The SQL configuration support is limited to Microsoft SQL Server stand-alone instances and a Microsoft SQL Server Always On availability group (AAG) configured with file share witness. Unsupported configurations include Microsoft SQL Server failover cluster instances that are configured with shared drives, and Microsoft SQL Server cluster-less AAG configurations.


- For Microsoft SQL Server AAG configurations, the database administrator specifies the AAG backup preferences for backup in the Microsoft SQL Server Management Studio (SSMS). These preferences control which AAG node is selected as the preferred node when you perform a transaction log backup of AAG databases.

### Procedure

1. Select **Protection > Protection Policies**.
2. In the **Protection Policies** window, click **Add**.  
The **Add Policy** wizard appears.
3. On the **Type** page, specify the following fields, and then click **Next**:
  - **Name**—Type a descriptive name for the protection policy.
  - **Description**—Type a description for the policy.
  - **Type**—Select **Virtual Machine**, which includes protection for SQL application-aware virtual machines.
4. On the **Purpose** page, select from the following options to indicate the purpose of the new protection policy group, and then click **Next**:
  - **Crash Consistent**—Select this type for point-in-time backup of virtual machines.
  - **Application Aware** —For virtual machines with a SQL application installed, select this type to quiesce the application to perform the SQL database and transaction log backup. When you select this type, you also need to provide Windows account credentials for the virtual machine. You can provide the credentials at the protection lifecycle level and/or the virtual machine asset level. When you provide the credentials at both levels, the virtual machine asset credentials override the policy credentials.
  - **Exclusion**—Select this type if there are virtual machine assets within the protection policy that you plan to exclude from data protection operations.
5. In the **Assets** page, select the unprotected assets that you want to back up as part of this protection policy, and then click **Next**.

If the virtual machines that you want to protect are not listed, do one of the following:

- Click **Find More Assets** to perform an updated asset discovery of the vCenter.
- Use the Search box to search by asset name.
- Select **vCenter Hierarchy** or **All Virtual Machines** from the filter on the right side of the window to display a different view.

 **Note:** When you configure a virtual machine application-aware protection policy to protect a Microsoft SQL Server Always On availability group (AAG), you must add all the virtual machines for that AAG to the same policy, to ensure proper protection. Failure to do so might result in missed transaction log backups.

For the virtual machine application-aware case, the **Assets** page displays a warning about the AAG policy configuration requirement.

6. On the **Schedule** page, click **+ Backup** to create a new schedule.
7. On the **Add Primary Backup** page, specify the backup schedule fields, and then click **OK**:
  - **Recurrence**—Specify how often backups will occur.
  - **Create Copy**—Specify how often to create an incremental backup.
  - **Transaction Log Every**—For application-aware protection policies, specify the interval in minutes for logs to be generated.

**Note:** For Microsoft SQL Server AAG configurations, the database administrator can specify the AAG backup preferences for a transaction log backup in the Microsoft SQL Server Management Studio.

- **Keep For**—Specify the retention period for the backup.
- **Start Time**—Specify the time of day to start initiating backups.
- **End Time**—Specify the time of day to stop initiating backups.

**Note:** Any running backups will complete.

- **Create Full**—Select this option if you want to periodically force a full (level 0) backup, and then specify how often to create these backups. When you select this option, the backup chain is reset.

**Note:** When a new asset is added to a protection policy during a scheduled backup window, the backup starts right away. However, if an asset is added to a protection policy outside of the scheduled backup window, the backup does not start until the next time that backups are configured to run.

If a new asset is added to a protection policy that has a weekly or monthly backup schedule and the current time is within the scheduled **Start Time** and **End Time**, the backup runs right away, regardless of the date. If the current time is not within the scheduled **Start Time** and **End Time**, the backup does not start until the next time that backups are configured to run.

The **Schedule** page updates with the added backup schedule.

**Note:** After completing a backup schedule, you can change any schedule details by selecting the check box next to the added schedule and clicking **Edit**.

8. To extend the latest primary backup copy to long-term retention:
  - a. Select the checkbox next to the added schedule and click **+ Backup**.
  - b. Complete the schedule details in the **Add Promotion Backup** dialog box, and then click **OK**.
9. To replicate these backups to a remote Data Domain system:
  - a. Select the checkbox next to the added schedule and click **Replicate**.
  - b. Complete the schedule details in the **Add Primary Replication** dialog box, and then click **OK**.

**Note:** To enable replication, ensure that you add a remote Data Domain system as the replication location. [Add Protection Storage](#) provides detailed instructions about adding a remote Data Domain system.

10. Select the check box next to the added schedule.
 

When you select the check box, the service level agreement (**SLA**), **Storage Name**, and **Network interface** lists are enabled for selection.
11. From the **SLA** list, select an existing service level agreement that you want to apply to this schedule, or select **Add** to create a SLA within the **Add Backup Service Level Agreement** window.

[Add a new SLA](#) provides instructions.

12. From the **Storage Name** list:
  - Select the backup destination from the list of existing Data Domain systems.



- To add a system, select **Add**, and complete the details in the **Storage Target** window. [Add Protection Storage](#) provides instructions.

When you select the destination storage, the **Space** field updates with the available capacity on the system.

13. Click **Set Storage Quotas** to set storage space restrictions for a Data Domain MTree or Storage Unit to prevent the consumption of excess space. There are two kinds of quota limits—hard limits and soft limits. You can set either a soft or hard limit or both a soft and hard limit. Both values must be integers, and the soft value must be less than the hard value.

**Note:** When you set a soft limit and the limit is reached, an alert is generated but data can still be written to the Data Domain. When you set a hard limit and the limit is reached, data cannot be written to the MTree. Therefore, all data protection operations fail until data is deleted from the MTree. The *Data Domain Operating System Administration Guide* provides more information about MTree quota configuration.

- a. **Capacity Quota** — Controls the total size of pre-compression data written to the Data Domain.
  - b. **Stream Quota** — The number of concurrent streams allowed on the system during data protection operations. Setting a **Stream Quota** limit can help ensure that system performance is not impacted negatively if a data protection operation is consuming too many system resources.
14. Select the **Retention Lock** check box to enable retention locking for these backups on the selected system.

**Note:** Primary backups are assigned a default retention lock period of 14 days. Replicated backups, however, are not assigned a default retention lock period. If you select this check box for a replicated backup, ensure that you set the **Keep For** field in the **Add Primary Replicate** backup schedule dialog to a minimum number of 14 days so that the replicated backup does not expire before the primary backup.

15. From the **Network interface** list, select a network interface card (NIC), if applicable.
16. Click **Next**.

The **Summary** page appears.

17. Review the protection policy group configuration details. Except for the protection policy type, you can click **Edit** next to any completed details to change the protection policy information. When completed, click **Finish**.

An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy. When the new protection policy group is created, PowerProtect Data Manager automatically performs a full backup. For virtual machines, if you have not yet added a VM Direct appliance, the backup is performed using the embedded VM Direct appliance. Subsequent backups are performed according to the schedule specified.


18. Click **OK** to exit the window, or click **Go to Jobs** to open the **Jobs** window to monitor the backup of the new protection policy group.

## On-demand backups of virtual machines

Once virtual assets have been added to a virtual machine protection policy, you can perform on-demand backups of individual virtual machines by using the **Backup Now** functionality in the PowerProtect Data Manager UI.

When a virtual machine is part of an application-aware protection policy, the ad-hoc backup is a full application-aware backup.

To perform an on-demand backup:

1. Select **Infrastructure > Assets**.
2. Select the **Virtual Machines** tab. A list of virtual assets for the discovered vCenter display.
3. Select a virtual machine from the table that has an associated protection policy.
  -  **Note:** You can only select one virtual machine at a time for on-demand backup, and the protection policy associated with this virtual machine cannot be an exclusion policy.
4. Click **Backup Now**. A notification appears indicating whether the request was processed successfully.

## Additional options for managing virtual machine backups

After a virtual machine protection policy backup is complete, additional options such as editing the retention period become available for virtual machine assets backed up as part of the policy.

Select **Infrastructure > Assets**. Select the **Virtual Machines** tab. The table lists the virtual machine assets that were discovered in the vCenter. Select an asset from the table and click **View Copies**. The **Copy Locations** pane identifies where the backups are stored.


In the left pane, click the storage icon to the right of the VM icon, for example, **DD**. The table in the right pane lists the backup copies. Depending on whether the asset is retention locked, you can perform the following functions from this window:

- Edit the retention period for a backup copy — Select a backup copy from the table and click **Edit Retention**.
- Delete a backup copy — If you no longer require one of the backup copies and the retention lock is not enabled for this copy, select the backup copy from the table and click **Delete**.


## Add a protection policy for SQL database protection

Use the PowerProtect Data Manager UI to add a protection policy group for the purposes of SQL database protection.

### About this task

 **Note:** If a database is protected in an Always On availability group, you cannot configure stand-alone backups of that database in a protection policy group.

### Procedure

1. Select **Protection > Protection Policy**.  
The **Protection Policy** window appears.
2. Click **Add**.  
The **Add Policy** wizard appears.
3. In the **Type** page, specify the new protection policies group fields. For example, if you are creating a protection policy for daily backups in the SQL production environment:
  - a. In the **Name** field, specify the name of the protection policy. For example, `SQL Prod Databases`
    -  **Note:** The name that you specify here becomes part of the Data Domain MTree entry.
  - b. In the **Description** field, specify a short description of the protection policy. For example, `SQL Prod Daily Backups`

- c. In the **Type** field, select **Microsoft SQL database**.
- d. Click **Next**.  
The **Purpose** page appears.
4. In the **Purpose** page, specify the following fields to indicate the purpose of the new protection policy group:
  - a. The type of protection policies group.  
For a SQL database, you can select from three types:
    - To use PowerProtect Data Manager to manage all protection centrally, click **Centralized Protection**.
    - To use SQL to create local backup protection, click **Self-Service Protection**. PowerProtect Data Manager creates a protection policy and manages extra stages.
    - If there are SQL assets within the protection policy that you plan to exclude from data protection operations, click **Exclusion**.
  - b. To specify the credentials, click **Set Credentials**. You can specify new credentials or select existing credentials from the list.
  - c. Click **Save**.
  - d. Click **Next**.  
The **Assets** page appears.
5. Select the unprotected assets that you want to add to the backup of this protection policy group. The window enables you to filter by asset name to locate the required assets.
6. Click **Next**.  
If you selected **Exclusion** in the **Purpose** page, the **Summary** page appears. Proceed to the final two steps.  
If you selected **Centralized Protection** or **Self-Service Protection**, the **Schedule** page appears.
7. Click **+ Backup**.  
The **Add Primary Backup** dialog box appears.
8. Specify the backup schedule fields:
  - For Centralized Protection:
    - a. In the **Recurrence** field, select the interval at which the backup job runs within the window that you specify.  
Recurrence relates to **Start Time** and **End Time** fields.  
When you select **Hourly**, **Daily**, **Weekly**, and **Monthly** recurrence, you are selecting the interval at which the backup job runs within the window that you specify.
    - b. In the **Create Full** field, specify the interval in hours to create a full backup.  
The interval should be between 1 hour to 12 hours.
    - c. To create an incremental differential backup, click **Differential**, and then specify the interval in minutes.
    - d. To create a log, click **Log**, and then specify the interval in minutes.
    - e. In the **Keep For** field, specify the retention time.
    - f. In the **Start Time** field, specify the time when new backups are initiated in this policy.
    - g. In the **End Time** field, specify the time after which no new backups are initiated in this policy. It does not mean that any policy that is running is stopped.

h. Click **OK**.

**Note:**

When a new asset is added to a protection policy during a scheduled backup window, the backup starts right away. However, if an asset is added to a protection policy outside of the scheduled backup window, the backup does not start until the next time that backups are configured to run.

If a new asset is added to a protection policy that has a weekly or monthly backup schedule and the current time is within the scheduled **Start Time** and **End Time**, the backup runs right away, regardless of the date. If the current time is not within the scheduled **Start Time** and **End Time**, the backup does not start until the next time that backups are configured to run.

The **Schedule** page updates with the newly added backup schedule.

- For Self-Service Protection:
  - a. In the **Keep For** field, specify the retention time.
  - b. Click **OK**.

After completing a backup schedule, you can change any schedule details by selecting the checkbox next to the added schedule and clicking **Edit**.

9. To reduce the number of backups when daily, weekly, and/or monthly backups coincide, turn on auto promotion:
  - a. Select the checkbox next to the added schedule and click **+ Backup**.
  - b. Complete the schedule details in the **Add Promotion Backup** dialog box, and then click **OK**.
10. To replicate these backups to a remote Data Domain system:
  - a. Select the checkbox next to the added schedule and click **Replicate**.
  - b. Complete the schedule details in the **Add Primary Replication** dialog box, and then click **OK**.

**Note:** To enable replication, ensure that you add a remote Data Domain system as the replication location. [Add Protection Storage](#) provides detailed instructions about adding a remote Data Domain system.

11. Select the check box next to the added schedule.
 

When you select the check box, the **SLA**, **Storage Name**, and **Network interface** lists are enabled for selection.
12. From the **SLA** list, select an existing service level agreement that you want to apply to this schedule, or select **Add** to create a SLA within the **Add Backup Service Level Agreement** window. [Add a Service Level Agreement](#) provides instructions.

13. From the **Storage Name** list:
  - Select the backup destination from the list of existing Data Domain systems.
  - To add a system, select **Add**, and complete the details in the **Storage Target** window. [Add Protection Storage](#) provides instructions.

When you select the destination storage, the **Space** field updates with the available capacity on the system.

14. From the **Network interface** list, select a network interface card (NIC), if applicable.
15. Click **Set Storage Quotas** to set storage space restrictions for a Data Domain MTree or Storage Unit to prevent the consumption of excess space. There are two kinds of quota

limits—hard limits and soft limits. You can set either a soft or hard limit or both a soft and hard limit. Both values must be integers, and the soft value must be less than the hard value.

**Note:** When you set a soft limit and the limit is reached, an alert is generated but data can still be written to the Data Domain. When you set a hard limit and the limit is reached, data cannot be written to the MTree. Therefore, all data protection operations fail until data is deleted from the MTree. The *Data Domain Operating System Administration Guide* provides more information about MTree quota configuration.

- a. **Capacity Quota** — Controls the total size of pre-compression data written to the Data Domain.
  - b. **Stream Quota** — The number of concurrent streams allowed on the system during data protection operations. Setting a **Stream Quota** limit can help ensure that system performance is not impacted negatively if a data protection operation is consuming too many system resources.
16. Select the **Retention Lock** check box to enable retention locking for these backups on the selected system.
 

**Note:** Primary backups are assigned a default retention lock period of 14 days. Replicated backups, however, are not assigned a default retention lock period. If you select this check box for a replicated backup, ensure that you set the **Keep For** field in the **Add Primary Replicate** backup schedule dialog box to a minimum number of 14 days so that the replicated backup does not expire before the primary backup.
  17. Click **Next**.  
The **Summary** page appears.
  18. Review the protection policy group configuration details. You can click **Edit** next to any completed window's details to change any information. When completed, click **Finish**.  
An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy. When a new protection policy is created, PowerProtect Data Manager performs the first full backup and subsequent backups according to the schedule specified.
  19. Click **OK** to exit the window, or click **Go to Jobs** to open the **Jobs** window to monitor the backup of the new protection policy group.

## Add a protection policy for Oracle database protection



Use the PowerProtect Data Manager UI to add a protection policy group for the purposes of Oracle database protection.

### Before you begin

- If you are creating protection policies for RAC databases, ensure that all nodes in the RAC environment are powered on and registered at the time of PLC creation. Otherwise protection may fail.
- You cannot add assets from a single Oracle host in two or more protection policies with the same Data Domain. You must add additional protection policies to a different DD. This is pertaining to issue ECDM-39456.
- For Oracle Instance Group assets, ensure that the maximum length of the hostname plus storage unit is 59. There are no special character limitations. For example, oracle\_database\_department\_123\_accounts.

## Procedure

1. Select **Protection > Protection Policy**.  
The **Protection Policy** window appears.
2. Click **Add**.  
The **Add Policy** wizard appears.
3. In the **Type** page, specify the new protection policies group fields. For example, if you are creating a protection policy for daily backups in the Oracle production environment:
  - a. In the **Name** field, specify the name of the protection policy. For example, `Oracle Prod Databases`.
 

 **Note:** The name that you specify here becomes part of the Data Domain MTree entry.
  - b. In the **Description** field, specify a short description of the protection policy. For example, `Oracle Prod Daily Backups`.
  - c. In the **Type** field, select **Oracle database**.
  - d. Click **Next**.  
The **Purpose** page appears.
4. In the **Purpose** page, specify the following fields to indicate the purpose of the new protection policy group:
  - a. The type of protection policies group.  
For an Oracle database, you can select from three types:
    - To use PowerProtect Data Manager to manage all protection centrally, click **Centralized Protection**
    - To use Oracle to create local backup protection, click **Self-Service Protection**. PowerProtect Data Manager creates a protection policy and manages extra stages.
    - If there are Oracle assets within the protection policy that you plan to exclude from data protection operations, click **Exclusion**.
  - b. To specify the credentials, click **Set Credentials**. You can specify new credentials or select existing credentials from the list.  
[Authentication requirements](#) on page 69 provides details about the authentication requirements for an Oracle database.  
 **Note:** Credentials that you set at the host level supersede the credentials that you set at the protection policy level.
  - c. Click **Next**.  
The **Assets** page appears.
5. Select the unprotected assets that you want to add to the backup of this protection policy group. The window enables you to filter by asset name to locate the required assets.  
Additionally, you can change the assets view to display all assets discovered by PowerProtect Data Manager, or a hierarchical view to display the assets in a tree structure underneath the application host. A hierarchical view might be helpful, for example, if you have added multiple Oracle or SQL databases, so that you can more easily identify which assets belong to which database.

6. Click **Next**.

If you selected **Exclusion** in the **Purpose** page, the **Summary** window appears. Proceed to the final two steps.

If you selected **Centralized Protection** or **Self-Service Protection**, the **Schedule** page appears.

7. Click **+ Backup**.

The **Add Primary Backup** dialog box appears.

## 8. Specify the backup schedule fields:

- For **Centralized Protection**:

- a. In the **Recurrence** field, select the interval at which the backup job runs within the window that you specify.

Recurrence relates to **Start Time** and **End Time** fields.

When you select **Hourly**, **Daily**, **Weekly**, and **Monthly** recurrence, you are selecting the interval at which the backup job runs within the window that you specify.

- b. In the **Create Full (Level 0)** field, specify the interval in hours to create a full backup. The interval should be between 1 hour to 12 hours.
- c. To create an incremental cumulative backup, click **Incremental Cumulative**, and then specify the interval in minutes.
- d. To create an incremental differential backup, click **Incremental Differential**, and then specify the interval in minutes.
- e. To create a log, click **Log**, and then specify the interval in minutes.
- f. In the **Keep For** field, specify the retention time.
- g. In the **Start Time** field, specify the time when new backups are initiated in this policy.
- h. In the **End Time** field, specify the time after which no new backups are initiated in this policy. It does not mean that any policy that is running is stopped.
- i. Click **OK**.

- **Note:**

When a new asset is added to a protection policy during a scheduled backup window, the backup starts right away. However, if an asset is added to a protection policy outside of the scheduled backup window, the backup does not start until the next time that backups are configured to run.

If a new asset is added to a protection policy that has a weekly or monthly backup schedule and the current time is within the scheduled **Start Time** and **End Time**, the backup runs right away, regardless of the date. If the current time is not within the scheduled **Start Time** and **End Time**, the backup does not start until the next time that backups are configured to run.

The **Schedule** page updates with the newly added backup schedule.

- For **Self-Service Protection**:

- a. In the **Keep For** field, specify the retention time.
- b. Click **OK**.

After completing a backup schedule, you can change any schedule details by selecting the checkbox next to the added schedule and clicking **Edit**.

## 9. To reduce the number of backups when daily, weekly, and/or monthly backups coincide, turn on auto promotion:

- a. Select the check box next to the added schedule and click **+ Backup**.

- b. Complete the schedule details in the **Add Promotion Backup** dialog box, and then click **OK**.
10. To replicate these backups to a remote Data Domain system:
  - a. Select the checkbox next to the added schedule and click **Replicate**.
  - b. Complete the schedule details in the **Add Primary Replication** dialog box, and then click **OK**.

**Note:** To enable replication, ensure that you add a remote Data Domain system as the replication location. [Add Protection Storage](#) provides detailed instructions about adding a remote Data Domain system.

11. Select the check box next to the added schedule.  
When you select the check box, the **SLA**, **Storage Name**, and **Network interface** lists are enabled for selection.

12. From the **SLA** list, select an existing service level agreement that you want to apply to this schedule, or click **Add** to create a SLA within the **Add Backup Service Level Agreement** window. [Add a Service Level Agreement](#) provides instructions.

13. From the **Storage Name** list:

- Select the backup destination from the list of existing Data Domain systems.
- To add a system, select **Add**, and complete the details in the **Storage Target** window. [Add Protection Storage](#) provides instructions.

When you select the destination storage, the **Space** field updates with the available capacity on the system.

14. From the **Network interface** list, select a network interface card (NIC), if applicable.
15. Click **Set Storage Quotas** to set storage space restrictions for a Data Domain MTree or Storage Unit to prevent the consumption of excess space. There are two kinds of quota limits—hard limits and soft limits. You can set either a soft or hard limit or both a soft and hard limit. Both values must be integers, and the soft value must be less than the hard value.

**Note:** When you set a soft limit and the limit is reached, an alert is generated but data can still be written to the Data Domain. When you set a hard limit and the limit is reached, data cannot be written to the MTree. Therefore, all data protection operations fail until data is deleted from the MTree. The *Data Domain Operating System Administration Guide* provides more information about MTree quota configuration.

- a. **Capacity Quota** — Controls the total size of pre-compression data written to the Data Domain.
  - b. **Stream Quota** — The number of concurrent streams allowed on the system during data protection operations. Setting a **Stream Quota** limit can help ensure that system performance is not impacted negatively if a data protection operation is consuming too many system resources.
16. Select the **Retention Lock** check box to enable retention locking for these backups on the selected system.

**Note:** Primary backups are assigned a default retention lock period of 14 days. Replicated backups, however, are not assigned a default retention lock period. If you select this check box for a replicated backup, ensure that you set the **Keep For** field in the **Add Primary Replicate** backup schedule dialog box to a minimum number of 14 days so that the replicated backup does not expire before the primary backup.



17. Click **Next**.

The **Summary** page appears.

18. Review the protection policy group configuration details. You can click **Edit** next to any completed window's details to change any information. When completed, click **Finish**.

An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy. When the new protection policy group is created, PowerProtect Data Manager automatically performs a full backup. Subsequent backups are performed according to the schedule specified.

19. Click **OK** to exit the window, or click **Go to Jobs** to open the **Jobs** window to monitor the backup of the new protection policy group.

## Add a protection policy for File System protection

Use the PowerProtect Data Manager UI to add a protection policy for the purposes of File System data protection.

### Before you begin

Review the prerequisites in the section [File System agent prerequisites](#) on page 80

### Procedure

1. Select **Protection > Protection Policies**.


The **Protection Policy** window appears.

2. Click **Add**.

The **Add Policy** window appears.

3. In the **Type** page, specify the new protection policies group fields. For example, if you are creating a protection policy for daily backups in the Windows 2012 Server:

- a. In the **Name** field, specify the name of the protection policy. For example, `File System Prod`

 **Note:** The name that you specify here becomes part of the Data Domain MTree entry.

- b. In the **Description** field, specify a short description of the protection policy. For example, `File System Prod Daily Backups`

- c. In the **Type** field, select **File System**.

- d. Click **Next**.

The **Purpose** page appears.

4. In the **Purpose** page, specify the following fields to indicate the purpose of the new protection policy:

- a. The type of protection policies group.

For File System, you can select from three types:

- To use PowerProtect Data Manager to manage all protection centrally, click **Centralized Protection**
- To use the File System to create local backup protection, click **Self-Service Protection**. PowerProtect Data Manager creates a protection policy and manages extra stages.


- If there are assets within the protection policy that you plan to exclude from data protection operations, click **Exclusion**.

b. Click **Next**.

The **Assets** page appears.

5. Select the unprotected assets that you want to add to the backup of this protection policy group. The window enables you to filter by asset name to locate the required assets.

Additionally, you can change the assets view to display all assets discovered by PowerProtect Data Manager, or a hierarchical view to display the assets in a tree structure underneath the application host. A hierarchical view might be helpful, for example, if you have added multiple File Systems, so that you can more easily identify which assets belong to which host.

 **Note:** PowerProtect Data Manager does not support including CSV and non-CSV volumes in the same protection policy.

6. Click **Next**.

If you selected **Exclusion** in the **Purpose** page, the **Summary** page appears. Proceed to the final two steps.

If you selected **Centralized Protection** or **Self-Service Protection**, the **Schedule** page appears.

7. Click **+ Backup**.

The **Add Primary Backup** dialog box appears.

8. Specify the backup schedule fields:

- For **Centralized Protection**:

- a. In the **Recurrence** field, select the interval at which the backup job runs within the window that you specify.

Recurrence relates to **Start Time** and **End Time** fields.

When you select **Hourly**, **Daily**, **Weekly**, and **Monthly** recurrence, you are selecting the interval at which the backup job runs within the window that you specify.

- b. **Create Copy**—Specify how often to create an incremental backup.

- c. To create a log, click **Log**, and then specify the interval in minutes.

- d. In the **Keep For** field, specify the retention time.

- e. In the **Start Time** field, specify the time when new backups will be initiated in this policy.

- f. In the **End Time** field, specify the time after which no new backup will be initiated in this policy. It does not mean that any policy that is running is stopped at this time.

- g. **Create Full**—Select this option if you want to periodically force a full (level 0) backup, and then specify how often to create these backups. By default, if you do not select this option, all subsequent backups are incremental backups.

 **Note:**

It is not mandatory to create periodic full backups. When you select this option, the File System agent forces the next backup to be a Full Backup. A full backup ensures protection from potential corruption that can be carried over from previous backups. However, these backups require more time and resources.

If you do not select this option, the File System agent identifies changes since the last full backup and uses the previous backup copy to create a new full backup.

h. Click **OK**.

**Note:**

When a new asset is added to a protection policy during a scheduled backup window, the backup starts right away. However, if an asset is added to a protection policy outside of the scheduled backup window, the backup does not start until the next time that backups are configured to run.

If a new asset is added to a protection policy that has a weekly or monthly backup schedule and the current time is within the scheduled **Start Time** and **End Time**, the backup runs right away, regardless of the date. If the current time is not within the scheduled **Start Time** and **End Time**, the backup does not start until the next time that backups are configured to run.

The **Schedule** page updates with the newly added backup schedule.

- For **Self-Service Protection**:
  - a. In the **Keep For** field, specify the retention time.
  - b. Click **OK**.

After completing a backup schedule, you can change any schedule details by selecting the checkbox next to the added schedule and clicking **Edit**.

9. To reduce the number of backups when daily, weekly, and/or monthly backups coincide, turn on auto promotion:
  - a. Select the check box next to the added schedule and click **+ Backup**.
  - b. Complete the schedule details in the **Add Promotion Backup** dialog box, and then click **OK**.
10. To replicate these backups to a remote Data Domain system:
  - a. Select the checkbox next to the added schedule and click **Replicate**.
  - b. Complete the schedule details in the **Add Primary Replication** dialog box, and then click **OK**.

**Note:** To enable replication, ensure that you add a remote Data Domain system as the replication location. [Add Protection Storage](#) provides detailed instructions about adding a remote Data Domain system.

11. Select the check box next to the added schedule.
 

When you select the check box, the **SLA**, **Storage Name**, and **Network interface** lists are enabled for selection.
12. From the **SLA** list, select an existing service level agreement that you want to apply to this schedule, or select **Add** to create a SLA within the **Add Backup Service Level Agreement** window. [Add a Service Level Agreement](#) provides instructions.
13. From the **Storage Name** list:
  - Select the backup destination from the list of existing Data Domain systems.
  - To add a system, select **Add**, and complete the details in the **Storage Target** window. [Add Protection Storage](#) provides instructions.

When you select the destination storage, the **Space** field updates with the available capacity on the system.

14. From the **Network interface** list, select a network interface card (NIC), if applicable.
15. Click **Set Storage Quotas** to set storage space restrictions for a Data Domain MTree or Storage Unit to prevent the consumption of excess space. There are two kinds of quota

limits—hard limits and soft limits. You can set either a soft or hard limit or both a soft and hard limit. Both values must be integers, and the soft value must be less than the hard value.

**Note:** When you set a soft limit and the limit is reached, an alert is generated but data can still be written to the Data Domain. When you set a hard limit and the limit is reached, data cannot be written to the MTree. Therefore, all data protection operations fail until data is deleted from the MTree. The *Data Domain Operating System Administration Guide* provides more information about MTree quota configuration.

- a. **Capacity Quota** — Controls the total size of pre-compression data written to the Data Domain.
  - b. **Stream Quota** — The number of concurrent streams allowed on the system during data protection operations. Setting a **Stream Quota** limit can help ensure that system performance is not impacted negatively if a data protection operation is consuming too many system resources.
16. Select the **Retention Lock** check box to enable retention locking for these backups on the selected system.
 

**Note:** Primary backups are assigned a default retention lock period of 14 days. Replicated backups, however, are not assigned a default retention lock period. If you select this check box for a replicated backup, ensure that you set the **Keep For** field in the **Add Primary Replicate** backup schedule dialog box to a minimum number of 14 days so that the replicated backup does not expire before the primary backup.
  17. Click **Next**.  
The **Summary** page appears.
  18. Review the protection policy group configuration details. You can click **Edit** next to any completed window's details to change any information. When completed, click **Finish**.  
An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy. When the new protection policy is created, PowerProtect Data Manager automatically performs a full backup.
  19. Click **OK** to exit the window, or click **Go to Jobs** to open the **Jobs** window to monitor the backup of the new protection policy group.

## Add a protection policy for Storage Direct protection

Use the PowerProtect Data Manager UI to add a protection policy for the purposes of Storage Direct data protection.

### Before you begin

- Review the prerequisites in the section [Storage Direct agent prerequisites](#) on page 88.
- If you have added a LUN to a storage group since the last SMIS server discovery, run a **Discover** of the SMIS server. [Add and discover the SMIS server for the Storage Direct agent](#) on page 113 provides information.
- Ensure that there is no lock on the VMAX. [Storage Direct agent limitations](#) on page 218 provides information.

### Procedure


1. Select **Protection > Protection Policies**.  
The **Protection Policy** window appears.

2. Click **Add**.

The **Add Policy** window appears.

3. In the **Type** page, specify the new protection policy fields.

- a. In the **Name** field, specify the name of the protection policy. For example, `Storage Direct VMAX Policy`

 **Note:** The name that you specify here becomes part of the Data Domain MTree entry.

- b. In the **Description** field, specify a short description of the protection policy. For example, `Storage Direct VMAX Policy Daily Backups`.

- c. In the **Type** field, select **Storage Group**.

- d. Click **Next**.

The **Purpose** page appears.

4. In the **Purpose** page, specify the following fields to indicate the purpose of the new protection policy:

- a. Select from one of the following options:


- If you are a new Storage Direct user, select **I want PPDM to automatically provision and manage all storage needed to achieve this objective**.
- If you are an existing Storage Direct user, select **I will provision and manage my own storage**.

- b. Click **Next**.

The **Assets** page appears.

5. Select the unprotected storage groups that you want to add to the backup of this protection policy group. Within this page, you can filter by host or asset name to locate the required assets. Ensure that any assets you add to the policy have a host name entry in the **Host** column.

The **Assets** page displays the storage groups attached to the host that are currently unprotected (storage groups that have not been assigned to a protection policy).

 **Note:** If the desired assets do not display, cancel the policy creation and run the Storage Direct host discovery again:

- a. Go to **Infrastructure > Asset Sources**.
- b. Select the **App/File System Host** tab.
- c. Select the Storage Direct agent host and click **Discover**.
- d. Go back to **Protection > Protection Policies** to recreate the protection policy.

6. Click **Next**.

The **Schedule** page appears.

7. Click **+ Backup**.

The **Add Primary Backup** dialog box appears.

8. In the **Keep For** field, specify the retention time, and then click **OK** to exit the dialog.

The **Schedule** page updates with the new details. You can change this information by selecting the check box next to the added schedule and clicking **Edit**.

9. Select the check box next to the added schedule for the primary backup.

If you are a new Storage Direct user, the **Storage Name** and **Network interface** lists and the **Retention Lock** check box are enabled for selection. If you are an existing Storage Direct user, the Data Domain destination is selected automatically and you will not be able to modify the selection. Additionally, the **Retention Lock** check box will be unselected and disabled.

10. From the **Storage Name** list:

- For the primary backup, select a destination from the list of existing Data Domain systems.
- For the replicated backup, select a second destination from the list of existing Data Domain systems.

When you select the destination storage, the **Space** field updates with the available capacity on the system.

11. From the **Network interface** list, select a network interface card (NIC), if applicable.

12. Select the **Retention Lock** check box to enable retention locking for these backups on the selected system.

Primary backups are assigned a default retention lock period of 14 days, so the backup will be locked for 14 days or until expiry of the retention period specified in the **Keep For** field, whichever is less.

13. Click **Set Storage Quotas** to set storage space restrictions for a Data Domain MTree or Storage Unit to prevent the consumption of excess space. There are two kinds of quota limits—hard limits and soft limits. You can set either a soft or hard limit or both a soft and hard limit. Both values must be integers, and the soft value must be less than the hard value.

**Note:** When you set a soft limit and the limit is reached, an alert is generated but data can still be written to the Data Domain. When you set a hard limit and the limit is reached, data cannot be written to the MTree. Therefore, all data protection operations fail until data is deleted from the MTree. The *Data Domain Operating System Administration Guide* provides more information about MTree quota configuration.

- a. **Capacity Quota** — Controls the total size of pre-compression data written to the Data Domain.
- b. **Stream Quota** — The number of concurrent streams allowed on the system during data protection operations. Setting a **Stream Quota** limit can help ensure that system performance is not impacted negatively if a data protection operation is consuming too many system resources.

14. To reduce the number of backups when daily, weekly, and/or monthly backups coincide, turn on auto promotion:

- a. Select the checkbox next to the added schedule and click **+ Backup**.
- b. Complete the schedule details in the **Add Promotion Backup** dialog box, and then click **OK**.

15. To replicate the primary backup to a secondary Data Domain system:

- a. Select the checkbox next to the added schedule and click **Replicate**. The **Add Primary Replication** dialog box appears, indicating that MTree replication will be added for replication of the backup to a secondary Data Domain system.

**Note:** The retention period used will be the same **Keep For** value that you specified for the backup schedule.

- b. Click **OK**.

**Note:** To enable replication, ensure that you add a second Data Domain system for use as the replication location. [Add Protection Storage](#) provides detailed instructions about adding a secondary or remote Data Domain system.

16. Click **Next**.

The **Summary** page appears.

17. Review the protection policy configuration details. You can click **Edit** next to any completed window's details to change any information. When completed, click **Finish**.

An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy.

18. Click **OK** to exit the window, or click **Go to Jobs** to open the **Jobs** window to monitor the backup of the new protection policy group.

The **Jobs** window breaks down the **Storage Group** protection by VMAX storage group. Click the link next to the storage group to open the **Details** pane, where you can view more specific information about the job tasks, such as:

- Creation of vDisks in the Data Domain and creation of backup and recovery storage groups.
- Encapsulation, which involves creating backup and restore FTS devices on the VMAX and linking the Data Domain vDisk with FTS.
- Creation of the initial snapshot backup, and linking of the snapshot to the protection storage group.
- Notification that a new configuration file has been pushed to the host.
- If replication was selected, notification that a job for MTree replication also was initiated.

Job tasks will vary depending on whether you are a new user or an existing Storage Direct user.

### After you finish

Execute the `protectpoint snapbackup create` command to perform the self-service backup. This command uses the configuration file that is created automatically upon the addition of storage groups to a **Storage Group** protection policy. The configuration file provides information about the VMAX and Data Domain system attributes and the storage groups being protected by this policy.

You can access the configuration file, for example, `VMAXPolicy1.config`, by navigating to the `C:\Program Files\DPSAPPS\ppfsagent\config` directory. The file name will contain the name you provided for the **Storage Group** policy.

**Note:** Do not make any changes to this configuration file.

Before executing the backup command, run the following command for the host to verify snapshots will be created for each storage group in the protection policy, and to ensure that a successful relationship has been established between the source device and the backup FTS device for movement of data from the VMAX to Data Domain.

```
symsnapvx - sid xxx -sg storage group name list
```

An **X** in the Flags section of this output, as shown in the following, indicates that the relationship has been established without any issues.

**Figure 6** Storage group list command output

```

\Users\Administrator>symnapox -sid 638 -sg sdm_..._SG3 list
page Group (SG) Name      : sdm_..._SG3
  Symmetrix ID           : 000196700638 (Microcode Version: 5977)

#
# Snapshot Name          Num   Flgs   Last Snapshot Timestamp
# Genes  FLRG TS
#-----
:07 PROTECTPOINT_SNAP_1564507274 1 .X.. .. Tue Jul 30 22:51:28 2019
:08 PROTECTPOINT_SNAP_1564507274 1 .X.. .. Tue Jul 30 22:51:28 2019

sgs:
[F]ailed      : X = Failed, . = No Failure
[L]ink        : X = Link Exists, . = No link Exists
[R]estore     : X = Restore Active, . = No Restore Active
[G]CM        : X = GCM, . = Non-GCM
[T]ype       : Z = zDP snapshot, . = normal snapshot
[S]ecured    : X = Secured, . = Not Secured

\Users\Administrator>_
  
```

Once the snapshot(s) and relationship are verified, you can run the following command to perform the self-service backup. Note that this command example is from a Windows system.

```

C:\Program Files\DPSAPPS\ppfsagent\config>protectpoint snapbackup create
description "Backup using sdm configuration" VMAX policy name.config
  
```

Upon successful completion of the backup, output similar to the following displays:

**Figure 7** Snapbackup command output

```

C:\Program Files\DPSAPPS\ppfsagent\config>protectpoint snapbackup create description "Backup using sdm configuration" config-file sp3.config
= Using VMAX configuration file "C:\Program Files\DPSAPPS\ppfsagent\config\sp3.config" ***
connecting to the configured Data Domain system, which may take some time.
creating snapshot.
snapshot is created.
successfully created the catalog record for backup ID 1564507049.
snapshot is completed. Starting the backup of backup ID '1564507049'.
updated the catalog record for DD '...' backup ID '1564507049' from state 'snap-ready' to 'in-progress'.
creating the backup with backup ID '1564507049'.
this command may take a long time to complete.
backup is completing for the host '...'.
backup created.
updated the catalog record for DD '...' backup ID '1564507049' from state 'in-progress' to 'complete'.
backup ID is 1564507049.
  
```

## Add a Cloud Tier protection policy

Add a protection policy for backups to cloud tier.

### Before you begin

Ensure that a Data Domain system is set up for cloud tiering. See [Add Data Domain cloud protection storage](#) on page 41.

### About this task

You can add a Cloud Tier protection policy for Self-Service protection by using a promotion backup schedule. For primary self-service protection, the Cloud Tier option is disabled.

### Procedure

1. Log in to PowerProtect Data Manager with administrator credentials.
2. Select **Protection > Protection Policies > Add**.
3. On the **Type** page, enter a name and description, select the type of system to back up, and click **Next**.
4. On the **Purpose** page, select the purpose (**Application Consistent**, **Application Aware**, or **Exclusion**).
5. On the **Assets** page, select the assets to be protected with this policy and click **Next**.
6. On the **Schedule** page, select **Backup**.
7. On the **Add Primary** page, set the following parameters, and then click **OK**:



- **Recurrence**—Cloud Tier backup requires a minimum of 2 weeks.
  - **Keep for**—Cloud Tier backup requires a minimum of 2 weeks.
  - Optionally, change the **Start Time** and/or **End Time**.
8. Select the protection policy that you created and select **Cloud Tier**.
  9. In the **Add Cloud Tier** dialog box, set the following parameters and then click **OK**:
    - Select the appropriate target from the **Cloud Target** list.
    - For **Tier After**, set a time of at least 2 weeks.

The Cloud Tier protection policy is created.

10. Click **Next**, verify the information, and then click **Finish**.


A new job is created, which you can view under the **Jobs** tab after the job completes.

## Edit a protection policy

Use the PowerProtect Data Manager UI to edit a protection policy name, description, or schedule.

### About this task

You can also edit a protection policy to add or remove assets. You cannot, however, modify a protection policy type or purpose. [Add or remove assets in a protection policy](#) on page 137 provides instructions.

 **Note:** You cannot remove assets from a **VMAX Storage Group** policy.

### Procedure

1. Select **Protection > Protection Policy**.  
The **Protection Policy** window opens.
2. Select the protection policy that you want to modify, and click **Edit**.  
The **Edit Policy** window opens on the **Summary** page.
3. In the **Name**, **Description**, or **Schedule** rows, click **Edit**.  
The **Edit Policy** window displays the appropriate page according to your selection. For example, if you click **Edit** next to the **Name** or **Description** rows, the **Type** page opens.
4. After making your changes, click **Next** to save the changes and go to the **Summary** page.
5. On the **Summary** page, click **Finish**  
An informational dialog displays.
6. Click **OK** to exit the dialog, or click **Go to Jobs** to open the **Jobs** window to monitor the backup of the new protection policy.

## Add or remove assets in a protection policy

Use the PowerProtect Data Manager UI to add or remove an asset in a protection policy.

### About this task

When a protection policy is edited and new assets are added, backups for the new assets start from the next scheduled FULL backup job for the protection policy.

### Procedure

1. Select **Protection > Protection Policy**.  
The **Protection Policy** window appears.
2. Select the protection policy that you want to modify, and click **Edit**.  
The **Edit Policy** window opens on the **Summary** page.
3. In the **Assets** row, click **Edit**.  
The **Assets** page appears.
4. To add an asset to the protection policy, click **+ Add**.  
The **Add Unprotected Assets** dialog displays any assets that are unprotected.
5. Select the unprotected assets that you want to add to the policy, and click **Add**.  
The added assets now appear in the table on the **Assets** page.
6. To remove assets, select the assets that you want to remove from the backup of this protection policy, and click **Delete**.  
The window enables you to filter by asset name to locate the required assets. You can change the assets view to display all assets that are discovered by PowerProtect Data Manager.
7. Click **Next** to save the changes and go to the **Summary** page.
8. In the **Summary** page, click **Finish**  
An informational dialog box appears.
9. Click **OK** to exit the dialog box, or click **Go to Jobs** to open the **Jobs** window to monitor the backup of the new protection policy.

## Removing expired backup copies


PowerProtect Data Manager deletes the backup copies of an asset automatically when the retention period of the copy expires.

Information about retention periods for each type of policy schedule is provided in the section [Policy retention time considerations](#) on page 116.

In order for an expired copy to be deleted, the asset must be managed by PowerProtect Data Manager and in one of the following states:

- **Protected** – The asset is currently assigned to a protection policy.
- **Previously Protected** – The asset has been unassigned from a protection policy and has not yet been re-assigned to another policy.

The automatic deletion is performed during the **Manage Copies** job, which consists of a batch of tasks for all assets in the policy.

 **Note:** For virtual machine assets, you can also manually delete a backup copy at any time from the **Assets** window if you no longer require the copy and the retention lock is not enabled. [Additional options for managing virtual machine backups](#) on page 122 provides more information.

## Export protection

This option enables you to export protection jobs and compliance records to a .CSV file so that you can download an Excel file of protection results data.

### Procedure

1. Select **Protection > Protection Policy**.

The **Protection Policy** window appears, which displays the following information:

- Asset type
- Purpose
- Group Name
- Number of Protected Assets
- Asset Capacity
- Number of Failures
- Number of SLA Violations

2. Select the protection policy for which you would like to export the protection records.

If you do not select a protection policy, PowerProtect Data Manager exports the protection records for all the protection policies.

3. Click **Export**.

The **Export Asset Protection** window appears.

4. Specify the following fields for the export:

- a. The **Time Range**.

The default is **Last 24 hours**.

This refers to the last complete midnight-to-midnight 24-hour period; that is, yesterday. So, any events that have occurred since the most recent midnight are not in the CSV export. For example, if you run the CSV export at 9am, any events that have occurred in the last 9 hours are not in the CSV export. This is to prevent the overlapping of or partial exporting when queried mid-day on a regular or irregular basis.

- b. The **Job Status**.

- c. Click **Download .CSV**.

If applicable, the navigation window appears for you to select the location to save the CSV file.

5. If applicable, save the .CSV file in the desired location and then click **Save**.

## Delete a protection policy

You can delete a protection policy that is not protecting any assets.

### Before you begin

If the policy you want to delete is protecting assets, you must associate those assets with a different protection policy before you can delete the policy.

### About this task

Use the PowerProtect Data Manager UI to delete a protection policy.

### Procedure

1. Select **Protection > Protection Policy**.
2. Select the policy you want to delete and click **Delete**.

## Add a Service Level Agreement

The **SLA Compliance** window in the PowerProtect Data Manager UI enables you to add a service level agreement (SLA) that identifies your Service Level Objectives (SLOs). You use the SLOs to verify that your protected assets are meeting the Service Level Agreements (SLAs).

### Procedure

1. Select **Protection > SLA Compliance**.

The **SLA Compliance** window displays with the following information:

- SLA Name
- Stage Type
- Policies At Risk
- Objectives Out of Compliance
- Impacted Assets

2. Select the type of asset for which you want to add the SLA, and click **Add**.

The **Add Service Level Agreement Type** window appears.

3. Select the type of SLA that you want to add, and then click **Next**.

- **Policy**. If you choose this type, go to step 4
- **Backup**. If you choose this type, go to step 5.
- **Promotion**. If you choose this type, go to step 6.
- **Replication**. If you choose this type, go to step 7.

You can select only one type of Service Level Agreement.

4. If you selected **Policy**, specify the following fields regarding the purpose of the new Policy SLA:

- a. The **SLA Name**.
- b. If applicable, select **Minimum Copies**, and specify the number of Backup and Replication.
- c. If applicable, select **Maximum Copies**, and specify the number of Backup and Replication.
- d. If applicable, select **Available Location** and select the applicable locations. To add a location, click **Add Location**.

Options are:

- **In**—Include locations of all copies in the SLO locations. Does not require every SLO location to have a copy.
- **Must In**—Include locations of all copies in the SLO locations. Requires every SLO location to have at least one copy.
- **Exclude**—Locations of all copies must be other than SLO locations.

- e. Click **Finish** and go to step 9.
5. If you selected **Backup**, specify the following fields regarding the purpose of the new Backup SLA:
- a. The **SLA Name**.
  - b. If applicable, select **Recovery Point Objective (RPO)**, and then set the duration. The purpose of a RPO is business continuity planning, and refers to the maximum targeted period in which data (transactions) might be lost from an IT service due to a major incident.
 

**Note:** You can select only **Recovery Point Objective** to configure as an independent objective in the SLA, or select both **Recovery Point Objective** and **Compliance Window**. If you select both, the RPO setting must be one of the following:

    - Greater than 24 hours or more than the Compliance window duration, in which case RPO validation will occur independent of the Compliance Window.
    - Less than or equal to the Compliance Window duration, in which case RPO validation will occur within the Compliance Window.
  - c. If applicable, select **Compliance Window**, and then set the duration, which refers to the time it takes to create the backup copy. Ensure that the **Start Time** and **End Time** of backup copy creation falls within the Compliance Window duration specified.
 

These are the times in which you can expect the specified activity to take place. Any specified activity that occurs outside of this **Start Time** and **End Time** triggers an alert.
  - d. If applicable, select the **Verify expired copies are deleted** option.
 



**Verify expired copies are deleted** is a compliance check to see if PowerProtect Data Manager is deleting expired copies. This option is disabled by default.
  - e. If applicable, set the Retention Time Objective, and specify the number of Days, Months, Weeks or Years.
  - f. If applicable, select the **Verify Retention Lock is enabled for all copies** option. This option is disabled by default.
  - g. Click **Finish**, and go to step 9.
 

The **SLA Compliance** window appears with the newly added SLA.
6. If you selected **Promotion**, specify the following fields regarding the purpose of the new Promotion SLA:
- a. The **SLA Name**.
  - b. If applicable, specify the Recovery Point Objective.
  - c. If applicable, select the **Verify expired copies are deleted** option.
 

**Verify expired copies are deleted** is a compliance check to see if PowerProtect Data Manager is deleting expired copies. This option is disabled by default.
  - d. If applicable, set the Retention Time Objective, and specify the number of Days, Months, Weeks or Years.
  - e. If applicable, select the **Verify Retention Lock is enabled for all copies** option. This option is disabled by default.
  - f. Click **Finish**, and go to step 9.
 

The **SLA Compliance** window appears with the newly added SLA.

7. If you selected **Replication**, specify the following fields regarding the purpose of the new Replication SLA:
  - a. The **SLA Name**.
  - b. If applicable, select the **Compliance Window**, and specify the **Start Time** and **End Time**.  
These are the times which are permissible and in which you can expect the specified activity to take place. Any specified activity that occurs outside of this start time and end time triggers an alert.
  - c. If applicable, select the **Verify expired copies are deleted** option.  
**Verify expired copies are deleted** is a compliance check to see if PowerProtect Data Manager is deleting expired copies. This option is disabled by default.
  - d. If applicable, set the Retention Time Objective, and specify the number of Days, Months, Weeks or Years.
  - e. If applicable, select the **Verify Retention Lock is enabled for all copies** option. This option is disabled by default.
  - f. Click **Finish**, and go to step 9.  
The **SLA Compliance** window appears with the newly added SLA.
8. Add the newly added SLA to the protection policy. Select **Protection > Protection Policy**.
9. In the **Schedule** section of the **Summary** window, click **Edit**.
10. Do one of the following, and then click **Next**:
  - Select the newly added Policy SLA from the **Set Policy Level SLA** list.
  - Create and add the new SLA policy from the **Set Policy Level SLA** list.
 The **Summary** window appears.
11. Click **Finish**.  
An informational message appears to confirm that PowerProtect Data Manager has saved the protection policy.
12. Click **Go to Jobs** to open the **Jobs** window to monitor the backup and compliance results, or click **OK** to exit.
 

 **Note:** Compliance checks occur automatically every day at 2 am Coordinated Universal Time (UTC).
13. In the **Jobs** window, click  next to an entry to view details on the SLA Compliance result.

## Export Asset Compliance

This option enables you to export compliance records to a CSV file so that you can download an Excel file of compliance results data.

### Procedure

1. Select **Protection > SLA Compliance**.

The **SLA Compliance** window appears. The PowerProtect Data Manager **SLA Compliance** window displays the following information:

- SLA Name
- Stage Type

- Policies At Risk
  - Objectives Out of Compliance
  - Impacted Assets
2. Select the SLA for which you would like to export the compliance records.
  3. Click **Export Asset Compliance**.  
The **Export Asset Compliance** window appears.
  4. Specify the following fields for the export:
    - a. The **Time Range**.  
The default is **Last 24 hours**.  
  
This refers to the last complete midnight-to-midnight 24 hour period; that is, yesterday. So, any events that have occurred since the most recent midnight are not included in the CSV export. For example, if you run the CSV export at 9am, any events that have occurred in the last 9 hours are not included in the CSV export. This is to prevent the overlapping of or partial exporting when queried mid-day on a regular or irregular basis.
    - b. The **Job Status**.
    - c. Click **Download .CSV**.  
  
If applicable, the navigation window appears for you to select the location to save the CSV file.
  5. If applicable, save the CSV file in the desired location and click **Save**.

## Dynamic filters

Dynamic filters enable you to automatically determine which assets are assigned to protection policies when the assets are discovered, based on the filter's rule definitions (rules for inclusion).

When you define a dynamic filter for a protection policy, note the following requirements:

- A protection policy must exist prior to creating the dynamic filter.
- An asset can only belong to one protection policy.
- Virtual machine tags created in the **vSphere Client** can only be applied to a dynamic filter.
- To ensure the protection of homogeneous assets, the dynamic filter must specify a storage asset type.
- A virtual machine application-aware protection policy that protects a Microsoft SQL Server Always On availability group (AAG) must include all the virtual machines of the AAG in the same protection group. Failure to meet this requirement might result in Microsoft SQL Server transaction log backups being skipped. Ensure that the dynamic filters are designed to include all the AAG virtual machines.

## Creating virtual machine tags in the vSphere Client

Creating virtual machine tags in the **vSphere Client** is supported by PowerProtect Data Manager with vSphere versions 6.5 and later. Tags enable you to attach metadata to the virtual assets in the vSphere inventory, which makes assets easier to sort and search for when creating a protection policy.

Asset inclusion in a PowerProtect Data Manager protection policy is based on the filtering criteria applied to user-defined rules that you specify when creating a dynamic filter.

When you create a tag in the **vSphere Client**, the tag must be assigned to a category in order to group related tags together. When defining a category, you can specify the object types to which


the tags will be applied and whether more than one tag in the category can be applied to an object. Within a single rule, you can apply up to 50 rule definitions to tags and categories, as shown in the following example where *Category* is the category name and *Bronze* is the tag name:

- Category: *Category1*, Tag: *Bronze1*
- Category: *Category2*, Tag: *Bronze2*
- Category: *Category3*, Tag: *Bronze3*
- ... Category: *Category50*, Tag: *Bronze50*

In the above example, category names and tag names that exceed 9 or 7 characters respectively, reduce the limit for rule definitions in a single rule to less than 50. When rule definitions exceed the maximum limit, no virtual machines are backed up as part of the group, because no members are associated with the group. As a best practice, keep the number of rule definitions within a single rule to 10 or fewer and, in cases where there are a large number of rule definitions within a single rule, keep the number of characters in category or tag names to 10 or fewer.

To view existing tags for vCenter in the **vSphere Client**, select **Menu > Tags & Custom Attributes**, and then select the **Tags** tab. Click a tag link in the table to view the objects associated with this particular tag.

For PowerProtect Data Manager to include tagged assets in a dynamic filter based on the tags created for the vCenter, you must assign at least one tag to at least one virtual machine. Note that tags associated with containers of virtual machines (for example, a virtual machine folder) are not currently supported for tag associations to assets.

 **Note:** Once virtual machines are associated with tags, the association is not reflected in the PowerProtect Data Manager UI until the timeout period has completed. The default timeout to fetch the latest inventory from vCenter is 15 minutes. When adding a dynamic filter and using tags as the asset filter, you must select **VM Tags**.

## Add a dynamic filter

Use the PowerProtect Data Manager UI to add dynamic filters. When an asset meets the filter conditions, the asset is automatically assigned to the protection policy that you define for the dynamic filter.

### Before you begin

#### Procedure

1. Select **Protection > Dynamic Filter**.

The **Dynamic Filter** window appears, which displays the following information:

- Dynamic Filter Name
- Priority
- Asset Filter
- Assigned Protection Policy

2. Click the **Virtual Machines**, **SQL Databases**, **Oracle Databases**, or **File System** tab to select the type of host for which you would like to add the dynamic filter, and then click **Add**.

The **Add Dynamic Filter** wizard opens on the **Protection Policy** page.

3. Select the target protection policy for the dynamic filter and click **Next**.

The **Asset Filter** page appears.

4. Specify the following fields to indicate the purpose of the new Dynamic Filter:



- a. **Name** For example, `SQL Rules Prod Finance`
- b. **Description** For example, `SQL Rules Prod Servers Finance`.

**Field:**

Using the three fields, build an asset filter that matches your purpose.

- From the list in the first field, select an asset name (such as Datacenter Name), characteristic (such as asset size), or a tag (VM Tags) that will be used as the rule criteria when searching for assets.
- From the list in the second field, select the matching criteria. For an asset name, you can select from several options including **Begins with**, **Ends with**, **Contains**, or **Equals**. For an asset characteristic such as size, you can select **Greater than** or **Less than**. For a virtual machine tag, you can only select **Includes**.
- In the third field, type a search phrase to apply to the rule criteria to determine a match.

For example, a rule with the filters `SQL Server Instance Name`, `Contains`, and `Finance` helps you create a rule to match the assets in your finance department to the selected protection policy.

- c. Click **Apply**.

Any asset that matches the rule and is not currently included in a PowerProtect Data Manager protection policy displays in the **Unprotected Assets matching filter** table

- d. Verify that the asset(s) that display in the **Unprotected Assets matching filter** table are the assets that you want to include in the protection policy. If not, clear the filter to view all unprotected assets and build your filter again.
- e. Click **Next**.

The **Summary** page appears.

5. Click **Finish**.

**Results**

The dynamic filter is run automatically upon creation.

**Manually run a dynamic filter**

PowerProtect Data Manager automatically runs dynamic filters when new assets are detected or when existing assets are modified. You can also run dynamic filters on demand.

**Procedure**

1. Select **Protection > Dynamic Filter**.

The **Dynamic Filter** window appears, which displays the following information:

- Dynamic Filter Name
- Priority
- Asset Filter
- Assigned Protection Policy

2. Select the desired dynamic filter(s) and click **Run**.

PowerProtect Data Manager runs all dynamic filters of the current asset type.

## Edit or delete a dynamic filter

Use the PowerProtect Data Manager UI to edit a dynamic filter. You can change the filter name, description, the filter itself, and the associated protection policy.

### Procedure

1. Select **Protection > Dynamic Filter**.

The **Dynamic Filter** window appears, which displays the following information:

- Dynamic Filter Name
- Priority
- Asset Filter
- Assigned Protection Policy

2. Select a dynamic filter and click **Edit**.

The **Summary** window appears.

3. To edit the name or description of the dynamic filter, modify the desired fields and click **Finish**.
4. To delete a dynamic filter, select the dynamic filter and click **Delete**.

When you click **Delete**, PowerProtect Data Manager will remove the assets that you added by dynamic filters. PowerProtect Data Manager will add those assets again if you do not update related dynamic filters.

## Change the priority of the existing dynamic filter

Use the PowerProtect Data Manager UI to change the priority of a dynamic filter.

### About this task

When multiple dynamic filters exist, you can define the priority of the dynamic filter. Priority determines which dynamic filter PowerProtect Data Manager applies for an asset if an asset matches multiple dynamic filters, and if the matching dynamic filters have conflicting actions. For example, if an asset protection policy assignment matches several dynamic filters and each dynamic filter specifies a different protection policy assignment, the protection policy is determined by the dynamic filter with the highest priority.

An integer is used to represent the priority of the dynamic filter. The smaller value has the higher priority.

### Procedure

1. Select **Protection > Dynamic Filter**.

The **Dynamic Filter** window appears, which displays the following information:

- Dynamic Filter Name
- Priority
- Asset Filter
- Assigned Protection Policy

2. To change a dynamic filter's priority, select the dynamic filter and click **Up** or **Down**.

The smaller value has the higher priority.

# CHAPTER 10

## Restoring Data and Assets

This section includes the following topics:

- [View copies](#) ..... 148
- [Restore a virtual machine or VMDK](#) ..... 148
- [Restore an application-aware virtual machine backup](#) ..... 159
- [Performing centralized restore of a File System host](#) ..... 159
- [Restore of Storage Direct backups in PowerProtect Data Manager](#) ..... 161
- [Restore the PowerProtect Data Manager server](#) ..... 162
- [Restore operations for cloud tier](#) ..... 163

## View copies

You can view summaries of protected copy sets in the system. PowerProtect Data Manager displays details such as the name of the storage system that contains the copy set, system usage, location, date the copy set was created, date the copy set expires, size, and recovery time.


### Procedure

1. From the PowerProtect Data Manager UI, select **Infrastructure > Assets**. Alternatively, select **Recovery > Assets**.

All the assets in the system display.

2. Select an asset, or select one of the following tabs to view assets by type:
  - **Virtual Machines.**
  - **Oracle Databases.**
  - **SQL Databases.**
  - **File System.**
  - **VMAX Storage Groups.**

The entire list of assets that are associated with this type displays in the right pane.

 **Note:** You can also search for assets by name.

3. To view more details, select an asset and click **View copies**.

The copy map consists of the root node and its child nodes. The root node in the left pane represents an asset, and information about copy locations displays in the right pane. The child nodes represent storage systems. When you click a child node, the right pane displays the storage system where the copy is stored, the number of copies, and details of each copy, including the time that each copy was created, the size of the copy, the backup type, and the retention time.

## Restore a virtual machine or VMDK

After virtual assets are backed up as part of a virtual machine protection policy in the PowerProtect Data Manager UI, you can perform image-level and file-level recoveries from individual or multiple virtual machine backups, and also restore individual virtual machine disks (VMDKs) to their original location.

All types of recoveries are performed from the **Recovery > Assets** window. Recovery options include the following:

- **Restore and Overwrite Original VM:** Restore to the original virtual machine.
- **Restore Individual Virtual Disks:** Restore select virtual disks to the original location.
- **Create and Restore to New VM:** Restore to a new virtual machine.
- **Instant Access VM:** Instant access to the virtual machine backup for browse and restore.
- **File Level Restore:** Restore individual files/folders the original or a new virtual machine
- **Direct Restore to ESXi:** Recover the virtual machine directly to an ESXi host without a vCenter server.

The **Restore** button, which launches the **Restore** wizard, is disabled until you select one or more virtual assets in the **Recovery > Assets** window. Selecting multiple assets disables the **View Copies** button, since this functionality is available within the first page of the **Restore** wizard.

To access the **Restore and Overwrite Original VM**, **Create and Restore to New VM**, and **Instant Access VM** recovery types, or the **Restore Individual Virtual Disks** option, select one or more virtual assets and then click **Restore** to launch the **Restore** wizard.

To access the **File Level Restore** and **Direct Restore to ESXi** recovery options, select a virtual asset and then click **View Copies**.

In both instances, you must select a backup copy in the first page of the **Restore** wizard before you can go to the **Options** page, which displays the available recovery options.

**Note:** For all options, recovery in the PowerProtect Data Manager UI can only be performed if the backup or replica is on a Data Domain system. If a replica backup does not exist on such storage, you must manually replicate this backup to Data Domain storage before performing the restore.

The following sections describe each recovery option and provide instructions to perform the recovery.

**Note:** SQL virtual machine full database and transaction log restore from application-aware virtual machine protection policies must be performed using Microsoft application agent tools. The section [Restore an application-aware virtual machine backup](#) provides more information.

## Prerequisites to restore a virtual machine

Review the following requirements before you restore a virtual machine in PowerProtect Data Manager:

- Users who want to perform a virtual machine restore must have **Admin** or **Export and Recovery Admin** privileges. Go to **Administration > Roles** and review the user profile to ensure that the user has the appropriate privileges. A user with the role "User" cannot perform a restore.
- Ensure that you have added the Data Domain system, the Data Domain Management Center (DDMC) or Data Domain Virtual Edition (DDVE), and the vCenter server, and that the protection of virtual machine copies has completed successfully. To check, go to **Infrastructure > Assets** and **Infrastructure > Asset Sources**.
- Ensure that protection of the virtual machines completed successfully. If the virtual machines have been backed up by a protection policy, the assets appear in the **Recovery > Assets** window.
- If performing a restore to a new location, ensure that sufficient space is available on the target datastore.
- Verify that the virtual machine copy that is selected for restore has not expired.

## Restore to original virtual machine

A Restore to the original virtual machine, also referred to as **Restore and Overwrite Original VM**, recovers a virtual machine backup to its original location on the vCenter, rolling the virtual machine(s) that you backed up with the protection policy in PowerProtect Data Manager to an earlier point in time. Use this process for restoring the production system.

### Before you begin

Review [Prerequisites to virtual machine restore](#) before you perform the following procedure.

### About this task

**Note:** If the original virtual machine was deleted, a **Restore and Overwrite Original VM** recovery attempts to re-create the virtual machine. However, if the original virtual machine

resources such as the datastore and cluster are no longer available, the restore fails and a **Restore to New** is required.

### Procedure

1. In the PowerProtect Data Manager UI, select **Recovery > Assets** and select the **Virtual Machines** tab.

The **Recovery** window displays all virtual machines available for recovery.


2. Select the checkbox next to the appropriate virtual machines and click **Restore**.

You can also use the filter in the **Name** column to search for the name of the specific virtual machine.

The **Recovery** wizard appears.

3. On the **Select Copy** page, for each virtual machine that is listed in the table, select the radio button next to the virtual machine and click **Choose Copy**.

The **Choose Copy** dialog box appears.

 **Note:** If you click **Next** without choosing a copy, the most recent backup copy is used.

4. If the backup is on a Data Domain system, click **DD**, and then select from one of the available copies that display in the table.
5. Click **OK** to save the selection and exit the dialog, and then click **Next**.
6. On the **Purpose** page, select **Restore Entire VMs** to restore the image-level virtual machine backup to the original location, and then click **Next**.

The **Restore Type** page displays.

7. On the **Restore Type** page, select **Restore and Overwrite Original VM**, and then click **Next**.

The **Options** page appears, displaying the current configuration of the virtual machine along with any disks that have been added since the last backup.

8. On the **Options** page, if there are any hard disks in the current virtual machine configuration that were not part of the original backup:
  - Select **Delete disks that will be detached** to remove these disks upon restore.
  - Unselect **Delete disks that will be detached** to keep these disks in their original folder(s) on the virtual machine after the restore. Note that these disks will not be in the virtual machine configuration, but after the restore you can then use the **vSphere Client** to manually reattach or download these disks as appropriate.
9. Click **Next**.

The **Summary** page appears with a confirmation message indicating that the virtual machine will be powered off and that the virtual machine in the datastore will revert to the point in time of the selected backup copy before being powered back on.

10. On the **Summary** page, click **Restore**.

An informational dialog box appears indicating that the restore has started.

11. Go to the **Jobs** window to monitor the restore.

A restore job appears with a progress bar and start time.


## Restore individual virtual disks

A virtual disk (VMDK) restore recovers individual VMDKs to their original location on the vCenter, rolling the VMDKs that you backed up with the protection policy in PowerProtect Data Manager to an earlier point in time.


### Before you begin

Review [Prerequisites to virtual machine restore](#) before you perform the following procedure.

### About this task

 **Note:** When you restore individual VMDKs, only the selected disks are restored. The virtual machine configuration does not change.

### Procedure

- In the PowerProtect Data Manager UI, select **Recovery > Assets** and select the **Virtual Machines** tab.  
The **Recovery** window displays all virtual machines available for recovery.
- Select the checkbox next to the appropriate virtual machines and click **Restore**.  
You can also use the filter in the **Name** column to search for the name of the specific virtual machine.  
The **Recovery** wizard appears.
- On the **Select Copy** page, for each virtual machine that is listed in the table, select the radio button next to the virtual machine and click **Choose Copy**.  
The **Choose Copy** dialog box appears.  
 **Note:** If you click **Next** without choosing a copy, the most recent backup copy is used.
- If the backup is on a Data Domain system, click **DD**, and then select from one of the available copies that display in the table.
- Click **OK** to save the selection and exit the dialog, and then click **Next**.
- On the **Purpose** page, select **Restore Individual Virtual Disks** to restore specific VMDKs, and then click **Next**.  
The **Select Disks** page displays.
- From the **Backup Properties** pane, select the VMDKs that you want to restore, and then click **Next**. Note that individual VMDKs can only be restored to the original location.  
The **Summary** page appears with a confirmation message indicating that the selected disk(s) will be overwritten in the current configuration with the copy from the backup.
- On the **Summary** page, click **Restore**.  
An informational dialog box appears indicating that the restore has started.
- Go to the **Jobs** window to monitor the restore.  
A restore job appears with a progress bar and start time.

## Restore to new

A restore to a new location enables you to create a new virtual machine using a copy of the original virtual machine backup. Other than having a new name or location and a new vSphere VM Instance

UUID, this copy is an exact replica of the virtual machine that you backed up with the protection policy in PowerProtect Data Manager.

### Before you begin

Review [Prerequisites to virtual machine restore](#) before you perform this procedure.

### Procedure


1. Select the checkbox next to the appropriate virtual machines and click **Restore**.

You can also use the filter in the **Name** column to search for the name of the specific virtual machine.


The **Recovery** wizard appears.

2. On the **Select Copy** page, for each virtual machine that is listed in the table, select the radio button next to the virtual machine and click **Choose Copy**.

The **Choose Copy** dialog box appears.

 **Note:** If you click **Next** without choosing a copy, the most recent backup copy is used.

3. If the backup is on a Data Domain system, click **DD**, and then select from one of the available copies that display in the table.
4. Click **OK** to save the selection and exit the dialog, and then click **Next**.
5. On the **Purpose** page, select whether you want to restore the entire virtual machine, or only specific virtual machine disks (VMDKs), and then click **Next**.


 **Note:** Individual VMDKs can only be restored to the original location.

6. On the **Restore Type** page, select **Create and Restore to New VM**, and then click **Next**.
7. On the **VM Information** page:
  - a. Select whether you want to use the original virtual machine name or rename the new virtual machine by appending a suffix to the original name. If the location for the new virtual machine restore will be a different folder than the original location, you can use the original name.
  - b. From the **Restore to vCenter** list, select the vCenter server for the new virtual machine restore. This list displays any vCenter server that has been added from the **Assets** window.  
  
When you select a vCenter server, available data centers appear.
  - c. Select the destination data center.
  - d. Click **Next**.
8. On the **Restore Location** page, select the location within this data center that you want to restore the virtual machine by expanding the hierarchical view. For example, select a specific cluster, and then select a host within the cluster. If you select an ESX host within this page, the next page is unnecessary. Click **Next**.

9. On the **ESX Host** page:
  - If you did not select a specific host in the previous step, select a host that is connected with the cluster, and then click **Next**.
  - If you selected a host in the previous step, this page indicates that a host is already selected and you can click **Next** to proceed.
10. On the **Disk Files Datastore** page, select the datastore where you want to restore the virtual machine disks, and then click **Next**.




- To restore all disks to the same location, keep the **Configure per disk** slider to the left, and then select the datastore from the **Storage** list.
  - To restore disks to different locations, move the **Configure per disk** slider to the right, and then:
    - a. Select a datastore for each disk from the **Storage** list.
    - b. Select the type of provisioning you want to apply to the disk from the **Disk Format** list.
11. On the **Options** page:
    - a. For **Select Access Level**, keep the slider set to **Yes** if you want to enable instant access for this restore.  
  
When you select this option, the virtual machine is created and powered on while temporarily accessing the VMDKs from Data Domain storage. Storage vMotion is initiated to the target datastore. The virtual machine becomes available for use when it is powered on.
    - b. (Optional) For the recovery options, select **Power on the virtual machine when the recovery completes** and **Reconnect the virtual machine's NIC when the recovery completes**. **Power on the virtual machine when the recovery completes** is selected by default when instant access is enabled.
    - c. Click **Next**.
  12. On the **Summary** page, verify that the information you specified in the previous steps is correct, and then click **Restore**.
  13. Go to the **Jobs** window to monitor the restore.

A restore job appears with a progress bar and start time. You can also click  next to the job to verify what steps have been performed, for example, if the instant access session has been created.


## Restore an instant access virtual machine

An instant access virtual machine restore enables you to create a new virtual machine directly from the original virtual machine backup on the Data Domain system for the purposes of instant backup validation and recovery of individual files. The instant access virtual machine is initially available for 7 days. This process does not copy or move any data from the Data Domain system to the production datastore. An instant access virtual machine restore also provides the option to move the virtual machine to a production datastore if you want to retain access to the virtual machine for a longer time.

### Procedure


1. Select the checkbox next to the desired virtual machines and click **Restore**.  
  
You can also use the filter in the **Name** column to search for the name of the specific virtual machine.  
  
The **Recovery** wizard appears.
2. On the **Select Copy** page, for each virtual machine that is listed in the table, select the radio button next to the virtual machine and click **Choose Copy**.  
  
The **Choose Copy** dialog box appears.  
 **Note:** If you click **Next** without choosing a copy, the most recent backup copy is used.
3. If the backup is on a Data Domain system, click **DD**, and then select from one of the available copies that display in the table.

4. Click **OK** to save the selection and exit the dialog, and then click **Next**.
5. On the **Purpose** page, select whether you want to restore the entire virtual machine, or only specific virtual machine disks (VMDKs), and then click **Next**.

 **Note:** Individual VMDKs can only be restored to the original location.

6. On the **Restore Type** page, select **Instant Access VM**, and then click **Next**.
7. On the **VM Information** page:
  - a. Select whether you want to use the original virtual machine name for the instant access virtual machine restore, or rename the instant access virtual machine by appending a suffix to the original name.
  - b. From the **Restore to vCenter** list, select the vCenter server for the instant access virtual machine restore. You can select the vCenter of the original virtual machine backup, or another vCenter. This list displays any vCenter server that has been added from the **Assets** window.

When you select a vCenter server, available data centers appear.

- c. Select the destination data center.
  - d. Click **Next**.
8. On the **Restore Location** page, select the location within this data center that you want to restore the virtual machine by expanding the hierarchical view. For example, select a specific cluster, and then select a host within the cluster. If you select an ESX host within this page, the next page is unnecessary. Click **Next**.
9. On the **ESX Host** page:
  - If you did not select a specific host in the previous step, select a host that is connected with the cluster, and then click **Next**.
  - If you selected a host in the previous step, this page indicates that a host is already selected and you can click **Next** to proceed.
10. On the **Options** page:
  - a. Specify a name for the Instant Access virtual machine.
  - b. (Optional) Select **Power on the virtual machine when the recovery completes** and **Reconnect the virtual machine's NIC when the recovery completes**, if desired. **Power on the virtual machine when the recovery completes** is selected by default for instant access virtual machine restores.
  - c. Click **Next**.
11. On the **Summary** page, verify that the information you specified in the previous steps is correct, and then click **Restore**.  
A confirmation message displays indicating that the restore has been initiated and providing the option to go to the **Jobs** window to monitor the restore progress.
12. Go to the **Jobs** window to view the entry for the instant access virtual machine recovery and verify when the recovery completes successfully. You can also click  next to the job to verify what steps have been performed, for example, if the instant access session has been created.

## Results

To monitor and manage the instant access virtual machine recovery, select **Recovery > Running Activities**, and then click the **Instant Access Sessions** tab. From this window, you can also extend the instant access virtual machine session beyond the default period of 7 days.

## Manage and monitor Instant Access Sessions

The **Instant Access Sessions** tab in the **Recovery > Running Activities** window enables you to manage the status of a virtual machine restore to new or instant access virtual machine restore (for example, by extending the availability period or deleting an instant access virtual machine) and monitor vMotion events.

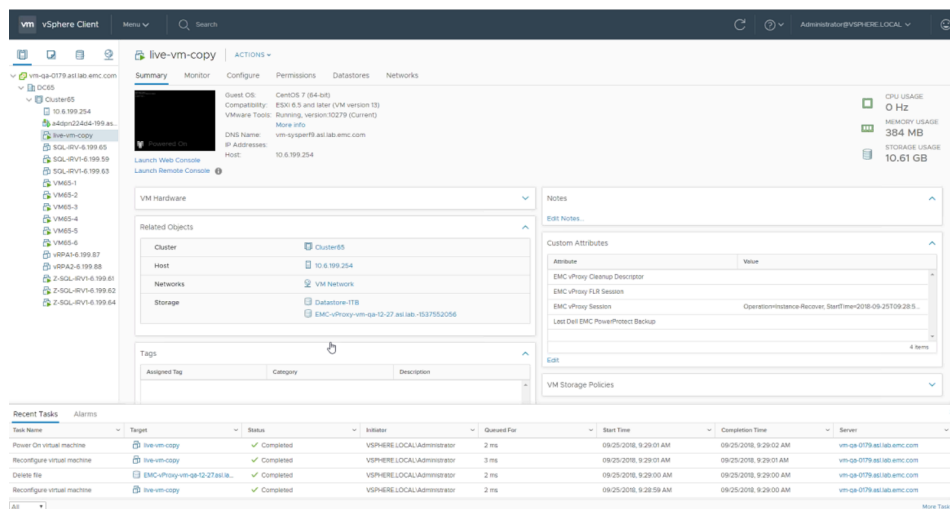
**Note:** The Instant Access Sessions used by a SQL application-aware self-service restore are displayed in the PowerProtect Data Manager UI, but management is disabled. Use the SQL application-aware self-service restore UI to manage these sessions.

When the Jobs window indicates that a recovery has completed successfully, go to **Recovery > Running Activities > Instant Access Sessions** to access information about the sessions. This window enables you to monitor and manage all exported copies that you have created from the Data Domain system. An active restore session with a state of **Mounting** indicates that the restore is still in progress. Once the state changes to **Mounted**, the restore is complete and the instant access virtual machine is ready. When you select the session in the table, you can choose from three options:

- **Extend** — Click to extend the number of days the instant access virtual machine restore is available. The default retention period of an instant access virtual machine restore is 7 days.
- **Migrate** — Click to open the **Migrate Storage vMotion** wizard, which enables you to move the instant access virtual machine to a protection datastore. [Migrate an instant access session](#) provides instructions.
- **Delete** — Click if you no longer require the active restore session. Note that you can also vMotion from inside of the vCenter server, and PowerProtect Data Manager will remove the Instant Access Session upon detection.

For instant access virtual machine restores, availability of the instant access virtual machine session is also indicated in the **vSphere Client**. The session appears in the **Recent Tasks** pane, and you can expand the cluster and select the instant access virtual machine to view summary information, as shown in the following figure.

**Figure 8** instant access virtual machine restore in the vSphere Client



## Migrate an Instant Access session


Once you validate that the instant access virtual machine is the virtual machine that you require for production, click **Migrate** to open the **Migrate Storage vMotion** wizard, which enables you to select the session and move the virtual machine to a production datastore.

### Procedure

1. Go to **Recovery > Running Activities**, and click the **Instant Access Sessions** tab.
2. Select a session from the table that is in **Mounted** state, and click **Migrate**.

The **Migrate Storage vMotion** wizard displays.

3. On the **Disk Files Datastore** page, select the datastore where you want to relocate the instant access virtual machine, and then click **Next**.
  - To migrate all VMDKs to the same datastore, keep the **Configure per disk** slider to the left, and then select the datastore from the **Storage** list.
  - To migrate VMDKs to separate datastores, move the **Configure per disk** slider to the right, and then:
    - a. Select a datastore for each disk from the **Storage** list.
    - b. Select the type of provisioning you want to apply to the disk from the **Disk Format** list.
4. On the **Summary** page, review the information to ensure that the details are correct, and then click **Migrate**.
5. Go to the **Jobs** window or the **Instant Access Sessions** window to view the progress of the migration.

In the **Jobs** window, the migration job appears with a progress bar and start time. You can also click  next to the job to verify what steps have been performed. In the **Instant Access Sessions** window, you can monitor the vMotion status of the migration. When a vMotion is in progress, the status indicates **VMotioning**. Once the storage vMotion for the session is complete, the status of the session changes to **Deleting** as the session is being removed from the **Instant Access Sessions** window.

## File level restore

A file level restore enables you to recover individual files from backups of virtual machines or VMDKs performed in PowerProtect Data Manager to a primary or secondary vCenter server.

### Before you begin

Review the section [Supported platform versions for file-level restore](#) for supported platform and operating system versions.

PowerProtect Data Manager only supports file level restore if the backup or replica is on a Data Domain device. If a replica backup does not exist on such storage, you must manually replicate this backup to Data Domain before performing the file level restore.

### About this task

 **Note:** File level restore in the PowerProtect Data Manager UI can only be performed by an administrator.

### Procedure

1. In the PowerProtect Data Manager UI, go to **Recovery > Assets** and select the **Virtual Machines** tab.

The **Recovery** window displays all of the virtual machines available for recovery.

2. Select the checkbox next to the desired virtual machine and click **View Copies**.

You can also use the filter in the **Name** column to search for the name of the specific virtual machine.


The **Recovery > Assets** window provides a map view in the left pane and copy details in the right pane.

When a virtual machine is selected in the map view, the virtual machine name displays in the right pane with the copy locations underneath. When you select a specific location in the left pane to view the copies, for example, on a Data Domain system, the copies on that system display in the right pane.

3. If the backup is on a Data Domain system, click **DD**, and then select from one of the available copies that display in the table.
4. In the right pane, select the checkbox next to the virtual machine backup you want to restore, and then click **File Level Restore**.


The **File Level Recover** wizard appears.

5. On the **Select Target VM** page, choose from one of the following options:
  - Perform the file-level restore to the original virtual machine.
  - Search for the destination virtual machine by typing the name.
  - Browse from the available vCenter servers to locate the destination virtual machine.
6. On the **Mount Copy** page:
  - a. Type the user credentials to access the virtual machine that you want to recover objects to in order to initiate the disk mount. This user should have privileges to install the **FLR Agent**, which is required to perform file level restore. For Windows virtual machines, this is an administrator account. For Linux virtual machines, this requires the root user account.

 **Note:** Once you approve storing the credentials for the virtual machine, the user credentials prompt will not appear unless the credentials change.


- b. (Optional) Leave **Keep FLR Agent Installed** selected if you want the FLR Agent to remain on the destination virtual machine after the restore completes.
- c. Click **Start Mount** to initiate the disk mount.

A progress bar identifies when the mount has completed.

 **Note:** You cannot browse the contents of the virtual machine backup until the mounting of the destination virtual machine completes successfully.

- d. When the mount completes successfully, click **Next**.

7. On the **Select Files to Recover** page:
  - a. Expand individual folders to browse the original virtual machine backup, and select the objects you want to restore to the destination virtual machine.
  - b. Click **Next**.

 **Note:** When browsing for objects to recover on this page, each directory/hard drive appears twice. Therefore, when you select an object from one location, the object will be selected in the duplicate location as well.

8. On the **Select Restore Location** page:
  - a. Browse the folder structure of the destination virtual machine to select the folder where you want to restore the objects.

- b. Click **Next**.
9. On the **Summary** page:
  - a. Review the information to ensure that the restore details are correct.
  - b. Click **Restore**.
10. Go to the **Jobs** window to monitor the restore.
 

A restore job appears with a progress bar and start time.

## Direct Restore to ESXi

If the virtual machine you protected with PowerProtect Data Manager was a vCenter virtual machine, but this virtual machine and vCenter is now lost or no longer available, Direct Restore to ESXi enables you to recover the virtual machine directly to an ESXi host without a vCenter server.

### Before you begin

**Direct Restore to ESXi** restore requires either the embedded or an added VM Direct appliance that is registered to PowerProtect Data Manager.


Additionally, ensure that you disconnect the ESXi host from the vCenter server.

### Procedure

1. In the PowerProtect Data Manager UI, go to **Recovery > Assets** and select the **Virtual Machines** tab.

The **Recovery** window displays all of the virtual machines available for recovery.

2. Select the checkbox next to the desired virtual machine and click **View Copies**.

 **Note:** If you cannot locate the virtual machine, you can also use the filter in the **Name** column to search for the name of the specific virtual machine.

The **Recovery > Asset** window provides a map view in the left pane and copy details in the right pane.

When a virtual machine is selected in the map view, the virtual machine name displays in the right pane with the copy locations underneath. When you select a specific location in the left pane to view the copies, for example, on a Data Domain system, the copies on that system display in the right pane.

3. If the backup is on a Data Domain system, click **DD**, and then select from one of the available copies that display in the table.
4. In the right pane, select the checkbox next to the virtual machine backup you want to restore, and then click **Direct Restore to ESXi**.

The **Direct Restore to ESXi** wizard appears.

5. On the **Options** page:
  - a. (Optional) Select **Reconnect the virtual machine's NIC when the recovery completes**, if desired. **Power on the virtual machine when the recovery completes** is selected by default.
  - b. Click **Next**.
6. On the **ESX Host Credentials** page:
  - a. In the **ESX Host** field, type the IP of the ESX server where you want to restore the virtual machine backup.
  - b. Specify the root **Username** and **Password** for the ESX Server.

- c. Click **Next**.
7. On the **Datastore** page, select the datastore where you want to restore the virtual machine disks, and then click **Next**.
  - To restore all of the disks to the same location, keep the **Configure per disk** slider to the left, and then select the datastore from the **Storage** list.
  - To restore disks to different locations, move the **Configure per disk** slider to the right, and then:
    - a. For each available disk that you want to recover, select a datastore from the **Storage** list.
    - b. Select the type of provisioning you want to apply to the disk from the **Disk Format** list.
8. On the **Summary** page:
  - a. Review the information to ensure that the details are correct.
  - b. Click **Restore**.
9. Go to the **Jobs** window to monitor the restore.
 

A restore job appears with a progress bar and start time.

## Restore an application-aware virtual machine backup

When virtual machine applications are protected within a protection policy in PowerProtect Data Manager, you can recover the application data using the Microsoft application agent.

The *PowerProtect Microsoft Application Agent SQL Server User Guide* provides instructions on how to restore an application-aware virtual machine using the VM Direct SQL Server Management Studio (SSMS) plug-in.

## Performing centralized restore of a File System host

When File Systems are protected within a protection policy in PowerProtect Data Manager, you can recover the File System data using the centralized PowerProtect Data Manager restore functionality, or directly using the self-service restore feature. The following section describes the procedure for centralized restore of File Systems in the PowerProtect Data Manager UI.

### Prerequisites for File System restores

Before performing centralized or self-service File System restores:

- Ensure that the target or destination volume is not a system volume.
- Ensure that the **File System agent** is not installed and running on the target volume.
- Ensure that there is sufficient space on the target volume for the restore.

## Centralized restore of File Systems in PowerProtect Data Manager

A File System host image-level restore enables you to recover data from backups of file systems performed in PowerProtect Data Manager.

### Before you begin


Ensure the following for Linux File System hosts:

- You have disabled Security-Enhanced Linux (SELinux) by running one of the following relevant commands:

- RHEL 7.x or CentOS7.x: `setsebool -P nis_enabled 1`
- RHEL 6.x or CentOS 6.x: `setsebool -P allow_ybind 1`
- You have installed the `iscsiadm` utility by installing one of the following relevant packages on the Linux client:
  - RHEL or CentOS: `iscsi-initiator-utils<version_number>.rpm`
  - SLES: `open-iscsi<version_number>.rpm`
- On SLES, if you want to start the `iscsiadm` utility for the first time, restart the iSCSI services by running the following command: `service open-iscsi restart`

### Procedure

1. In the PowerProtect Data Manager UI, select **Recovery > Assets** and select the **File System** tab.  
The **Recovery** window displays all of the file systems available for recovery.
2. Select the checkbox next to the desired file system and click **View Copies**.  
You can also use the **Search** field or the filter in the **Name** column to locate a specific file system.  
The **Recovery > Assets** window provides a map view in the left pane and copy details in the right pane.  
When a file system is selected in the map view, the file system name displays in the right pane with the copy locations underneath. When you select a specific location in the left pane to view the copies, for example, on a Data Domain system, the copies on that system display in the right pane.
3. Click **DD**, and then select from one of the available copies that display in the table.
4. In the right pane, select the checkbox next to the file system backup you want to restore, and then click **Restore**.  
The **Restore** wizard appears.
5. On the **Select Target Location** page, choose from one of the following options, and then click **Next**.
  - Restore to original — Restore the file system to the original location.
  - Restore to a new location on the original host — Select the destination file system asset (volume) from the list of available assets on the host.
  - Restore to a new host — Browse from the available hosts to locate and select a destination host and file system.

 **Note:** If the destination file system asset already contains some data, this data will be overwritten.
6. On the **Summary** page:
  - a. Review the information to ensure that the restore details are correct.
  - b. Click **Restore**.
7. Go to the **Jobs** window to monitor the restore.  
A restore job appears with a progress bar and start time.



# Restore of Storage Direct backups in PowerProtect Data Manager


A Storage Direct host image-level restore enables you to recover data from storage group snapshot backups by using the PowerProtect Data Manager UI.

## Before you begin

If performing a **Restore to Original**, unmount all of the production LUNs in the original storage group.

If performing a **Restore to New**, unmount all of the LUNs in the destination storage group.

## About this task

 **Note:** You cannot perform a restore from a replicated backup on a secondary Data Domain system.

## Procedure

1. In the PowerProtect Data Manager UI, go to **Recovery > Assets** and select the **VMAX Storage Groups** tab.

The **Recovery** window displays all of the storage groups.


2. Select the checkbox next to the storage group that contains the backup, and click **View Copies**.

You can also use the **Search** field or the filter in the **Name** column to locate a specific storage group.

The **Recovery > Assets** window provides a map view in the left pane and copy details in the right pane.

When you select a specific location in the left pane to view the copies, for example, on a Data Domain system, the copies on that system display in the right pane.

3. In the left pane, click **DD** to display the available copies.
4. In the right pane, select the checkbox next to the storage group snapshot backup you want to restore, and then choose one of the following restore types:

- Click **Restore to Original** to perform a rollback restore to the same location on the original host.
  -  **Note:** If, after the original backup, you saved any additional files to this location that were not part of the backup, these files will be removed upon rollback.
- Click **Restore to New** to perform the restore to a different location on the original host, or to a different host.

If you selected **Restore to Original**, the **Restore VMAX Storage Group to original location** dialog box appears. Click **OK** to start the restore. You can now proceed to step 7. If you selected **Restore to New**, the **VMAX Restore** wizard appears.

5. On the **Choose the Alternate VMAX** page, select the VMAX where the destination storage group resides, and then click **Next**.

For the alternate VMAX host, if you select a VMAX other than the source VMAX, you will also be required to perform the following:

- a. Select a storage group and Data Domain.
- b. In the newly created configuration file that was pushed by the PowerProtect Data Manager server, note the storage group name (the value of `VMAX_FASTX_RESTORE_SG`, `DDDISK_USER`, and `RESTORE_DEVICE_POOL`).

- c. Create a storage group in the alternate VMAX with the value specified in the configuration file (*VMAX\_FASTX\_RESTORE\_SG*).
- d. Add vDisk devices in the Data Domain to a vDisk pool specified in the configuration file (*RESTORE\_DEVICE\_POOL*).
- e. Encapsulate these vDisk devices and add them to the storage group created in step b.
6. On the **Choose the VMAX Storage Group** page, select the destination storage group where the data will be rolled back to. The alternate storage group should have the same size LUN and geometry as the source storage group.
7. Click **Finish**.  
Once the restore completes successfully, you can mount LUNs in the destination storage group to any host.
8. Go to the **Jobs** window to monitor the restore.  
A restore job appears with a progress bar and start time.

## Restore the PowerProtect Data Manager server

You can restore PowerProtect Data Manager server persisted data as a new instance using any of the backups. A System Administrator can carry out the restore.

### Before you begin

Ensure that:

- The PowerProtect Data Manager version that is deployed on your system and the backups you are using for the restore match.
- The network configuration is the same on the newly deployed PowerProtect Data Manager system as on the failed instance that you are restoring.

### Procedure

1. Deploy the PowerProtect Data Manager OVA and power it on.
2. Select **Restore Backup**.
3. Specify the following storage information:
  - a. Data Domain System IP where the recovery backups are stored.
  - b. Data Domain NSF Export Path where the recovery backups are stored.
  - c. Click **Connect**.
4. Select the PowerProtect Data Manager instance that you would like to restore, and click **OK**.
5. Select the backup file that you would like to use for recovery, and click **Recover**.
6. Specify the lockbox passphrase associated with the backup, and start the recovery.

This will initiate the recovery and display the progress status. The recovery process can take approximately eight minutes before the URI is redirected to the PowerProtect Data Manager login. If the recovery status shows progress as Failed, refer to [Recover a failed PowerProtect Data Manager backup](#) on page 205

### After you finish

After a successful recovery:

- The time zone of the PowerProtect Data Manager instance is set to the same as that of the backup.

- The OS user passwords and PowerProtect Data Manager login are set to the lockbox phrase previously provided in step 6.

## Restore operations for cloud tier

Restore operations of backups that have been tiered to the cloud are identical to normal restore operations.

The PowerProtect Data Manager software recalls a copy of the backup from the cloud to the active tier of the Data Domain system, and then performs a restore of the backup from the active tier to the client. The status appears as Cloud. The backup is stored on the Data Domain cloud tier after the restore. The copy of the backup on the Data Domain active tier is used for restore operation and is deleted after 10 days.

## Restore from cloud tier

### Procedure

1. Select **Recovery > Assets**, click **DD**, and then select from one of the available copies that appear in the table.
2. Click **Recall**, and specify how long the copy should be kept on the active tier.  
The copy is moved and the **Location** changes from Cloud to Local.
3. Click the appropriate restore option.
4. Select the recalled copy and click **Edit Recall Retention**.
5. Select the recalled copy to retier the copy to the active tier.



# CHAPTER 11

## Performing Self-service Backup and Restore of Application and File System Agents

This section includes the following topics:

- [Performing self-service backups of Microsoft SQL databases](#)..... 166
- [Performing self-service backups of Oracle databases](#)..... 166
- [Performing self-service backups of File Systems](#)..... 167
- [Performing self-service backups of Microsoft SQL databases](#)..... 168
- [Restore a SQL application host](#)..... 168
- [Restore an Oracle application host](#)..... 168
- [Performing self-service restore of a File System host](#)..... 169

## Performing self-service backups of Microsoft SQL databases

To enable self-service protection, when you create the SQL protection policy, select **Self-Service Protection**.

When performing a self-service stand-alone backup of an AAG asset, the backups display under the AAG asset.

Chapter 4, Backing Up SQL Server with Application Direct, in the *PowerProtect Microsoft Application Agent SQL Server User Guide* provides instructions on how to perform self-service SQL Server backups.

## Performing self-service backups of Oracle databases

To enable self-service protection, when you create the Oracle protection policy, select **Self-Service Protection**.

To perform a self-service or manual backup of an Oracle database, you must create and run an RMAN backup script. The Oracle RMAN documentation provides detailed information about how to create the backup scripts. The documentation also describes all the supported backup features.

The following example shows an RMAN script that performs a full backup of the database and its archive logs:

```
connect target username/password;

run {
  allocate channel c1 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
  libddobk.so', ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ,
  BACKUP_HOST=bu-ddbealin-17.lss.emc.com)';

  backup database include current controlfile format '%U' plus archivelog;

  release channel c1;
}
```

The `libddobk.so` library location and the `RMAN_AGENT_HOME`, `STORAGE_UNIT`, and `BACKUP_HOST` settings must be specified in the `allocate channel` command. All other parts of the script are standard RMAN commands.

To increase the parallelism of the backup, you can allocate more channels:

```
connect target username/password;

run {
  allocate channel c1 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
  libddobk.so', ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ,
  BACKUP_HOST=bu-ddbealin-17.lss.emc.com)');
  allocate channel c2 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
  libddobk.so', ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ,
  BACKUP_HOST=bu-ddbealin-17.lss.emc.com)');
  allocate channel c3 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
  libddobk.so', ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ,
  BACKUP_HOST=bu-ddbealin-17.lss.emc.com)');
  allocate channel c4 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
  libddobk.so', ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ,
  BACKUP_HOST=bu-ddbealin-17.lss.emc.com)');

  backup database include current controlfile format '%U' plus archivelog;

  release channel c1;
```

```
release channel c2;
release channel c3;
release channel c4;
}
```

## Performing self-service backups of File Systems

A host with the File System Agent installed requires a PowerProtect Data Manager server to back up file systems. However, an administrator can configure a retention policy only instead of a complete backup.

To back up file systems manually and use PowerProtect Data Manager for compliance purposes, register the host to PowerProtect Data Manager, create a self-service protection policy, and configure only the retention policy.

**Note:** To enable self-service protection, select **Self-Service Protection** when you create the File Systems protection policy in the PowerProtect Data Manager UI.

After a host is registered with PowerProtect Data Manager and assets are added to a self-service protection policy, use the `ddfssv` command to run self-service or manual backups on the host file system assets, as in the following example:

```
ddfssv -LL -l FULL -a DFA_SI_DD_HOST=IPv4 address -a DFA_SI_DD_USER=username
(for example, PLC-Protection) -a DFA_SI_DEVICE_PATH=device path (for example, /
PLCProtection/LVMs/2))
```

Where:

**-l {full | incr}**

Specifies the type of the backup to perform such as full (`full`), or incremental (`incr`). The default value is `full`.

**-a "DFA\_SI\_DD\_HOST=<server\_name>"**

Specifies the name of the Data Domain server that contains the storage unit where you want to back up the databases.

**-a "DFA\_SI\_DEVICE\_PATH=<storage\_unit\_and\_path>"**

Specifies the name and the path of the storage unit where you want to direct the backup.

**-a "DFA\_SI\_DD\_USER=<username>"**

Specifies the protection storage username.

You must register the hostname and the protection storage username in the lockbox to enable the Microsoft application agent to retrieve the password for the registered user.

These details are provided in the `.app.settings` file on both Linux and Windows hosts. If the default installation path was used, the `.app.settings` file is at `/opt/dpsfsagent/settings/.app.settings` on a Linux host and `C:\Program Files\DPSFSAGENT\settings\.app.settings` on a Windows host. More information about how to use the `admin` utility to query the list of backups for an asset, see [Using the `ddfadmin` utility for File Systems](#).

**Note:** This command uses only the retention period that was specified when the self-service protection policy was created.

To perform a self-service backup, use the storage unit and username that was created on the Data Domain system when the policy was created. PowerProtect Data Manager discovers these backups and enables centralized restore operations. You can also perform a manual restore operation.

## Performing self-service backups of Microsoft SQL databases

To enable self-service protection, when you create the SQL protection policy, select **Self-Service Protection**.

When performing a self-service stand-alone backup of an AAG asset, the backups display under the AAG asset.

Chapter 4, Backing Up SQL Server with Application Direct, in the *PowerProtect Microsoft Application Agent SQL Server User Guide* provides instructions on how to perform self-service SQL Server backups.

## Restore a SQL application host

You can perform database or table-level restores directly to the SQL application host using the Microsoft application agent.

Chapter 6, Restoring Application Direct Backups, in the *PowerProtect Microsoft Application Agent SQL Server User Guide* provides instructions on how to restore an application-aware SQL Server backup.

## Restore an Oracle application host

You can perform database restores directly to the Oracle application host by using the Oracle RMAN agent.

To perform an Oracle database restore, you must prepare the database and then run an RMAN script to restore the data. The RMAN documentation provides detailed information about how to prepare the database and create the RMAN restore script. The documentation also describes all the supported restore features.

The following example shows an RMAN script that performs a complete restore of the database to the current time, after the database has been prepared:

```
connect target username/password;

run {
allocate channel c1 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so', ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ,
BACKUP_HOST=bu-ddbealin-17.lss.emc.com)';

restore database;
recover database;

release channel c1;
}
```

The `libddobk.so` library location and the `RMAN_AGENT_HOME`, `STORAGE_UNIT`, and `BACKUP_HOST` settings must be specified in the `allocate channel` command. All other parts of the script are standard RMAN commands.

To increase the parallelism of the restore, you can allocate more channels:

```
connect target username/password;

run {
allocate channel c1 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so', ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ,
```



```

BACKUP_HOST=bu-ddbealin-17.lss.emc.com)');');
allocate channel c2 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so', ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ,
BACKUP_HOST=bu-ddbealin-17.lss.emc.com)');');
allocate channel c3 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so', ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ,
BACKUP_HOST=bu-ddbealin-17.lss.emc.com)');');
allocate channel c4 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so', ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ,
BACKUP_HOST=bu-ddbealin-17.lss.emc.com)');');

restore database;
recover database;

release channel c1;
release channel c2;
release channel c3;
release channel c4;
}

```

## Performing self-service restore of a File System host

When File Systems are protected within a protection policy in PowerProtect Data Manager, you can recover the File System data using the centralized PowerProtect Data Manager restore functionality, or directly using the self-service restore feature. The following section describes the procedure for self-service restore of File Systems.

### Prerequisites for File System restores

Before performing centralized or self-service File System restores:

- Ensure that the target or destination volume is not a system volume.
- Ensure that the **File System agent** is not installed and running on the target volume.
- Ensure that there is sufficient space on the target volume for the restore.

## Using the ddfsadmin utility for File Systems

The ddfsadmin utility provides the following command line options for File System recovery.

### ddfsadmin backup query

Before running the `ddfsrc` command to perform a self-service image-level restore of File Systems, you can use the `ddfsadmin backup` command to query a list of all the local and remote backups taken for a particular host, as shown in the following:

```
ddfsadmin backup query -local -v=volume name -t=time value [h = hour, d = days, w = weeks, m = months] queries the local record file for listing backups.
```

```
ddfsadmin backup query -remote -d=Protection storage system -s=storage unit -u=username -p=DD password -c=hostname -v=volume name -t=time value [h = hour, d = days, w = weeks, m = months] queries the record file on the protection storage system for listing backups.
```

### Example 3 Example usage

```
ddfsadmin backup query -local -v="C:\\\" -t=5 will display a list of local backups in C:\ taken within the last five days.
```

## ddfsadmin sync

The following is the usage for the `ddfsadmin sync` command:

```

sync -local options: Sync local record file with record file on DD
sync -remote options: Sync remote record file with file in the local
options:
  -d=<DD host>: Protection storage system host IP
  -u=<DD username>: Protection storage system username
  -s=<DD device path>: Protection storage system device path
  -p=<DD password>: Protection storage system password.[Optional]

```

### Example 4 Example usage

```
ddfsadmin sync -local -d x.x.x.x -u username -s /dev_path
```

## Self-service image-level restore of File Systems

You can perform self-service image-level restores of file systems to the original location by using the `ddfsrc` command. Note that this restore is not supported in the following scenarios:

- When the restore destination is the C:\ volume, which can result in the operating system becoming unavailable.
- When the restore destination is a volume with the File System agent installed.

**Note:** To perform File System restore to an alternate location, use the centralized restore method in the PowerProtect Data Manager UI, as described in the section [Centralized restore of File Systems in PowerProtect Data Manager](#) on page 159

Before running `ddfsrc`, use the `ddfsadmin backup` command to list the local backups for a particular host and obtain the ID of the save set you want to restore. [Using the ddfsadmin utility for File Systems](#) provides more information about the `ddfsadmin backup` command.

To restore from a particular backup, specify the ID of the save set as an input to the `ddfsrc` command, as in the following example:

```
ddfsrc -h DFA_SI_DEVICE_PATH=device path (for example, /fsa2) -h
DFA_SI_DD_HOST=Protection storage system IPv4 address -c BackupClientHostName
(for alternate host restore) -h DFA_SI_DD_USER=Protection storage system
username (for example, sysadmin) -h DFA_SI_DD_PASSWORD=Protection storage system
password -S 1551407738 -r file path (for example, /volume1_ext3) -i y.
```

Where:

**-h "DFA\_SI\_DEVICE\_PATH=<storage\_unit\_and\_path>"**

Specifies the name and the path of the storage unit that contains the backup.

**-h "DFA\_SI\_DD\_HOST=<server\_name>"**

Specifies the name of the protection storage system server that contains the backup. When you have a remote (secondary) protection storage system server that has replicated databases to restore, type the name of the secondary server. A user on the secondary protection storage system server must be in the same group as the primary protection storage system server.

**-h "DFA\_SI\_DD\_USER=<Protection storage system\_user>"**

Specifies the protection storage system username. You must register the hostname and the DD Boost username in the lockbox to enable Microsoft application agent to retrieve the password for the registered user.

**-h "DFA\_SI\_DD\_PASSWORD=<DProtection storage system\_password>"**

Specifies the password of the protection storage system user.

A password is only required in this command if restoring to a new host. If you are a file system administrator and need the password to use for a particular storage system, storage unit and user, contact the backup administrator. If restoring to the original host, the password will be picked up from the lockbox.

## Self-service file-level restore of File Systems

You can perform self-service file-level restores of File Systems using the `ddfsrc` command with the `-I` option.

Before executing the command, create a file that contains the list of file(s) to be restored. Provide the location of this file as an input to the `-I` option, as shown in the following example

**Example 5** `ddfsrc` command with input file specified

```
ddfsrc -h DFA_SI_DEVICE_PATH=Protection storage unit -h
DFA_SI_DD_HOST=Protection storage system IP address -c
BackupClientHostName (for alternate host restore) -h
DFA_SI_DD_USER=Protection storage system username -h
DFA_SI_DD_PASSWORD=Protection storage system password -S savetime-
value -I path-of-file-containing-list-of-files-for-restore -i R -d
destination-path-for-restoring-files
```



# CHAPTER 12

## Preparing for and Recovering from a Disaster

This section includes the following topics:

- [Managing system backups](#) ..... 174
- [Manage PowerProtect Data Manager backups for disaster recovery](#) ..... 174
- [Prepare the Data Domain recovery target](#) ..... 175
- [Configure backups for disaster recovery](#) ..... 175
- [Configure PowerProtect Data Manager server disaster recovery backups](#) ..... 176
- [Record settings for disaster recovery](#) ..... 176
- [Restore PowerProtect Data Manager from an external Data Domain system](#) ..... 177

## Managing system backups

The PowerProtect Data Manager system protection service enables you to protect the persistent data of a PowerProtect Data Manager system from catastrophic loss by creating a series of system backups.

Each backup is considered a “full” backup although it is created in an incremental manner. The persistent data that is saved in a backup includes the Lockbox and Elasticsearch databases. The backup operation creates a point-in-time snapshot of the database while the system is in a quiesced state. While the system is quiesced, user functionality is limited. After the snapshot completes and while PowerProtect Data Manager copies the snapshots to the Data Domain storage unit, full user functionality is restored. If the system fails to quiesce, PowerProtect Data Manager still takes a backup, which is marked as *crash consistent* instead of *application consistent*.

To store system backups, you must configure and assign a private Data Domain storage unit for the PowerProtect Data Manager system. The system protection service enables you to manage the frequency and start time of an automated system backup, perform on-demand backups, and define the length of time that the system backups are available for recovery.

## Manage PowerProtect Data Manager backups for disaster recovery

View PowerProtect Data Manager backups and perform manual backups.

### Before you begin

### About this task

You can view the last 5 PowerProtect Data Manager backups.

### Procedure

1. From the PowerProtect Data Manager UI, select **System Settings > DR Backups > Manage Backups**.
2. To perform a manual backup:

You can back up to only one Data Domain host at a time. When you enter new Data Domain information for backup, you overwrite the existing Data Domain host for backup. If there are more than one external Data Domain systems, you can change which Data Domain has the backup.

- a. Click **Backup Now**.

The **Enter a name for your backup** dialog appears.

- b. [Optional] Type a name for your backup.

You can leave the backup name blank, and PowerProtect Data Manager provides a name for the backup using the naming convention `UserDR-`. If you provide a name with the convention that PowerProtect Data Manager uses for scheduled backups, which is `SystemDR`, PowerProtect Data Manager displays an error.

- c. Click **Start**.

3. To delete a backup:
  - a. Select a backup from the list.

- b. Click **Delete**.

The system displays a warning to confirm you want to delete the backup. Click **Yes** to proceed.


4. Click **Close**.

## Prepare the Data Domain recovery target

Before you can configure PowerProtect Data Manager for backup and recovery, you must configure the NFS export on the Data Domain target system.

### Procedure

1. Use a Web browser to log in to the Data Domain System Manager as the system administrator user.
2. In the **Summary** tab in the **Protocols** pane, select **NFS Exports > Create Export**.
3. In the **Create NFS Export** window, provide the following information, and then click **OK**.
  - **Export Name**—the name of the Data Domain MTree
  - **Directory Path**—the full directory path for Data Domain MTree that you created. Ensure that you use the same name for the directory.

 **Note:** For an external Data Domain system, specify a path similar to the following, /data/coll/<path>. Where <path> is the MTree used to store the DR backups.
4. When the progress message indicates that the save operation is complete, click **Close**.
5. In the **Summary** tab in the **Protocols** pane, click **NFS Exports**.
6. Under **NFS Protocols > Exports**, select the Data Domain MTree from the list of exports and click **Add Clients**.
7. In the **Add Clients** window, provide the following information, and then click **OK**.
  - **Client**—IP address or host name of the PowerProtect Data Manager.
  - Accept the default settings for the rest of the fields.
  - **Current Selection**—Ensure that the list includes `no_root_squash`, which is required for permission for your system to change the directory structure on the NFS share.

## Configure backups for disaster recovery

Configure your system to automatically create backups in the event of a disaster or catastrophic outage.

### Before you begin

Ensure that you have configured Data Domain as a replication location. See [Prepare the Data Domain recovery target](#) on page 175.

### Procedure

1. Log in to PowerProtect Data Manager as administrator.
2. Select **System Settings > DR Backups > Configuration**.
3. Enter the following information, and then click **Save**.
  - Select **Enable backup**.

- **Data Domain System**—IP address or host name of the Data Domain System where you created the MTree with NFS Export
- **NFS Export Path**—the path of the NFS Export

### Results

The initial backup runs, and then backups are automatically triggered every hour.

## Configure PowerProtect Data Manager server disaster recovery backups

Configure disaster recovery protection for the PowerProtect Data Manager system and the system metadata.

### Before you begin

For external Data Domain system backups, ensure that you carry out the procedure described in [Configure the Data Domain system](#) on page 237.

### Procedure

1. From the PowerProtect Data Manager UI, select **System Settings > DR Backups > Configuration**.
2. Configure the backup with the following attributes:
  - a. In the **Data Domain System** field, type the Data Domain system to back up.
  - b. In the **NFS Export Path** field, type the path where backups are stored on the target Data Domain system.
3. Click **Save**.

## Record settings for disaster recovery

Plan for disaster recovery by recording vital information.

### About this task

In the event of a major outage, you will need certain information to recover your systems.

### Procedure

- Ensure that you record the following information on a local drive outside PowerProtect Data Manager:
  - PowerProtect Data Manager build number—Customer Support can provide this information. It is not mandatory.
  - Port Groups—Log in to the vSphere Client, right-click the appliance name and select **Edit Settings**. Record the port group settings that are assigned to PowerProtect Data Manager.
  - NFS export details—Click the System Settings icon and select **DR Backups > Configuration**. Under **Backup**, record the host IP address and the NFS Export Path.
  - Run the `GET /Configurations API (api/v2/configurations)` from PowerProtect Data Manager and save the details for network information.



# Restore PowerProtect Data Manager from an external Data Domain system


You can restore PowerProtect Data Manager from an external Data Domain system where the data is replicated.

## Before you begin

- Ensure that all the information listed in [Record settings for disaster recovery](#) on page 176 is available.
- Ensure that the FQDN of the PowerProtect Data Manager is the same as the host name.
- Ensure that the VM for PowerProtect Data Manager is powered on.
- Ensure that you have set up the recovery target system. See [Prepare the Data Domain recovery target](#) on page 175.

## About this task

When your primary PowerProtect Data Manager system fails because of a major event, deploy a new PowerProtect Data Manager system and recover the backup from the external Data Domain system.

 **Note:** If your recovery system is on a different FQDN, see [Troubleshoot recovery of PowerProtect Data Manager](#) on page 212.

## Procedure

1. Use the .ova file to deploy a new PowerProtect Data Manager system.
2. On the **Install** window under **Welcome**, select **Restore Backup** and click **Next**.
3. Under **Select File**, enter the Data Domain System and NFS Export Path where the backup is located, and then click **Connect**.

A list of the available recovery backups on Data Domain appears.

4. Select the backup from which to recover the system, and click **OK**.
5. Provide the Lockbox Passphrase and click **Start**.

When the Passphrase is verified, the recovery starts. Recovery can take a few minutes.

## Results

When recovery is complete, the PowerProtect Data Manager login page appears.



# CHAPTER 13

## Managing Alerts, Jobs, and Tasks

This section includes the following topics:

- [Configure Alert Notifications](#)..... 180
- [View and manage System Alerts](#)..... 180
- [View and manage System Alerts](#)..... 181
- [Monitoring and viewing jobs](#)..... 181
- [Monitor and view tasks](#)..... 182
- [Restart a job or task](#)..... 182
- [Cancel a job or task](#)..... 183
- [Export logs for a job or task](#)..... 184

## Configure Alert Notifications

The **Alert Notifications** window of the UI enables you to configure email notifications for PowerProtect Data Manager alerts.

### Procedure

1. Select **Administration > Alert Notifications**  
The **Alert Notifications** window appears with a table that displays the details for existing notifications.
2. Click **Add**.  
The **Add Alert Notification** dialog appears.
3. In the **Name** field, type name of the individual or group who will receive the notification email.
4. In the **Email** field:
  - a. Specify the email address and/or alias that notifications will be sent to. This field is required in order to create an alert notification. Ensure that multiple entries are separated by a comma.
  - b. Click **Test Email** to ensure that a valid SMTP configuration exists.
5. From the **Category** list, select the notification category.
6. From the **Severity** list, select the notification severity.
7. In the **Duration** field, specify the amount of time that the notification will display.
8. In the **Subject** field, optionally type the subject that you would like to attach to the notification email.
9. Click **Save** to save your changes and exit the dialog.


### Results

The **Alert Notifications** window updates with the new alert notification. At any time, you can **Edit**, **Delete**, or **Disable** the notification by selecting the entry in the table and using the buttons in this window.

## View and manage System Alerts

System alerts enable you to determine if there are issues with the PowerProtect Data Manager system or any data protection operations in PowerProtect Data Manager. Alerts are classified into three categories — critical, warning, and informational. You can monitor alert messages from the **Alerts** window and export log files.

### Procedure


1. In the PowerProtect Data Manager UI left navigation pane, select **Alerts**.  
The **Alerts** window displays alert information in a table. You can filter the alerts by Severity, Date, Category, or Acknowledge.
2. Select the **System** tab.
3. To view more details about a specific alert, click  next to the entry in the table.
4. Select one or more alerts in the table and click **Acknowledge** to acknowledge that you have reviewed the alert information, and **Add/Edit Note** to append information to an alert.

- To export the log file for an alert to a .csv file, select the alert and click **Export**.

## View and manage System Alerts

Alerts enable you to track the performance of data protection operations in PowerProtect Data Manager so that you can determine whether there is compliance to service level objectives. You can access the system alerts from the **Alerts** window.

### Procedure


- In the PowerProtect Data Manager UI left navigation pane, select **Alerts**.  
The **Alerts** window displays alert information in a table. You can filter the alerts by Severity, Date, Category, or Acknowledge.
- Select the **System** tab.
- To view more details about a specific entry, click  next to the entry in the table.
- To acknowledge the system alert, select the alerts and click **Acknowledge**.
- To add or edit a note for the system alert, click **Add/Edit Note**, and when finished, click **Save**.

## Monitoring and viewing jobs

The **Jobs** window in the PowerProtect Data Manager UI enables you to monitor the status of certain data protection, system, and maintenance jobs and to view details. To perform analysis or troubleshooting, you can view a detailed log of a failed job.

To access the **Jobs** window, open the PowerProtect Data Manager UI left navigation pane, and select **Jobs**. The **Jobs** window appears, displaying completed jobs by default.

The **Jobs** window provides you with options to filter and sort the information that appears:

- Filter jobs by Completed or Running—By default, the **Jobs** window displays completed jobs. To display only running jobs, at the top of the **Jobs** window, click **Running**.
- Filter jobs by time range—By default, the **Jobs** window displays all jobs regardless of time range. To display jobs for a specific time range, select an option:
  - All
  - 1 Week
  - 3 Days
  - 1 Day
- Filter jobs by **Description**, **Policy Name**, **Job Type**, **Asset Type**, **Start Time**, **Status**, or **Events**, by clicking  in their respective column.
- Sort jobs by **Description**, **Policy Name**, **Job Type**, **Asset Type**, and **Start Time** by clicking the column heading.

You can use the **Search** field to filter jobs based on a search string. When you type a keyword in the **Search** field, the PowerProtect Data Manager UI filters the results as you type. To clear the search filter, remove all keywords from the **Search** field.




To view details for a job, click  next to the job name.

You can also monitor the status of individual tasks, view task details, and perform certain operations on tasks.

## Monitor and view tasks

When you drill down within a job, you can view the status of specific tasks within a job. This information can be helpful when troubleshooting to determine whether one or more tasks caused a job to fail.

### Procedure


1. In the PowerProtect Data Manager UI left navigation pane, select **Jobs**.  
The **Jobs** window appears.
2. Click  to the left of the job name.  
The **Details** pane appears on the right.
3. In the **Task Summary** section, click the link that indicates the total number of tasks.  
A new window opens to display a list of all tasks for the job. You can view the following information for a task:
  - Details
  - Task Name
  - Status
  - Asset Name
  - Start Time
  - Duration
  - Data Transferred
 The success or failure of individual tasks is indicated in the **Status** column.
4. (Optional) Sort and filter the information that appears:
  - To sort tasks by **Task Name**, **Status**, or **Asset Name**, click a column heading.
  - To filter tasks by **Task Name**, **Status**, or **Asset Name**, click  in their respective column.
  - To filter tasks based on a search string, type the string in the **Search** field.
5. To view task details and summary information, click  to the left of an individual job task, and then complete the following steps:
  - a. On the **Steps** tab, review the summary information, which describes the task activity.  
To view the information for a step, expand the step by clicking the arrow (>).
  - b. On the **Details** tab, review the details for the task.

## Restart a job or task


You can restart a failed virtual machine backup in the **Jobs** window of the PowerProtect Data Manager UI.

### About this task

When you click **Restart**, the job or task restarts immediately, regardless of the scheduled activity window.

 **Note:** If a policy with both protection and Cloud Data Recovery (CDR) stages fails, the CDR job is cancelled and cannot be restarted.

### Procedure

1. In the PowerProtect Data Manager UI left navigation pane, select **Jobs**.  
The **Jobs** window appears, displaying only completed jobs by default. You can filter the information that appears in the **Jobs** window. [Monitoring and viewing jobs](#) on page 181 provides more information.
2. To restart a failed job, select **Running**, select the failed job from the list, and then click **Restart**.
3. To restart a failed task:
  - a. Click  to the left of the job name.  
The **Details** pane appears on the right.
  - b. In the **Task Summary** section, click the link that indicates the total number of tasks.
  - c. Select a failed task, and then click **Restart**.
  - d. Click **Close**.


### Results

To view the status of the restarted job or task, select **Running** at the top of the **Jobs** window. The status indicates **Running** or **Queued**.



## Cancel a job or task


From the PowerProtect Data Manager UI, you can cancel a backup that is still in progress, or any asset protection and replication activities when the tasks are queued.

### About this task

 **Note:** The **Cancel** operation is only available for supported jobs and tasks.

### Procedure

1. In the PowerProtect Data Manager UI left navigation pane, select **Jobs**.  
The **Jobs** window appears, displaying only completed jobs by default. You can filter the information that appears in the **Jobs** window. [Monitoring and viewing jobs](#) on page 181 provides more information.
2. To cancel a job, select **Running**, select a job that is in-progress, and then click **Cancel**.  
 **Note:** If a job is almost complete, the cancellation might fail. If the cancellation fails, a message displays indicating that the job cannot be canceled.
3. To cancel an individual task:
  - a. Click  to the left of the job name.  
The **Details** pane appears on the right.
  - b. In the **Task Summary** section, click the link that indicates the total number of tasks.
  - c. Select a task that is in-progress, and then click **Cancel**.

 **Note:** If a task is almost complete, the cancellation might fail. If the cancellation fails, a message displays indicating that the task cannot be canceled.

d. Click **Close**.


### Results

The **Jobs** window displays the status of the canceled job or task. If the cancellation is successful, then the status eventually changes to **Canceled**. If the cancellation is not successful, then the status might indicate either **Success** or **Critical**.


## Export logs for a job or task

The PowerProtect Data Manager UI enables you to export and view a detailed log of a job or task. You can view logs to perform analysis or troubleshooting.

### About this task

 **Note:** You can only export logs for failed jobs and tasks that have a log available to download. If a log is available to download, the **Export Log** button is enabled.

### Procedure

1. In the PowerProtect Data Manager UI left navigation pane, select **Jobs**.  
The **Jobs** window appears, displaying only completed jobs by default. You can filter the information that appears in the **Jobs** window. [Monitoring and viewing jobs](#) on page 181 provides more information.
2. To export a log for a completed job, select a job from the list, and then click **Export Log**.
3. To export a log for a completed task:
  - a. Click  to the left of the job name.  
The **Details** pane appears on the right.
  - b. In the **Task Summary** section, click the link that indicates the total number of tasks.
  - c. Select a completed task, and then click **Export Log**.



# CHAPTER 14

## Upgrading the PowerProtect Data Manager Software

This topic presents the following topics:

- [Upgrade the software from PowerProtect Data Manager version 19.1.....](#) 186
- [Upgrade PowerProtect Data Manager from version 19.2 and later.....](#) 187
- [Managing certificates after upgrading from versions earlier than PowerProtect Data Manager version 19.1.....](#) 188

# Upgrade the software from PowerProtect Data Manager version 19.1

Use this procedure to upgrade from PowerProtect Data Manager version 19.1.

## Before you begin

- Ensure that you have administrator credentials. Only an administrator can initiate the upgrade.
- If you have not configured Secure Remote Services (SRS), download the upgrade package from [Dell EMC Support Downloads and Drivers](#).
- Check for running tasks and cancel them or allow them to complete.
- Disable any Protection Policies that are scheduled to run in the next few hours.
- Take a snapshot of the system: Select the PowerProtect VM in the vSphere Client, right click, and then select **Snapshot > Take snapshot** .

## About this task

You can upgrade the system by manually downloading upgrade packages or by connecting to an SRS gateway. When PowerProtect Data Manager is licensed and you have registered the SRS gateway host with PowerProtect Data Manager, you can upgrade using SRS. When an upgrade package is available, the packages are uploaded to the SRS gateway. The appliance checks the SRS gateway once a day for available upgrade packages or you can manually check for upgrade packages.


An upgrade package can upgrade one or more of the following:

- The PowerProtect Data Manager, including application agent installers stored on the PowerProtect Data Manager virtual machine
- External VM Direct appliance
- External CDRS servers

## Procedure

1. Log in to PowerProtect Data Manager with administrator credentials.
2. Select **System Settings > Upgrade**.
  - If you have registered SRS, the UI lists the latest available PowerProtect Data Manager package.
  - If the system is unable to locate an upgrade package or if you are using the manual package download method:
    - a. Click **Upload Upgrade File**, browse to the path that contains the upgrade package, select the package, and click **Open**.
    - b. Wait until the package status is Available, and then click **OK**.
3. (Optional) Click **Perform upgrade**.

A dialog box lists any areas that require attention, such as an indication that the upgrade is disruptive or requires a reboot and warnings about running tasks or active sessions that should be addressed before the upgrade. Click the links provided to go to the management page for the active events, where you can cancel them or allow them to complete before continuing.

 **Note:** The upgrade can proceed even if jobs, IA sessions, or CDR jobs are active, but this is not recommended.

The dialog box also lists any required certificates. Continuing indicates acceptance of the certificate.

4. Enter the Lockbox Passphrase, if required.

The upgrade begins. The browser is redirected to the Upgrade Manager UI on port 14443. This enables you to monitor upgrade progress while the PowerProtect Data Manager components are shutdown for the upgrade.

**Note:** To monitor the update status if the connection to the appliance closes, connect to `https://IP_address_appliance:14443`.

When the upgrade completes successfully, the browser is redirected back to the main PowerProtect Data Manager UI logon page.

5. Log in to PowerProtect Data Manager and return to the **Upgrade** page to verify that the state of the upgrade is **Installed**.

### Results

The overall package status covers critical upgrades for the PowerProtect Data Manager. Other subcomponents, such as Agents and vProxies, may still be processing, or even fail. This does not impact the overall status of the upgrade. You can view the state of each subcomponent by expanding the package that was installed.

**Note:** If the upgrade fails, you must delete the failed package before uploading a new package (or the same package) to try again.

### After you finish

If you created a manual snapshot, use the vSphere Client to delete the snapshot:

1. Right-click the appliance and select **Manage Snapshots**.
2. In the **Manage Snapshots** window, select the snapshot and click **Delete**.

## Upgrade PowerProtect Data Manager from version 19.2 and later

Use this procedure to upgrade PowerProtect Data Manager from version 19.2 or later.

### Before you begin

When the following prerequisites are met, upgrade packages are automatically downloaded, the upgrade process automatically stops all running jobs, puts the system into maintenance mode, and creates a snapshot of the system. If the upgrade fails or is aborted, the system uses the snapshot to roll back to the previous state. Once the system is rolled back or upgraded successfully, the snapshot is automatically deleted.

- Ensure that you have administrator credentials. Only a PowerProtect Data Manager administrator can initiate the upgrade.
- Ensure that your system is registered with Secure Remote Services (SRS). [Register the Secure Remote Services gateway](#) on page 227 provides instructions.
- Ensure that automatic upgrade package downloads is enabled. [Enable automatic upgrade package downloads](#) on page 231 provides more information.
- To enable automatic snapshots, ensure that the vCenter hosting PowerProtect Data Manager is added as an asset source. [Add a VMware vCenter Server](#) on page 102 provides more information.
- Check for running tasks and cancel them or allow them to complete.
- Disable any Protection Policies that are scheduled to run in the next few hours.

**About this task**

A notification appears in the UI when an upgrade package is available.

An upgrade package can upgrade one or more of the following:

- The PowerProtect Data Manager, including application agent installers stored on the PowerProtect Data Manager virtual machine
- External VM Direct appliance
- External CDRS servers


**Procedure**

1. Log in to PowerProtect Data Manager with administrator credentials.
2. Select **System Settings > Upgrade**.

The UI lists the latest available PowerProtect Data Manager upgrade package. Click the down arrow next to the package name to view details about the contents.

3. Click **Upgrade**, enter the Lockbox passphrase, if required, and then click **Continue**.
4. Click **Yes** to continue with the upgrade.

The upgrade begins. The browser is redirected to the Upgrade Manager UI on port 14443. This enables you to monitor upgrade progress while the PowerProtect Data Manager components are shutdown for the upgrade.

 **Note:** To monitor the update status if the connection to the appliance closes, connect to `https://IP_address_appliance:14443`.

The Upgrade Manager status bar enables you to abort the upgrade, if necessary. When the upgrade completes successfully, the browser is redirected back to the main PowerProtect Data Manager UI logon page.

**Results**

- The **Upgrade** page indicates the status of the upgrade.
- If the upgrade fails:
  1. Click the **Export logs** button to download the log files.
  2. Click **Rollback to snapshot**.
  3. In the **Upgrade** page, click **Delete** to delete the failed upgrade package.
  4. Review the log files to determine the cause of the failure.
  5. Remedy the issues, and then retry the upgrade.

## Managing certificates after upgrading from versions earlier than PowerProtect Data Manager version 19.1

Use this procedure to ensure that certificates existing on the pre-upgrade system also exist on the post-upgrade system.

**Before you begin**

Ensure that you update any expired certificates on external systems to valid certificates.

**Procedure**

1. Log in to the PowerProtect Data Manager operating system with administrator credentials.
2. Run the upgrade command:

```
/usr/local/brs/lib/secretsmgr/bin/secretsmgr-tls-upgrade
```

The system displays the external system certificates.

3. Verify each certificate as trusted or untrusted: At the prompt for each certificate, type `y` to accept.

Any other character rejects the certificate. Expired certificates are automatically rejected.



# CHAPTER 15

## Best Practices and Troubleshooting

This section includes the following topics:

- [Compatibility information](#)..... 192
- [Power off the PowerProtect Data Manager OVA](#)..... 192
- [Creating a dedicated vCenter user account and assigning the role in vCenter](#)..... 192
- [Best practices with the VM Direct appliance](#)..... 195
- [Troubleshooting backup configuration issues](#)..... 200
- [Troubleshooting virtual machine backup issues](#)..... 201
- [Recover a failed PowerProtect Data Manager backup](#)..... 205
- [Troubleshooting virtual machine restore issues](#)..... 205
- [Troubleshoot recovery of PowerProtect Data Manager](#)..... 212
- [Application agent and File System agent co-existence](#)..... 212
- [Microsoft application agent for SQL Server application-aware protection](#)..... 214
- [Troubleshooting Microsoft Application Agent discoveries on Windows 2008 and Application Direct](#)..... 216
- [Supporting more than 50 database clients](#)..... 216
- [File System agent limitations](#)..... 216
- [Storage Direct agent limitations](#)..... 218
- [Time synchronization required between PowerProtect Data Manager and the systems it interfaces with](#)..... 221
- [PowerProtect Data Manager allows completion of protection policy when storage unit on the Data Domain cannot be created](#)..... 221
- [Viewing the DD Boost storage unit password](#)..... 221

## Compatibility information

Software compatibility information for the PowerProtect Data Manager software is provided in the eLab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.

## Power off the PowerProtect Data Manager OVA

### Before you begin

Stop any tasks or services that are in process.

### Procedure

1. In vCenter, select the VM that has the PowerProtect Data Manager OVA on it, which you would like to power off.
2. Right-click and select **Shutdown**.  
For additional details on VMware UI, refer to VMware vendor documentation.
3. Alternatively, select **Reboot**.

## Creating a dedicated vCenter user account and assigning the role in vCenter

Dell EMC strongly recommends that you set up a separate vCenter user account at the root level of the vCenter that is strictly dedicated for use with PowerProtect Data Manager and the VM Direct protection engine.

Use of a generic user account such as “Administrator” might make future troubleshooting efforts difficult as it might not be clear which “Administrator” actions are actually interfacing, or communicating, with PowerProtect Data Manager. Using a separate vCenter user account ensures maximum clarity if it becomes necessary to examine vCenter logs.

You can specify the credentials for this vCenter user account when you add the vCenter as an asset source in the UI. Note that when adding the vCenter, ensure that you specify a user whose role is defined at the vCenter level, as opposed to being restricted to a lower level container object in the vSphere object hierarchy.

## Specify the required privileges for a dedicated vCenter user account

You can use the **vSphere Client** to specify the required privileges for the dedicated vCenter user account, or you can use the **PowerCLI**, which is an interface for managing vSphere. The following table includes the privileges required for this user.

### About this task

**Table 23** Minimum required vCenter user account privileges

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
Alarms	<ul style="list-style-type: none"> <li>• Create alarm</li> <li>• Modify alarm</li> </ul>	<pre>\$privileges = @( 'System.Anonymous', 'System.View', 'System.Read', 'Global.ManageCustomFields',</pre>
Datastore	<ul style="list-style-type: none"> <li>• Allocate space</li> </ul>	



Table 23 Minimum required vCenter user account privileges (continued)

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
	<ul style="list-style-type: none"> <li>Browse datastore</li> <li>Configure datastore</li> <li>Low-level file operations</li> <li>Move datastore</li> <li>Remove datastore</li> <li>Remove file</li> <li>Rename datastore</li> </ul>	'Global.SetCustomField', 'Global.LogEvent', 'Global.CancelTask', 'Global.Licenses', 'Global.Settings', 'Global.DisableMethods', 'Global.EnableMethods', 'Folder.Create', 'Datastore.Rename', 'Datastore.Move', 'Datastore.Delete', 'Datastore.Browse', 'Datastore.DeleteFile', 'Datastore.FileManagement', 'Datastore.AllocateSpace', 'Datastore.Config', 'Network.Config', 'Network.Assign', 'Host.Config.Storage', 'VirtualMachine.Inventory.Create', 'VirtualMachine.Inventory.Register', 'VirtualMachine.Inventory.Delete', 'VirtualMachine.Inventory.Unregister', 'VirtualMachine.Interact.PowerOn', 'VirtualMachine.Interact.PowerOff', 'VirtualMachine.Interact.Reset', 'VirtualMachine.Interact.ConsoleInteract', 'VirtualMachine.Interact.DeviceConnection', 'VirtualMachine.Interact.SetCDMedia', 'VirtualMachine.Interact.ToolsInstall', 'VirtualMachine.Interact.GuestControl', 'VirtualMachine.GuestOperations.Query', 'VirtualMachine.GuestOperations.Modify', 'VirtualMachine.GuestOperations.Execute', 'VirtualMachine.Config.Rename', 'VirtualMachine.Config.Annotation', 'VirtualMachine.Config.AddExistingDisk', 'VirtualMachine.Config.AddNewDisk', 'VirtualMachine.Config.RemoveDisk', 'VirtualMachine.Config.RawDevice', 'VirtualMachine.Config.HostUSBDevice', 'VirtualMachine.Config.CPUCount', 'VirtualMachine.Config.Memory', 'VirtualMachine.Config.AddRemoveDevice', 'VirtualMachine.Config.EditDevice', 'VirtualMachine.Config.Settings', 'VirtualMachine.Config.Resource', 'VirtualMachine.Config.UpgradeVirtualHardware', 'VirtualMachine.Config.ResetGuestInfo', 'VirtualMachine.Config.AdvancedConfig', 'VirtualMachine.Config.DiskLease', 'VirtualMachine.Config.SwapPlacement', 'VirtualMachine.Config.DiskExtend', 'VirtualMachine.Config.ChangeTracking', 'VirtualMachine.Config.ReloadFromPath', 'VirtualMachine.Config.ManagedBy', 'VirtualMachine.State.CreateSnapshot', 'VirtualMachine.State.RevertToSnapshot', 'VirtualMachine.State.RemoveSnapshot', 'VirtualMachine.Provisioning.MarkAsTemplate', 'VirtualMachine.Provisioning.DiskRandomAccess', 'VirtualMachine.Provisioning.DiskRandomRead', 'VirtualMachine.Provisioning.PutVmFiles', 'Resource.AssignVMToPool', 'Resource.HotMigrate', 'Resource.ColdMigrate',
Extension	<ul style="list-style-type: none"> <li>Register extension</li> <li>Unregister extension</li> <li>Update extension</li> </ul>	
Folder	<ul style="list-style-type: none"> <li>Create folder</li> </ul>	
Global	<ul style="list-style-type: none"> <li>Cancel task</li> <li>Disable methods</li> <li>Enable methods</li> <li>Licenses</li> <li>Log event</li> <li>Manage custom attributes</li> <li>Settings</li> <li>Set custom attribute</li> </ul>	
Host	<ul style="list-style-type: none"> <li>Configuration &gt; Storage partition configuration</li> </ul>	
Network	<ul style="list-style-type: none"> <li>Assign network</li> <li>Configure</li> </ul>	
Resource	<ul style="list-style-type: none"> <li>Assign virtual machine to resource pool</li> <li>Migrate powered off virtual machine</li> <li>Migrate powered on virtual machine</li> </ul>	
Sessions	<ul style="list-style-type: none"> <li>Validate session</li> </ul>	
Tasks	<ul style="list-style-type: none"> <li>Create task</li> <li>Update task</li> </ul>	
vApp	<ul style="list-style-type: none"> <li>Export</li> <li>Import</li> <li>vApp application configuration</li> </ul>	
Virtual Machine		

**Table 23** Minimum required vCenter user account privileges (continued)

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
Configuration	<ul style="list-style-type: none"> <li>• Add existing disk</li> <li>• Add new disk</li> <li>• Add or remove device</li> <li>• Advanced</li> <li>• Change CPU count</li> <li>• Change resource</li> <li>• Configure managed by</li> <li>• Disk change tracking</li> <li>• Disk Lease</li> <li>• Extend virtual disk</li> <li>• Host USB device</li> <li>• Memory</li> <li>• Modify device settings</li> <li>• Raw device</li> <li>• Reload from path</li> <li>• Remove disk</li> <li>• Rename</li> <li>• Reset guest information</li> <li>• Set annotation</li> <li>• Settings</li> <li>• Swapfile placement</li> <li>• Upgrade virtual machine compatibility</li> </ul>	<pre>'Alarm.Create', 'Alarm.Edit', 'Task.Create', 'Task.Update', 'Sessions.ValidateSession', 'Extension.Register', 'Extension.Update', 'Extension.Unregister', 'VApp.ApplicationConfig', 'VApp.Export', 'VApp.Import' ) New-VIRole -Name 'PowerProtect' -Privilege (Get-VIPrivilege -Id \$privileges)</pre>
Guest Operations	<ul style="list-style-type: none"> <li>• Guest operation modifications</li> <li>• Guest operation program execution</li> <li>• Guest operation queries</li> </ul>	
Interactions	<ul style="list-style-type: none"> <li>• Configure CD media</li> <li>• Console interaction</li> <li>• Device Connection</li> <li>• Guest operating system management by VIX API</li> <li>• Power off</li> <li>• Power on</li> <li>• Reset</li> <li>• VMware Tools install</li> </ul>	
Inventory	<ul style="list-style-type: none"> <li>• Create new</li> </ul>	

**Table 23** Minimum required vCenter user account privileges (continued)

Setting	vCenter 6.0 and later required privileges	PowerCLI equivalent required privileges
	<ul style="list-style-type: none"> <li>Register</li> <li>Remove</li> <li>Unregister</li> </ul>	
Provisioning	<ul style="list-style-type: none"> <li>Allow disk access</li> <li>Allow read-only disk access</li> <li>Allow virtual machine download</li> <li>Mark as Template</li> </ul>	
Snapshot Management	<ul style="list-style-type: none"> <li>Create snapshot</li> <li>Remove Snapshot</li> <li>Revert to snapshot</li> </ul>	

## Best practices with the VM Direct appliance

Observe the following best practices when using PowerProtect Data Manager with the VM Direct protection engine.

- Install **VMware Tools** on each virtual machine by using the **vSphere Client**. VMware Tools adds additional backup and recovery capabilities that quiesce certain processes on the guest operating system prior to backup.
- Use **Hot Add** transport mode for faster backups and restores and less exposure to network routing, firewall, and SSL certificate issues. To support **Hot Add** mode, deploy the VM Direct appliance on an ESXi host that has a path to the storage that holds the target virtual disk(s) for backup.

**Note:** **Hot Add** mode requires VMware hardware version 7 or later. Ensure all virtual machines that you want to back up are using Virtual Machine hardware version 7 or later.

For sites that contain a large number of virtual machines that do not support **Hot Add** requirements, Network Block Device (NBD) transport mode will be used. This can cause congestion on the ESXi host management network. Plan your backup network carefully for large scale NBD installs. You may consider configuring one of the following options:

- Set up Management network redundancy.
- Set up backup network to ESXi for NBD.
- Set up storage heartbeats. <http://www.vmware.com/files/pdf/techpaper/vmw-vsphere-high-availability.pdf> provides more information.
- If you have vFlash-enabled disks and are using hotadd transport mode, ensure that you configure the vFlash resource for the VM Direct host with sufficient resources (greater than or equal to the virtual machine resources), or migrate the VM Direct appliance to a host with vFlash already configured. Otherwise, backup of any vFlash-enabled disks will fail with the error "VDDK Error: 13: You do not have access rights to this file," and the error "The available virtual flash resource '0' MB ('0' bytes) is not sufficient for the requested operation" on the vCenter server.
- Avoid deploying VMs with IDE virtual disks; using IDE virtual disks degrades backup performance. Use SCSI virtual disks instead whenever possible.

**Note:** You cannot use **Hot Add** mode with IDE Virtual disks and therefore backup of these disks will be performed using NBD mode.

- During policy configuration, assign virtual machines to a protection group based on logical grouping to allow for better scheduling of backups that will help you avoid resource contention and create more organized logs for review.
- When configuring or unconfiguring a very large number of virtual machines (300 or more) in a protection policy, an error message might display indicating that the request is too large. You can click **OK** and proceed, but system performance will be impacted due to the size of the request. As a best practice, it is recommended to use dynamic filters to automatically determine which assets are assigned to protection policies when the assets are discovered.
- When you plan the backups, ensure that PowerProtect Data Manager supports the disk types that you use in the environment. Currently, PowerProtect Data Manager does not support the following disk types:
  - Independent (persistent and non-persistent)
  - RDM Independent - Virtual Compatibility Mode
  - RDM Physical Compatibility Mode
- The VM Direct appliance uses Changed Block Tracking (CBT) by default. If CBT is disabled on the virtual machine, then it will enable CBT automatically. If you add a disk to the virtual machine after the first full backup, for the next policy run a full backup will be performed automatically for the newly added disk, and an incremental backup will be performed for the existing disk.
- When backing up thin-provisioned Virtual Machines or disks for Virtual Machines on NFS datastores, an NFS datastore recovery does not preserve thin provisioning. VMware knowledge base article 2137818 at <http://kb.vmware.com/kb/2137818> provides more information.
- Virtual Machines with extremely high IO may face hangs during consolidation due to the ESXi forced operation called synchronous consolidate. Plan your backups of such Virtual Machines according to the amount of workload on the Virtual Machine.


## Software and hardware requirements

The following table lists the required components for PowerProtect Data Manager and the VM Direct protection engine.

**Table 24** PowerProtect Data Manager and VM Direct appliance requirements

Component	Requirements
PowerProtect Data Manager with the VM Direct appliance	Version 19.2 or later
vCenter Server	<ul style="list-style-type: none"> <li>• vSphere and ESXi versions 6.0, 6.5, 6.7.</li> <li>• <b>Note:</b> Version 6.5 and later is required to perform Microsoft SQL Server application-aware protection.</li> </ul> <p>Refer to VMware documentation on physical host requirements for the ESXi hosts:</p> <ul style="list-style-type: none"> <li>• <a href="#">ESXi 6.5 minimum requirements</a></li> <li>• <a href="#">ESXi 6.0 hardware requirements</a></li> </ul>
VMware Tools	Version 10 or later.

**Table 24** PowerProtect Data Manager and VM Direct appliance requirements (continued)

Component	Requirements
	 <b>Note:</b> Version 10.1 and later is required to perform Microsoft SQL Server application-aware protection.
Data Domain	<ul style="list-style-type: none"> <li>• A minimum of one configured DD Boost device is required. Note that all models of Data Domain are supported.</li> <li>• Data Domain operating system (DDOS) version 6.1 and later and the Data Domain Management Console (DDMC).</li> <li>• Make note of the hosts writing backups to your Data Domain(s).</li> </ul>
Web browser	The latest version of the Google Chrome browser in order to access the PowerProtect Data Manager UI.

## PowerProtect Data Manager resource requirements on VMware environment

PowerProtect Data Manager has the following minimum system requirements for the VMware environment (ESXi server) it is running on:

- 10 CPU cores
- 18 GB (The ESXi server requires at least 18 GB of RAM available for PowerProtect Data Manager)
- Five total disks:
  - Disk 1 of 100 GB
  - Disk 2 of 500 GB
  - Disk 3 of 10 GB
  - Disk 4 of 10 GB
  - Disk 5 of 5 GB
- One 1-GB NIC

## Configuration checklist for common issues

The following configuration checklist provides best practices and troubleshooting tips that might help resolve some common issues.

### Basic configuration

Review the following basic configuration requirements:

- Synchronize system time between vCenter and ESX/ESXi/vSphere.
- Assign IPs carefully — do not reuse any IP addresses.
- Use Fully Qualified Domain Names (FQDNs) where possible.
- For any network related issue, confirm that forward and reverse DNS lookups work for each host in the datazone.

### Virtual machine configuration

Review the following virtual machine configuration requirements:

- Ensure that the virtual machine has access to and name resolution for the Data Domain system.
- Ensure that the virtual machine firewall has port rules for Data Domain.
- For application-aware backups, ensure that Microsoft SQL Server instances are enabled for data protection using a SYSTEM account, as described in the software and security requirements section of the topic [Microsoft Application Agent for SQL Server application-aware protection](#).

## VM Direct appliance performance and scalability

The VM Direct appliance performance and scalability depends on several factors, including the number of vCenter Servers and proxies and the number of concurrent virtual machine backups. The following table provides information on these scalability factors and maximum recommendations, in addition to concurrence recommendations for sessions created from backups using the VM Direct Engine.

The count of sessions is driven by the number of proxies, and backups running through this server.

**Table 25** Performance and scalability factors

Component	Maximum limit	Recommended count	Notes
Number of concurrent NBD backups per ESXi Server	50 (10G network)		VMware uses Network File Copy (NFC) protocol to read VMDK using NBD transport mode. You need one VMware NFC connection for each VMDK file being backed up. The VMware Documentation provides more information on vCenter NFC session connection limits.
Concurrent VMDK backups per vCenter Server		100	Can be achieved with a combination of the number of proxies multiplied by the number of configured Hot Add sessions per VM Direct appliance.
Number of proxies per vCenter Server		4	A limit of 25 concurrent backup and recovery sessions.
Number of files/directories per file level recovery	200,000		File-level recovery is recommended for quickly recovering a small set of files. Image-level or VMDK-level recoveries are optimized and recommended for recovering a large set of files/folders.

**Table 26** Proxy session limits by proxy type

Component	Total number of sessions (backup and recovery) maximum	Notes
Added (External) VM Direct appliance	25	
Embedded VM Direct appliance (the proxy pre-bundled with the PowerProtect Data Manager software)	4	The embedded proxy is only used as a fallback when all other proxies are disabled or in Failed state.

## Increasing the number of instant access sessions

PowerProtect Data Manager supports up to 32 concurrent instant access sessions at the storage level.

You can increase the number of sessions by adding an external VM Direct appliance and modifying a configuration file to override the automatically deployed proxy's maximum sessions value. Note that sessions created in excess of the maximum concurrent sessions supported will be queued for 24 hours before timing out. To increase the number of concurrent sessions manually to match the capability of the underlying cluster, perform the following steps.

1. Create a file named `vmdm_recovery.properties` in the `/usr/local/brs/lib/vmdm/config/` directory.
2. Add the parameter value to override the default value. For example:  
`vmdm_recovery.queue.ia_session_allowance=32`
3. Run `vmdm stop` and then `vmdm start` to restart the vmdm service.

## Enabling or disabling Changed Block Tracking

The VM Direct Engine uses changed block tracking (CBT) automatically upon the first virtual machine backup so that only changed disk areas on the virtual machine are backed up. Some virtual machines, however, do not support CBT and you may be required to disable CBT for those virtual machines.

A vCenter administrator can control the application of CBT by using the custom field **EMC VM Direct Disable CBT** in the **vSphere Client**. You can set this custom field to **true** to disable CBT, or **false** to enable CBT. If you do not set this field for a virtual machine, or the field is not present, CBT is enabled by default for that virtual machine.

To set CBT for virtual machines, perform the following:

1. Log into the **vSphere Client** (vSphere versions 6 and earlier) or **vSphere Web Client** (vSphere versions 6.5 and later) as an administrator.
2. Select a virtual machine in the vCenter tree, and then click the **Summary** tab.
3. Edit the virtual machine attributes:
  - In vSphere versions 6.x and earlier, click **Edit** in the **Annotation** box.
  - In vSphere versions 6.5 and later, click **Edit** under **Custom Attributes**.
4. Locate the **EMC VM Direct Disable CBT** field, or create a string for **EMC VM Direct Disable CBT**. The string must match the field name exactly and is case-sensitive.
5. Set the value to **true** to disable CBT on the virtual machine, or to **false** (or leave the field blank) to enable CBT on the virtual machine. Setting or resetting the field for one virtual machine does not affect the other virtual machines in the vCenter.

### Fixing CBT if corrupted on virtual machine

If CBT becomes corrupted on the virtual machine, warnings similar to the following appear in the backup logs:

```
WARN: Change block tracking needs to be reset.
WARN: Change Block Tracking could not be reset, causing full backup: Second attempt failed.
NOTICE: Change block tracking cannot be reset by proxy. Please remediate VM.
```

If these messages appear, you can use PowerCLI commands to disable and then enable CBT without powering off the virtual machines as described in the VMware knowledgebase article at <https://kb.vmware.com/selfservice/search.do?>

[cmd=displayKC&docType=kc&docTypeID=DT\\_KB\\_1\\_1&externalId=1031873](#), or perform the following steps to clean up CBT:

1. Power down the virtual machine.
2. Remove CBT flags.
3. Delete CTK files from the datastore.
4. Power ON the virtual machine.

## Configure a backup to support vSAN datastores

Backup and recovery functionality is supported for vSAN virtual machines.


### About this task

When performing backups or restores of virtual machines residing on vSAN datastores, it is highly recommended to deploy the VM Direct appliance on a vSAN datastore. A VM Direct appliance deployed on any one vSAN datastore can be used for backing up virtual machines from other vSAN or non-vSAN datastores by using **Hot Add** or **nbdssl** transport modes, as applicable.


## Disable SSL certification on the vCenter Server

If the vCenter's SSL certificate cannot be trusted automatically, a dialog box appears when adding the vCenter Server as an asset source in the PowerProtect Data Manager UI, requesting certificate approval. It is highly recommended that you do not disable certificate enforcement.

If disabling of the SSL certificate is required, you can perform the following procedure.

 **WARNING** These steps should only be performed if you are very familiar with certificate handling and the issues that can arise from disabling a certificate.

1. Create the following files (and file contents) in the `/home/admin` directory on the VM Direct appliance:
  - A file named `cbs_vmware_connection.properties` with the line `cbs.vmware_connection.ignore_vcenter_certificate=true`
  - A file named `vmdm_vmware_connection.properties` with the line `vmdm.vmware_connection.ignore_vcenter_cert=true`
  - A file named `.vmdm_discovery.properties` with the line `vmdm.discovery.ignore_vcenter_cert=true`

 **Note:** Note the period at the start of this file.
2. Run `cbs stop` to stop the cbs service, and then `cbs start` to restart the service.
3. Run `vmdm stop` to stop the vmdm service, and then `vmdm start` to restart the service.
4. Perform a test to determine if SSL certificate disabling was successful by adding a vCenter Server using the vCenter's IP address (if the SSL certificate uses FQDN), and then verify that the asset source was added and virtual machine discovery was successful.

## Troubleshooting backup configuration issues

The following section provides a list of error messages that might appear when you configure an appliance backup configuration.

**Data Domain storage unit mount command failed with error: 'Cannot mount *full path*: Access is denied'**

This error message appears when an NFS export does not exist on the Data Domain System for the full path to the DD Boost Storage Unit.



To resolve this issue, ensure that you have configured an NFS export for the full path of the DD Boost storage unit and that the appliance is an Export client.

**Data Domain storage unit mount command failed with error: 'Cannot resolve FQDN: The name or service not known'**

This error message appears when the appliance cannot contact the Data Domain System by using the specified FQDN. To resolve this issue, ensure that you can resolve the FQDN and IP address of the Data Domain System.

## Troubleshooting virtual machine backup issues

This section provides information about issues related to virtual machine backup operations with the VM Direct protection engine.

### VM Direct limitations and unsupported features

Review the following limitations and unsupported features related to the VM Direct appliance.

**VMware limitations by vSphere version**

VMware limitations for vSphere 6.0 and later versions are available at <https://configmax.vmware.com/home>. For vSphere 5.5, go to <https://www.vmware.com/pdf/vsphere5/r55/vsphere-55-configuration-maximums.pdf>.

**VM Direct appliance configuration settings cannot be modified after adding the VM Direct appliance**

After adding a VM Direct appliance, the only field you can modify is the **Transport Mode**. Any other configuration changes require you to delete and then re-add the VM Direct appliance. [Additional VM Direct actions](#) on page 109 provides more information.

**Limitations to SQL Server application consistent data protection**

Review the SQL Server application-consistent protection support limitations in the section [Microsoft application agent for SQL Server application-aware protection](#) on page 214.

**Network configuration settings are not restored with virtual machine after recovery of a vApp backup**

Network configuration settings are not backed up with the virtual machine as part of a vApp backup. As a result, when you restore a vApp backup, you must manually reconfigure the network settings.

**VM Direct appliance configured with dual stack is not supported**

The VM Direct appliance does not support dual stack (IPv4 and IPv6) addressing. If you want to run backups and restores using the VM Direct appliance, use IPv4 only addressing.

**Virtual machine alert "VM MAC conflict" may appear after successful recovery of virtual machine**

After performing a successful recovery of a virtual machine through vCenter version 6, an alert may appear indicating a "VM MAC conflict" for the recovered virtual machine, even though the new virtual machine will have a different and unique MAC address. You must manually acknowledge the alert or clear the alert after resolving the MAC address conflict. Note that this alert can be triggered even when the MAC address conflict is resolved.

The VMware release notes at [http://pubs.vmware.com/Release\\_Notes/en/vsphere/60/vsphere-vcenter-server-60u2-release-notes.html](http://pubs.vmware.com/Release_Notes/en/vsphere/60/vsphere-vcenter-server-60u2-release-notes.html) provide more information.

**Protection fails for virtual machine name containing { or }**

A PowerProtect Data Manager virtual machine protection policy fails to back up virtual machines that contain the special characters { or } in the name. This limitation exists with vSphere versions previous to 6.7. If you do not have vSphere 6.7 installed, avoid using these two characters in virtual machine names.

**Datastore names cannot contain special characters**

Using special characters in datastore names can cause problems with the VM Direct Engine, such as failed backups and restores. Special characters include the following: % & \* \$ # @ ! \ / : \* ? " < > | ; , and so on.

**Hot Add backups fail when datacenter names contain special characters**

Virtual machine backups fail when the datacenter name contains special characters and the transport mode specified for VM Direct backups is **Hot Add only**. Avoid using special characters in the datacenter name, for example, "Datacenter\_#2@3", or specify **Hotadd with fallback to Network Block Device** for the transport mode.

**Hot Add backups fail when virtual machine protection policy configured with Virtual Flash Read Cache value**

When using **Hot Add** transport mode for a virtual machine protection policy, the backup fails with the following error if configured with the Virtual Flash Read Cache (vFRC) value:

```
"Backup has FAILED. Failed to backup
virtual disk \"Hard disk <no.>\". Failed to initialize Block
Reader. Failed to open source VMDK \<dataStore
name>/<VM Name.vmdk>\": VDDK Error: 13: You do not have
access rights to this file. (500)".
```

**Backups fail for resource pools recreated with the same name as deleted pool**

When you delete a resource pool in vCenter and then recreate a resource pool with the same name, backups fail. Re-configure the protection group with the newly created resource pool.

**Data Domain Boost over fibre channel not supported**

PowerProtect Data Manager does not support Data Domain Boost over fibre channel (DFC).

**SAN transport mode not supported**

PowerProtect Data Manager supports only the Hot Add and NBD transport modes. The Hot Add mode is the default transport mode. For a protection policy, you can specify to use only Hot Add mode, only NBD mode, or Hot Add mode with fallback to NBD of Hot Add is not available.

**Specify NBD for datastores if VM Direct should use NBD mode only**

For a VM Direct appliance that will only use NBD transport mode, you must also specify the datastores for which you want the proxy to perform only NBD backups to ensure that any backups of virtual machines running on these datastores are always performed using NBD mode. This also ensures that the same NBD-only proxies are never used for backups of virtual machines residing on any other datastores.

**Backup of individual folders within a virtual machine is not supported**

PowerProtect Data Manager only supports image-level backup and disk-level backup. You cannot perform backups of individual folders within the virtual machine.

**I/O contention when all Virtual Machines on a single data store**

I/O contention may occur during snapshot creation and backup read operations when all Virtual Machines reside on a single datastore.

### VMware snapshot for backup is not supported for independent disks

When using independent disks you cannot perform VMware snapshot for backup.

## Managing command execution for VM Direct Agent operations on Linux

The **VM Direct Agent** automatically creates a PAM service file named `vproxyra` in the `/etc/pam.d` `system` directory, if the file does not already exist.

This file, which enables you to manage command execution through the **VM Direct Agent**, is modeled on the corresponding `vmtoolsd` file. The settings in this file permit command execution by any user who is able to perform VM Direct operations on the guest virtual machine. A system administrator can further modify this file to specify which users can perform **VM Direct Agent** operations, for example, file-level restore and SQL application-aware protection. For more information on the configuration of PAM service files, see the system documentation for your specific guest virtual machine operating system.

## SQL Server application-consistent backups fail with error "Unable to find VSS metadata files in directory"

SQL Server application-consistent virtual machine backups might fail with the following error when the `disk.EnableUUID` variable for the virtual machine is set to `False`.

```
Unable to find VSS metadata files in directory C:\Program Files\DPSAPPS
\MSVMAPPAGENT\tmp\VSSMetadata.xxxx.
```

To resolve this issue, ensure that the `disk.EnableUUID` variable for the virtual machines included in an SQL Server application-consistent backup is set to `True`.

## Failed to lock Virtual Machine for backup: Another EMC VM Direct operation 'Backup' is active on VM

This error message appears when a backup fails for a virtual machine, when previous backups of the virtual machine was abruptly ended and the VM annotation string was not cleared.

To resolve this issue, clear the annotation string value for the virtual machine.

1. Connect to the vCenter server and navigate **Home > Inventory > Hosts and Clusters**.
2. Select the virtual machine, and then select the **Summary** tab.
3. Clear the value that appears in the **EMC Proxy Session** field.

## vMotion operations are not allowed during active backup operations

The vSphere vMotion feature enables the live migration of running virtual machines from one physical server to another. You cannot run vMotion operations on the VM Direct appliance or VMware Backup appliance during active backup operations. This is expected behavior. Wait until all backup operations have completed prior to performing a vMotion operation.

## Backups fail if certain characters are used in the virtual machine name, datastore, folder, or datacenter names

When you use spaces or special characters in the virtual machine name, datastore, folder, or datacenter names, the `.vmx` file is not included in the backup. The VM Direct appliance does not

back up objects that include the following special characters, in the format of character/escape sequence:

- & %26
- + %2B
- / %2F
- = %3D
- ? %3F
- % %25
- \ %5C
- ~ %7E
- ] %5D

## Lock placed on virtual machine during backup and recovery operations continues for 24 hours if VM Direct appliance fails

During VM Direct backup and recovery operations, a lock is placed on the virtual machine. If a VM Direct appliance failure occurs during one of these sessions, the lock is extended to a period of 24 hours, during which full backups and transaction log backups will fail with the following error until the lock is manually released:

```
Cannot lock VM 'W2K8R2-SQL-2014' (vm-522): Another EMC vProxy operation 'Backup' is active on VM vm-522.
```

### Workaround

To manually release the lock on the virtual machine:

1. Open the **vSphere Web Client**.
2. Select the virtual machine and select **Summary**.
3. Select **Custom attribute** and click **Edit**.
4. Remove the attribute **EMC VM Direct Session**.

## Trailing spaces not supported in SQL database names

Due to a VSS limitation, you cannot use trailing spaces within the names of SQL databases protected by an application-consistent data protection policy.

## SQL databases skipped during virtual machine transaction log backup

When an advanced application-consistent policy is enabled with transaction log backup, the `msvmagent_appbackup.exe` program evaluates databases to determine if transaction log backup is appropriate.

If transaction log backup is not appropriate for a database, the database will automatically be skipped. Databases are skipped for the following reasons:

**Table 27** SQL Skipped Database Cases and Descriptions

Case	Description
Database has been restored	When a database has been restored, this database will be skipped during transaction log backup because there is no Backup Promotion.

**Table 27** SQL Skipped Database Cases and Descriptions (continued)

Case	Description
System Database	System databases are automatically skipped for transaction log backup.
Database State	Database is not in a state that allows backup. For example, the database is in the NORECOVERY state.
Recovery Model	Database is in SIMPLE recovery model, which does not support transaction log backup
Other Backup Product	Most recent backup for the database was performed by a different backup product.
New Database	Database was created after most recent full backup.
Backup Failure	Database was in state to allow backup, backup was attempted, but backup failed.

All skipped databases will be backed up as part of the next full backup. Also, a skipped database will not result in `msvmagent_appbackup.exe` failure. The only instance in which `msvmagent_appbackup.exe` would potentially fail is if all databases failed to back up.

The `msvmagent_appbackup.exe` program generates a history report of the databases, if the database backup status was success/skipped/failed, and a reason if they were skipped or failed if applicable. This history report is visible in the action logs for the VM Direct Engine, which are available as part of the appbackup logs.

**Note:** For SQL virtual machine application-consistent data protection, the SQL and operating system versions follow the NMM support matrix available at <http://compatibilityguide.emc.com:8080/CompGuideApp/>.

## Accessing Knowledge Base Articles

Additional troubleshooting information is available through the Featured VMware Documentation Sets website at <https://www.vmware.com/support/pubs/>. Select **Support > Search Knowledge Base**.

## Recover a failed PowerProtect Data Manager backup

### Procedure

1. Redeploy the PowerProtect Data Manager OVA.
2. Call Dell EMC Technical support.

## Troubleshooting virtual machine restore issues

The following topics provide information on troubleshooting virtual machine restore failures.

### Virtual machine protection copy does not display under available copies

If a virtual machine protection copy does not display under the available copies in PowerProtect Data Manager, verify the following:

- Ensure that protection of the virtual machine completed successfully.
- Check that the desired copy has not expired according to the PowerProtect Data Manager protection policy.

- Run a discovery of the Data Domain Management Center (DDMC) and ensure that discovery completed successfully for virtual machine copies.
- Check the discovery logs for any exceptions or errors that might have occurred during discovery.

### Virtual machine restore fails with name resolution error

A virtual machine restore might fail with the following error due to network issues between Data Domain and PowerProtect Data Manager or the vCenter/ESXi:

```
com.emc.brs.vmdm.http.HttpsConnector - null: Temporary failure in name
resolution
java.net.UnknownHostException : null: Temporary failure in name resolution
```

Ensure that you have proper name resolution between the Data Domain and PowerProtect Data Manager /vCenter/ESX.

### DD NFS share not removed after restore to original

The DD NFS share might not be removed after a successful virtual machine restore to original. When this occurs, the restore hangs and the following DD NFS clients appear enabled in the Data Domain.

**Figure 9** DD NFS clients still enabled after restore

```
/data/coll/ECM-PP4W-37/vProxy-vm-qa-0187.aal.lab.emc.com-58e24edf-17f0-4d00-a53d-da6494a3af1b 10.25.11.197 (secmaya_rv,no_root_squash,no_all_squash,secure,nolog)
/data/coll/ECM-PP4W-37/vProxy-vm-qa-0187.aal.lab.emc.com-58e24edf-17f0-4d00-a53d-da6494a3af1b 10.6.249.100 (secmaya_rv,no_root_squash,no_all_squash,secure,nolog)
/data/coll/ECM-PP4W-37/vProxy-vm-qa-0187.aal.lab.emc.com-58e24edf-17f0-4d00-a53d-da6494a3af1b 10.4.249.140 (secmaya_rv,no_root_squash,no_all_squash,secure,nolog)
/data/coll/ECM-PP4W-37/vProxy-vm-qa-0187.aal.lab.emc.com-58e24edf-17f0-4d00-a53d-da6494a3af1b fe80:1250:56ff:fe6d:eb03 (secmaya_rv,no_root_squash,no_all_squash,secure,nolog)
/data/coll/ECM-PP4W-37/vProxy-vm-qa-0187.aal.lab.emc.com-58e24edf-17f0-4d00-a53d-da6494a3af1b fe80:122f:d0ff:fe07:d0f2 (secmaya_rv,no_root_squash,no_all_squash,secure,nolog)
```

If you encounter this issue, you can wait 24 hours for PowerProtect Data Manager to clean up the DD NFS shares, or you can stop the restore and clean up the DD NFS clients manually by performing the following steps:

1. Restart the VMDM service by typing `/usr/local/brs/lib/vmdm/bin/vmdm restart`.
2. Clean up DD NFS clients by typing `nfs del <Path> <Client>`.
3. In the vSphere Client's **Configuration** tab, manually unmount the `EMC-vProxy-vm-qa-xxxxxx` DDNFS datastore that is mounted on the ESXi host.

### Virtual machine restore fails with error due to VM Direct corruption

A virtual machine restore might fail with the following error due to corruption of the VM Direct Engine that is running in PowerProtect Data Manager:

```
com.emc.dpsg.vproxy.client.VProxyManager - Error(createSession):
javax.net.ssl.SSLException:
Unrecognized SSL message, plaintext connection
```

Ensure that the `vproxyd` service is running in PowerProtect Data Manager by typing the following command.

```
ps xa | grep vproxy
```

Ensure that the `vproxy rpm` is installed as expected in PowerProtect Data Manager by typing the following command.

```
rpm -qa | grep vProxy
```

When logged in as the root user, restart the `vproxyd` service on PowerProtect Data Manager by typing the following command.

```
systemctl restart vproxyd
```

### Virtual machine restore fails with error "Unable to create NAS Datastore"

A virtual machine restore might fail with the following error when a change is made to the DD restore user role in Data Domain:

```
Unable to create NAS Datastore: Unable to create NFS export at 'irv-dd9500-skyline1.as1.lab.emc.com:/data/col1/eCDM-SU-1497653922167/vProxy-vm-qa-1084.as1.lab.emc.com-abfd110d-cdfa-4517-9485-27767ef75d35':
```

Ensure that the DD user performing the restore has the **admin** role. You can change the user's status in Data Domain by identifying the Data Domain user that starts with **ecdmsu-admin** and using the following commands:

To check the user's status, type `user show list`

To change the role of the user, type `user change role <ecdmsu-admin-xxxxxxxxxxxx> admin`

### Virtual machine restore fails with error "User UserEARA does not have proper privileges"

A virtual machine restore fails with the error "User UserEARA does not have proper privileges" when the user does not have adequate privileges to perform the restore operation.

Ensure that the PowerProtect Data Manager user performing the restore belongs to System Tenant and has the Export and Recovery Admin role.

### Virtual machine restore fails when the previous restore of this virtual machine is in progress or did not complete

A virtual machine restore fails with the following error if the previous restore operation for the same virtual machine is still in progress or did not complete successfully:

```
Error : There is another running restore operation that conflicts with this request.
```

If the previous restore operation for this virtual machine is still in progress, monitor the progress in PowerProtect Data Manager until the restore completes. If the virtual machine restore is complete but the task stops responding, then you must manually cancel the restore in PowerProtect Data Manager by restarting the VMDM service. You can restart the VMDM service by typing `/usr/local/brs/lib/vmdm/bin/vmdm restart`.

## Troubleshooting instant access restore failures

An instant access restore consists of two stages. First, a virtual machine is made available in the UI as an instant access virtual machine without moving the virtual machine to permanent storage. Second, storage vMotion is initiated to migrate the virtual machine to permanent storage.

If at any point during the migration a restore failure occurs, the instant access session is not automatically removed until after the expiration period for an instant access virtual machine restore, which is 7 days by default. This behavior is intentional for the following reasons:

- To avoid data loss, since changes might have been made to the virtual machine during that time
- To provide you with the opportunity to fix the issue (for example, to free up space on the restore destination or choose a different datastore) and then take the appropriate action

When the cause of the failure is determined and/or fixed, you can use the **Instant Access Sessions** window of the UI to retry the migration, or save the data and delete the instant access virtual machine, as required. The section [Manage and monitor Instant Access Sessions](#) provides detailed information about these actions.

## FLR Agent for virtual machine file-level restore

The VM Direct **FLR Agent** is required for file-level restore operations and is installed automatically on the target virtual machine when you initiate a file-level restore and provide the virtual machine credentials.

The **FLR Agent** installation on Linux virtual machines requires that you use the root account. If non-root credentials are provided for the target virtual machine, the **FLR Agent** installation fails, even if this user has privileges similar to a root user. Once the **FLR Agent** installation is completed by a root user, you can perform file-level restore operations as a non-root user.

**FLR Agent** installation on Windows virtual machines requires that you use administrative privileges. If the provided credentials for the target virtual machine do not have administrative privileges, the **FLR Agent** installation fails.

On Linux, to perform a file-level restore using a non-root user, ensure that the **FLR Agent** has already been installed on the target virtual machine using the root user account. Otherwise, ensure that you are using a supported platform and the root user is specified, and click **OK**. For Linux, file-level restore is only supported on Red Hat Enterprise Linux versions 6 and 7, and SuSE Linux Enterprise Server versions 11 and 12.

On Windows, to perform a file-level restore using a non-administrator user, ensure that the **FLR Agent** is already installed on the target machine using administrative privileges. Otherwise, ensure that an administrative user is specified, and click **OK**.

### FLR Agent installation on Windows virtual machines with User Account Control enabled

Performing the **FLR Agent** installation on User Account Control (UAC) enabled Windows virtual machine requires you to either provide the credentials of the administrator user, or to disable UAC during the **FLR Agent** installation and then re-enable upon completion.

On Windows versions 7, 8, and 10, the administrator account is disabled by default. To enable the account, complete the following steps:

1. To activate the account, open a command prompt in administrative mode, and then type `net user administrator /active: yes`.
2. To set a password for the administrator account, go to **Control Panel > User Accounts** and select the **Advanced** tab. Initially, the account password is blank.
3. In the **User Accounts** pane, right-click the user and select **Properties**, and then clear the **Account is disabled** option.

To disable UAC during the **FLR Agent** installation and then re-enable on completion of the installation, complete the following steps:

1. Initiate a file-level restore to launch the **FLR Agent installation** window. The **FLR Agent** installation is automatically started during a mount operation if it is not already installed on the destination virtual machine.
2. In the **FLR Agent installation** window, select the **Keep VM Direct FLR on target virtual machine** option.
3. Open **regedit** and change the **EnableLUA** registry key value at `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` to `0x00000000`. By default, this is set to 1.
4. Proceed with the **FLR Agent** installation.
5. Open **regedit** and reset the **EnableLUA** registry key to the previous value to re-enable UAC.

## Updating the Microsoft Application Agent and FLR Agent software


The **Microsoft Application Agent** and **FLR Agent** software required to perform SQL application-aware data protection and file-level restore operations will be automatically updated on the target



virtual machine by the VM Direct appliance during the file-level restore operation. The VM Direct appliance detects the available software on the client and updates the Agent software with the new version of software from its repository. If the update does not occur automatically, contact a Dell EMC technical support professional for a procedure to update the VM Direct software repository with the latest version of the Agent software packages.

## Supported platform versions for file-level restore

File-level restore is only supported for the following platforms and operating system versions.

 **Note:** Platforms/operating systems are qualified for file-level restore support using the default file system for these platforms.

- RedHat Enterprise Linux versions 6.x and 7.x
- SuSE Linux Enterprise Server versions 11.x and 12.x
- Debian version 9.1
- Ubuntu version 17.10
- CentOS version 7.2
- Oracle Enterprise Linux version 7.2
- Windows 7, 8, 10, Server 2008, 2012, 2016 (all 64-bit platforms and R2, where applicable) for FAT, and NTFS.

### Support for Debian or Ubuntu operating system

VM Direct file-level restore is supported on the Debian/Ubuntu operating system. To configure the Debian or Ubuntu guest operating system for file-level restore, perform the following steps.

#### About this task

 **Note:** File-level restore is not supported on Debian/Ubuntu ext4 file systems.

#### Procedure

1. Log in to the system console as a non-root user.
2. Run the `sudo passwd root` command.  
Enter the new password twice to set a password for the root account.
3. Run the `sudo passwd -u root` command to unlock the root account.
4. Specify the root user credentials in the **Dell EMC Data Protection Restore Client** and proceed to complete the file-level restore operation at least once.  
While performing the file-level restore operation for the first time, remember to select **Keep FLR agent**.
5. After performing the above steps at least once, you can revert the root account to the locked state and use non-root account for future file-level restore requests. Non-root user can lock the root account with the `sudo passwd -l root` command.

### Operating system utilities required for file-level restore

On Linux and Windows, the installed operating system must include several standard utilities in order to use file-level restore. Depending on the target operating system for restore and the types of disks or file systems in use, some of these standard utilities, however, may not be included.

The following utilities and programs may be required for performing file-level restore.

On Windows:

- `msiexec.exe`
- `diskpart.exe`
- `cmd.exe`

On Linux:

- `blkid`
- `udevadm`
- `readlink`
- `rpm`
- `bash`

**Note:** On Linux LVM, LVM2 rpm version 2.02.117 or later is required. Also, additional binaries required on Linux LVM include `dmsetup`, `lvm`, and `vgimportclone`.

## File-level restore and SQL restore limitations

This section provides a list of limitations that apply to file-level restore and individual SQL database and instance restore.

Consider the following:

- The VM Direct **FLR Agent** is installed automatically on the target virtual machine for file-level restore when a disk mount operation is initiated. The mount, however, fails and the **FLR Agent** is not installed if the user does not have sufficient administrator privileges. Ensure that the user performing file-level restore is a system administrator. Note that adding a user to the Administrators group does not grant this user sufficient privileges to perform this operation.
- When performing a file-level restore, VMDKs will fail to mount with the following error if the **FLR Agent** service is not running on the target virtual machine: "Cannot connect to vProxy Agent: dial tcp <127.0.0.1:<port>: connectex: No connection could be made because the target machine actively refused it."
- If you no longer require the VM Direct **FLR Agent** on the target virtual machine, the agent must be properly uninstalled. If you manually delete VM Direct FLR Agent files instead of uninstalling the agent, and at some point reinstall the agent, subsequent mount attempts to perform restores will fail.

To uninstall the VM Direct **FLR Agent** on Linux:

1. Execute the following command: `/opt/emc/vproxyra/bin/preremove.sh`.
2. Uninstall FLR agent package by running `rpm -e emc-vProxy-FLRAgent`.
3. If the uninstall fails due to a broken installation or other issue, you can force removal of the package by running `rpm -e --force emc-vProxy-FLRAgent`.

To uninstall the VM Direct **FLR Agent** on Windows:

1. Select **Control Panel > Programs > Programs and Features**.
  2. Locate **EMC VM Direct FLR**.
  3. Right-click the program and select **Uninstall**.
- When a file-level restore or SQL restore operation is in progress on a virtual machine, no other backup or recovery operation can be performed on this virtual machine. Wait until the file-level restore session completes before starting any other operation on the virtual machine.
  - Clean up from a suspended or cancelled mount operation requires a restart of the virtual machine before you can initiate a new mount for the file-level restore.
  - When you enable Admin Approval Mode (AAM) on the operating system for a virtual machine (for example, by setting `Registry/FilterAdministratorToken` to 1), the administrator

user cannot perform a file-level restore to the end user's profile, and an error displays indicating "Unable to browse destination." For any user account control (UAC) interactions, the administrator must wait for the mount operation to complete, and then access the backup folders located at `C:\Program Files (x86)\EMC\vProxy FLR Agent\flr\mountpoints` by logging into the guest virtual machine using Windows Explorer or a command prompt.

- When you perform file-level restore on Windows 2012 R2 virtual machines, the volumes listed under the virtual machine display as "unknown." File-restore operations are not impacted by this issue.
- When you perform file-level restore on Ubuntu/Debian platforms, you must enable the root account in the operating system. By default, the root account will be in locked state.
- You can only restore files and/or folders from a Windows backup to a Windows machine, or from a Linux backup to a Linux machine.
- You must install VMware Tools version 10 or later. For best results, ensure that all virtual machines run the latest available version of VMware Tools. Older versions are known to cause failures when you perform browse actions during file-level restore or SQL restore operations.
- You can perform file-level restore across vCenters as long as the vCenters are configured in PowerProtect Data Manager, and the source and target virtual machine have the same guest operating system. For example, Linux to Linux, or Windows to Windows.
- File-level restore does not support the following virtual disk configurations:
  - LVM thin provisioning
  - Unformatted disks
  - FAT16 file systems
  - FAT32 file systems
  - Extended partitions (Types: 05h, 0Fh, 85h, C5h, D5h)
  - Two or more virtual disks mapped to single partition
  - Encrypted partitions
  - Compressed partitions
- File-level restore of virtual machines with Windows dynamic disks is supported with the following limitations:
  - The restore can only be performed when recovering to a virtual machine different from the original. Also, this virtual machine cannot be a clone of the original.
  - The restore can only be performed by virtual machine administrator users.
  - If Windows virtual machines were created by cloning or deploying the same template, then all of these Windows virtual machines may end up using the same GUID on their dynamic volumes.
- File-level restore does not restore or browse symbolic links.
- File-level restore of Windows 8, Windows Server 2012 and Windows Server 2016 virtual machines is not supported on the following file systems:
  - Deduplicated NTFS
  - Resilient File System (ReFS)
  - EFI bootloader

## Troubleshoot recovery of PowerProtect Data Manager

When the FQDN of the recovery site is different from the FQDN of the primary site, a mount error might occur and the recovery process requires a few extra steps.

### About this task

If a mount error occurs during recovery, follow this work-around procedure.

### Procedure

1. On the Data Domain system where the backup is located, delete the replication pair and mount it for PowerProtect Data Manager.
2. When recovery is complete, on PowerProtect Data Manager, regenerate the certificates using the following command.
 

```
sudo -H -u admin /usr/local/brs/puppet/scripts/generate_certificates.sh -c
```
3. Restart the system and select the URL of the primary PowerProtect Data Manager system. The `https://PPDM IP/#/progress` page appears and recovery resumes.
4. Log in to the primary PowerProtect Data Manager.
 

The PowerProtect Data Manager VM vCenter console shows an error, which you can ignore.
5. Open the primary PowerProtect Data Manager using the original IP address and log in.


### Results

Recovery is complete.

## Application agent and File System agent co-existence

PowerProtect Data Manager supports the coexistence of the Microsoft SQL Application agent with the File System agent on Windows, and the Oracle agent with the File System agent on Linux, which enables you to protect the SQL or Oracle database with the host file system. The following co-existence scenarios are supported:

- Both agents in managed mode (registered to PowerProtect Data Manager)
- The SQL or Oracle agent in standalone mode, with the File System agent registered to PowerProtect Data Manager

 **Note:** The latest version of each agent must be installed if both agents are registered to PowerProtect Data Manager. In the single agent co-existence scenario (SQL or Oracle agent in standalone mode), the File System agent is supported in managed mode only.

The steps for installation and usage for each agent are the same.

The table below lists the supported use cases and limitations.

Category	Supported cases	Current limitations
Agent installation and uninstallation	1. New installation of both agents with: <ol style="list-style-type: none"> <li>a. SQL Application agent or Oracle Application</li> </ol>	<ul style="list-style-type: none"> <li>• Uninstalling the last agent installed on the host unregisters the host from PowerProtect Data Manager. Any new agent</li> </ul>

Category	Supported cases	Current limitations
	<p>agent in standalone or managed mode.</p> <p>b. File System agent in managed mode.</p> <ol style="list-style-type: none"> <li>2. New installation of an agent in managed mode with an already existing agent in standalone mode.</li> <li>3. New installation of an agent in standalone mode with an already existing agent in managed mode.</li> <li>4. Repair of an already existing agent installation.</li> <li>5. Uninstallation of agents.</li> </ol>	<p>installation that occurs after the uninstall will have to be newly registered to the PowerProtect Data Manager server.</p> <ul style="list-style-type: none"> <li>• Similar to the agent installations, uninstallation of each agent is performed separately.</li> </ul>
Host Registration and Un-registration	<ol style="list-style-type: none"> <li>1. Registration of an installed agent to the PowerProtect Data Manager server.</li> <li>2. Changing the registration of an already registered agent to a different PowerProtect Data Manager server.</li> <li>3. Un-registration of agents from the PowerProtect Data Manager server.</li> </ol>	<ul style="list-style-type: none"> <li>• Both agents, if operating in managed mode, should be registered to the same PowerProtect Data Manager server only. There is no option to register each agent to a different PowerProtect Data Manager server.</li> <li>• On an already registered host, performing a direct registration (explicitly using <code>register.sh/register.bat</code>) with a different PowerProtect Data Manager server IP will un-register the host from the current PowerProtect Data Manager server and register the host to the new server. Standalone agents will continue to operate in standalone mode and will not be registered.</li> <li>• Un-registering a host will un-register all of the managed agents installed on that host. Standalone agents will not be affected.</li> </ul>

Category	Supported cases	Current limitations
		<ul style="list-style-type: none"> <li>After un-registering a host, the host's assets will still display in the UI in order to support restore of these assets to a different host. However, backups will not be initiated on these assets as the protection policies will be disabled.</li> </ul>
Backup and restore features	<ol style="list-style-type: none"> <li>Protection policy creation supported on all registered agents.</li> <li>All scheduled protection policy backups are supported on both agents as per individual protection policies.</li> <li>Self-service backups are supported on both agents.</li> <li>Restores are supported on both agents.</li> <li>Compliance is supported on both agents as per the individual Service Level Agreements (SLAs).</li> </ol>	

## Microsoft application agent for SQL Server application-aware protection

The Microsoft application agent is a component of the PowerProtect Data Manager data protection solution for VMware virtual machines.

A PowerProtect Data Manager application-aware VM protection policy uses the Microsoft application agent to provide advanced application-consistent protection for the following SQL workloads:

- SQL Server full backup to Data Domain—Configure a PowerProtect Data Manager protection policy with the application-aware option to perform a SQL Server backup to a Data Domain device as part of a VMware image-level backup. A SQL Server full backup is performed during the in-guest quiesce by **VMware Tools**. When the backup is performed as part of the VMware image-level backup, the SQL data files are backed up as part of the VMDKs during the VM Direct backup. After completing the backup, the Microsoft application agent is automatically run on the virtual machine to catalog the SQL server backup on the Data Domain associated with the protection policy.
- Transaction log backup—When configuring a PowerProtect Data Manager protection policy with the **Application Aware** option, set an interval for **Transaction log backup** to enable transaction log backups for SQL instances running on the virtual machine, and specify the

frequency of backups. The Microsoft application agent is run on the virtual machine to perform the transaction log backup. Backups are written directly to the Data Domain associated with the protection policy. A transaction log backup is only performed for databases in the proper state; otherwise, databases are skipped.

- Database restore, flat file restore, table-level restore, or database Instant Access restore to the source virtual machine or an alternate virtual machine. To perform restores to an alternate virtual machine, that virtual machine must be an asset of PowerProtect Data Manager. However, instance-level restores can only be performed to the original source instance. For more details on how to use Microsoft application agent to restore SQL databases backed up with an application-aware VM protection policy, see the *PowerProtect Microsoft Application Agent SQL Server User Guide*.

The Microsoft application agent software package is bundled with the PowerProtect Data Manager appliance, and is automatically configured on a virtual machine when you add the virtual machine asset to a VM application-aware protection policy. As part of the VM protection policy configuration, both the VM Direct Agent and the Microsoft application agent are installed on the virtual machine. The Microsoft application agent installation includes the software components required for self-service restore, including the **SQL Server Management Studio Microsoft App Agent** plug-in and **ItemPoint**. After the agent installations, configuration information for the Data Domain is also sent to the virtual machine, calling the Microsoft application agent to perform the lockbox configuration. Subsequent protection policy backups and self-service restore operations jobs will also use this information without any further action required. During application-aware SQL Server full backups and transaction log backups, PowerProtect Data Manager upgrades the VM Direct Agent and Microsoft application agent software packages as required.

The virtual machine credentials provided in the protection policy or within the virtual machine asset are used during Microsoft application agent installation and during SQL Server full and transaction log backups. The Microsoft application agent is first called to validate the virtual machine SQL configuration. The agent verifies that the SQL Server is installed and running, and that the provided virtual machine credentials have the necessary permissions to perform an SQL Server backup.

In order to perform SQL Server application-consistent data protection for virtual machines, the Microsoft application agent requires the following:

- The Microsoft application agent runs under the virtual machine credentials provided in the VM protection policy or virtual machine asset for installation and data protection operations. Configure all SQL Server instances on the virtual machine to grant account rights for this account to perform SQL database backup and recovery operations:
  - Add the account to SQL logins.
  - Grant the account the sysadmin role.
- Network connectivity, hostname resolution, and firewall ports between the Data Domain device and the virtual machines that are part of SQL Server application-consistent protection policies and restore to alternate operations. This connectivity is required to enable the Microsoft application agent to perform client direct operations to Data Domain.
- VMware vCenter server version 6.5 or later.
- VMware ESXi server version 6.5 or later.
- VMware Tools version 10.1 or later.
- Enable the UUID attribute (*disk.EnableUUID=TRUE*) in the **vSphere Client**.
- The virtual machine must use SCSI disks only, and the number of available SCSI slots must at least match the number of disks. For example, a virtual machine with 7 disks will only require one SCSI controller, but a virtual machine with 8 disks will require 2 SCSI controllers.

- The VM Direct Engine requires live network connectivity to the ESXi where the targeted SQL virtual machine resides.

## Troubleshooting Microsoft Application Agent discoveries on Windows 2008 and Application Direct

When you perform a Microsoft Application Agent discovery on Windows 2008 on PowerProtect Data Manager and Application Direct versions 4.5 and 4.6, the PowerProtect Data Manager agent uses the `wmic.exe` command to discover the installed programs. The default PowerProtect Data Manager agent installation on Windows 2008 R2 produces an error in the `ecdmagent` log, and discovery fails.

In Some Windows 2008 environments, the `wmic.exe` command does not work properly when you run it from the local user or local system account, and it causes the following error: Failed to run wmic: ERROR: error running command `wmic.exe product where name like 'DDBEA and ProtectPoint Microsoft app agent' or name like 'Microsoft Application agent' get Name, Version /format:csv`: exit status 44210 To avoid the error and ensure that Microsoft Application Agent discoveries on Windows 2008 and Application Direct succeed, run the `wmic.exe` command as domain administrator instead of local administrator.

## Supporting more than 50 database clients

### About this task

If you are supporting more than 50 database clients and the following error message is displayed, perform the following steps:

```
Error:Protect Databases failed. The service is unavailable"
```

### Procedure

1. Modify the following parameter in the `/usr/local/brs/lib/zuul/conf/application.yml` file.  

$$\text{MaxTotalConnections} = (\text{Number of clients} * 12)$$
2. Increase the value in the `MaxTotalConnections` parameter by a factor of 12 for every client. For example, to protect 70 SQL clients, set the parameter to `MaxTotalConnections=840`.
3. Restart the Zuul service:

```
zuul restart
```

## File System agent limitations

Review the following limitations related to File System agent support in PowerProtect Data Manager.

- File System agent block-based backups will exclude the following:
  - Application files such as SQL and Exchange.



- HyperVisor files. Note that the File System agent is installed primarily in the guest operating system for the backup of guest file system volumes, and is not dependent on the underlying HyperVisor.
  - Data belonging to individual application writers.
  - Unsupported application writer's files.
- For any ESXi version 6.5 and earlier host with Trident storage attached, the Windows operating system deployment/installation cannot proceed and File System agent backup and restore operations will fail if the *DiskMaxIOSize* parameter is not configured with the proper value. Ensure that you set the *DiskMaxIOSize* to 1024 KB.
- It is recommended to use different mount points for each drive. Reusing mount points might cause unexpected issues during File System discovery.
- The File System agent does not support non-English operating systems. Software compatibility information for the PowerProtect Data Manager software and the File System agent is provided in the eLab Navigator, available at <https://elabnavigator.emc.com/eln/modernHomeDataProtection>.
- If a Windows or Linux File System host is unregistered from PowerProtect Data Manager and then re-registered with a different FQDN, because PowerProtect Data Manager recognizes the registration as a new host by its new name, duplicate asset entries will appear in the UI—those for the host registered earlier, as well as for the host registered by the new name. This does not impact backup and restore functionality on the new host.
- IPv6 is not supported. Use IPv4 instead.
- Image-level recovery to a system volume is not supported.
- Recovery of ReFS or deduplicated volumes to Windows 2008 R2 is not supported.
- If File System host discovery does not occur on Windows hosts, verify that the `fs plugin - adm-fs-4.0.0-1-SNAPSHOT-windows-amd64.exe` plug-in file has been copied to `C:\Program Files\DPSFSAGENT\ADM Agent\bin`. Note that copying the file to this location can take 10-15 minutes. When the plug-in file appears in this location, initiate a manual discovery from the UI's **Asset sources** window.
- File system discovery requires an ext3, ext4, or XFS file system type. Note, however, that PowerProtect Data Manager does not support ext4 file systems on SuSE Linux Enterprise Server (SLES) version 11 SP1-SP4 platforms.
- If a Windows or Linux File System host has DNS incorrectly configured or is part of a workgroup with a dummy DNS suffix added, centralized restore of a backup copy performed on this host will fail. This is because the storage name on the protection storage system is created with the actual shortname of the host, and does not include the incorrect suffix. For the same reason, a restore from PowerProtect Data Manager will also fail if the host name or domain name of the client is changed and then re-registered to PowerProtect Data Manager. As a workaround, use the `ddfsrc` command with the `-c` flag, with the short name as input to restore the required copies. More information on how to use the `ddfsrc` command is provided in the section [Performing self-service restore of a File System host](#) on page 169.
- If the File System agent will co-exist with the Microsoft SQL or Oracle application agents, it is recommended that you use either the IP address or FQDN for registering both agents. Registering one agent using an IP address and another using the FQDN will require you to re-approve the host in PowerProtect Data Manager, and might cause other unexpected inconsistencies.
- For a protection policy backup with assets from different hosts, the backup status displays as "Failed" in the UI if the backup of one asset within the policy fails.

- Running the `ddfssv` and `ddfsrc` commands to perform self-service backup and restore of File Systems fails if you provide the Data Domain host name for the `DFA_SI_DD_HOST` variable.
- A File System backup might fail with the error `Insufficient space exists in the volume group for creating shadow of the volume` when there is not enough space in the volume group for a block based backup to succeed. Each volume group on LVM2 or VxVM must have at least 10% free space.
- On the Linux hosts that have the UEFI Secure Boot option enabled, block based backup drivers do not load, and the error message `insmod: ERROR: could not insert module /lib/modules/3.10.0-693.el7.x86_64/extra/nsrbbb.ko: Required key not available` appears. As a workaround, you can disable the Secure Boot option.
- On Linux, the block based incremental backups consistently fail and display a message similar to `save: Block Based Error subsystem error while performing Block Based Backup`. Check if any other process is already accessing the snapshot, or delete the snapshot manually, and then try again.
- If the Bytes of sector sizes of the source and target volumes are different, PowerProtect Data Manager does not support block based image recoveries. For example, you cannot perform a block based image recovery of a volume that has 4096 as the Bytes of sector size to a volume that has 512 as the Bytes of sector size, and vice versa.

## Storage Direct agent limitations

Review the following limitations that apply to PowerProtect Data Manager support for the Storage Direct agent.

### Co-existence of the Storage Direct agent with other application agents is not supported

PowerProtect Data Manager 19.2 does not support the co-existence of the Storage Direct agent with other application agents such as Oracle or SQL in PowerProtect Data Manager.

### LUN expansion not supported for existing Storage Direct users

The LUN expansion feature is not currently supported for existing Storage Direct users updating to the Storage Direct agent for PowerProtect Data Manager 19.2.

### SDFSA install/upgrade fails on trying to install using absolute path

An SDFSA installation or upgrade fails when performed using the absolute path. For example:

#### Example 6 Installation using absolute path

```
[root@xxxxxx /]# /Softwares/builds/sdfsa_19.2_36/install.sh
2019/09/18 23:18:42 adm-agent rpm not found in current working
directory...
```

#### Example 7 Upgrade using absolute path

```
[root@xxxxxx sd_cfs]# /Softwares/builds/sdfsa_19.2_40/install.sh -u
2019/09/17 01:49:35 storedirectagent rpm not found in current
working directory...
/Softwares/builds/sdfsa_19.2_40/install.sh: line 595: [: -gt: unary
operator expected
```

**Example 7 Upgrade using absolute path (continued)**

```

/Softwares/builds/sdfsa_19.2_40/install.sh: line 597: [: -gt: unary
operator expected
/Softwares/builds/sdfsa_19.2_40/install.sh: line 599: [: -gt: unary
operator expected
/Softwares/builds/sdfsa_19.2_40/install.sh: line 601: [: -gt: unary
operator expected
2019/09/17 01:49:35 storagedirectagent rpm not found in current
working directory...
rpm -U --quiet --test
rpm: no packages given for install
2019/09/17 01:49:35 storagedirectagent upgrade failed...
2019/09/17 01:49:35 storagedirectagent upgrade failed...

```

To work around this issue, change the directory to the location of `install.sh` and run `./install.sh`.

### Encapsulation fails during policy creation if retention lock exists on VMAX or SMIS services not running

During protection policy creation, a process called encapsulation occurs, which involves creating backup and restore FTS devices on the VMAX and linking the Data Domain vDisk with FTS. If a retention lock exists on the VMAX, or if the SMIS services are not running, encapsulation fails.

To ensure that there is no retention lock on the VMAX, run the following command as the `root` user from the SMIS server:

```
symcfg list -lockn all
```

Output similar to the following displays:

S Y M M E T R I X		L O C K S			
SymmID	Attachment	Lock Status	Lock Number	Lock Usage	Time Held (Sec)
000196700638	Local	Locked	15	Config Change	13572 ->
Almost 4 hours					
000192604348	Remote	N/A	N/A	N/A	N/A
000297000476	Remote	N/A	N/A	N/A	N/A

If SMIS services are not running, an exception appears in the logs indicating that the `storsvd` service is not available and so a connection to SMIS cannot be established using the SYMAPI calls. If this exception occurs:

1. Run the following command as the `root` user from the SMIS server to verify the status of `storsvd`:  

```
./stordaemon show storsrvd
```

If the service is unavailable, the message `*** Daemon storsrvd is not currently running` appears.
2. Restart the service by running `./stordaemon start storsrvd`.
3. Run the `./stordaemon show storsrvd` command again to verify the status is now **Running**.
4. To view the remote server details, run `./stordaemon action storsrvd -cmd show server`.
5. To view the network configuration, run `./stordaemon action storsrvd -cmd show -netinfo`.

## Encapsulation fails with error "SYMAPI\_C\_NET\_HANDSHAKE\_FAILED"

If the encapsulation of a device fails with the error `SYMAPI_C_NET_HANDSHAKE_FAILED`:

1. Ensure that proper name resolution can occur by verifying that the PowerProtect Data Manager server/SMIS server and SDA host are resolvable by either DNS or the hosts file.
2. Perform the following steps to ensure that the PowerProtect Data Manager server can obtain all the necessary information from the SMIS server:
  - Log in to PowerProtect Data Manager as an administrator.
  - Go to the `/usr/emc/API/symapi/config/netcnfg` directory.
  - Verify that the server entry exists. For example, `<ConnectionName> - TCP/IP <hostname> <ipaddress> 2707 -.`
  - Verify whether the Solutions Enabler base daemon is running. For example:

```
admin@xxxxx:~> stordaeomon list -all
Available Daemons ('[*]': Currently Running, '[NI]': Not Installed):
[*] storapid          EMC Solutions Enabler Base Daemon
    storgnsd          EMC Solutions Enabler GNS Daemon
    storrdfd          EMC Solutions Enabler RDF Daemon
    storevntd         EMC Solutions Enabler Event Daemon
[*] storwatchd       EMC Solutions Enabler Watchdog Daemon
    storsrmd          EMC Solutions Enabler SRM Daemon
```

- Export the environment variables `SYMCLI_CONNECT_TYPE=REMOTE` and `SYMCLI_CONNECT=<ConnectionName>`.
- Execute `symcfg list`. The command output should display all VMAX/PowerMax that have been added to the SMIS server.

## Configuration file validation fails when multiple storage group assets selected for policy inclusion if configuration file is not formatted correctly

When you select multiple storage group assets as part of a **VMAX Storage Group** protection policy in PowerProtect Data Manager, if the configuration file is not formatted correctly, validation fails. For example, a configuration file with the following format might be pushed to the host:

```
DDBOOST_USER = 148_78-xxxxx-932c9
DEVICE_HOST = IP address
DEVICE_PATH = /148_78-xxxxx-932c9-SU
DDVDISK_USER = 148_78-xxxxx-932c9
#RESTORE_DEVICE_POOL = 148_78-xxxxx-932c9
#RESTORE_DEVICE_GROUP = R-sdm_xxxxx_SG7-0638
#RESTORE_DEVICE_GROUP = R-sdm_xxxxx_SG8-0638
# DD_BOOST_FC =
# DD_PORT =
VMAX_FASTX_RESTORE_SG = R-sdm_xxxxx_SG7-0638
#VMAX_FASTX_RESTORE_SG = R-sdm_xxxxx_SG8-0638
```

To work around this issue, comment the `VMAX_FASTX_RESTORE_SG` attribute and un-comment `RESTORE_DEVICE_POOL` and one of the entries for `RESTORE_DEVICE_GROUP`.

## MTree replication fails when adding replication stage for multiple protection policies if assets have the same user/vDisk pool

For an existing Storage Direct user who has upgraded to the Storage Direct agent for PowerProtect Data Manager 19.2, an MTree replication job fails with an error similar to the following if you have the same user/vDisk pool for protected assets and you attempt to create multiple protection policies for these assets with a replication stage.

```
Unable to create DataDomain user xxxx, User xxxx already exists.
```

To work around this issue, manually add the secondary Data Domain details in the configuration file.

### Replication not supported for assets in a Storage Group policy for existing Storage Direct users if replication already configured for stand-alone agent

The addition of a replication stage as part of a Storage Group protection policy in PowerProtect Data Manager is not supported for existing Storage Direct users' assets if replication has already been configured on the stand-alone Storage Direct (ProtectPoint) agent.

To import these assets for primary backup policy creation, you need to remove the secondary Data Domain details from the configuration file before importing the file during the Storage Direct agent for PowerProtect Data Manager 19.2 upgrade

## Time synchronization required between PowerProtect Data Manager and the systems it interfaces with

The PowerProtect Data Manager system time is synchronized with the ESXi host system time. It is critical to PowerProtect Data Manager operation that the PowerProtect Data Manager system time matches the systems that it interfaces with. Otherwise, compliance check will fail.

Dell EMC recommends that the ESXi host, and all of the systems that the ESXi host interfaces with, be configured to use a NTP server.

## PowerProtect Data Manager allows completion of protection policy when storage unit on the Data Domain cannot be created

When adding a protection policy in PowerProtect Data Manager, creation of a storage unit on the selected Data Domain system fails if you reach the maximum Mtree count on the Data Domain. However, PowerProtect Data Manager allows you to finish adding the protection policy without the storage unit. If you subsequently run a backup of this protection policy, instead of the backup failing or an error message displaying, the backup hangs indefinitely.

If this occurs, clean up on the Data Domain is required in order to continue backup operations on this device.

## Viewing the DD Boost storage unit password

PowerProtect Data Manager provides a script to retrieve the password of a DD Boost unit that is configured as a backup target.

### Before you begin

This process requires the name of the Data Domain MTree where the DD Boost storage unit resides.

### Procedure

1. SSH to the PowerProtect Data Manager appliance as the **admin** user.
2. Navigate to the `/usr/local/brs/puppet/scripts` directory.
3. Obtain the DD Boost storage unit password by typing the following command:

```
./get_<DD-MTree-Name>_credential.py PLC-PROTECTION-1551667983302
```



# CHAPTER 16

## Modifying the System Settings

This section includes the following topics:

- [System settings](#).....224
- [System Support](#).....227
- [Modifying the PowerProtect Data Manager virtual machine disk settings](#).....235
- [Configure the Data Domain system](#)..... 237

## System settings


You can use the PowerProtect Data Manager UI to modify system settings that are typically configured during PowerProtect Data Manager installation.

To access **System Settings**, click the  icon in the top-right.

### Modify the network settings

Perform the following steps if you want to modify the IP address, subnet mask, gateway, and DNS servers that are defined for the appliance.

#### Procedure

1. Select **System Settings > System > Network**.
2. Update the fields as necessary:
  - **Domain Name**
  - **IP Address**  
 **Note:** When you change the domain name or IP address, the system becomes unavailable until all components are restarted.
  - **Subnet Mask**
  - **Gateway**
  - **Primary DNS**
  - **Secondary DNS**
3. Click **Save**.

### Modify the appliance time zone

Perform the following steps if you want to modify the time zone for the PowerProtect Data Manager appliance.


#### Procedure

1. Select **System Settings > System > Timezone**.
2. In the **Timezone** field, select the desired time zone from the menu.
3. Click **Save**.

### Change the system root user password

Perform the following steps if you want to change the password for the root user.

#### Before you begin

 **Note:** Changing the password only changes the password for the UI login, and not the appliance. Make note of your original appliance password in case you require this password for appliance operations.

#### Procedure

1. Select **System Settings > Authentication**.  
The **System Users** window appears.



2. Select **User name** of the user password that you want to edit and click **Edit**.  
The **Change the password for the root user window** appears.
3. Type the existing password in the **Old Password** field.
4. Type the new password in the **New Password** field, and then retype it in the **Confirm Password** field.
5. Click **Save**.

## Enable replication encryption

You can select the **Replication Encryption** option within the PowerProtect Data Manager UI to ensure that replicated content is encrypted while in-flight to the destination storage and then decrypted before being saved on the destination.

### About this task

Note that the encryption settings on both the source and destination systems must match in order to ensure successful replication. For example, if you enable in-flight encryption in PowerProtect Data Manager, the setting must be explicitly enabled on each source and destination server before defining the PowerProtect Data Manager replication objective. If encryption is enabled after the initial definition of replication objectives, any replication jobs initiated during the period that the source and destination server encryption settings did not match will fail.

### Procedure

1. Select **System Settings > Security**.  
The **Security** dialog appears.
2. Move the **Replication Encryption** slider to the right, and then click **Save**.

### After you finish

The **Infrastructure > Storage** window of the PowerProtect Data Manager UI displays the status of the in-flight encryption setting for all attached storage systems.

**Note:** For systems with DD OS version 6.2 and earlier installed, the status might display as **Unknown**. DD OS version 6.3 and later supports Authentication Mode. DD OS versions earlier than version 6.3 support only Anonymous authentication mode. PowerProtect Data Manager supports only Anonymous and Two-way authentication modes. Ensure that both source and destination system servers use the same authentication mode.

You can take additional steps on your PowerProtect Data Manager server to enable in-flight encryption on connected Data Domain systems by using **Data Domain System Manager**, as described in the *Data Domain Operating System Administration Guide*.

## License types

Learn about the licenses that are available.

The following list provides information about the license types:

- **Trial license**—Applied automatically on installation of PowerProtect Data Manager and enables full use of the product without applying a license key for up to 90 days. When the trial period ends, PowerProtect Data Manager continues to operate with full functionality, so you can apply a permanent license.
- **Front-end protected capacity by terabyte or FETB**—The primary model of eLicensing, which is based on the actual capacity that you want to protect. For example, you can purchase a 100-TB license, which enables you to protect up to 100 TB of actual data.
- **Socket-based**—Licensed per CPU socket on virtual machine hosts being backed up and/or replicated.

**Note:** When you upgrade from a previous release, for example, 3.0.0-18, to PowerProtect Data Manager, any existing license and its associated secure remote services (SRS) connection are removed from the system, and replaced with the 90-day trial license. If you have a valid FETB or Socket-based license for PowerProtect Data Manager, ensure that you upload this license and set up the associated SRS connection.

### Perpetual and term-based (subscription) licensing

Licensed software is offered in perpetual and term-based licenses. Your quote will identify whether your license rights are perpetual or term-based.

A perpetual license enables you to use the software for as long as you are in compliance with the terms of the license agreement.

A term-based license enables you to use the software for a specified period of time, as long as you are in compliance with the terms of the license agreement. At the end of the license term, you must either stop using the software, extend the license term, or purchase new licenses through an agreement with Dell EMC.

## PowerProtect Data Manager licenses

The License area in **Settings** provides PowerProtect Data Manager license status details, such as capacity usage and software ID number. You can also add a license file to the PowerProtect Data Manager.

### Before you begin


You can obtain the `.xml` license file from the Dell EMC license management website. To obtain the license file, you must have the License Authorization Code (LAC), which was emailed from Dell EMC. If you have not received the LAC, contact your customer support representative.

### About this task

To review existing license information, go to **Settings > License**.

To add a license, perform the following steps.

### Procedure

1. Click the System Settings icon along the top-right: .
2. Go to **Settings > License > Upload file**.
3. Do one of the following:
  - Copy and paste license file text into the **License** window.
  - Browse to the location where a license file is located, select the license file and click **Open**.

The license file content appears in the **License** window.
4. Click **Save**.

### Results

A message appears in the **License** window to confirm that the license is successfully added.

## System Support

You can use the PowerProtect Data Manager UI to manage and modify support settings, such as the mail server setup and Secure Remote Services registration, that are typically configured during installation.

To access the **Support** window, click the  icon in the top-right, and then select **System Settings > Support**.

### Register the Secure Remote Services gateway

Secure Remote Services (SRS) enables you to register PowerProtect Data Manager with a gateway host IP address for remote access. You can register only one SRS gateway for PowerProtect Data Manager. After PowerProtect Data Manager is registered, Technical Support Engineers can remotely connect to PowerProtect Data Manager to troubleshoot issues, and you can upgrade PowerProtect Data Manager by using SRS version 3.36.20.10 or later.

#### Before you begin

- You must apply a valid PowerProtect Data Manager license appliance.
- You must have an SRS gateway ServiceLink account open and deployed. Your Dell EMC Sales representative can assist you.

#### About this task

If you update a license file with a different SWID, the SRS gateway requires the new SWID. Reregister the license file with the SRS gateway to ensure the SRS gateway has the new SWID.

#### Procedure

1. From the PowerProtect Data Manager UI, select **System Settings > Support > Secure Remote Services**
2. Enter the following information:
  - The hostname or IP address of the virtual machine that is deployed for SRS.
  - The username and password for the SRS gateway account. The SRS gateway account credentials are provided by the ServiceLink team.
3. Click **Save** to complete registration of the SRS gateway.

 **Note:** Currently, you can use only an IPv4 address for the gateway. IPv6 is not supported.

### Remove the Secure Remote Services gateway

#### Before you begin

You must disable Auto Support to delete Secure Remote Services. If you have Auto Support enabled, you will receive an error message when you attempt to delete Secure Remote Services.

#### About this task

Use the following procedure to remove the Secure Remote Services gateway.

#### Procedure

1. From the PowerProtect Data Manager UI, select **System Settings > Support > Auto Support**.

2. Move the **Enable Auto Support** slider to **Disabled**, and then click **Save**.
3. Select **System Settings > Support > Secure Remote Services**  
The **Secure Remote Services Configuration** dialog box appears.
4. Click **Delete** to remove the Secure Remote Services gateway.

## Callhome

When you register an SRS gateway, you also enable the Callhome feature, which allows Technical Support Engineers to collect data that is related to troubleshooting device and PowerProtect Data Manager software issues. Callhome does not collect any personal information.

Callhome populates three reports—a telemetry report, an alert summary report, and a PowerProtect Central report. The following table lists the information that Callhome collects for the telemetry report.

**Table 28** Telemetry report information

Category	Type of information collected
PowerProtect Data Manager appliance	<ul style="list-style-type: none"> <li>• Date of the last upgrade</li> <li>• Any applied patches</li> <li>• Version of the appliance</li> <li>• Uptime (in days) since the last appliance reboot</li> <li>• Operating system version</li> <li>• Installation date</li> <li>• Telemetry report last sent date</li> <li>• System upgrade packages</li> <li>• Hostname</li> <li>• Node ID</li> <li>• Time zone</li> <li>• Secondard DNS configured</li> <li>• Number of additional users</li> <li>• Backup configured</li> <li>• Backup storage type</li> </ul>
Asset Sources	<ul style="list-style-type: none"> <li>• DDMC instances</li> <li>• XMS instances</li> <li>• vCenter instances</li> <li>• SMIS instances</li> <li>• SQL groups instances</li> <li>• RecoverPoint instances</li> </ul>
Hosts information	<ul style="list-style-type: none"> <li>• ESXi hosts</li> <li>• ESXi cluster hosts</li> <li>• Application hosts</li> </ul>

**Table 28** Telemetry report information (continued)

Category	Type of information collected
Data Domain inventory	<ul style="list-style-type: none"> <li>• Number of Data Domain systems</li> <li>• Data Domain operating system version and system ID</li> <li>• MTree inventory</li> <li>• Asset source ID</li> <li>• Serial number</li> <li>• Model</li> <li>• Data Domain system capacity</li> </ul>
PowerProtect Data Manager operational inventory	<ul style="list-style-type: none"> <li>• Asset information (number of assets, asset groups, assets protected versus unprotected)</li> <li>• Protection policies (number of policies)</li> <li>• Tags (number of tags and tag categories)</li> <li>• Active protection policy details (assets and their types, objectives for each stage)</li> <li>• Failed jobs</li> <li>• Application agents</li> <li>• SLA violations</li> <li>• External proxies</li> </ul>
Integrated Storage	<ul style="list-style-type: none"> <li>• General Information (Model type, system serial number, installed hardware, MAC addresses, WWPN's, alerts)</li> <li>• Server Usage</li> <li>• Active Tier resources, Filesys compression,</li> <li>• General Status (System Memory summary, Alerts, Alert History, Network Hardware, Trust information, Certificate details, Disk Status, Filesys status, NFS status, lw-status)</li> <li>• Software Configuration (License details)</li> <li>• Virtual Hardware Configuration (Network configuration, Hardware details, PCI info, System Ports)</li> <li>• Cluster configuration (Node details, Storage Policy, Compute Policy)</li> <li>• File System cleaning configuration and statistics</li> <li>• File System encryption configuration/status</li> <li>• File System statistics</li> <li>• File System compression statistics that relate to deduplication and compression achievements of ingested data.</li> <li>• Network statistics</li> <li>• NFS Statistics</li> <li>• DD Boost Statistics</li> <li>• Storage Layer Statistics</li> </ul>

**Table 28** Telemetry report information (continued)

Category	Type of information collected
	<ul style="list-style-type: none"> <li>• System Statistics</li> <li>• Processes information</li> <li>• Kernel information</li> </ul>
Usage	<ul style="list-style-type: none"> <li>• Amount of data that is protected</li> </ul>
Licensing	<ul style="list-style-type: none"> <li>• Status of the applied license</li> </ul>
Compliance in last 24 hours	<ul style="list-style-type: none"> <li>• FETB in compliance</li> <li>• FETB out of compliance</li> </ul>

Callhome collects details about the following objects for the PowerProtect Central report:

- Protection Life Cycle
- Service Level Agreement
- Assets
- Storage Systems
- Data targets
- Protection Details
- Compliance Details
- Audit logs

## Set up the email server

The Email Setup area on the PowerProtect Data Manager **System Settings** area enables you to set SMTP email server information to send emails for resetting local user passwords and customized alert notifications.

### Procedure

1. Select **System Settings > Support > Email Setup**.
2. Populate the following fields:
  - a. **Mail Server**  
The SMTP mail server.
  - b. **Email from:**  
The email address at which you would like to receive the PowerProtect Data Manager autosupport email.
  - c. [Optional] **Recipient for Test Email:**  
The email address to which you would like to send the PowerProtect Data Manager test email.
  - d. [Optional] **Port:**  
The default port is 25. PowerProtect Data Manager supports using nondefault ports.  
If the SMTP port is deleted, you must manually choose any nondefault port that is not in use anywhere else.

**e. User Name:**

The user name associated with the PowerProtect Data Manager SMTP email server.

**f. Password:**

The password associated with the PowerProtect Data Manager SMTP email server.

**3. Click Send Test Email.**

PowerProtect Data Manager sends a test email.

**4. Click Save.**

## Add Auto Support

When auto support is enabled, auto support information, telemetry reports, alert summary, and PowerProtect Central reports will be sent.

### About this task

If Secure Remote Services and SMTP are both configured, this information will be sent via Secure Remote Services.

### Procedure

1. Select **System Settings > Support > Auto Support**.

The **Auto Support** window appears. The PowerProtect Data Manager

2. Change the `Enable Auto Support` option to **Disabled** or **Enabled**, and click **Save**.

When you enable Auto Support, the **Telemetry Software Terms** page displays. Review and scroll down to the bottom of the page to accept the terms, and then click **Save** to save your changes.

When you disable Auto Support, PowerProtect Data Manager stops sending error and telemetry data to SRS or the SMTP server. PowerProtect Data Manager continues to send information for upgrades and other information.

 **Note:** You must disable Auto Support to delete SRS.

## Enable automatic upgrade package downloads

Enable upgrade packages to be downloaded automatically through SRS.

### About this task

If this feature is disabled, the system alerts you when a new package is available through SRS. When the feature is enabled, the system automatically downloads available packages, and then alerts you when the package is downloaded.

### Procedure


1. Select **System Settings > Support > Secure Remote Services**.

2. Select **Automatically download upgrade packages**, and then click **Save**.

## Add a log bundle

Use the following procedure to add a log bundle.

### About this task

 **Note:** You can add a maximum of 10 log bundles.

**Procedure**

1. Select **System Settings > Support > Logs**.
2. Click **Add** to add a log bundle.

The **Add Log Bundle** window appears.

3. Select the systems for the log bundle (**Data Manager** and/or **VM Direct**), set the log bundle duration, and click **Save**.

The range can be a maximum period of 7 days up to the current date. The range must be a minimum of 1 day.

The **Jobs** window displays the progress of the log bundle creation. Additionally, a green banner in the UI indicates that the log bundle has successfully been created. If you want to dismiss the banner, click **X**.

4. To delete the log bundle, select the box to the left of log bundle and click **Delete**.

The **Log Capacity** indicates how much space in GB remains on the disk for logs and the percentage of the disk in use for log storage.


5. To download the log bundle, click the bundle name.

## Monitor system state and system health

In addition to the summary system health view provided in the PowerProtect Data Manager UI's **Dashboard** window, the **System Settings > Support** window provides a further breakdown of PowerProtect Data Manager system health information.

### Monitor system component health

Through the **Settings** window, you can monitor the state of the appliance and the health of each system component. .

To view the health of system components, click the  icon in the top-right, select **System Settings > Support**, and then select **System Health**.

The following table provides a summary of each component state.

**Table 29** Component status

Status	Description
Running	This state appears when the associated service or component is running with full functionality. When all components are in running state, the state of the appliance is operational.
Initializing	This state appears when the component is starting. When the component successfully starts, the state changes to Running.
Maintenance	This state appears when the associated service is in maintenance. In the maintenance state, components have limited functionality. Infrastructure services do not go into maintenance state. When other components are in maintenance, the appliance state is also maintenance.
Quiesce	This state appears when the service that is associated with the component is stopping.
Shut down	This state appears when the service has stopped.



**Table 29** Component status (continued)

Status	Description
No response	This state appears when the service that is associated with the component is running, but the service is not responding.

### Business Service components

The following table summarizes the business services health components.

**Table 30** Business Service components

System option	Description
Application Data Management Service	Provides the status of the Application Data Management Service.
Common Business Service	Provides the status of the Common Business Service.
Storage Manager	Provides the status of the Storage Manager.
VMDM	Provides the status of the VMDM service.
Replication Manager	Provides the status of the Replication Manager service.
Cloud Manager	Provides the status of the Cloud Manager service.

### Core Service system health components

The following table summarizes the core services system health components.

**Table 31** Core system health components

System option	Description
Authentication	Provides the status of the Authentication Service.
Event	Provides the status of the Event Service.
Log Manager	Provides the status of the Log Manager service.
Server Disaster Recovery	Provides the status of a system disaster recovery
System Manager	Provides the status of the System Manager.

### Infrastructure Service system health components

The following table summarizes the Infrastructure system health components.

**Table 32** Infrastructure system health components

System option	Description
API Gateway	Provides the status of the API Gateway service.
Catalog Store	Provides the status of the Catalog database.

**Table 32** Infrastructure system health components (continued)

System option	Description
HTTP Proxy	Provides the status of the HTTP Proxy service.
Message Bus	Provides the status of the Message Bus.
Secrets Manager	Provides the status of the Secrets Manager service.
Service Manager	Provides the status of the Service service.
Service Registry	Provides the status of the Service Registry service.
UI	Provides the status of the User Interface service.
Workflow Database	Provides the status of the Workflow database.

### Management Service system health components

The following table summarizes the Management system health components.

**Table 33** Management system health components

System option	Description
Historical	Provides the status of the Historical Data Service.
Monitoring Server	Provides the status of the Server.
Scheduler	Provides the status of the Scheduler service.
Telemetry Manager	Provides the status of the Telemetry Manager service.
Workflow Manager	Provides the status of the Workflow Manager service.

### Protection Service system health component

The following table summarizes the Protection system health component.

**Table 34** Protection system health components

System option	Description
Compliance Verification	Provides the compliance status.
Discovery	Provides the status of the Discovery Service.

## Configure PowerProtect Central reporting

You can enable or disable PowerProtect Central data collection for Dell EMC storage systems.

### Before you begin

- Add a valid license in **Settings > License**.
- Set up SRS in **Settings > Support > SRS**.

### About this task

PowerProtect Central is a no-cost SaaS/cloud-based management application that proactively monitors and measures the overall health of Dell EMC systems through intelligent, comprehensive,

and predictive analytics. The data reported to PowerProtect Central includes configuration data, historical metrics and health score data.

#### Procedure

1. Select **System Settings > Support > Auto Support**.
2. Click **Enable Auto Support** or **Disable Auto Support**.

#### Results

When Auto Support is enabled, PowerProtect Central reports are sent automatically. To log in to PowerProtect Central, click the **Reporting** menu item, or go to <https://powerprotectcentral.emc.com>

For more information on PowerProtect Central, refer to the PowerProtect Central Online Support site.

## Modifying the PowerProtect Data Manager virtual machine disk settings

Follow the steps in this section, under the guidance and recommendations of Dell EMC Support, to expand the size of the data disk and system disk, and modify the memory configuration.

### Modify the virtual machine memory configuration

Adjust the PowerProtect Data Manager virtual machine memory configuration to support changes in the protection environment.

#### Before you begin

Shut down PowerProtect Data Manager and the VM Direct appliance.

#### Procedure

1. Log in to the **vSphere Web Client**.
2. Right-click the appliance and select **Edit Settings**.  
The **Edit Settings** window appears with the **Virtual Hardware** button selected.
3. In the **Memory** field, specify the new memory value.  
Ensure that the value you specify does not exceed 16 times the amount of memory the virtual machine has when powered on and is a multiple of 4 MB.
4. Click **OK**.

### Modify the data disk size

Follow these steps to expand the size of a data disk that is single partitioned and has the log partition is on the system disk.

#### Procedure

1. Perform the following steps from the **vSphere Web Client**:
  - a. Right-click the VM Direct appliance and select **Shut Down Guest OS**.
  - b. After the power off completes, right-click the appliance and select **Edit Settings**.  
The **Edit Settings** window appears with the **Virtual Hardware** button selected.
  - c. Increase the provisioned size of Hard disk 2 to the desired size, and then click **OK**.

**Note:** You cannot decrease the provisioned size of the disk.

- d. Right-click the VM Direct appliance and select **Power On**.
2. Perform the following steps from the appliance console, as the root user.

**Note:** If you use `ssh` to connect to the appliance, log in with the admin account, and then use the `su` command to change to the root account.

- a. Reboot the appliance by typing `reboot`.
- b. On the **GNU GRUB** menu, press `Esc` to edit the GNU GRUB menu.
- c. In the edit screen, search for the line that starts with `linux`, and then add word `single` before the entry `splash=0`

The following figure provides an example of the edit screen with the updated text.

**Figure 10** Editing the GNU GRUB menu

```

GNU GRUB  version 2.02~beta2

b-4b3e-9ea0-095884f96a1a
  else
    search --no-floppy --fs-uuid --set=root 1b63aeb7-38db-4b3e-9ea0-0\
95884f96a1a
  fi
  echo          'Loading Linux 3.12.59-60.45-default ...'
  linux         /vmlinuz-3.12.59-60.45-default root=UUID=7c833cdd-543e\
-4b90-a4fa-373d74a21f8b ${extra_cmdline} resume=/dev/disk/by-uuid/851043aa\
-36b6-4783-a346-d668b29ed327 single splash=0 quiet showopts crashkernel=220\
M-:110M
  echo          'Loading initial ramdisk ...'
  initrd        /initrd-3.12.59-60.45-default

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
a command-line or ESC to discard edits and return to the GRUB menu.
    
```

- d. Press **Ctrl-x** to reboot into single-user mode.
- e. When prompted, type the password for the root account.
- f. Unmount the data disk, by typing `umount /data01`.
- g. Start the partition utility, by typing `parted`, and then perform the following tasks:
  - a. Type `select /dev/sdb`.
  - b. Type `print`. If you are prompted to fix issues, type `fix` at each prompt. The output displays the new disk size in the **Size** field and the current size in the table.
  - c. Type `resize 1 new_size`. Where `new_size` is the value that appears in the **Size** field in the output of the `print` command.  
  
For example, to resize the disk to 700 GB, type: `resize 1 752GB`
  - d. Type `quit`.

3. Reboot the VM Direct appliance by typing `systemctl reboot`.
4. Log in to the console as the root user.



**Note:** If you use `ssh` protocol to connect to the VM Direct appliance, log in with the admin account, and then use the `su` command to change to the root account.

5. Grow the xfs file system by typing `xfs_growfs -d /data01`.
6. Confirm the new partition size by typing `df -h`.

## Modify the system disk size

Follow these steps to expand the size of a data disk when the log partition is the last partition on the system disk.

### Procedure

1. Perform the following steps from the **vSphere Web Client**:
  - a. Right-click the VM Direct appliance and select **Shut Down Guest OS**.
  - b. After the power off completes, right-click the appliance and select **Edit Settings**.  
The **Edit Settings** window appears with the **Virtual Hardware** button selected.
  - c. Increase the provisioned size of Hard disk 1 to the desired size, and then click **OK**.  
 **Note:** You cannot decrease the provisioned size of the disk.
  - d. Right-click the VM Direct appliance and select **Power On**.
2. Boot from a SuSE Linux Enterprise Server (SLES) version 12 CD.
3. Start the partition utility, by typing `parted`, and then perform the following tasks.
  - a. Type `select /dev/sdx`.
  - b. Type `print`. If you are prompted to fix issues, type `fix` at each prompt. The output displays the new disk size in the **Size** field and the current size in the table.
  - c. Type `quit`.
4. Reboot the VM Direct appliance by typing `systemctl reboot`.
5. Log in to the console as the root user.  
 **Note:** If you use `ssh` protocol to connect to the VM Direct appliance, log in with the admin account, and then use the `su` command to change to the root account.
6. Grow the xfs file system by typing `xfs_growfs -d /data01`.
7. Confirm the new partition size by typing `df -h`.

## Configure the Data Domain system

### Before you begin

Before you can use Data Domain to protect the system, use NFS to export the MTree that PowerProtect Data Manager uses on the Data Domain system. The setup on Data Domain requires that you add the PowerProtect Data Manager client with `no_root_squash`.

### Procedure

1. Use a web browser to log in to the **Data Domain System Manager** as the system administrator.
2. In the **Summary** tab, **Protocols** pane, select **NFS export > create export**.  
The **Create NFS Exports** window appears.
3. In the **Create NFS Exports** window:

- a. In the **Export Name** field, specify the name of the Data Domain MTree.
- b. If you have not yet created the Data Domain MTree, follow the prompts to create the MTree and click **Close**.
- c. In the **Directory path** field, specify the full directory path for Data Domain MTree that you created. Ensure that you use the same name for the directory.
- d. Click **OK**.  

A message appears to indicate that the NFS export configuration save is in progress and then complete.
- e. Click **Close**.

# CHAPTER 17

## PowerProtect plug-in within the vSphere Client

This chapter includes the following topics:

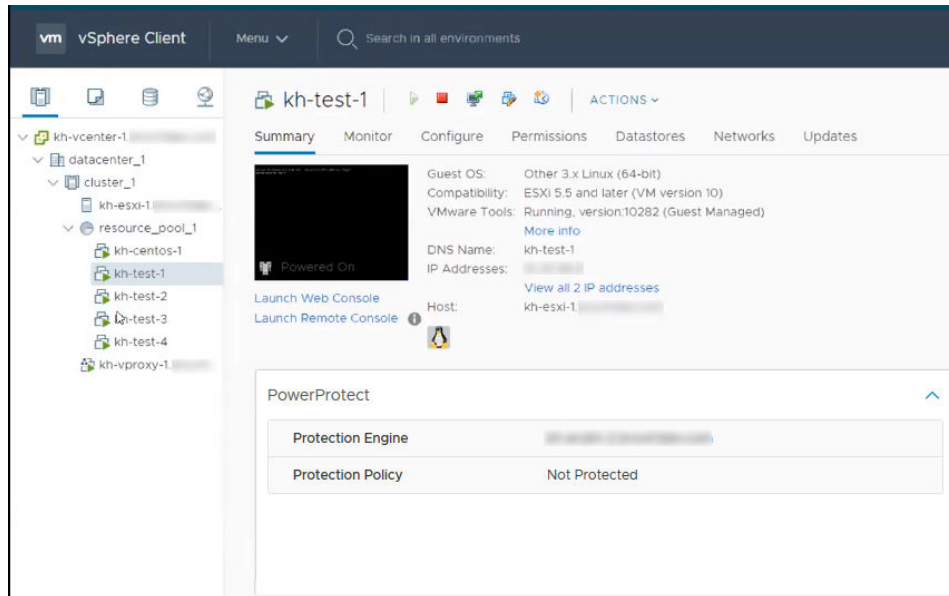
- [Overview of the PowerProtect plug-in within the vSphere Client](#)..... 240
- [Prerequisites to using the PowerProtect plug-in within the vSphere Client](#)..... 241
- [Monitor virtual machine protection copies](#).....242
- [Restore a virtual machine protection copy in the vSphere Client](#).....242

# Overview of the PowerProtect plug-in within the vSphere Client

Upon adding a vCenter Server and enabling the **vSphere Plugin** option in the PowerProtect Data Manager UI, a subset of the UI's functionality becomes available within the **vSphere Client**.

When the plug-in is installed, the PowerProtect Data Manager portlet appears within the **Summary** window of the **vSphere Client**, as shown in the following.

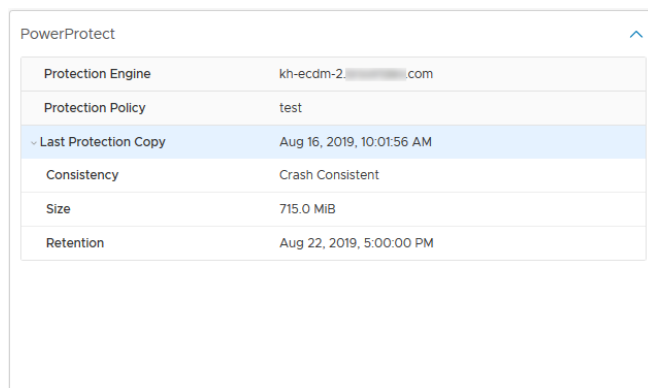
**Figure 11** PowerProtect portlet in the vSphere Client



**Note:** If you are logged into the **vSphere Client** when the vCenter discovery occurs in PowerProtect Data Manager, ensure that you log out and then log back in for PowerProtect to display.

If the virtual assets in the vCenter have not yet been assigned to a virtual machine protection policy in PowerProtect Data Manager, only the PowerProtect Data Manager name displays in the portlet when you select a virtual machine. Adding the virtual machine to a PowerProtect Data Manager protection policy updates the portlet with more information, as shown in the following figure.

**Figure 12** PowerProtect portlet with protected virtual machine





Once you complete the tasks to set up and run a virtual machine protection policy in PowerProtect Data Manager, you can perform the following PowerProtect Data Manager functionality within the **vSphere Client**:

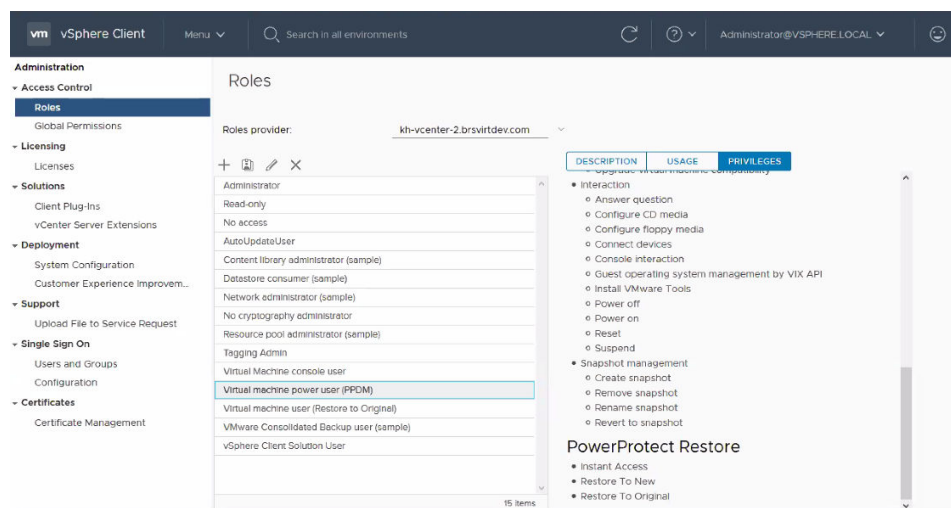
- In the **Summary** window, view information about protection policies and, if policies have been run in PowerProtect Data Manager, information about available protection copies.
- In the **Monitor** window, actively monitor in-progress backup and restore operations for the virtual machine protection policy, and view information for successfully completed protection copies that are available for restore.
- Perform a Restore to Original, Restore to New, or Instant Access restore. You can initiate a restore from the **Monitor** window, or by right-clicking a virtual machine and selecting **PowerProtect > Restore**.

## Prerequisites to using the PowerProtect plug-in within the vSphere Client

To use the PowerProtect plug-in within the **vSphere Client** for restore operations, complete the following tasks in the **vSphere Client** and the PowerProtect Data Manager UI.

- Add and discover the vCenter Server in the PowerProtect Data Manager UI's **Infrastructure > Asset Sources** window, ensuring that you move the **vSphere Plugin** slider to the right in order to enable the plug-in. [Add a VMware vCenter Server](#) on page 102 provides information.
- Verify that the virtual machine assets for the vCenter have been discovered in the **Infrastructure > Assets** window. [Virtual asset discovery](#) on page 104 provides information.
- For the Virtual machine power user group in the **vSphere Client**, open the **Edit Role** window (**Administration > Users and Groups**), select **PowerProtect Restore**, and then add the following required PowerProtect Data Manager privileges:
  - All PowerProtect restore privileges
  - Instant Access
  - Restore to New
  - Restore to Original

**Figure 13** PowerProtect privileges added for the Virtual machine power user



**Note:** If you edit the vCenter Server in the PowerProtect Data Manager UI to unregister the **vSphere Plugin** for PowerProtect Data Manager, these PowerProtect Data Manager privileges are not removed from the user group.

- For the virtual asset (virtual machine, cluster, host) and all its child elements, add permissions to the Virtual machine power user group that you have enabled with PowerProtect Data Manager privileges. To add these permissions, select the asset in the left pane of the **vSphere Client**, and then click the **Permissions** tab.
- Add a virtual machine protection policy in the PowerProtect Data Manager UI's **Protection > Protection Policies** window to schedule a backup of the virtual machine(s). [Add a protection policy for virtual machine protection](#) on page 118 provides information.

## Monitor virtual machine protection copies

You can use the **Monitoring** window in the **vSphere Client** to view protection copies that are available for restore. You can also launch a restore from this window.

To view information about completed protection policy backups, in the navigation pane select **PowerProtect > Protection Copies**. The view provided is identical to what you would see in the PowerProtect Data Manager UI **Infrastructure** window, with a copy map that enables you to view the available protection copies when you click on the storage icon (DD), as described in [Additional options for managing virtual machine backups](#) on page 122.

To view the status of active operations for both backups initiated from the PowerProtect Data Manager UI and those from **vSphere Client**, expand the **Recent Tasks** pane at the bottom of the window. You can also view this pane from the **Summary** window.

## Restore a virtual machine protection copy in the vSphere Client

You can use the **vSphere Client** PowerProtect Data Manager plug-in functionality to initiate a recovery of a PowerProtect Data Manager virtual machine protection policy backup.

### About this task

Available recovery options in the **vSphere Client** include:

- **Restore to Original:** Restore the virtual machine to the original location on the same vCenter.
- **Restore to New:** Restore the virtual machine to a new location on the original vCenter or a different vCenter.
- **Instant Access:** Restore the backup as a live virtual machine so that you can view the backup and then determine whether you want to do a full restore. Instant Access sessions are made available for a default period of 7 days, which can be extended.


You can initiate the restore in one of two ways, as described in the following procedure.

### Procedure


1. Access the backup copy by using one of the following methods:
  - Right-click the virtual machine in the left pane and select **PowerProtect > Restore**. The **Restore** wizard opens on the **Select Copy** page. You can now skip to step 3.
  - With the virtual machine selected in the **Summary** window, go to the **Monitor** window and, in the left navigation pane, select **PowerProtect > Protection Copies**.
2. Select the storage icon (**DD**) to access the backup copies, choose from one of the available copies that displays in the table, and then click **Restore**. The **Restore** wizard opens on the **Options** page. You can now skip to step 4.

3. On the **Select Copy** page, for each virtual machine that is listed in the table, select the radio button next to the virtual machine and click **Choose Copy**.

The **Choose Copy** dialog appears.

 **Note:** If you click **Next** without choosing a copy, the most recent backup copy is used.

4. If the backup is on a Data Domain system, click **DD**, and then select from one of the available copies that display in the table.
5. On the **Purpose** page, select whether you want to restore the entire virtual machine, or only specific virtual machine disks (VMDKs), and then click **Next**.

 **Note:** Individual VMDKs can only be restored to the original location.

6. On the **Restore Type** page, select from one of three available restore options. The wizard updates to display the pages relevant to the restore type that you select, and are identical to the **Restore** wizards for these options that appear in the PowerProtect Data Manager UI. Note, however, that selections such as the vCenter, resource pool, and datastore will be limited to what the logged in vSphere user has access to, and not necessarily what an administrator user in the PowerProtect Data Manager UI would be able to view and select.
  - For Instant Access restore, review the section [Restore an instant access virtual machine](#) on page 153.
  - For Restore to New, review the section [Restore to new](#) on page 151.
  - For Restore to Original, review the section [Restore to original virtual machine](#) on page 149.
7. On the **Summary** page, review your selections and then click **Restore**.

## Results

An entry for the restore job displays in the **Recent Tasks** pane of the **Monitor** window, and also the **Recovery > Running Activities** window of the PowerProtect Data Manager UI.

## After you finish

For Instant Access restores, when the virtual machine is powered on and you select the virtual machine in the left pane of the **Summary** window, the session information displays within the **PowerProtect** portlet. If you require this session for longer than the time you specified during setup, you can click **Extend Session** and increase session availability by up to 7 days.



# CHAPTER 18

## VMware Cloud on Amazon Web Services (AWS) Support

This chapter includes the following topics:

- [PowerProtect Data Manager image backup and recovery for VMware Cloud on AWS](#)..... 246
- [Configure the VMware Cloud on AWS web portal console](#)..... 246
- [Amazon AWS web portal requirements](#).....247
- [Interoperability with VMware Cloud on AWS product features](#)..... 247
- [vCenter server inventory requirements](#)..... 248
- [VMware Cloud on AWS configuration best practices](#)..... 248
- [Add a VM Direct appliance](#)..... 248
- [Protection and recovery operations](#)..... 249
- [Interoperability with VMware Cloud on AWS product features](#).....250
- [Unsupported operations in VMware Cloud on AWS](#) ..... 250
- [Troubleshooting VMware Cloud on AWS](#) ..... 250

# PowerProtect Data Manager image backup and recovery for VMware Cloud on AWS

PowerProtect Data Manager provides image backup and restore support for VMware Cloud on Amazon Web Services (AWS).

Using PowerProtect Data Manager to protect virtual machines that are running in VMware Cloud on AWS is similar to how you protect the virtual machines in an on-premises data center. This section provides information on network configuration requirements, PowerProtect Data Manager best practices for VMware Cloud on AWS, and unsupported PowerProtect Data Manager operations for VMware Cloud on AWS.

To perform data protection and disaster recovery tasks in VMware Cloud on AWS, consider the following recommendations and requirements for the backup infrastructure deployment:

- Deploy PowerProtect Data Manager in a VMware Cloud on AWS environment.
- Deploy the VM Direct Appliance in VMware Cloud on AWS environment. Deploy at least one VM Direct Appliance per each SDDC cluster in the VMware Cloud on AWS.
- Clone backups to another Data Domain running either in the same AWS geographical location or in a different AWS geographical location. This type of deployment enables backup copies to be stored for longer retention, leveraging the AWS network for transferring data at lower latency and cost when compared to the public Internet.
- Store backups outside of the VMware Cloud on AWS environment. For example, store backups on the Amazon AWS VPC. This type of deployment enables efficient data transfer over the fast ENI connection that is used by VMware to communicate with Amazon AWS.
- Clone your backups to another Data Domain system that is running either in the same AWS geographical location or in a different AWS geographical location. This type of deployment enables backup copies to be stored for longer retention, leveraging the AWS network for transferring data at lower latency and cost when compared to the public Internet.

## Configure the VMware Cloud on AWS web portal console

Domain Name System (DNS) resolution is critical for deployment and configuration of PowerProtect Data Manager, the PowerProtect Data Manager external proxy, and the Data Domain appliance. All infrastructure components should be resolvable through a Fully Qualified Domain Name (FQDN). Resolvable means that components are accessible through both forward (A) and reverse (PTR) lookups.

In the VMware Cloud on AWS web portal console, ensure that the following requirements are met:

- By default, there is no external access to the vCenter Server system in the Software Defined Data Center (SDDC). You can open access to the vCenter Server system by configuring a firewall rule. To enable communication to the vCenter public IP address from the SDDC logical network, set the firewall rule in the compute gateway of VMware Cloud on AWS. If the firewall rule is not configured in the SDDC, PowerProtect Data Manager does not allow you to add the vCenter Server.
- The default compute gateway firewall rules prevent all virtual machine traffic from reaching the internet. To enable the PowerProtect Data Manager virtual machine to connect to the internet, create a compute gateway firewall rule. This action enables outbound traffic on the logical network that the PowerProtect Data Manager Server virtual machine is connected to.
- Configure DNS to allow machines in the SDDC to resolve Fully Qualified Domain Names (FQDNs) to IP addresses belonging to the internet. If the DNS server is not configured in the

SDDC, the PowerProtect Data Manager server does not allow you to add the vCenter Server by using the server's public FQDN or IP address.

- It is recommended that you deploy the Data Domain system as a virtual appliance in the Amazon Virtual Private Cloud (VPC). During the SDDC creation, connect the SDDC to an AWS account, and then select a VPC and subnet within that account.
- The Data Domain system running in the Amazon VPC must be connected to the VMware SDDC through the VMware Cloud Elastic Network Interfaces (ENIs). This action allows the SDDC, the services in the AWS VPC, and subnet in the AWS account to communicate without having to route traffic through the internet gateway.
- The same ENI channel is recommended for access to Data Domain systems. For more information about configuring ENIs, see <https://vmc.vmware.com/console/aws-link>.
- If DDVE is running in the Amazon VPC, configure the inbound and outbound firewall rules of the compute gateway for Data Domain connectivity. For detailed information on what incoming on outgoing ports need to be opened for PowerProtect-VM proxy solution, refer to the *PowerProtect Data Manager 19.2 Security Configuration Guide*.
- If using NSX-T, configure the DNS to resolve to the internal IP address of the vCenter server. Navigate to **SDDC Management > Settings > vCenter FQDN** and select the **Private vCenter IP address** so that you can directly access the management network over the built-in firewall. Additionally, ensure that you open TCP port 443 of the vCenter server in both the management gateway and the compute gateway.

## Amazon AWS web portal requirements

In the Amazon AWS web portal, ensure that the following requirements are met:

- If Data Domain is running in your Amazon VPC, configure the inbound and outbound firewall rules of your Amazon VPC security group to provide connectivity between the VMware SDDC compute gateway and Data Domain connectivity.
- If you are replicating from one Data Domain system to another, configure the inbound rule for the security group in AWS to allow all traffic from the respective private IPs of the Data Domain Virtual Editions running in your Amazon VPC.
- If you have more than one Data Domain running in AWS to perform replication, both Data Domain systems must have the ability to ping each other using the FQDNs.

## Interoperability with VMware Cloud on AWS product features

VMware Cloud on AWS has certain restrictions on workloads and resource pools. To ensure proper operation, select the Workload and Compute sections in AWS.

Do not use the non-accessible areas. :

- vsanDatastore datastore
- Management VMs folder in VMs and Templates view
- Mgmt-ResourcePool resource pool in Hosts and Clusters view

## vCenter server inventory requirements

In the vCenter server inventory of your SDDC, ensure that the following requirements are met:

- An internal DNS name lookup server must be running inside the vCenter inventory. This will be referenced by all the workloads running in the VMware SDDC.
- The internal DNS server must have **Forwarders** enabled to access the internet. This action is required to resolve the vCenter Server's public FQDN.  
Forwarders are DNS servers that the server can use to resolve DNS queries for records that the server cannot resolve.

## VMware Cloud on AWS configuration best practices

For VMware Cloud on AWS support, ensure that the following requirements are met:

- When deploying or configuring PowerProtect Data Manager or the VM Direct appliance, ensure that correct DNS server IP points to the internal DNS server that is running in the vCenter inventory.
- Ensure that both forward and reverse lookup entries in the internal DNS server are in place for all of the required components, such as PowerProtect Data Manager, VM Direct appliance, and the DDVE appliance.
- If using NSX-T, add the vCenter server to PowerProtect Data Manager by using the FQDN.
- If using NSX-V, add the vCenter server to PowerProtect Data Manager by using the public FQDN of the vCenter server.
- When adding the vCenter server to PowerProtect Data Manager, specify the login credentials for the *cloudadmin@vmc.local* user.
- When configuring the VM Direct appliance in a VMware Cloud on AWS environment, ensure that you select the transport mode as Hot Add only. VMware Cloud on AWS does not support the NBD transport mode.

## Add a VM Direct appliance

In the **Protection Engines** window, perform the following steps to deploy a VM Direct appliance to facilitate data movement with the VM Direct protection engine.

### About this task

The PowerProtect Data Manager software comes bundled with an embedded VM Direct appliance, which is automatically used as a fallback proxy for performing backups and restores when the added external proxies fail or are disabled. Dell EMC recommends that you deploy external proxies because the embedded proxy has limited capacity for performing parallel backups.


### Procedure

1. In the **VM Direct Engines** pane of the **Protection Engines** window, click **Add**.
2. In the **Add VM Direct Engines** dialog box, fill out the required fields (marked with an asterisk).


Consider the following:

- Only IPv4 addresses are supported for the **Gateway**, **IP Address**, **Netmask**, and **Primary DNS**.
- If you have added multiple vCenter Server instances, the **vCenter to Deploy** list enables you to choose the vCenter where you want to deploy the VM Direct Engine.



 **NOTICE** Do NOT select the internal vCenter in this step.

- The **ESX Host/Cluster** list enables you to choose on which cluster or ESX host you want to deploy the additional VM Direct Engine.
- The **Network** list shows all the networks that are available under the selected ESX Host/Cluster.
- The **Data Store** list shows all datastores that are accessible to the selected ESX Host/Cluster based on ranking (whether the datastores are shared, local, or NFS), and available capacity (the datastore with the most capacity appearing at the top of the list).
- You can choose the specific datastore on which the VM Direct appliance will reside or leave the default selection of **<automatic>** to enable PowerProtect Data Manager to determine the best location to host the VM Direct appliance.
- The **Transport Mode** list enables you to force using only Hot Add or only Network Block Device (NBD) transport modes or to default to Hot Add mode and fallback to NBD only if Hot Add cannot be used.

 **Note:** When configuring the VM Direct appliance in a VMware Cloud on AWS environment, ensure that you select the transport mode as Hot Add only. VMware Cloud on AWS does not support the NBD transport mode.

### 3. Click **Save**.

The VM Direct appliance is added to the **VM Direct Engines** pane. Note that it may take several minutes before the additional VM Direct appliance is registered in PowerProtect Data Manager. The VM Direct appliance appears in the vSphere Client window.

### Results

When an extra VM Direct appliance is deployed and registered, this appliance is used by PowerProtect Data Manager instead of the embedded VM Direct appliance for any data protection operations involving virtual machine protection policies, unless all added VM Direct appliances are unavailable. If no added VM Direct appliance is available, the embedded VM Direct appliance is used as a fallback to perform limited scale backups and restores. If you do not want to use an added VM Direct appliance, you can disable that proxy. [Additional VM Direct actions](#) on page 109 provides more information.

### After you finish

If the VM Direct appliance deployment fails, review the network configuration of PowerProtect Data Manager in the **System Settings** window to correct any inconsistencies in network properties. After successfully completing the network reconfiguration, you must delete the failed VM Direct appliance and then add the VM Direct appliance in the **Protection Engines** window.

When configuring the VM Direct appliance in a VMware Cloud on AWS environment, if the VM Direct appliance is deployed to the root of the cluster instead of inside the Compute-ResourcePool, you must move the VM Direct appliance inside the Compute-ResourcePool.

## Protection and recovery operations

Using PowerProtect Data Manager to protect virtual machines that are running in VMware Cloud on AWS is similar to how you protect the virtual machines in an on-premises data center.

Once you complete the tasks to set up and run a virtual machine protection policy in PowerProtect Data Manager, you can perform the following PowerProtect Data Manager functionality:

- In the **Summary** window, view information about protection policies and, if policies have been run in PowerProtect Data Manager, information about available protection copies.

- In the **Monitor** window, actively monitor in-progress backup and restore operations for the virtual machine protection policy, and view information for successfully completed protection copies that are available for restore.
- Perform a Restore to Original, Restore to New, or Instant Access restore. You can initiate a restore from the **Monitor** window, or by right-clicking a virtual machine and selecting **PowerProtect > Restore**.

## Interoperability with VMware Cloud on AWS product features

VMware Cloud on AWS has certain restrictions on workloads and resource pools. To ensure proper operation, select the Workload and Compute sections in AWS.

Do not use the non-accessible areas. :

- vsanDatastore datastore
- Management VMs folder in VMs and Templates view
- Mgmt-ResourcePool resource pool in Hosts and Clusters view

## Unsupported operations in VMware Cloud on AWS

PowerProtect Data Manager image backup and restore in VMware Cloud on AWS does not currently support the following operations:

- Application-consistent data protection for MS-SQL with the VM Direct appliance.
- File-level restore from an image-level backup if using NSX-V. Note that this operation is supported if using NSX-T.
- Instant access recovery of an image-level backup.
- Emergency restore (image-level restore directly to an ESXi host, bypassing the vCenter).
- Image-level backups and restores that use NBD or the NBDSSL transport mode.
- VM Direct appliance that is configured with dual-stack or IPv6.
- If a datacenter is placed inside a folder in the SDDC, image backup and restore is not supported.
- VM Backup and Recovery plugin (HTML5) for vSphere is not supported.

## Troubleshooting VMware Cloud on AWS

When restoring as new VM, the reconnect NIC option might not work correctly.

### Workaround

1. Edit the settings of the restored new VM and change the network to "VM Network" and then click **Apply**.
2. Reopen the **Edit Setting Configuration** pane of the VM and then change the network to the correct NSX-T network logical switch.
3. Click **Connect**.